EC-Council

Exam Questions 312-50v10

Certified Ethical Hacker v10

NEW QUESTION 1
- (Exam Topic 1)
What would you enter, if you wanted to perform a stealth scan using Nmap?

A. nmap -sU
B. nmap -sS
C. nmap -sM
D. nmap -sT

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

A. Time Keeper
B. NTP
C. PPP
D. OSPP

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

A. End of Line Comment
B. UNION SQL Injection
C. Illegal/Logically Incorrect Query
D. Tautology

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.
What is the main security risk associated with this scenario?

A. External script contents could be maliciously modified without the security team knowledge
B. External scripts have direct access to the company servers and can steal the data from there
C. There is no risk at all as the marketing services are trustworthy
D. External scripts increase the outbound company data traffic which leads greater financial losses

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is considered as one of the most reliable forms of TCP scanning?

A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL Scan
D. Xmas Scan

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Code injection is a form of attack in which a malicious user:

A. Inserts text into a data field that gets interpreted as code
B. Gets the server to execute arbitrary code using a buffer overflow
C. Inserts additional code into the JavaScript running in the browser
D. Gains access to the codebase on the server and inserts new code

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

A. SSH communications are encrypted it's impossible to know who is the client or the server
B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

A. Command Injection Attacks
B. File Injection Attack
C. Cross-Site Request Forgery (CSRF)
D. Hidden Field Manipulation Attack

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers
B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

A. Double quotation
B. Backslash
C. Semicolon
D. Single quotation

Answer: D

NEW QUESTION 11
- (Exam Topic 1)
What is the main security service a cryptographic hash provides?

A. Integrity and ease of computation
B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 14
- (Exam Topic 1)
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating
C. Piggybacking
D. Announced

Answer: B

NEW QUESTION 15
- (Exam Topic 1)
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PPP
B. IPSEC
C. PEM
D. SET

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
Which of the following provides a security professional with most information about the system’s security posture?

A. Wardriving, warchalking, social engineering
B. Social engineering, company site browsing, tailgating
C. Phishing, spamming, sending trojans
D. Port scanning, banner grabbing, service identification

Answer: D

NEW QUESTION 21
- (Exam Topic 1)
You are monitoring the network of your organizations. You notice that: Which of the following solution will you suggest?

A. Block the Blacklist IP’s @ Firewall
B. Update the Latest Signatures on your IDS/IPS
C. Clean the Malware which are trying to Communicate with the External Blacklist IP’s
D. Both B and C

Answer: D

NEW QUESTION 23
- (Exam Topic 1)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (Hig
D. Medium, Low)
E. Identifies sources of harm to an IT syste
F. (Natural, Huma
G. Environmental)

Answer: C

NEW QUESTION 24
- (Exam Topic 1)
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. Suicide Hacker
B. Black Hat
C. White Hat
D. Gray Hat

Answer: D

NEW QUESTION 25
- (Exam Topic 1)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. “GET/restricted/goldtransfer?to=Rob&from=1 or 1=1’ HTTP/1.1Host: westbank.com”
B. “GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com”
C. “GET/restricted/bank.getaccount(‘Ned’) HTTP/1.1 Host: westbank.com”
D. “GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com”

Answer: B

NEW QUESTION 28
- (Exam Topic 1)
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 33
- (Exam Topic 1)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
What kind of Web application vulnerability likely exists in their software?

A. Host-Based Intrusion Detection System
B. Security through obscurity
C. Defense in depth
D. Network-Based Intrusion Detection System

Answer: C

NEW QUESTION 35
- (Exam Topic 1)
When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives
B. Rise False positives Rise False Negatives
C. Decrease the false positives
D. Decrease False negatives

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall
B. Stateful firewall
C. Packet firewall
D. Web application firewall

Answer: D

NEW QUESTION 43
- (Exam Topic 1)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

A. Authentication
B. Confidentiality
C. Integrity
D. Non-Repudiation

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

A. None of these scenarios compromise the privacy of Alice’s data
B. Agent Andrew subpoenas Alice, forcing her to reveal her private ke
C. However, the cloud server successfully resists Andrew’s attempt to access the stored data
D. Hacker Harry breaks into the cloud server and steals the encrypted data
E. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.
B. Containers may full fill disk space of the host.
C. A compromise container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 48
- (Exam Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
B. Asymmetric cryptography is computationally expensive in compariso
C. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
D. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
E. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D

NEW QUESTION 52
- (Exam Topic 1)
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

A. Nmap
B. Cain & Abel
C. Nessus
D. Snort

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
A virus that attempts to install itself inside the file it is infecting is called?

A. Tunneling virus
B. Cavity virus
C. Polymorphic virus
D. Stealth virus

Answer: B

NEW QUESTION 57
- (Exam Topic 1)
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Answer: C

NEW QUESTION 58
- (Exam Topic 1)
In the field of cryptanalysis, what is meant by a “rubber-hose" attack?

A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
B. Extraction of cryptographic secrets through coercion or torture.
C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.
Your email message looks like this: From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37

The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?

A. Email Phishing
B. Email Masquerading
C. Email Spoofing
D. Email Harvesting

Answer: C

NEW QUESTION 62
- (Exam Topic 1)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

NEW QUESTION 65
- (Exam Topic 1)
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

A. Black-Hat Hackers A
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hacker

Answer: C

NEW QUESTION 70
- (Exam Topic 1)
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

A. Hire a security consultant to provide direction.
B. Do not back up cither the credit card numbers or then hashes.
C. Back up the hashes of the credit card numbers not the actual credit card numbers.
D. Encrypt backup tapes that are sent off-site.

Answer: A

NEW QUESTION 74
- (Exam Topic 1)
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

A. Identifying operating systems, services, protocols and devices
B. Modifying and replaying captured network traffic
C. Collecting unencrypted information about usernames and passwords
D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 79
- (Exam Topic 1)
During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Answer: C

NEW QUESTION 81
- (Exam Topic 1)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?

A. ACK flag scanning
B. TCP Scanning
C. IP Fragment Scanning
D. Inverse TCP flag scanning

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. –T0
B. –T5
C. -O
D. -A

Answer: B

NEW QUESTION 90
- (Exam Topic 1)
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends “many” IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:

A. Just a network monitoring tool
B. A signature-based IDS
C. A hybrid IDS
D. A behavior-based IDS

Answer: A

NEW QUESTION 91
- (Exam Topic 2)
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Answer: A

NEW QUESTION 92
- (Exam Topic 2)
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical
B. Procedural
C. Technical
D. Compliance

Answer: B

NEW QUESTION 97
- (Exam Topic 2)
Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

Answer: A

NEW QUESTION 100
- (Exam Topic 2)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

Answer: A

NEW QUESTION 101
- (Exam Topic 2)
Which of the following is an application that requires a host application for replication?

A. Micro

B. Worm
C. Trojan
D. Virus

Answer: D

Explanation:
Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".
References: https://en.wikipedia.org/wiki/Computer_virus

NEW QUESTION 105
- (Exam Topic 2)
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Answer: A

NEW QUESTION 106
- (Exam Topic 2)
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine

Answer: C

NEW QUESTION 108
- (Exam Topic 2)
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon
B. Single quote
C. Exclamation mark
D. Double quote

Answer: B

NEW QUESTION 110
- (Exam Topic 2)
Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Answer: C

NEW QUESTION 115
- (Exam Topic 2)
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing

Answer: B

NEW QUESTION 117
- (Exam Topic 2)
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC

C. 128 bit and CCMP
D. 128 bit and TKIP

Answer: C

NEW QUESTION 122
- (Exam Topic 2)
A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config
D. Ipconfig firewall show config

Answer: A

NEW QUESTION 126
- (Exam Topic 2)
What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode
B. Enabling port forwarding on the router
C. Installing the router outside of the network's firewall
D. Disabling the router from accepting broadcast ping messages

Answer: D

NEW QUESTION 130
- (Exam Topic 2)
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

Answer: D

NEW QUESTION 134
- (Exam Topic 2)
Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

Answer: A

NEW QUESTION 138
- (Exam Topic 2)
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Answer: C

NEW QUESTION 142
- (Exam Topic 2)
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

Answer: C

NEW QUESTION 146
- (Exam Topic 2)
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

Answer: B

Explanation:
A full restore is required.

NEW QUESTION 151
- (Exam Topic 2)
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 153
- (Exam Topic 2)
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

Answer: A

NEW QUESTION 154
- (Exam Topic 2)
Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

Answer: B

NEW QUESTION 155
- (Exam Topic 2)
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

Answer: D

NEW QUESTION 156
- (Exam Topic 2)
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Answer: A

NEW QUESTION 161
- (Exam Topic 2)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

Answer: B

NEW QUESTION 166
- (Exam Topic 2)
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

Answer: B

NEW QUESTION 168
- (Exam Topic 2)
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.
B. Allow full DNS zone transfers.
C. Remove A records for internal hosts.
D. Enable null session pipes.

Answer: C

NEW QUESTION 171
- (Exam Topic 2)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
D. NMAP -P 192.168.1/17

Answer: A

NEW QUESTION 173
- (Exam Topic 2)
What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Answer: C

NEW QUESTION 175
- (Exam Topic 2)
Which security control role does encryption meet?

A. Preventative
B. Detective
C. Offensive
D. Defensive

Answer: A

NEW QUESTION 177
- (Exam Topic 2)
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto
C. Ike-scan
D. Arp-scan

Answer: C

NEW QUESTION 179
- (Exam Topic 2)
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key

B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Answer: C

NEW QUESTION 183
- (Exam Topic 2)
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Answer: C

NEW QUESTION 187
- (Exam Topic 2)
Which of the following is a strong post designed to stop a car?

A. Gate
B. Fence
C. Bollard
D. Reinforced rebar

Answer: C

NEW QUESTION 190
- (Exam Topic 2)
An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

Answer: D

NEW QUESTION 194
- (Exam Topic 2)
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

Answer: B

NEW QUESTION 199
- (Exam Topic 2)
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
B. The session cookies generated by the application do not have the HttpOnly flag set.
C. The victim user must open the malicious link with a Firefox prior to version 3.
D. The web application should not use random tokens.

Answer: D

NEW QUESTION 204
- (Exam Topic 2)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

Answer: A

NEW QUESTION 209
- (Exam Topic 2)

What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

Answer: D

NEW QUESTION 211
- (Exam Topic 2)
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 216
- (Exam Topic 2)
How can rainbow tables be defeated?

