



EC-Council

Exam Questions 312-50v10

Certified Ethical Hacker v10

NEW QUESTION 1

- (Exam Topic 1)

What does the -oX flag do in an Nmap scan?

- A. Perform an express scan
- B. Output the results in truncated format to the screen
- C. Perform an Xmas scan
- D. Output the results in XML format to a file

Answer: D

NEW QUESTION 2

- (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 3

- (Exam Topic 1)

Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets the password to an encrypted file) from a person by a coercion or torture?

- A. Chosen-Cipher text Attack
- B. Ciphertext-only Attack
- C. Timing Attack
- D. Rubber Hose Attack

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123?

- A. Telnet
- B. POP3
- C. Network Time Protocol
- D. DNS

Answer: C

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 act requires employer's standard national numbers to identify them on standard transactions?

- A. SOX
- B. HIPAA
- C. DMCA
- D. PCI-DSS

Answer: B

NEW QUESTION 7

- (Exam Topic 1)

Darius is analysing IDS logs. During the investigation, he noticed that there was nothing suspicious found and an alert was triggered on normal web application traffic. He can mark this alert as:

- A. False-Negative
- B. False-Positive
- C. True-Positive
- D. False-Signature

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service. What is the name of the process by which you can determine those critical business?

- A. Risk Mitigation
- B. Emergency Plan Response (EPR)
- C. Disaster Recovery Planning (DRP)
- D. Business Impact Analysis (BIA)

Answer: D

NEW QUESTION 9

- (Exam Topic 1)

Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?

- A. Internet Key Exchange (IKE)
- B. Oakley
- C. IPsec Policy Agent
- D. IPsec driver

Answer: A

NEW QUESTION 10

- (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)

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server? The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.

- A. My Doom
- B. Astacheldraht
- C. R-U-Dead-Yet?(RUDY)
- D. LOIC

Answer: C

NEW QUESTION 15

- (Exam Topic 1)

Which is the first step followed by Vulnerability Scanners for scanning a network?

- A. TCP/UDP Port scanning
- B. Firewall detection
- C. OS Detection
- D. Checking if the remote host is alive

Answer: D

NEW QUESTION 18

- (Exam Topic 1)

The collection of potentially actionable, overt, and publicly available information is known as

- A. Open-source intelligence
- B. Human intelligence
- C. Social intelligence
- D. Real intelligence

Answer: A

NEW QUESTION 21

- (Exam Topic 1)

Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?

- A. SHA-2
- B. SHA-3
- C. SHA-1
- D. SHA-0

Answer: C

NEW QUESTION 23

- (Exam Topic 1)

You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

- A. Botnet Attack
- B. Spear Phishing Attack
- C. Advanced Persistent Threats
- D. Rootkit Attack

Answer: A

NEW QUESTION 27

- (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 30

- (Exam Topic 1)

When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?

- A. Data items and vulnerability scanning
- B. Interviewing employees and network engineers
- C. Reviewing the firewalls configuration
- D. Source code review

Answer: A

NEW QUESTION 32

- (Exam Topic 1)

What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

- A. Black-box
- B. Announced
- C. White-box
- D. Grey-box

Answer: D

NEW QUESTION 35

- (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 39

- (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 42

- (Exam Topic 1)

An attacker scans a host with the below command. Which three flags are set? (Choose three.)

#nmap -sX host.domain.com

- A. This is ACK sca
- B. ACK flag is set
- C. This is Xmas sca
- D. SYN and ACK flags are set
- E. This is Xmas sca
- F. URG, PUSH and FIN are set
- G. This is SYN sca
- H. SYN flag is set

Answer: C

NEW QUESTION 44

- (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 46

- (Exam Topic 1)

Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?