A. Password salting
B. Use of non-dictionary words
C. All uppercase character passwords
D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 221
- (Exam Topic 2)
Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

Answer: D

NEW QUESTION 226
- (Exam Topic 2)
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Answer: D

NEW QUESTION 230
- (Exam Topic 2)
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Answer: D

NEW QUESTION 233
- (Exam Topic 2)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Answer: D

NEW QUESTION 240
- (Exam Topic 2)
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

NEW QUESTION 243
- (Exam Topic 2)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Answer: A

NEW QUESTION 245
- (Exam Topic 2)
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:
Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Answer: D

NEW QUESTION 249
- (Exam Topic 2)
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

Answer: A

NEW QUESTION 253
- (Exam Topic 2)
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

Answer: B

NEW QUESTION 258
- (Exam Topic 2)
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25

C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

Answer: D

NEW QUESTION 259
- (Exam Topic 2)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box
B. grey box
C. red box
D. black box

Answer: D

NEW QUESTION 261
- (Exam Topic 2)
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Explanation:
Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.
References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

NEW QUESTION 264
- (Exam Topic 2)
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus
B. Polymorphic virus
C. Tunneling virus
D. Stealth virus

Answer: D

NEW QUESTION 269
- (Exam Topic 2)
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 270
- (Exam Topic 2)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Answer:

A

NEW QUESTION 273
- (Exam Topic 2)
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 278
- (Exam Topic 2)
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Answer: A

NEW QUESTION 281
- (Exam Topic 2)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

Answer: D

NEW QUESTION 282
- (Exam Topic 3)
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation’s Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 286
- (Exam Topic 3)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

Answer: A

NEW QUESTION 291
- (Exam Topic 3)
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

Answer: D

NEW QUESTION 296
- (Exam Topic 3)
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT

B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

Answer: B

NEW QUESTION 298
- (Exam Topic 3)
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Answer: C

NEW QUESTION 300
- (Exam Topic 3)
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 302
- (Exam Topic 3)
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Answer: D

NEW QUESTION 304
- (Exam Topic 3)
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1
C. RC4
D. MD4

Answer: B

NEW QUESTION 307
- (Exam Topic 3)
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Answer: D

NEW QUESTION 311
- (Exam Topic 3)
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

Answer: B

NEW QUESTION 313

- (Exam Topic 3)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

Answer: A

NEW QUESTION 314
- (Exam Topic 3)
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

Answer: D

NEW QUESTION 319
- (Exam Topic 3)
In the OSI model, where does PPTP encryption take place?

A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

Answer: C

NEW QUESTION 323
- (Exam Topic 3)
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Answer: D

NEW QUESTION 326
- (Exam Topic 3)
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Answer: D

NEW QUESTION 329
- (Exam Topic 3)
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

Answer: C

NEW QUESTION 332
- (Exam Topic 3)
Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
B. It is compatible with various databases including Access, Oracle, and SQL.
C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 334
- (Exam Topic 3)
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit
B. Audit, standards based, regulatory
C. Contractual, regulatory, industry
D. Legislative, contractual, standards based

Answer: D

NEW QUESTION 339
- (Exam Topic 3)
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Answer: B

NEW QUESTION 342
- (Exam Topic 3)
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

A. Threaten to publish the penetration test results if not paid.
B. Follow proper legal procedures against the company to request payment.
C. Tell other customers of the financial problems with payments from this company.
D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Answer: B

NEW QUESTION 346
- (Exam Topic 3)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

Answer: C

NEW QUESTION 349
- (Exam Topic 3)
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

Answer: C

NEW QUESTION 350
- (Exam Topic 3)
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Answer: B

NEW QUESTION 353
- (Exam Topic 3)
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Answer: A

NEW QUESTION 358
- (Exam Topic 4)
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?

A. Metagoofil
B. Armitage
C. Dimitry
D. cdpsnarf

Answer: A

Explanation:
Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.
References:
http://www.edge-security.com/metagoofil.php

NEW QUESTION 360
- (Exam Topic 4)
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

A. Encryption
B. Protocol Isolation
C. Alternate Data Streams
D. Out of band signalling

Answer: A

Explanation:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
References:
http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

NEW QUESTION 364
- (Exam Topic 4)
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?

A. site: target.com filetype:xls username password email
B. inurl: target.com filename:xls username password email
C. domain: target.com archive:xls username password email
D. site: target.com file:xls username password email

Answer: A

Explanation:
If you include site: in your query, Google will restrict your search results to the site or domain you specify. If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in
suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and “checklist.”
References:
http://www.googleguide.com/advanced_operators_reference.html

NEW QUESTION 365
- (Exam Topic 4)
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Intrusion Prevention System
B. Wireless Access Point
C. Wireless Access Control List
D. Wireless Analyzer

Answer: A

Explanation:
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).
References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

NEW QUESTION 370
- (Exam Topic 4)
A common cryptographical tool is the use of XOR. XOR the following binary values:
10110001
00111010

A. 10001011
B. 11011000
C. 10011101
D. 10111100

Answer: A

Explanation:
The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".
References: https://en.wikipedia.org/wiki/XOR_gate

NEW QUESTION 374
- (Exam Topic 4)
How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a reply packet for a specific IP, asking for the MAC address.
D. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Answer: A

Explanation:
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.
References:
http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

NEW QUESTION 379
- (Exam Topic 4)
What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of the target network.
B. Network security would be in a "best state" posture.
C. It is best to catch critical infrastructure unpatched.
D. The tester could not provide an honest analysis.

Answer: A

Explanation:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.
A possible solution to this danger is to conduct intermittent “unannounced” penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with “announced” penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.
References:
http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

NEW QUESTION 381
- (Exam Topic 4)
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.srcport==514 && ip.src==192.168.0.99
C. tcp.dstport==514 && ip.dst==192.168.0.0/16
D. tcp.srcport==514 && ip.src==192.168.150

Answer: A

Explanation:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.
References: https://wiki.wireshark.org/DisplayFilters

NEW QUESTION 384
- (Exam Topic 4)
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?

A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

Answer: A

Explanation:
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be run.
References: https://nmap.org/book/man-host-discovery.html

NEW QUESTION 385
- (Exam Topic 4)
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.

Answer: A

Explanation:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
References: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

NEW QUESTION 387
- (Exam Topic 4)
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

A. Application
B. Circuit
C. Stateful
D. Packet Filtering

Answer: A

Explanation:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.
References:
http://searchsoftwarequality.techtarget.com/definition/application-firewall

NEW QUESTION 388
- (Exam Topic 4)
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.
What is the best approach?

A. Install Cryptcat and encrypt outgoing packets from this server.
B. Install and use Telnet to encrypt all outgoing traffic from this server.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Answer: A

Explanation:
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.
References:
http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-014

NEW QUESTION 390
- (Exam Topic 4)
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

A. Botnet Trojan
B. Turtle Trojans
C. Banking Trojans
D. Ransomware Trojans

Answer: A

Explanation:
In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

NEW QUESTION 394
- (Exam Topic 4)
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.
Which command-line utility are you most likely to use?

A. Grep
B. Notepad
C. MS Excel
D. Relational Database

Answer: A

Explanation:
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. References: https://en.wikipedia.org/wiki/Grep

NEW QUESTION 399
- (Exam Topic 4)
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code

Answer: A

Explanation:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.
References: https://www.techopedia.com/definition/26655/boot-sector-virus

NEW QUESTION 401
- (Exam Topic 4)
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.
What should you do?

A. Forward the message to your company’s security response team and permanently delete the message from your computer.
B. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation

Answer: A

Explanation:
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.
References:
https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NEW QUESTION 405
- (Exam Topic 4)
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluejacking
C. Bluesmacking
D. Bluesnarfing

Answer:

A

NEW QUESTION 410
- (Exam Topic 4)
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW
B. Cain & Abel
C. SET
D. John the Ripper

Answer: A

Explanation:
chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.
References: https://en.wikipedia.org/wiki/Chntpw

NEW QUESTION 414
- (Exam Topic 4)
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Answer: A

Explanation:
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
References:
http://www.bbc.co.uk/webwise/guides/about-bluetooth

NEW QUESTION 417
- (Exam Topic 4)
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Terms of Engagement
B. Project Scope
C. Non-Disclosure Agreement
D. Service Level Agreement

Answer: A

NEW QUESTION 421
- (Exam Topic 4)
This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

A. RSA
B. SHA
C. RC5
D. MD5

Answer: A

Explanation:
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.
Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.
References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

NEW QUESTION 423
- (Exam Topic 4)
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. TCP
B. UPD
C. ICMP
D. UPX

Answer: A

Explanation:
At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.
References: https://www.exploit-db.com/papers/13587/

NEW QUESTION 427
- (Exam Topic 4)
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. footprinting
B. network mapping
C. gaining access
D. escalating privileges

Answer: A

Explanation:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.
References:
http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

NEW QUESTION 428
- (Exam Topic 4)
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Injection
B. Cross Site Scripting
C. Cross Site Request Forgery
D. Path disclosure

Answer: A

Explanation:
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
References: https://www.owasp.org/index.php/Top_10_2013-Top_10

NEW QUESTION 432
- (Exam Topic 4)
Which of the following statements is TRUE?

A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.

Answer: A

Explanation:
The OSI layer 2 is where packet sniffers collect their data. References: https://en.wikipedia.org/wiki/Ethernet_frame

NEW QUESTION 433
- (Exam Topic 4)
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.
What is this style of attack called?

A. zero-day
B. zero-hour
C. zero-sum
D. no-day

Answer: A

Explanation:
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
References: https://en.wikipedia.org/wiki/Stuxnet

NEW QUESTION 434

- (Exam Topic 4)
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Aircrack-ng
B. Airguard
C. WLAN-crack
D. wificracker

Answer: A

Explanation:
Aircrack-ng is a complete suite of tools to assess WiFi network security.
The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.
References:
http://www.aircrack-ng.org/doku.php?id=aircrack-ng

NEW QUESTION 437
- (Exam Topic 4)
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. AH permiscuous
C. ESP confidential
D. AH Tunnel mode

Answer: A

Explanation:
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

NEW QUESTION 439
- (Exam Topic 4)
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?