- A. [cache:]
- B. [site:]
- C. [inurl:]
- D. [link:]

Answer: B

NEW QUESTION 47

- (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 51

- (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 52

- (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 56

- (Exam Topic 1)

The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

- A. Have the network team document the reason why the rule was implemented without prior manager approval.
- B. Monitor all traffic using the firewall rule until a manager can approve it.
- C. Do not roll back the firewall rule as the business may be relying upon it, but try to get manager approval as soon as possible.
- D. Immediately roll back the firewall rule until a manager can approve it

Answer: D

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 60

- (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 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 64

- (Exam Topic 1)

Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

- A. Produces less false positives
- B. Can identify unknown attacks
- C. Requires vendor updates for a new threat
- D. Cannot deal with encrypted network traffic

Answer: B

NEW QUESTION 66

- (Exam Topic 1)

A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

- A. tcp.port != 21

- B. tcp.port = 23
- C. tcp.port ==21
- D. tcp.port ==21 || tcp.port ==22

Answer: D

NEW QUESTION 70

- (Exam Topic 1)

Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious Java scripts. After opening one of them, he noticed that it is very hard to understand the code and that all codes differ from the typical Java script. What is the name of this technique to hide the code and extend analysis time?

- A. Encryption
- B. Code encoding
- C. Obfuscation
- D. Steganography

Answer: A

NEW QUESTION 74

- (Exam Topic 1)

Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.

Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.

In this context, what can you say?

- A. Bob can be right since DMZ does not make sense when combined with stateless firewalls
- B. Bob is partially right
- C. He does not need to separate networks if he can create rules by destination IPs, one by one
- D. Bob is totally wrong
- E. DMZ is always relevant when the company has internet servers and workstations
- F. Bob is partially right
- G. DMZ does not make sense when a stateless firewall is available

Answer: C

NEW QUESTION 75

- (Exam Topic 1)

What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

- A. Cross-site request forgery
- B. Cross-site scripting
- C. Session hijacking
- D. Server side request forgery

Answer: A

NEW QUESTION 78

- (Exam Topic 2)

Which of the following processes evaluates the adherence of an organization to its stated security policy?

- A. Vulnerability assessment
- B. Penetration testing
- C. Risk assessment
- D. Security auditing

Answer: D

NEW QUESTION 79

- (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 84

- (Exam Topic 2)

Which of the following is a preventive control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail
- D. Continuity of operations plan

Answer: A

NEW QUESTION 87

- (Exam Topic 2)

How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?

- A. Defeating the scanner from detecting any code change at the kernel
- B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
- C. Performing common services for the application process and replacing real applications with fake ones
- D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

Answer: D

NEW QUESTION 90

- (Exam Topic 2)

After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

- A. SHA1
- B. Diffie-Helman
- C. RSA
- D. AES

Answer: A

NEW QUESTION 93

- (Exam Topic 2)

Which of the following examples best represents a logical or technical control?

- A. Security tokens
- B. Heating and air conditioning
- C. Smoke and fire alarms
- D. Corporate security policy

Answer: A

NEW QUESTION 98

- (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 100

- (Exam Topic 2)

A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?

- A. Firewall-management policy
- B. Acceptable-use policy
- C. Remote-access policy
- D. Permissive policy

Answer: C

NEW QUESTION 101

- (Exam Topic 2)

A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

- A. Forensic attack
- B. ARP spoofing attack
- C. Social engineering attack
- D. Scanning attack

Answer: C

NEW QUESTION 102

- (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 104

- (Exam Topic 2)

An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

- A. Classified
- B. Overt
- C. Encrypted
- D. Covert

Answer: D

NEW QUESTION 106

- (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 108

- (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 111

- (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 115

- (Exam Topic 2)

At a Windows Server command prompt, which command could be used to list the running services?

- A. Sc query type= running
- B. Sc query \\servername
- C. Sc query
- D. Sc config

Answer: C

NEW QUESTION 118

- (Exam Topic 2)

What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

- A. Scripting languages are hard to learn.
- B. Scripting languages are not object-oriented.
- C. Scripting languages cannot be used to create graphical user interfaces.
- D. Scripting languages are slower because they require an interpreter to run the code.

Answer: D

NEW QUESTION 123

- (Exam Topic 2)

A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

- A. Fraggle
- B. MAC Flood
- C. Smurf
- D. Tear Drop

Answer: B

NEW QUESTION 128

- (Exam Topic 2)

While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

- A. Packet filtering firewall
- B. Application-level firewall
- C. Circuit-level gateway firewall
- D. Stateful multilayer inspection firewall

Answer: C

NEW QUESTION 133

- (Exam Topic 2)

Smart cards use which protocol to transfer the certificate in a secure manner?