A. Watering Hole Attack
B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack

Answer: A

Explanation:
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

NEW QUESTION 442
- (Exam Topic 4)
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. tcpdump
B. nessus
C. etherea
D. Jack the ripper

Answer: A

Explanation:
tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP
and other packets being transmitted or received over a network to which the computer is attached. References: https://en.wikipedia.org/wiki/Tcpdump

NEW QUESTION 445
- (Exam Topic 4)
What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process
B. Security Policy
C. Internal Procedure
D. Metrics

Answer: A

Explanation:
The activities within the incident management process include:
References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

NEW QUESTION 450
- (Exam Topic 4)
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.
Which of the following terms best matches the definition?

A. Ransomware
B. Adware
C. Spyware
D. Riskware

Answer: A

Explanation:
Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.
References: https://en.wikipedia.org/wiki/Ransomware

NEW QUESTION 451
- (Exam Topic 4)
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?

A. Threat
B. Attack
C. Vulnerability
D. Risk

Answer: A

Explanation:
A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
References: https://en.wikipedia.org/wiki/Threat_(computer)

NEW QUESTION 455
- (Exam Topic 4)
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Hosts
B. Sudoers
C. Boot.ini
D. Networks

Answer: A

Explanation:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.
References: https://en.wikipedia.org/wiki/Hosts_(file)

NEW QUESTION 460
- (Exam Topic 4)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?

A. Social engineering
B. Tailgating
C. Piggybacking
D. Eavesdropping

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential

information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION 463
- (Exam Topic 4)
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24

Answer: A

Explanation:
command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

NEW QUESTION 467
- (Exam Topic 4)
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?

A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.

Answer: A

Explanation:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.
References: https://capec.mitre.org/data/definitions/303.html

NEW QUESTION 470
- (Exam Topic 5)
The "black box testing" methodology enforces which kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Answer: A

Explanation:
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.
References: https://en.wikipedia.org/wiki/Black-box_testing

NEW QUESTION 475
- (Exam Topic 5)
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.
What Web browser-based security vulnerability was exploited to compromise the user?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Clickjacking
D. Web form input validation

Answer: A

Explanation:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.
Example and characteristics
If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

NEW QUESTION 478
- (Exam Topic 5)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat the same attack against all L2 switches of the network.
D. He will repeat this action so that it escalates to a DoS attack.

Answer: A

NEW QUESTION 482
- (Exam Topic 5)
Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG
B. SMS
C. SNMP
D. ICMP

Answer: A

Explanation:
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.
References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

NEW QUESTION 485
- (Exam Topic 5)
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Protect the payload and the headers
B. Authenticate
C. Encrypt
D. Work at the Data Link Layer

Answer: D

NEW QUESTION 489
- (Exam Topic 5)
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router

Answer: A

Explanation:
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 493
- (Exam Topic 5)
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Vulnerability scanner
B. Protocol analyzer
C. Port scanner
D. Intrusion Detection System

Answer: A

Explanation:
A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.
References: https://en.wikipedia.org/wiki/Vulnerability_scanner

NEW QUESTION 496
- (Exam Topic 5)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability
C. SQL injection vulnerability
D. Web site defacement vulnerability

Answer: A

Explanation:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 501
- (Exam Topic 5)
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

Answer: B

NEW QUESTION 506
- (Exam Topic 5)
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

A. RST
B. ACK
C. SYN-ACK
D. SYN

Answer: D

NEW QUESTION 508
- (Exam Topic 5)
What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?

A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
B. Manipulate format strings in text fields
C. SSH
D. SYN Flood

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.
Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

NEW QUESTION 510
- (Exam Topic 5)
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

A. NT:LM
B. LM:NT
C. LM:NTLM
D. NTLM:LM

Answer: B

NEW QUESTION 511
- (Exam Topic 5)

What two conditions must a digital signature meet?

A. Has to be unforgeable, and has to be authentic.
B. Has to be legible and neat.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique.

Answer: A

NEW QUESTION 512
- (Exam Topic 5)
Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC
B. PEM
C. SET
D. PPP

Answer: A

NEW QUESTION 517
- (Exam Topic 5)
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Answer: D

NEW QUESTION 521
- (Exam Topic 5)
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal Whitebox
B. External, Whitebox
C. Internal, Blackbox
D. External, Blackbox

Answer: C

NEW QUESTION 523
- (Exam Topic 5)
Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 527
- (Exam Topic 5)
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS

Answer: A

Explanation:
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.
References: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

NEW QUESTION 531

- (Exam Topic 5)
Which of the following security operations is used for determining the attack surface of an organization?

A. Running a network scan to detect network services in the corporate DMZ
B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Using configuration management to determine when and where to apply security patches

Answer: A

Explanation:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.
References:
http://meisecurity.com/home/consulting/consulting-network-scanning/

NEW QUESTION 535
- (Exam Topic 5)
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: ACK, ACK-SYN, SYNConnection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: FIN, ACK-FIN, ACK

Answer: D

NEW QUESTION 540
- (Exam Topic 5)
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com

Answer: D

NEW QUESTION 545
- (Exam Topic 5)
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet

Answer: D

NEW QUESTION 548
- (Exam Topic 5)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok.
B. He needs to add the command ""ip address"" just before the IP address.
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
D. He needs to change the address to 192.168.1.0 with the same mask.

Answer: C

NEW QUESTION 550
- (Exam Topic 5)
Which of the following statements regarding ethical hacking is incorrect?

A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
B. Testing should be remotely performed offsite.
C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
D. Ethical hacking should not involve writing to or modifying the target systems.

Answer: A

Explanation:
Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.
References:

http://searchsecurity.techtarget.com/definition/ethical-hacker

NEW QUESTION 551
- (Exam Topic 5)
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

A. The sequence does not matte
B. Both steps have to be performed against all hosts.
C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
D. First the ping sweep to identify live hosts and then the port scan on the live host
E. This way he saves time.
F. The port scan alone is adequat
G. This way he saves time.

Answer: C

NEW QUESTION 554
- (Exam Topic 5)
____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

A. DNSSEC
B. Zone transfer
C. Resource transfer
D. Resource records

Answer: A

NEW QUESTION 559
- (Exam Topic 5)
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Password protected files
B. Hidden folders
C. BIOS password
D. Full disk encryption.

Answer: D

NEW QUESTION 564
- (Exam Topic 5)
Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password
B. A fingerprint scanner and his username and password.
C. Disable his username and use just a fingerprint scanner.
D. His username and a stronger password.

Answer: B

NEW QUESTION 567
- (Exam Topic 5)
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

A. Network-based intrusion detection system (NIDS)
B. Host-based intrusion detection system (HIDS)
C. Firewalls
D. Honeypots

Answer: A

NEW QUESTION 572
- (Exam Topic 5)
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

A. Use cryptographic storage to store all PII
B. Use encrypted communications protocols to transmit PII
C. Use full disk encryption on all hard drives to protect PII
D. Use a security token to log into all Web applications that use PII

Answer: A

Explanation:
As a matter of good practice any PII should be protected with strong encryption.
References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

NEW QUESTION 576
- (Exam Topic 5)
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark
B. Maltego
C. Metasploit
D. Nessus

Answer: C

NEW QUESTION 580
- (Exam Topic 5)
Scenario:
What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution
B. HTML Injection
C. Session Fixation
D. ClickJacking Attack

Answer: D

NEW QUESTION 585
- (Exam Topic 5)
What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Answer: A

NEW QUESTION 590
- (Exam Topic 5)
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk
B. Inherent risk
C. Deferred risk
D. Impact risk

Answer: A

Explanation:
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
References: https://en.wikipedia.org/wiki/Residual_risk

NEW QUESTION 592
- (Exam Topic 5)
What is the role of test automation in security testing?

A. It can accelerate benchmark tests and repeat them with a consistent test setu
B. But it cannot replace manual testing completely.
C. It is an option but it tends to be very expensive.
D. It should be used exclusivel
E. Manual testing is outdated because of low speed and possible test setup inconsistencies.
F. Test automation is not usable in security due to the complexity of the tests.

Answer: A

NEW QUESTION 594
- (Exam Topic 5)
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Sniffing
C. Eavesdropping
D. Scanning

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.
References: https://en.wikipedia.org/wiki/Social_engineering_(security)

NEW QUESTION 596
- (Exam Topic 5)
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

A. RADIUS
B. DIAMETER
C. Kerberos
D. TACACS+

Answer: A

Explanation:
Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.
References: https://en.wikipedia.org/wiki/RADIUS

NEW QUESTION 600
- (Exam Topic 5)
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?

A. Phishing
B. Whaling
C. Tailgating
D. Masquerading

Answer: C

NEW QUESTION 605
- (Exam Topic 5)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit

Answer: A

Explanation:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION 610
- (Exam Topic 5)
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.
What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Intrusion Prevention System (IPS)
C. Network sniffer
D. Vulnerability scanner

Answer: A

Explanation:
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.
References: https://en.wikipedia.org/wiki/Packet_analyzer

NEW QUESTION 612
- (Exam Topic 5)
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.

Answer: A

NEW QUESTION 616
- (Exam Topic 5)
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

Answer: C

NEW QUESTION 618
- (Exam Topic 6)
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
B. Vulnerabilities in the application layer are independent of the network laye
C. Attacks and mitigation techniques are almost identical.
D. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
E. Vulnerabilities in the application layer are greatly different from IPv4.

Answer: B

NEW QUESTION 622
- (Exam Topic 6)
Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Answer: B

NEW QUESTION 623
- (Exam Topic 6)
A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation, it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

A. The client cannot see the SSID of the wireless network
B. The WAP does not recognize the client’s MAC address.
C. The wireless client is not configured to use DHCP.
D. Client is configured for the wrong channel

Answer: B

NEW QUESTION 624
- (Exam Topic 6)
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. Windows
B. Unix
C. Linux
D. OS X

Answer: A

NEW QUESTION 627
- (Exam Topic 6)
Which Type of scan sends a packets with no flags set?

A. Open Scan
B. Null Scan
C. Xmas Scan
D. Half-Open Scan

Answer: B

NEW QUESTION 632
- (Exam Topic 6)
Which of the following is NOT an ideal choice for biometric controls?

A. Iris patterns
B. Fingerprints
C. Height and weight
D. Voice

Answer: C

NEW QUESTION 637
- (Exam Topic 6)
Which of the following is a wireless network detector that is commonly found on Linux?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Answer: A

NEW QUESTION 638
- (Exam Topic 6)
A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

A. Turtle Trojans
B. Ransomware Trojans
C. Botnet Trojan
D. Banking Trojans

Answer: C

NEW QUESTION 642
- (Exam Topic 6)
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25

Answer: B

NEW QUESTION 645
- (Exam Topic 6)
What is the term coined for logging, recording and resolving events in a company?

A. Internal Procedure
B. Security Policy
C. Incident Management Process
D. Metrics

Answer: C

NEW QUESTION 648
- (Exam Topic 6)
A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

A. Insufficient security management
B. Insufficient database hardening
C. Insufficient input validation
D. Insufficient exception handling

Answer: B

NEW QUESTION 649
- (Exam Topic 6)
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log
C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Answer: B

NEW QUESTION 653

- (Exam Topic 6)
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5
B. $250
C. $125
D. $65.2

Answer: A

NEW QUESTION 657
- (Exam Topic 6)
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. ping
C. tracert
D. tcpdump

Answer: D

NEW QUESTION 661
- (Exam Topic 6)
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.
How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Answer: B

NEW QUESTION 663
- (Exam Topic 6)
Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254
B. nmap -sP 192.168.1.254
C. nmap -sX 192.168.1.254
D. nmap -sV 192.168.1.254

Answer: C

NEW QUESTION 667
- (Exam Topic 6)
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

A. Social Engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

Answer: A

NEW QUESTION 670
- (Exam Topic 6)
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

A. NET FILE
B. NET USE
C. NET CONFIG
D. NET VIEW

Answer: B

NEW QUESTION 673
- (Exam Topic 6)
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap

D. Ethereal with Winpcap

Answer: A

NEW QUESTION 675
- (Exam Topic 6)
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy

Answer: B

NEW QUESTION 678
- (Exam Topic 6)
Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

A. Intrusion Detection System
B. Vulnerability scanner
C. Port scanner
D. Protocol analyzer

Answer: B

NEW QUESTION 682
- (Exam Topic 6)
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

A. Scanning
B. Reconnaissance
C. Escalation
D. Enumeration

Answer: B

NEW QUESTION 686
- (Exam Topic 6)
XOR is a common cryptographic tool. 10110001 XOR 00111010 is?

A. 10111100
B. 11011000
C. 10011101
D. 10001011

Answer: D

NEW QUESTION 688
- (Exam Topic 6)
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

A. Preparation phase
B. Containment phase
C. Recovery phase
D. Identification phase

Answer: A

NEW QUESTION 689
- (Exam Topic 6)
Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

A. Use digital certificates to authenticate a server prior to sending data.
B. Verify access right before allowing access to protected information and UI controls.
C. Verify access right before allowing access to protected information and UI controls.
D. Validate and escape all information sent to a server.

Answer: D

NEW QUESTION 694
- (Exam Topic 6)
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock

Answer: A

NEW QUESTION 699
- (Exam Topic 6)
Name two software tools used for OS guessing? (Choose two.)

A. Nmap
B. Snadboy
C. Queso
D. UserInfo
E. NetBus

Answer: AC

NEW QUESTION 703
- (Exam Topic 6)
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

Answer: C

NEW QUESTION 705
- (Exam Topic 6)
Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

A. In a cool dry environment
B. Inside the data center for faster retrieval in a fireproof safe
C. In a climate controlled facility offsite
D. On a different floor in the same building

Answer: C

NEW QUESTION 707
- (Exam Topic 6)
Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

A. Metasploit
B. Wireshark
C. Maltego
D. Cain & Abel

Answer: C

NEW QUESTION 709
- (Exam Topic 6)
If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ
B. Reviewing the need for a security clearance for each employee
C. Using configuration management to determine when and where to apply security patches
D. Training employees on the security policy regarding social engineering

Answer: A

NEW QUESTION 710
- (Exam Topic 6)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.
77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 714
- (Exam Topic 6)
Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

A. http-git
B. http-headers
C. http enum
D. http-methods

Answer: D

NEW QUESTION 715
- (Exam Topic 6)
What kind of risk will remain even if all theoretically possible safety measures would be applied?

A. Residual risk
B. Inherent risk
C. Impact risk
D. Deferred risk

Answer: A

NEW QUESTION 718
- (Exam Topic 6)
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

A. Stateful
B. Application
C. Circuit
D. Packet Filtering

Answer: B

NEW QUESTION 723
- (Exam Topic 6)
What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

A. $440
B. $100
C. $1320
D. $146

Answer: D

NEW QUESTION 727
- (Exam Topic 6)
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

Answer: C

NEW QUESTION 728
.....

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
- (Exam Topic 1)
What would you enter, if you wanted to perform a stealth scan using Nmap?

A. nmap -sU
B. nmap -sS
C. nmap -sM
D. nmap -sT

Answer: B

NEW QUESTION 2
- (Exam Topic 1)
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occurring during non-business hours. After further examination of all login activities, it is noticed that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realizes the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux servers to synchronize the time has stopped working?

A. Time Keeper
B. NTP
C. PPP
D. OSPP

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

A. End of Line Comment
B. UNION SQL Injection
C. Illegal/Logically Incorrect Query
D. Tautology

Answer: D

NEW QUESTION 4
- (Exam Topic 1)
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach.
After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:

A. Although the approach has two phases, it actually implements just one authentication factor
B. The solution implements the two authentication factors: physical object and physical characteristic
C. The solution will have a high level of false positives
D. Biological motion cannot be used to identify people

Answer: B

NEW QUESTION 5
- (Exam Topic 1)
Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company.
What is the main security risk associated with this scenario?

A. External script contents could be maliciously modified without the security team knowledge
B. External scripts have direct access to the company servers and can steal the data from there
C. There is no risk at all as the marketing services are trustworthy
D. External scripts increase the outbound company data traffic which leads greater financial losses

Answer: A

NEW QUESTION 6
- (Exam Topic 1)
Which of the following is considered as one of the most reliable forms of TCP scanning?

A. TCP Connect/Full Open Scan
B. Half-open Scan
C. NULL Scan
D. Xmas Scan

Answer: A

NEW QUESTION 7
- (Exam Topic 1)
Code injection is a form of attack in which a malicious user:

A. Inserts text into a data field that gets interpreted as code
B. Gets the server to execute arbitrary code using a buffer overflow
C. Inserts additional code into the JavaScript running in the browser
D. Gains access to the codebase on the server and inserts new code

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

A. SSH communications are encrypted it's impossible to know who is the client or the server
B. Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
C. Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server
D. Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

Answer: C

NEW QUESTION 9
- (Exam Topic 1)
Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did not intend?

A. Command Injection Attacks
B. File Injection Attack
C. Cross-Site Request Forgery (CSRF)
D. Hidden Field Manipulation Attack

Answer: C

NEW QUESTION 10
- (Exam Topic 1)
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?

A. The use of security agents in clients' computers
B. The use of DNSSEC
C. The use of double-factor authentication
D. Client awareness

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

A. Double quotation
B. Backslash
C. Semicolon
D. Single quotation

Answer: D

NEW QUESTION 11
- (Exam Topic 1)
What is the main security service a cryptographic hash provides?

A. Integrity and ease of computation
B. Message authentication and collision resistance
C. Integrity and collision resistance
D. Integrity and computational in-feasibility

Answer: D

NEW QUESTION 14
- (Exam Topic 1)
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering

B. Tailgating
C. Piggybacking
D. Announced

Answer: B

NEW QUESTION 15
- (Exam Topic 1)
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

A. PPP
B. IPSEC
C. PEM
D. SET

Answer: B

NEW QUESTION 20
- (Exam Topic 1)
Which of the following provides a security professional with most information about the system’s security posture?

A. Wardriving, warchalking, social engineering
B. Social engineering, company site browsing, tailgating
C. Phishing, spamming, sending trojans
D. Port scanning, banner grabbing, service identification

Answer: D

NEW QUESTION 21
- (Exam Topic 1)
You are monitoring the network of your organizations. You notice that: Which of the following solution will you suggest?

A. Block the Blacklist IP’s @ Firewall
B. Update the Latest Signatures on your IDS/IPS
C. Clean the Malware which are trying to Communicate with the External Blacklist IP’s
D. Both B and C

Answer: D

NEW QUESTION 23
- (Exam Topic 1)
Which of the following steps for risk assessment methodology refers to vulnerability identification?

A. Determines if any flaws exist in systems, policies, or procedures
B. Assigns values to risk probabilities; Impact values.
C. Determines risk probability that vulnerability will be exploited (Hig
D. Medium, Low)
E. Identifies sources of harm to an IT syste
F. (Natural, Huma
G. Environmental)

Answer: C

NEW QUESTION 24
- (Exam Topic 1)
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner’s permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

A. Suicide Hacker
B. Black Hat
C. White Hat
D. Gray Hat

Answer: D

NEW QUESTION 25
- (Exam Topic 1)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

A. “GET/restricted/goldtransfer?to=Rob&from=1 or 1=1’ HTTP/1.1Host: westbank.com”
B. “GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com”
C. “GET/restricted/bank.getaccount(‘Ned’) HTTP/1.1 Host: westbank.com”
D. “GET/restricted/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com”

Answer: B

NEW QUESTION 28
- (Exam Topic 1)
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Answer: C

NEW QUESTION 33
- (Exam Topic 1)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
What kind of Web application vulnerability likely exists in their software?

A. Host-Based Intrusion Detection System
B. Security through obscurity
C. Defense in depth
D. Network-Based Intrusion Detection System

Answer: C

NEW QUESTION 35
- (Exam Topic 1)
When tuning security alerts, what is the best approach?

A. Tune to avoid False positives and False Negatives
B. Rise False positives Rise False Negatives
C. Decrease the false positives
D. Decrease False negatives

Answer: A

NEW QUESTION 39
- (Exam Topic 1)
Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.
Which of the following types of firewalls can protect against SQL injection attacks?

A. Data-driven firewall
B. Stateful firewall
C. Packet firewall
D. Web application firewall

Answer: D

NEW QUESTION 43
- (Exam Topic 1)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

A. Authentication
B. Confidentiality
C. Integrity
D. Non-Repudiation

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?

A. None of these scenarios compromise the privacy of Alice’s data
B. Agent Andrew subpoenas Alice, forcing her to reveal her private ke
C. However, the cloud server successfully resists Andrew’s attempt to access the stored data
D. Hacker Harry breaks into the cloud server and steals the encrypted data
E. Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before

Answer: D

NEW QUESTION 47
- (Exam Topic 1)
Why containers are less secure that virtual machines?