- A. Extensible Authentication Protocol (EAP)
- B. Point to Point Protocol (PPP)
- C. Point to Point Tunneling Protocol (PPTP)
- D. Layer 2 Tunneling Protocol (L2TP)

Answer: A

NEW QUESTION 138

- (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 143

- (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 147

- (Exam Topic 2)

A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

- A. Segregation of duties
- B. Undue influence
- C. Lack of experience
- D. Inadequate disaster recovery plan

Answer: A

NEW QUESTION 151

- (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 154

- (Exam Topic 2)

Which of the following describes the characteristics of a Boot Sector Virus?

- A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
- B. Moves the MBR to another location on the hard disk 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: B

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 157

- (Exam Topic 2)

When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

- A. Drops the packet and moves on to the next one
- B. Continues to evaluate the packet until all rules are checked
- C. Stops checking rules, sends an alert, and lets the packet continue
- D. Blocks the connection with the source IP address in the packet

Answer: B

NEW QUESTION 161

- (Exam Topic 2)

A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

- A. Locate type=ns
- B. Request type=ns
- C. Set type=ns
- D. Transfer type=ns

Answer: C

NEW QUESTION 163

- (Exam Topic 2)

When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

- A. Network tap
- B. Layer 3 switch
- C. Network bridge
- D. Application firewall

Answer: A

NEW QUESTION 166

- (Exam Topic 2)

What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

- A. Injecting parameters into a connection string using semicolons as a separator
- B. Inserting malicious Javascript code into input parameters
- C. Setting a user's session identifier (SID) to an explicit known value
- D. Adding multiple parameters with the same name in HTTP requests

Answer: A

NEW QUESTION 169

- (Exam Topic 2)

What is the main reason the use of a stored biometric is vulnerable to an attack?

- A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
- B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
- C. A stored biometric is no longer "something you are" and instead becomes "something you have".
- D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

Answer: D

NEW QUESTION 174

- (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 178

- (Exam Topic 2)

Which of the following types of firewall inspects only header information in network traffic?

- A. Packet filter
- B. Stateful inspection
- C. Circuit-level gateway
- D. Application-level gateway

Answer: A

NEW QUESTION 181

- (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 184

- (Exam Topic 2)

Which of the following is an example of an asymmetric encryption implementation?

- A. SHA1
- B. PGP
- C. 3DES
- D. MD5

Answer: B

NEW QUESTION 189

- (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 190

- (Exam Topic 2)

A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

- A. Information reporting
- B. Vulnerability assessment
- C. Active information gathering
- D. Passive information gathering

Answer: D

NEW QUESTION 193

- (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 194

- (Exam Topic 2)

Which tool can be used to silently copy files from USB devices?

- A. USB Grabber
- B. USB Dumper
- C. USB Sniffer
- D. USB Snoopy

Answer: B

NEW QUESTION 199

- (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 202

- (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 203

- (Exam Topic 2)

A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

- A. -sO
- B. -sP
- C. -sS
- D. -sU

Answer: B

NEW QUESTION 204

- (Exam Topic 2)

Bluetooth uses which digital modulation technique to exchange information between paired devices?

- A. PSK (phase-shift keying)
- B. FSK (frequency-shift keying)
- C. ASK (amplitude-shift keying)
- D. QAM (quadrature amplitude modulation)

Answer: A

Explanation:

Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK.

References:

<http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php>

NEW QUESTION 208

- (Exam Topic 2)

An NMAP scan of a server shows port 69 is open. What risk could this pose?

- A. Unauthenticated access
- B. Weak SSL version
- C. Cleartext login
- D. Web portal data leak

Answer: A

NEW QUESTION 210

- (Exam Topic 2)

Which of the following business challenges could be solved by using a vulnerability scanner?

- A. Auditors want to discover if all systems are following a standard naming convention.
- B. A web server was compromised and management needs to know if any further systems were compromised.
- C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
- D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

Answer: D

NEW QUESTION 213

- (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 218

- (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 220

- (Exam Topic 2)

An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

- A. g++ hackersExploit.cpp -o calc.exe
- B. g++ hackersExploit.py -o calc.exe
- C. g++ -i hackersExploit.pl -o calc.exe
- D. g++ --compile -i hackersExploit.cpp -o calc.exe

Answer: A

NEW QUESTION 224

- (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 226

- (Exam Topic 2)

Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

- A. Firewall
- B. Honeypot
- C. Core server
- D. Layer 4 switch

Answer: B

NEW QUESTION 230

- (Exam Topic 2)

A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:

NMAP -n -sS -P0 -p 80 ***.***.**.* What type of scan is this?