A. Host OS on containers has a larger surface attack.
B. Containers may full fill disk space of the host.
C. A compromise container may cause a CPU starvation of the host.
D. Containers are attached to the same virtual network.

Answer: A

NEW QUESTION 48
- (Exam Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

A. Symmetric algorithms such as AES provide a failsafe when asymmetric methods fail.
B. Asymmetric cryptography is computationally expensive in compariso
C. However, it is well-suited to securely negotiate keys for use with symmetric cryptography.
D. Symmetric encryption allows the server to securely transmit the session keys out-of-band.
E. Supporting both types of algorithms allows less-powerful devices such as mobile phones to use symmetric encryption instead.

Answer: D

NEW QUESTION 52
- (Exam Topic 1)
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

A. Nmap
B. Cain & Abel
C. Nessus
D. Snort

Answer: D

NEW QUESTION 55
- (Exam Topic 1)
A virus that attempts to install itself inside the file it is infecting is called?

A. Tunneling virus
B. Cavity virus
C. Polymorphic virus
D. Stealth virus

Answer: B

NEW QUESTION 57
- (Exam Topic 1)
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

A. Disable unused ports in the switches
B. Separate students in a different VLAN
C. Use the 802.1x protocol
D. Ask students to use the wireless network

Answer: C

NEW QUESTION 58
- (Exam Topic 1)
In the field of cryptanalysis, what is meant by a “rubber-hose" attack?

A. Attempting to decrypt cipher text by making logical assumptions about the contents of the original plain text.
B. Extraction of cryptographic secrets through coercion or torture.
C. Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
D. A backdoor placed into a cryptographic algorithm by its creator.

Answer: B

NEW QUESTION 61
- (Exam Topic 1)
Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.
Your email message looks like this: From: jim_miller@companyxyz.com
To: michelle_saunders@companyxyz.com Subject: Test message
Date: 4/3/2017 14:37

The employee of Company XYZ receives your email message. This proves that Company XYZ's email gateway doesn't prevent what?

A. Email Phishing
B. Email Masquerading
C. Email Spoofing
D. Email Harvesting

Answer: C

NEW QUESTION 62
- (Exam Topic 1)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

A. Libpcap
B. Awinpcap
C. Winprom
D. Winpcap

Answer: D

NEW QUESTION 65
- (Exam Topic 1)
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

A. Black-Hat Hackers A
B. Script Kiddies
C. White-Hat Hackers
D. Gray-Hat Hacker

Answer: C

NEW QUESTION 70
- (Exam Topic 1)
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

A. Hire a security consultant to provide direction.
B. Do not back up cither the credit card numbers or then hashes.
C. Back up the hashes of the credit card numbers not the actual credit card numbers.
D. Encrypt backup tapes that are sent off-site.

Answer: A

NEW QUESTION 74
- (Exam Topic 1)
When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

A. Identifying operating systems, services, protocols and devices
B. Modifying and replaying captured network traffic
C. Collecting unencrypted information about usernames and passwords
D. Capturing a network traffic for further analysis

Answer: B

NEW QUESTION 79
- (Exam Topic 1)
During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

A. Private keys
B. User passwords
C. Public keys
D. Public and private keys

Answer: C

NEW QUESTION 81
- (Exam Topic 1)
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?

A. ACK flag scanning
B. TCP Scanning
C. IP Fragment Scanning
D. Inverse TCP flag scanning

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. –T0
B. –T5
C. -O
D. -A

Answer: B

NEW QUESTION 90
- (Exam Topic 1)
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends “many” IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:

A. Just a network monitoring tool
B. A signature-based IDS
C. A hybrid IDS
D. A behavior-based IDS

Answer: A

NEW QUESTION 91
- (Exam Topic 2)
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

A. non-repudiation.
B. operability.
C. security.
D. usability.

Answer: A

NEW QUESTION 92
- (Exam Topic 2)
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical
B. Procedural
C. Technical
D. Compliance

Answer: B

NEW QUESTION 97
- (Exam Topic 2)
Which tool would be used to collect wireless packet data?

A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

Answer: A

NEW QUESTION 100
- (Exam Topic 2)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

Answer: A

NEW QUESTION 101
- (Exam Topic 2)
Which of the following is an application that requires a host application for replication?

A. Micro

B. Worm
C. Trojan
D. Virus

Answer: D

Explanation:
Computer viruses infect a variety of different subsystems on their hosts. A computer virus is a malware that, when executed, replicates by reproducing itself or infecting other programs by modifying them. Infecting computer programs can include as well, data files, or the boot sector of the hard drive. When this replication succeeds, the affected areas are then said to be "infected".
References: https://en.wikipedia.org/wiki/Computer_virus

NEW QUESTION 105
- (Exam Topic 2)
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

Answer: A

NEW QUESTION 106
- (Exam Topic 2)
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine

Answer: C

NEW QUESTION 108
- (Exam Topic 2)
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon
B. Single quote
C. Exclamation mark
D. Double quote

Answer: B

NEW QUESTION 110
- (Exam Topic 2)
Which of the following techniques will identify if computer files have been changed?

A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

Answer: C

NEW QUESTION 115
- (Exam Topic 2)
When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing

Answer: B

NEW QUESTION 117
- (Exam Topic 2)
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC

C. 128 bit and CCMP
D. 128 bit and TKIP

Answer: C

NEW QUESTION 122
- (Exam Topic 2)
A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config
D. Ipconfig firewall show config

Answer: A

NEW QUESTION 126
- (Exam Topic 2)
What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode
B. Enabling port forwarding on the router
C. Installing the router outside of the network's firewall
D. Disabling the router from accepting broadcast ping messages

Answer: D

NEW QUESTION 130
- (Exam Topic 2)
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

A. if (billingAddress = 50) {update field} else exit
B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

Answer: D

NEW QUESTION 134
- (Exam Topic 2)
Which of the following is a hashing algorithm?

A. MD5
B. PGP
C. DES
D. ROT13

Answer: A

NEW QUESTION 138
- (Exam Topic 2)
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

Answer: C

NEW QUESTION 142
- (Exam Topic 2)
Low humidity in a data center can cause which of the following problems?

A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

Answer: C

NEW QUESTION 146
- (Exam Topic 2)
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

Answer: B

Explanation:
A full restore is required.

NEW QUESTION 151
- (Exam Topic 2)
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

Answer: B

NEW QUESTION 153
- (Exam Topic 2)
A botnet can be managed through which of the following?

A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

Answer: A

NEW QUESTION 154
- (Exam Topic 2)
Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query
B. Results matching “accounting” in domain target.com but not on the site Marketing.target.com
C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
D. Results for matches on target.com and Marketing.target.com that include the word “accounting”

Answer: B

NEW QUESTION 155
- (Exam Topic 2)
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

Answer: D

NEW QUESTION 156
- (Exam Topic 2)
Which set of access control solutions implements two-factor authentication?

A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

Answer: A

NEW QUESTION 161
- (Exam Topic 2)
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap
B. Tailgating
C. Shoulder surfing
D. Social engineering

Answer: B

NEW QUESTION 166
- (Exam Topic 2)
One advantage of an application-level firewall is the ability to

A. filter packets at the network level.
B. filter specific commands, such as http:post.
C. retain state information for each packet.
D. monitor tcp handshaking.

Answer: B

NEW QUESTION 168
- (Exam Topic 2)
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.
B. Allow full DNS zone transfers.
C. Remove A records for internal hosts.
D. Enable null session pipes.

Answer: C

NEW QUESTION 171
- (Exam Topic 2)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.
B. NMAP -P 192.168.0.0/16
C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0
D. NMAP -P 192.168.1/17

Answer: A

NEW QUESTION 173
- (Exam Topic 2)
What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

Answer: C

NEW QUESTION 175
- (Exam Topic 2)
Which security control role does encryption meet?

A. Preventative
B. Detective
C. Offensive
D. Defensive

Answer: A

NEW QUESTION 177
- (Exam Topic 2)
Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP
B. Nikto
C. Ike-scan
D. Arp-scan

Answer: C

NEW QUESTION 179
- (Exam Topic 2)
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key

B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Answer: C

NEW QUESTION 183
- (Exam Topic 2)
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

Answer: C

NEW QUESTION 187
- (Exam Topic 2)
Which of the following is a strong post designed to stop a car?

A. Gate
B. Fence
C. Bollard
D. Reinforced rebar

Answer: C

NEW QUESTION 190
- (Exam Topic 2)
An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

Answer: D

NEW QUESTION 194
- (Exam Topic 2)
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

Answer: B

NEW QUESTION 199
- (Exam Topic 2)
Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
B. The session cookies generated by the application do not have the HttpOnly flag set.
C. The victim user must open the malicious link with a Firefox prior to version 3.
D. The web application should not use random tokens.

Answer: D

NEW QUESTION 204
- (Exam Topic 2)
Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

Answer: A

NEW QUESTION 209
- (Exam Topic 2)

What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

Answer: D

NEW QUESTION 211
- (Exam Topic 2)
How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

Answer: A

NEW QUESTION 216
- (Exam Topic 2)
How can rainbow tables be defeated?

A. Password salting
B. Use of non-dictionary words
C. All uppercase character passwords
D. Lockout accounts under brute force password cracking attempts

Answer: A

NEW QUESTION 221
- (Exam Topic 2)
Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

Answer: D

NEW QUESTION 226
- (Exam Topic 2)
Which command line switch would be used in NMAP to perform operating system detection?

A. -OS
B. -sO
C. -sP
D. -O

Answer: D

NEW QUESTION 230
- (Exam Topic 2)
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21. During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?

A. True negatives
B. False negatives
C. True positives
D. False positives

Answer: D

NEW QUESTION 233
- (Exam Topic 2)
What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

Answer: D

NEW QUESTION 237
- (Exam Topic 2)
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

Answer: D

NEW QUESTION 240
- (Exam Topic 2)
Passive reconnaissance involves collecting information through which of the following?

A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

Answer: D

NEW QUESTION 243
- (Exam Topic 2)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

Answer: A

NEW QUESTION 245
- (Exam Topic 2)
A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:
Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

Answer: D

NEW QUESTION 249
- (Exam Topic 2)
ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

Answer: A

NEW QUESTION 253
- (Exam Topic 2)
During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

Answer: B

NEW QUESTION 258
- (Exam Topic 2)
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25

C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

Answer: D

NEW QUESTION 259
- (Exam Topic 2)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box
B. grey box
C. red box
D. black box

Answer: D

NEW QUESTION 261
- (Exam Topic 2)
Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

Answer: D

NEW QUESTION 263
- (Exam Topic 2)
Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.

Answer: B

Explanation:
Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.
References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

NEW QUESTION 264
- (Exam Topic 2)
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus
B. Polymorphic virus
C. Tunneling virus
D. Stealth virus

Answer: D

NEW QUESTION 269
- (Exam Topic 2)
Least privilege is a security concept that requires that a user is

A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

Answer: A

NEW QUESTION 270
- (Exam Topic 2)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS
B. IANA
C. CAPTCHA
D. IETF

Answer:

A

NEW QUESTION 273
- (Exam Topic 2)
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.
B. Encrypt the data on the hard drive.
C. Use a strong logon password to the operating system.
D. Back up everything on the laptop and store the backup in a safe place.

Answer: B

NEW QUESTION 278
- (Exam Topic 2)
Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

Answer: A

NEW QUESTION 281
- (Exam Topic 2)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

Answer: D

NEW QUESTION 282
- (Exam Topic 3)
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation’s Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure
C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

Answer: A

NEW QUESTION 286
- (Exam Topic 3)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she’s asking the CEH to take.

Answer: A

NEW QUESTION 291
- (Exam Topic 3)
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

Answer: D

NEW QUESTION 296
- (Exam Topic 3)
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT

B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

Answer: B

NEW QUESTION 298
- (Exam Topic 3)
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

Answer: C

NEW QUESTION 300
- (Exam Topic 3)
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

Answer: D

NEW QUESTION 302
- (Exam Topic 3)
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

Answer: D

NEW QUESTION 304
- (Exam Topic 3)
Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5
B. SHA-1
C. RC4
D. MD4

Answer: B

NEW QUESTION 307
- (Exam Topic 3)
Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

Answer: D

NEW QUESTION 311
- (Exam Topic 3)
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

Answer: B

NEW QUESTION 313

- (Exam Topic 3)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

Answer: A

NEW QUESTION 314
- (Exam Topic 3)
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

Answer: D

NEW QUESTION 319
- (Exam Topic 3)
In the OSI model, where does PPTP encryption take place?

A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

Answer: C

NEW QUESTION 323
- (Exam Topic 3)
While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
<script>alert(" Testing Testing Testing ")</script>
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

Answer: D

NEW QUESTION 326
- (Exam Topic 3)
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

Answer: D

NEW QUESTION 329
- (Exam Topic 3)
Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

Answer: C

NEW QUESTION 332
- (Exam Topic 3)
Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
B. It is compatible with various databases including Access, Oracle, and SQL.
C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

Answer: A

NEW QUESTION 334
- (Exam Topic 3)
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit
B. Audit, standards based, regulatory
C. Contractual, regulatory, industry
D. Legislative, contractual, standards based

Answer: D

NEW QUESTION 339
- (Exam Topic 3)
Which type of security document is written with specific step-by-step details?

A. Process
B. Procedure
C. Policy
D. Paradigm

Answer: B

NEW QUESTION 342
- (Exam Topic 3)
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

A. Threaten to publish the penetration test results if not paid.
B. Follow proper legal procedures against the company to request payment.
C. Tell other customers of the financial problems with payments from this company.
D. Exploit some of the vulnerabilities found on the company webserver to deface it.

Answer: B

NEW QUESTION 346
- (Exam Topic 3)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin

Answer: C

NEW QUESTION 349
- (Exam Topic 3)
A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

Answer: C

NEW QUESTION 350
- (Exam Topic 3)
Which of the following is an example of IP spoofing?

A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

Answer: B

NEW QUESTION 353
- (Exam Topic 3)
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Answer: A

NEW QUESTION 358
- (Exam Topic 4)
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?

A. Metagoofil
B. Armitage
C. Dimitry
D. cdpsnarf

Answer: A

Explanation:
Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company. Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.
References:
http://www.edge-security.com/metagoofil.php

NEW QUESTION 360
- (Exam Topic 4)
You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).
What is the best way to evade the NIDS?

A. Encryption
B. Protocol Isolation
C. Alternate Data Streams
D. Out of band signalling

Answer: A

Explanation:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.
References:
http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

NEW QUESTION 364
- (Exam Topic 4)
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?

A. site: target.com filetype:xls username password email
B. inurl: target.com filename:xls username password email
C. domain: target.com archive:xls username password email
D. site: target.com file:xls username password email

Answer: A

Explanation:
If you include site: in your query, Google will restrict your search results to the site or domain you specify. If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in
suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and “checklist.”
References:
http://www.googleguide.com/advanced_operators_reference.html

NEW QUESTION 365
- (Exam Topic 4)
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Intrusion Prevention System
B. Wireless Access Point
C. Wireless Access Control List
D. Wireless Analyzer

Answer: A

Explanation:
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).
References: https://en.wikipedia.org/wiki/Wireless_intrusion_prevention_system

NEW QUESTION 370
- (Exam Topic 4)
A common cryptographical tool is the use of XOR. XOR the following binary values:
10110001
00111010

A. 10001011
B. 11011000
C. 10011101
D. 10111100

Answer: A

Explanation:
The XOR gate is a digital logic gate that implements an exclusive or; that is, a true output (1/HIGH) results if one, and only one, of the inputs to the gate is true. If both inputs are false (0/LOW) or both are true, a false output results. XOR represents the inequality function, i.e., the output is true if the inputs are not alike otherwise the output is false. A way to remember XOR is "one or the other but not both".
References: https://en.wikipedia.org/wiki/XOR_gate

NEW QUESTION 374
- (Exam Topic 4)
How does the Address Resolution Protocol (ARP) work?

A. It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
C. It sends a reply packet for a specific IP, asking for the MAC address.
D. It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Answer: A

Explanation:
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.
References:
http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

NEW QUESTION 379
- (Exam Topic 4)
What is the benefit of performing an unannounced Penetration Testing?

A. The tester will have an actual security posture visibility of the target network.
B. Network security would be in a "best state" posture.
C. It is best to catch critical infrastructure unpatched.
D. The tester could not provide an honest analysis.

Answer: A

Explanation:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.
A possible solution to this danger is to conduct intermittent “unannounced” penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with “announced” penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.
References:
http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

NEW QUESTION 381
- (Exam Topic 4)
You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.
What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.srcport==514 && ip.src==192.168.0.99
C. tcp.dstport==514 && ip.dst==192.168.0.0/16
D. tcp.srcport==514 && ip.src==192.168.150

Answer: A

Explanation:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.
References: https://wiki.wireshark.org/DisplayFilters

NEW QUESTION 384
- (Exam Topic 4)
> NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?

A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

Answer: A

Explanation:
NMAP -sn (No port scan)
This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be run.
References: https://nmap.org/book/man-host-discovery.html

NEW QUESTION 385
- (Exam Topic 4)
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

A. ICMP could be disabled on the target server.
B. The ARP is disabled on the target server.
C. TCP/IP doesn't support ICMP.
D. You need to run the ping command with root privileges.

Answer: A

Explanation:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.
Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.
References: https://en.wikipedia.org/wiki/Internet_Control_Message_Protocol

NEW QUESTION 387
- (Exam Topic 4)
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

A. Application
B. Circuit
C. Stateful
D. Packet Filtering

Answer: A

Explanation:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.
References:
http://searchsoftwarequality.techtarget.com/definition/application-firewall

NEW QUESTION 388
- (Exam Topic 4)
You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.
What is the best approach?

A. Install Cryptcat and encrypt outgoing packets from this server.
B. Install and use Telnet to encrypt all outgoing traffic from this server.
C. Use Alternate Data Streams to hide the outgoing packets from this server.
D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

Answer: A

Explanation:
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.
References:
http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-014

NEW QUESTION 390
- (Exam Topic 4)
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content. Which sort of trojan infects this server?

A. Botnet Trojan
B. Turtle Trojans
C. Banking Trojans
D. Ransomware Trojans

Answer: A

Explanation:
In computer science, a zombie is a computer connected to the Internet that has been compromised by a hacker, computer virus or trojan horse and can be used to perform malicious tasks of one sort or another under remote direction. Botnets of zombie computers are often used to spread e-mail spam and launch denial-of-service attacks. Most owners of zombie computers are unaware that their system is being used in this way. Because the owner tends to be unaware, these computers are metaphorically compared to zombies. A coordinated DDoS attack by multiple botnet machines also resembles a zombie horde attack.

NEW QUESTION 394
- (Exam Topic 4)
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.
Which command-line utility are you most likely to use?

A. Grep
B. Notepad
C. MS Excel
D. Relational Database

Answer: A

Explanation:
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression. References: https://en.wikipedia.org/wiki/Grep

NEW QUESTION 399
- (Exam Topic 4)
Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program
D. Overwrites the original MBR and only executes the new virus code

Answer: A

Explanation:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.
References: https://www.techopedia.com/definition/26655/boot-sector-virus

NEW QUESTION 401
- (Exam Topic 4)
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.
What should you do?

A. Forward the message to your company’s security response team and permanently delete the message from your computer.
B. Reply to the sender and ask them for more information about the message contents.
C. Delete the email and pretend nothing happened
D. Forward the message to your supervisor and ask for her opinion on how to handle the situation

Answer: A

Explanation:
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.
References:
https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NEW QUESTION 405
- (Exam Topic 4)
Which of the following is not a Bluetooth attack?

A. Bluedriving
B. Bluejacking
C. Bluesmacking
D. Bluesnarfing

Answer:

A

NEW QUESTION 410
- (Exam Topic 4)
You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW
B. Cain & Abel
C. SET
D. John the Ripper

Answer: A

Explanation:
chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.
References: https://en.wikipedia.org/wiki/Chntpw

NEW QUESTION 414
- (Exam Topic 4)
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?