- A. Quick scan
- B. Intense scan
- C. Stealth scan
- D. Comprehensive scan

Answer: C

NEW QUESTION 234

- (Exam Topic 2)

One way to defeat a multi-level security solution is to leak data via

- A. a bypass regulator.
- B. steganography.
- C. a covert channel.
- D. asymmetric routing.

Answer: C

NEW QUESTION 236

- (Exam Topic 2)

Which of the following items of a computer system will an anti-virus program scan for viruses?

- A. Boot Sector
- B. Deleted Files
- C. Windows Process List
- D. Password Protected Files

Answer: A

NEW QUESTION 240

- (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 244

- (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](https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters)

NEW QUESTION 247

- (Exam Topic 2)

A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

- A. Perform a vulnerability scan of the system.
- B. Determine the impact of enabling the audit feature.
- C. Perform a cost/benefit analysis of the audit feature.
- D. Allocate funds for staffing of audit log review.

Answer: B

NEW QUESTION 248

- (Exam Topic 2)

Which of the following programs is usually targeted at Microsoft Office products?

- A. Polymorphic virus

- B. Multipart virus
- C. Macro virus
- D. Stealth virus

Answer: C

Explanation:

A macro virus is a virus that is written in a macro language: a programming language which is embedded inside a software application (e.g., word processors and spreadsheet applications). Some applications, such as Microsoft Office, allow macro programs to be embedded in documents such that the macros are run automatically when the document is opened, and this provides a distinct mechanism by which malicious computer instructions can spread.

References: https://en.wikipedia.org/wiki/Macro_virus

NEW QUESTION 249

- (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 253

- (Exam Topic 2)

Which of the following parameters enables NMAP's operating system detection feature?

- A. NMAP -sV
- B. NMAP -oS
- C. NMAP -sR
- D. NMAP -O

Answer: D

NEW QUESTION 255

- (Exam Topic 2)

Which of the following is a symmetric cryptographic standard?

- A. DSA
- B. PKI
- C. RSA
- D. 3DES

Answer: D

NEW QUESTION 256

- (Exam Topic 2)

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

- A. Fast processor to help with network traffic analysis
- B. They must be dual-homed
- C. Similar RAM requirements
- D. Fast network interface cards

Answer: B

Explanation:

Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.

References: <https://en.wikipedia.org/wiki/Dual-homed>

NEW QUESTION 258

- (Exam Topic 2)

Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

- A. Netstat WMI Scan
- B. Silent Dependencies
- C. Consider unscanned ports as closed
- D. Reduce parallel connections on congestion

Answer: D

NEW QUESTION 261

- (Exam Topic 2)

A security policy will be more accepted by employees if it is consistent and has the support of

- A. coworkers.
- B. executive management.
- C. the security officer.
- D. a supervisor.

Answer: B

NEW QUESTION 264

- (Exam Topic 2)

What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

- A. They do not use host system resources.
- B. They are placed at the boundary, allowing them to inspect all traffic.
- C. They are easier to install and configure.
- D. They will not interfere with user interfaces.

Answer: A

NEW QUESTION 265

- (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 267

- (Exam Topic 2)

When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

- A. A bottom-up approach
- B. A top-down approach
- C. A senior creation approach
- D. An IT assurance approach

Answer: B

NEW QUESTION 272

- (Exam Topic 2)

What statement is true regarding LM hashes?

- A. LM hashes consist in 48 hexadecimal characters.
- B. LM hashes are based on AES128 cryptographic standard.
- C. Uppercase characters in the password are converted to lowercase.
- D. LM hashes are not generated when the password length exceeds 15 characters.

Answer: D

NEW QUESTION 276

- (Exam Topic 3)

Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

- A. Key registry
- B. Recovery agent
- C. Directory
- D. Key escrow

Answer: D

NEW QUESTION 280

- (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 284

- (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 286

- (Exam Topic 3)

Which element of Public Key Infrastructure (PKI) verifies the applicant?

- A. Certificate authority
- B. Validation authority
- C. Registration authority
- D. Verification authority

Answer: C

NEW QUESTION 288

- (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 290

- (Exam Topic 3)

SOAP services use which technology to format information?