A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

Answer: A

Explanation:
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
References:
http://www.bbc.co.uk/webwise/guides/about-bluetooth

NEW QUESTION 417
- (Exam Topic 4)
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A. Terms of Engagement
B. Project Scope
C. Non-Disclosure Agreement
D. Service Level Agreement

Answer: A

NEW QUESTION 421
- (Exam Topic 4)
This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

A. RSA
B. SHA
C. RC5
D. MD5

Answer: A

Explanation:
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.
Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.
References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

NEW QUESTION 423
- (Exam Topic 4)
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. TCP
B. UPD
C. ICMP
D. UPX

Answer: A

Explanation:
At the establishment of a TCP session the client starts by sending a SYN-packet (SYN=synchronize) with a sequence number. To hijack a session it is required to send a packet with a right seq-number, otherwise they are dropped.
References: https://www.exploit-db.com/papers/13587/

NEW QUESTION 427
- (Exam Topic 4)
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A. footprinting
B. network mapping
C. gaining access
D. escalating privileges

Answer: A

Explanation:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.
References:
http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

NEW QUESTION 428
- (Exam Topic 4)
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

A. Injection
B. Cross Site Scripting
C. Cross Site Request Forgery
D. Path disclosure

Answer: A

Explanation:
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
References: https://www.owasp.org/index.php/Top_10_2013-Top_10

NEW QUESTION 432
- (Exam Topic 4)
Which of the following statements is TRUE?

A. Sniffers operate on Layer 2 of the OSI model
B. Sniffers operate on Layer 3 of the OSI model
C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
D. Sniffers operate on the Layer 1 of the OSI model.

Answer: A

Explanation:
The OSI layer 2 is where packet sniffers collect their data. References: https://en.wikipedia.org/wiki/Ethernet_frame

NEW QUESTION 433
- (Exam Topic 4)
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.
What is this style of attack called?

A. zero-day
B. zero-hour
C. zero-sum
D. no-day

Answer: A

Explanation:
Stuxnet is a malicious computer worm believed to be a jointly built American-Israeli cyber weapon. Exploiting four zero-day flaws, Stuxnet functions by targeting machines using the Microsoft Windows operating system and networks, then seeking out Siemens Step7 software.
References: https://en.wikipedia.org/wiki/Stuxnet

NEW QUESTION 434

- (Exam Topic 4)
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

A. Aircrack-ng
B. Airguard
C. WLAN-crack
D. wificracker

Answer: A

Explanation:
Aircrack-ng is a complete suite of tools to assess WiFi network security.
The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.
References:
http://www.aircrack-ng.org/doku.php?id=aircrack-ng

NEW QUESTION 437
- (Exam Topic 4)
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode
B. AH permiscuous
C. ESP confidential
D. AH Tunnel mode

Answer: A

Explanation:
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

NEW QUESTION 439
- (Exam Topic 4)
Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?

A. Watering Hole Attack
B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phising Attack

Answer: A

Explanation:
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

NEW QUESTION 442
- (Exam Topic 4)
Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. tcpdump
B. nessus
C. etherea
D. Jack the ripper

Answer: A

Explanation:
tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP
and other packets being transmitted or received over a network to which the computer is attached. References: https://en.wikipedia.org/wiki/Tcpdump

NEW QUESTION 445
- (Exam Topic 4)
What is the process of logging, recording, and resolving events that take place in an organization?

A. Incident Management Process
B. Security Policy
C. Internal Procedure
D. Metrics

Answer: A

Explanation:
The activities within the incident management process include:
References: https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

NEW QUESTION 450
- (Exam Topic 4)
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.
Which of the following terms best matches the definition?

A. Ransomware
B. Adware
C. Spyware
D. Riskware

Answer: A

Explanation:
Ransomware is a type of malware that can be covertly installed on a computer without knowledge or intention of the user that restricts access to the infected computer system in some way, and demands that the user pay a ransom to the malware operators to remove the restriction. Some forms of ransomware systematically encrypt files on the system's hard drive, which become difficult or impossible to decrypt without paying the ransom for the encryption key, while some may simply lock the system and display messages intended to coax the user into paying. Ransomware typically propagates as a Trojan.
References: https://en.wikipedia.org/wiki/Ransomware

NEW QUESTION 451
- (Exam Topic 4)
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?

A. Threat
B. Attack
C. Vulnerability
D. Risk

Answer: A

Explanation:
A threat is at any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.
References: https://en.wikipedia.org/wiki/Threat_(computer)

NEW QUESTION 455
- (Exam Topic 4)
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.
Which file does the attacker need to modify?

A. Hosts
B. Sudoers
C. Boot.ini
D. Networks

Answer: A

Explanation:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.
References: https://en.wikipedia.org/wiki/Hosts_(file)

NEW QUESTION 460
- (Exam Topic 4)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?

A. Social engineering
B. Tailgating
C. Piggybacking
D. Eavesdropping

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential

information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION 463
- (Exam Topic 4)
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.
What is the best nmap command you will use?

A. nmap -T4 -F 10.10.0.0/24
B. nmap -T4 -r 10.10.1.0/24
C. nmap -T4 -O 10.10.0.0/24
D. nmap -T4 -q 10.10.0.0/24

Answer: A

Explanation:
command = nmap -T4 -F
description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.
References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

NEW QUESTION 467
- (Exam Topic 4)
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?

A. The port will ignore the packets.
B. The port will send an RST.
C. The port will send an ACK.
D. The port will send a SYN.

Answer: A

Explanation:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.
References: https://capec.mitre.org/data/definitions/303.html

NEW QUESTION 470
- (Exam Topic 5)
The "black box testing" methodology enforces which kind of restriction?

A. Only the external operation of a system is accessible to the tester.
B. Only the internal operation of a system is known to the tester.
C. The internal operation of a system is only partly accessible to the tester.
D. The internal operation of a system is completely known to the tester.

Answer: A

Explanation:
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.
References: https://en.wikipedia.org/wiki/Black-box_testing

NEW QUESTION 475
- (Exam Topic 5)
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.
What Web browser-based security vulnerability was exploited to compromise the user?

A. Cross-Site Request Forgery
B. Cross-Site Scripting
C. Clickjacking
D. Web form input validation

Answer: A

Explanation:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.
Example and characteristics
If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

NEW QUESTION 478
- (Exam Topic 5)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
B. He will activate OSPF on the spoofed root bridge.
C. He will repeat the same attack against all L2 switches of the network.
D. He will repeat this action so that it escalates to a DoS attack.

Answer: A

NEW QUESTION 482
- (Exam Topic 5)
Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG
B. SMS
C. SNMP
D. ICMP

Answer: A

Explanation:
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.
References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

NEW QUESTION 485
- (Exam Topic 5)
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Protect the payload and the headers
B. Authenticate
C. Encrypt
D. Work at the Data Link Layer

Answer: D

NEW QUESTION 489
- (Exam Topic 5)
Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System
B. Firewall
C. Proxy
D. Router

Answer: A

Explanation:
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

NEW QUESTION 493
- (Exam Topic 5)
To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Vulnerability scanner
B. Protocol analyzer
C. Port scanner
D. Intrusion Detection System

Answer: A

Explanation:
A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.
They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.
References: https://en.wikipedia.org/wiki/Vulnerability_scanner

NEW QUESTION 496
- (Exam Topic 5)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

A. Cross-site scripting vulnerability
B. Cross-site Request Forgery vulnerability
C. SQL injection vulnerability
D. Web site defacement vulnerability

Answer: A

Explanation:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 501
- (Exam Topic 5)
Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

Answer: B

NEW QUESTION 506
- (Exam Topic 5)
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

A. RST
B. ACK
C. SYN-ACK
D. SYN

Answer: D

NEW QUESTION 508
- (Exam Topic 5)
What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?

A. Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
B. Manipulate format strings in text fields
C. SSH
D. SYN Flood

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.
Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.
References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

NEW QUESTION 510
- (Exam Topic 5)
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

A. NT:LM
B. LM:NT
C. LM:NTLM
D. NTLM:LM

Answer: B

NEW QUESTION 511
- (Exam Topic 5)

What two conditions must a digital signature meet?

A. Has to be unforgeable, and has to be authentic.
B. Has to be legible and neat.
C. Must be unique and have special characters.
D. Has to be the same number of characters as a physical signature and must be unique.

Answer: A

NEW QUESTION 512
- (Exam Topic 5)
Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC
B. PEM
C. SET
D. PPP

Answer: A

NEW QUESTION 517
- (Exam Topic 5)
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

Answer: D

NEW QUESTION 521
- (Exam Topic 5)
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal Whitebox
B. External, Whitebox
C. Internal, Blackbox
D. External, Blackbox

Answer: C

NEW QUESTION 523
- (Exam Topic 5)
Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

Answer: C

NEW QUESTION 527
- (Exam Topic 5)
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS

Answer: A

Explanation:
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.
A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.
References: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

NEW QUESTION 531

- (Exam Topic 5)
Which of the following security operations is used for determining the attack surface of an organization?

A. Running a network scan to detect network services in the corporate DMZ
B. Training employees on the security policy regarding social engineering
C. Reviewing the need for a security clearance for each employee
D. Using configuration management to determine when and where to apply security patches

Answer: A

Explanation:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.
References:
http://meisecurity.com/home/consulting/consulting-network-scanning/

NEW QUESTION 535
- (Exam Topic 5)
What is the correct process for the TCP three-way handshake connection establishment and connection termination?

A. Connection Establishment: FIN, ACK-FIN, ACKConnection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: ACK, ACK-SYN, SYNConnection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACKConnection Termination: FIN, ACK-FIN, ACK

Answer: D

NEW QUESTION 540
- (Exam Topic 5)
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com
B. hping2 --set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com

Answer: D

NEW QUESTION 545
- (Exam Topic 5)
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet

Answer: D

NEW QUESTION 548
- (Exam Topic 5)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

A. The network must be down and the nmap command and IP address are ok.
B. He needs to add the command ""ip address"" just before the IP address.
C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.
D. He needs to change the address to 192.168.1.0 with the same mask.

Answer: C

NEW QUESTION 550
- (Exam Topic 5)
Which of the following statements regarding ethical hacking is incorrect?

A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
B. Testing should be remotely performed offsite.
C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
D. Ethical hacking should not involve writing to or modifying the target systems.

Answer: A

Explanation:
Ethical hackers use the same methods and techniques, including those that have the potential of exploiting vulnerabilities, to test and bypass a system's defenses as their less-principled counterparts, but rather than taking advantage of any vulnerabilities found, they document them and provide actionable advice on how to fix them so the organization can improve its overall security.
References:

http://searchsecurity.techtarget.com/definition/ethical-hacker

NEW QUESTION 551
- (Exam Topic 5)
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

A. The sequence does not matte
B. Both steps have to be performed against all hosts.
C. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
D. First the ping sweep to identify live hosts and then the port scan on the live host
E. This way he saves time.
F. The port scan alone is adequat
G. This way he saves time.

Answer: C

NEW QUESTION 554
- (Exam Topic 5)
____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

A. DNSSEC
B. Zone transfer
C. Resource transfer
D. Resource records

Answer: A

NEW QUESTION 559
- (Exam Topic 5)
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Password protected files
B. Hidden folders
C. BIOS password
D. Full disk encryption.

Answer: D

NEW QUESTION 564
- (Exam Topic 5)
Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password
B. A fingerprint scanner and his username and password.
C. Disable his username and use just a fingerprint scanner.
D. His username and a stronger password.

Answer: B

NEW QUESTION 567
- (Exam Topic 5)
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

A. Network-based intrusion detection system (NIDS)
B. Host-based intrusion detection system (HIDS)
C. Firewalls
D. Honeypots

Answer: A

NEW QUESTION 572
- (Exam Topic 5)
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

A. Use cryptographic storage to store all PII
B. Use encrypted communications protocols to transmit PII
C. Use full disk encryption on all hard drives to protect PII
D. Use a security token to log into all Web applications that use PII

Answer: A

Explanation:
As a matter of good practice any PII should be protected with strong encryption.
References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

NEW QUESTION 576
- (Exam Topic 5)
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark
B. Maltego
C. Metasploit
D. Nessus

Answer: C

NEW QUESTION 580
- (Exam Topic 5)
Scenario:
What is the name of the attack which is mentioned in the scenario?

A. HTTP Parameter Pollution
B. HTML Injection
C. Session Fixation
D. ClickJacking Attack

Answer: D

NEW QUESTION 585
- (Exam Topic 5)
What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

Answer: A

NEW QUESTION 590
- (Exam Topic 5)
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk
B. Inherent risk
C. Deferred risk
D. Impact risk

Answer: A

Explanation:
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.
References: https://en.wikipedia.org/wiki/Residual_risk

NEW QUESTION 592
- (Exam Topic 5)
What is the role of test automation in security testing?

A. It can accelerate benchmark tests and repeat them with a consistent test setu
B. But it cannot replace manual testing completely.
C. It is an option but it tends to be very expensive.
D. It should be used exclusivel
E. Manual testing is outdated because of low speed and possible test setup inconsistencies.
F. Test automation is not usable in security due to the complexity of the tests.

Answer: A

NEW QUESTION 594
- (Exam Topic 5)
Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering
B. Sniffing
C. Eavesdropping
D. Scanning

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.
References: https://en.wikipedia.org/wiki/Social_engineering_(security)

NEW QUESTION 596
- (Exam Topic 5)
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

A. RADIUS
B. DIAMETER
C. Kerberos
D. TACACS+

Answer: A

Explanation:
Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services. These networks may incorporate modems, DSL, access points, VPNs, network ports, web servers, etc.
References: https://en.wikipedia.org/wiki/RADIUS

NEW QUESTION 600
- (Exam Topic 5)
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?

A. Phishing
B. Whaling
C. Tailgating
D. Masquerading

Answer: C

NEW QUESTION 605
- (Exam Topic 5)
During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit

Answer: A

Explanation:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

NEW QUESTION 610
- (Exam Topic 5)
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.
What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A. Protocol analyzer
B. Intrusion Prevention System (IPS)
C. Network sniffer
D. Vulnerability scanner

Answer: A

Explanation:
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.
References: https://en.wikipedia.org/wiki/Packet_analyzer

NEW QUESTION 612
- (Exam Topic 5)
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.
B. He can open it and read the user ids and corresponding passwords.
C. The file reveals the passwords to the root user only.
D. He cannot read it because it is encrypted.

Answer: A

NEW QUESTION 616
- (Exam Topic 5)
What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

Answer: C

NEW QUESTION 618
- (Exam Topic 6)
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.
B. Vulnerabilities in the application layer are independent of the network laye
C. Attacks and mitigation techniques are almost identical.
D. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.
E. Vulnerabilities in the application layer are greatly different from IPv4.

Answer: B

NEW QUESTION 622
- (Exam Topic 6)
Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Answer: B

NEW QUESTION 623
- (Exam Topic 6)
A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation, it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

A. The client cannot see the SSID of the wireless network
B. The WAP does not recognize the client’s MAC address.
C. The wireless client is not configured to use DHCP.
D. Client is configured for the wrong channel

Answer: B

NEW QUESTION 624
- (Exam Topic 6)
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. Windows
B. Unix
C. Linux
D. OS X

Answer: A

NEW QUESTION 627
- (Exam Topic 6)
Which Type of scan sends a packets with no flags set?

A. Open Scan
B. Null Scan
C. Xmas Scan
D. Half-Open Scan

Answer: B

NEW QUESTION 632
- (Exam Topic 6)
Which of the following is NOT an ideal choice for biometric controls?

A. Iris patterns
B. Fingerprints
C. Height and weight
D. Voice

Answer: C

NEW QUESTION 637
- (Exam Topic 6)
Which of the following is a wireless network detector that is commonly found on Linux?

A. Kismet
B. Abel
C. Netstumbler
D. Nessus

Answer: A

NEW QUESTION 638
- (Exam Topic 6)
A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

A. Turtle Trojans
B. Ransomware Trojans
C. Botnet Trojan
D. Banking Trojans

Answer: C

NEW QUESTION 642
- (Exam Topic 6)
As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25

Answer: B

NEW QUESTION 645
- (Exam Topic 6)
What is the term coined for logging, recording and resolving events in a company?

A. Internal Procedure
B. Security Policy
C. Incident Management Process
D. Metrics

Answer: C

NEW QUESTION 648
- (Exam Topic 6)
A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

A. Insufficient security management
B. Insufficient database hardening
C. Insufficient input validation
D. Insufficient exception handling

Answer: B

NEW QUESTION 649
- (Exam Topic 6)
Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log
B. ./snort -dev -l ./log
C. ./snort -dev -o ./log
D. ./snort -dev -p ./log

Answer: B

NEW QUESTION 653

- (Exam Topic 6)
The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5
B. $250
C. $125
D. $65.2

Answer: A

NEW QUESTION 657
- (Exam Topic 6)
TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap
B. ping
C. tracert
D. tcpdump

Answer: D

NEW QUESTION 661
- (Exam Topic 6)
While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.
How can you modify your scan to prevent triggering this event in the IDS?

A. Scan more slowly.
B. Do not scan the broadcast IP.
C. Spoof the source IP address.
D. Only scan the Windows systems.

Answer: B

NEW QUESTION 663
- (Exam Topic 6)
Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254
B. nmap -sP 192.168.1.254
C. nmap -sX 192.168.1.254
D. nmap -sV 192.168.1.254

Answer: C

NEW QUESTION 667
- (Exam Topic 6)
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

A. Social Engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

Answer: A

NEW QUESTION 670
- (Exam Topic 6)
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

A. NET FILE
B. NET USE
C. NET CONFIG
D. NET VIEW

Answer: B

NEW QUESTION 673
- (Exam Topic 6)
You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap

D. Ethereal with Winpcap

Answer: A

NEW QUESTION 675
- (Exam Topic 6)
Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy

Answer: B

NEW QUESTION 678
- (Exam Topic 6)
Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

A. Intrusion Detection System
B. Vulnerability scanner
C. Port scanner
D. Protocol analyzer

Answer: B

NEW QUESTION 682
- (Exam Topic 6)
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

A. Scanning
B. Reconnaissance
C. Escalation
D. Enumeration

Answer: B

NEW QUESTION 686
- (Exam Topic 6)
XOR is a common cryptographic tool. 10110001 XOR 00111010 is?

A. 10111100
B. 11011000
C. 10011101
D. 10001011

Answer: D

NEW QUESTION 688
- (Exam Topic 6)
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

A. Preparation phase
B. Containment phase
C. Recovery phase
D. Identification phase

Answer: A

NEW QUESTION 689
- (Exam Topic 6)
Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

A. Use digital certificates to authenticate a server prior to sending data.
B. Verify access right before allowing access to protected information and UI controls.
C. Verify access right before allowing access to protected information and UI controls.
D. Validate and escape all information sent to a server.

Answer: D

NEW QUESTION 694
- (Exam Topic 6)
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock

Answer: A

NEW QUESTION 699
- (Exam Topic 6)
Name two software tools used for OS guessing? (Choose two.)

A. Nmap
B. Snadboy
C. Queso
D. UserInfo
E. NetBus

Answer: AC

NEW QUESTION 703
- (Exam Topic 6)
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

Answer: C

NEW QUESTION 705
- (Exam Topic 6)
Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

A. In a cool dry environment
B. Inside the data center for faster retrieval in a fireproof safe
C. In a climate controlled facility offsite
D. On a different floor in the same building

Answer: C

NEW QUESTION 707
- (Exam Topic 6)
Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

A. Metasploit
B. Wireshark
C. Maltego
D. Cain & Abel

Answer: C

NEW QUESTION 709
- (Exam Topic 6)
If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ
B. Reviewing the need for a security clearance for each employee
C. Using configuration management to determine when and where to apply security patches
D. Training employees on the security policy regarding social engineering

Answer: A

NEW QUESTION 710
- (Exam Topic 6)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.
77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites
B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system
C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number
D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

Answer: B

NEW QUESTION 714
- (Exam Topic 6)
Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

A. http-git
B. http-headers
C. http enum
D. http-methods

Answer: D

NEW QUESTION 715
- (Exam Topic 6)
What kind of risk will remain even if all theoretically possible safety measures would be applied?

A. Residual risk
B. Inherent risk
C. Impact risk
D. Deferred risk

Answer: A

NEW QUESTION 718
- (Exam Topic 6)
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

A. Stateful
B. Application
C. Circuit
D. Packet Filtering

Answer: B

NEW QUESTION 723
- (Exam Topic 6)
What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

A. $440
B. $100
C. $1320
D. $146

Answer: D

NEW QUESTION 727
- (Exam Topic 6)
What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

Answer: C

NEW QUESTION 728
.....

Relate Links

100% Pass Your 312-50v10 Exam with Exambible Prep Materials

https://www.exambible.com/312-50v10-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/