- A. SATA
- B. PCI
- C. XML
- D. ISDN

Answer: C

NEW QUESTION 293

- (Exam Topic 3)

Which security strategy requires using several, varying methods to protect IT systems against attacks?

- A. Defense in depth
- B. Three-way handshake
- C. Covert channels
- D. Exponential backoff algorithm

Answer: A

NEW QUESTION 297

- (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 301

- (Exam Topic 3)

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

- A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
- B. The root CA stores the user's hash value for safekeeping.
- C. The CA is the trusted root that issues certificates.
- D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

Answer: C

NEW QUESTION 304

- (Exam Topic 3)

Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?

- A. Certificate issuance
- B. Certificate validation
- C. Certificate cryptography
- D. Certificate revocation

Answer: B

NEW QUESTION 308

- (Exam Topic 3)

Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

- A. Penetration testing
- B. Social engineering
- C. Vulnerability scanning
- D. Access control list reviews

Answer: A

NEW QUESTION 313

- (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 317

- (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 318

- (Exam Topic 3)

Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

- A. Regulatory compliance
- B. Peer review
- C. Change management
- D. Penetration testing

Answer: C

NEW QUESTION 321

- (Exam Topic 3)

Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

- A. WebBugs
- B. WebGoat
- C. VULN_HTML
- D. WebScarab

Answer: B

NEW QUESTION 325

- (Exam Topic 3)

An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

- A. Unplug the network connection on the company's web server.
- B. Determine the origin of the attack and launch a counterattack.
- C. Record as much information as possible from the attack.

D. Perform a system restart on the company's web server.

Answer: C

NEW QUESTION 328

- (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 330

- (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 334

- (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 336

- (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 340

- (Exam Topic 4)

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

- A. Payment Card Industry (PCI)
- B. Center for Disease Control (CDC)
- C. Institute of Electrical and Electronics Engineers (IEEE)
- D. International Security Industry Organization (ISIO)

Answer: A

Explanation:

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

References: https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

NEW QUESTION 341

- (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 344

- (Exam Topic 4)

It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

Which of the following vulnerabilities is being described?

- A. Shellshock
- B. Rootshock
- C. Rootshell
- D. Shellbash

Answer: A

Explanation:

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.

References: [https://en.wikipedia.org/wiki/Shellshock_\(software_bug\)](https://en.wikipedia.org/wiki/Shellshock_(software_bug))

NEW QUESTION 348

- (Exam Topic 4)

A common cryptographic 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 353

- (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 354

- (Exam Topic 4)

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

- A. Private
- B. Public
- C. Shared
- D. Root

Answer: A

Explanation:

The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.

An attack may also reveal private keys of compromised parties. References: <https://en.wikipedia.org/wiki/Heartbleed>

NEW QUESTION 358

- (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 360

- (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 363

- (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 364

- (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_\(cryptosystem\)](https://en.wikipedia.org/wiki/RSA_(cryptosystem))

NEW QUESTION 365

- (Exam Topic 4)

When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

What nmap script will help you with this task?

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

Answer: A

Explanation:

You can check HTTP method vulnerability using NMAP. Example: `#nmap -script=http-methods.nse 192.168.0.25` References: <http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/>

NEW QUESTION 366

- (Exam Topic 4)

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

- A. Service Oriented Architecture
- B. Object Oriented Architecture
- C. Lean Coding
- D. Agile Process

Answer: A

Explanation:

A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

NEW QUESTION 367

- (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 371

- (Exam Topic 4)

Which regulation defines security and privacy controls for Federal information systems and organizations?

- A. NIST-800-53
- B. PCI-DSS
- C. EU Safe Harbor
- D. HIPAA

Answer: A

Explanation:

NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.

References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

NEW QUESTION 374

- (Exam Topic 4)

After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

- A. Create User Account
- B. Disable Key Services
- C. Disable IPTables
- D. Download and Install Netcat

Answer:

A

NEW QUESTION 376

- (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 378

- (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 380

- (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 384

- (Exam Topic 4)

While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

- A. Web Parameter Tampering
- B. Cookie Tampering
- C. XSS Reflection
- D. SQL injection

Answer: A

Explanation:

The Web Parameter Tampering attack is based on the manipulation of parameters exchanged between client and server in order to modify application data, such as user credentials and permissions, price and quantity of products, etc. Usually, this information is stored in cookies, hidden form fields, or URL Query Strings, and is used to increase application functionality and control.

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

NEW QUESTION 389

- (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 390

- (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 392

- (Exam Topic 4)

You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account. What should you do?

- A. Report immediately to the administrator
- B. Do not report it and continue the penetration test.
- C. Transfer money from the administrator's account to another account.
- D. Do not transfer the money but steal the bitcoins.

Answer: A

NEW QUESTION 396

- (Exam Topic 5)

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

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

Answer: A

Explanation:

MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

References: https://en.wikipedia.org/wiki/MAC_filtering

NEW QUESTION 401

- (Exam Topic 5)

Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

- A. Scalability
- B. Speed
- C. Key distribution
- D. Security

Answer: B

NEW QUESTION 402

- (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 406

- (Exam Topic 5)

The "gray box testing" methodology enforces what kind of restriction?

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

Answer: A

Explanation:

A black-box tester is unaware of the internal structure of the application to be tested, while a white-box tester has access to the internal structure of the application. A gray-box tester partially knows the internal structure, which includes access to the documentation of internal data structures as well as the algorithms used.
References: https://en.wikipedia.org/wiki/Gray_box_testing

NEW QUESTION 409

- (Exam Topic 5)

Which of the following tools can be used for passive OS fingerprinting?

- A. tcpdump
- B. nmap
- C. ping
- D. tracer

Answer: A

Explanation:

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.
References:
<http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html>

NEW QUESTION 414

- (Exam Topic 5)

A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

- A. File system permissions
- B. Privilege escalation
- C. Directory traversal
- D. Brute force login

Answer: A

Explanation:

To upload files the user must have proper write file permissions.
References:
http://codex.wordpress.org/Hardening_WordPress

NEW QUESTION 418

- (Exam Topic 5)

What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

- A. Firewalking
- B. Session hijacking
- C. Network sniffing
- D. Man-in-the-middle attack

Answer: A

NEW QUESTION 421

- (Exam Topic 5)

The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

- A. Hack attack
- B. Sniffing
- C. Dumpster diving
- D. Spying

Answer: C

NEW QUESTION 422

- (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 423

- (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](https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors)

NEW QUESTION 425

- (Exam Topic 5)

PGP, SSL, and IKE are all examples of which type of cryptography?

- A. Public Key
- B. Secret Key
- C. Hash Algorithm
- D. Digest

Answer: A

Explanation:

Public-key algorithms are fundamental security ingredients in cryptosystems, applications and protocols. They underpin various Internet standards, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS), S/MIME, PGP, Internet Key Exchange (IKE or IKEv2), and GPG.

References: https://en.wikipedia.org/wiki/Public-key_cryptography

NEW QUESTION 428

- (Exam Topic 5)

An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

What is the most likely cause?

- A. The network devices are not all synchronized.
- B. Proper chain of custody was not observed while collecting the logs.
- C. The attacker altered or erased events from the logs.
- D. The security breach was a false positive.

Answer: A

Explanation:

Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

References:

http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D561

NEW QUESTION 432

- (Exam Topic 5)

Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol?

- A. Based on XML
- B. Provides a structured model for messaging
- C. Exchanges data between web services
- D. Only compatible with the application protocol HTTP

Answer: D

NEW QUESTION 434

- (Exam Topic 5)

In Risk Management, how is the term "likelihood" related to the concept of "threat?"

- A. Likelihood is the probability that a threat-source will exploit a vulnerability.
- B. Likelihood is a possible threat-source that may exploit a vulnerability.
- C. Likelihood is the likely source of a threat that could exploit a vulnerability.
- D. Likelihood is the probability that a vulnerability is a threat-source.

Answer: A

Explanation:

The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References:

<http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attac>

NEW QUESTION 436

- (Exam Topic 5)

What is the difference between the AES and RSA algorithms?

- A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
- B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
- C. Both are symmetric algorithms, but AES uses 256-bit keys.
- D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

Answer: B

NEW QUESTION 437

- (Exam Topic 5)

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

- A. Civil
- B. International
- C. Criminal
- D. Common

Answer: A

NEW QUESTION 440

- (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 441

- (Exam Topic 5)

Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, small-sized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

- A. Whisker
- B. tcpsplice
- C. Burp
- D. Hydra

Answer: A

Explanation:

One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References: https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

NEW QUESTION 443

- (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 448

- (Exam Topic 5)

A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

- A. Network elements must be hardened with user ids and strong password
- B. Regular security tests and audits should be performed.
- C. As long as the physical access to the network elements is restricted, there is no need for additional measures.
- D. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.
- E. The operator knows that attacks and down time are inevitable and should have a backup site.

Answer: A

NEW QUESTION 453

- (Exam Topic 5)

Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

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

Answer: A

Explanation:

Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: [https://en.wikipedia.org/wiki/Kismet_\(software\)](https://en.wikipedia.org/wiki/Kismet_(software))

NEW QUESTION 455

- (Exam Topic 5)

Which method of password cracking takes the most time and effort?

- A. Brute force
- B. Rainbow tables
- C. Dictionary attack
- D. Shoulder surfing

Answer: A

Explanation:

Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

References: https://en.wikipedia.org/wiki/Password_cracking

NEW QUESTION 458

- (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 463

- (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 464

- (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 469

- (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 matter
- 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 adequate
- G. This way he saves time.

Answer: C

NEW QUESTION 473

- (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 476

- (Exam Topic 5)

What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

- A. User Access Control (UAC)
- B. Data Execution Prevention (DEP)
- C. Address Space Layout Randomization (ASLR)
- D. Windows firewall

Answer: B

NEW QUESTION 481

- (Exam Topic 5)

Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

- A. Fuzzy-testing the code
- B. Third party running the code
- C. Sandboxing the code
- D. String validating the code

Answer: A

NEW QUESTION 484

- (Exam Topic 5)

When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

- A. The amount of time it takes to convert biometric data into a template on a smart card.
- B. The amount of time and resources that are necessary to maintain a biometric system.
- C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
- D. How long it takes to setup individual user accounts.

Answer: C

NEW QUESTION 485

- (Exam Topic 5)

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

- A. Only using OSPFv3 will mitigate this risk.
- B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
- C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
- D. Disable all routing protocols and only use static routes.

Answer: B

NEW QUESTION 490

- (Exam Topic 5)

Which of these options is the most secure procedure for storing backup tapes?

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

Answer: A

Explanation:

An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.

References:

<http://www.entrustm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy>

NEW QUESTION 491

- (Exam Topic 5)

In order to have an anonymous Internet surf, which of the following is best choice?

- A. Use SSL sites when entering personal information
- B. Use Tor network with multi-node
- C. Use shared WiFi
- D. Use public VPN

Answer: B

NEW QUESTION 492

- (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 497

- (Exam Topic 5)

In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

- A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
- B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
- C. A blacklist of companies that have their mail server relays configured to be wide open.
- D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

Answer: B

NEW QUESTION 500

- (Exam Topic 5)

Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

- A. msfpayload
- B. msfcli
- C. msfencode
- D. msfd

Answer: C

NEW QUESTION 501

- (Exam Topic 5)

The "white box testing" methodology enforces what kind of restriction?

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

Answer: A

Explanation:

White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION 506

- (Exam Topic 5)

You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

- A. Scan servers with Nmap
- B. Physically go to each server
- C. Scan servers with MBSA
- D. Telnet to every port on each server

Answer: A

NEW QUESTION 508

- (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 510

- (Exam Topic 5)

A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

- A. Ignore it.
- B. Try to sell the information to a well-paying party on the dark web.
- C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
- D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

Answer: C

NEW QUESTION 511

- (Exam Topic 5)

You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

- A. False Negative
- B. False Positive
- C. True Negative
- D. True Positive

Answer: A

Explanation:

A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References: https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

NEW QUESTION 513

- (Exam Topic 5)

Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Ricardo using?

- A. Steganography
- B. Public-key cryptography
- C. RSA algorithm
- D. Encryption

Answer: A

Explanation:

Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

References: <https://en.wikipedia.org/wiki/Steganography>

NEW QUESTION 515

- (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 516

- (Exam Topic 6)

While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

- A. Clickjacking
- B. Web Form Input Validation
- C. Cross-Site Request Forgery
- D. Cross-Site Scripting

Answer: C

NEW QUESTION 521

- (Exam Topic 6)

When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?

- A. AH Tunnel mode
- B. AH promiscuous
- C. ESP transport mode
- D. ESP confidential

Answer: C

NEW QUESTION 526

- (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 527

- (Exam Topic 6)

It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

- A. Containment
- B. Eradication
- C. Recovery
- D. Discovery

Answer: A

NEW QUESTION 532

- (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 534

- (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 536

- (Exam Topic 6)

.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

- A. Collision Attack
- B. Evil Twin Attack
- C. Sinkhole Attack
- D. Signal Jamming Attack

Answer: B

NEW QUESTION 540

- (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 544

- (Exam Topic 6)

SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

- A. It used TCP as the underlying protocol.
- B. It uses community string that is transmitted in clear text.
- C. It is susceptible to sniffing.
- D. It is used by all network devices on the market.

Answer: BD

NEW QUESTION 547

- (Exam Topic 6)

While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

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

Answer: C

NEW QUESTION 549

- (Exam Topic 6)

Backing up data is a security must. However, it also has certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?

- A. A backup is the source of Malware or illicit information
- B. A backup is incomplete because no verification was performed
- C. A backup is unavailable during disaster recovery
- D. An unencrypted backup can be misplaced or stolen

Answer: D

NEW QUESTION 552

- (Exam Topic 6)

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139.

What protocol is most likely to be listening on those ports?

- A. Finger
- B. FTP
- C. Samba
- D. SMB

Answer: D

NEW QUESTION 554

- (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 556

- (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 559

- (Exam Topic 6)

What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?

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

Answer: B

NEW QUESTION 561

- (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 565

- (Exam Topic 6)

It is a widely used 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. This protocol is specifically designed for transporting event messages. Which of the following is being described?

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

Answer: C

NEW QUESTION 566

- (Exam Topic 6)

Which type of cryptography does SSL, IKE and PGP belongs to?

- A. Secret Key
- B. Hash Algorithm
- C. Digest
- D. Public Key

Answer: D

NEW QUESTION 571

- (Exam Topic 6)

What does a type 3 code 13 represent? (Choose two.)

- A. Echo request
- B. Destination unreachable
- C. Network unreachable
- D. Administratively prohibited
- E. Port unreachable
- F. Time exceeded

Answer: BD

NEW QUESTION 573

- (Exam Topic 6)

What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

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

Answer: C

NEW QUESTION 574

- (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 578

- (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 579

- (Exam Topic 6)

A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

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

Answer: C

NEW QUESTION 580

- (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 582

- (Exam Topic 6)

A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

- A. True Positive
- B. False Negative
- C. False Positive
- D. False Positive

Answer: B

NEW QUESTION 583

- (Exam Topic 6)

The following are types of Bluetooth attack EXCEPT ?

- A. Bluejacking
- B. Bluesmaking
- C. Bluesnarfing
- D. Bluedriving

Answer: D

NEW QUESTION 586

- (Exam Topic 6)

Which specific element of security testing is being assured by using hash?

- A. Authentication
- B. Integrity
- C. Confidentiality
- D. Availability

Answer: B

NEW QUESTION 587

- (Exam Topic 6)

Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

- A. Shellshock
- B. Rootshell
- C. Rootshock
- D. Shellbash

Answer: A

NEW QUESTION 592

- (Exam Topic 6)

Which service in a PKI will vouch for the identity of an individual or company?

- A. KDC
- B. CA
- C. CR
- D. CBC

Answer: B

NEW QUESTION 593

- (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 598

- (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 600

- (Exam Topic 6)

Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network 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 would you implement?

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

Answer: D

NEW QUESTION 605

- (Exam Topic 7)

Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.

What is this document called?

- A. Information Audit Policy (IAP)
- B. Information Security Policy (ISP)
- C. Penetration Testing Policy (PTP)
- D. Company Compliance Policy (CCP)

Answer: B

NEW QUESTION 608

- (Exam Topic 7)

Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

What do you think Tess King is trying to accomplish? Select the best answer.

- A. A zone harvesting
- B. A zone transfer
- C. A zone update
- D. A zone estimate

Answer: B

NEW QUESTION 609

- (Exam Topic 7)

E- mail scams and mail fraud are regulated by which of the following?

- A. 18 U.S.
- B. pa
- C. 1030 Fraud and Related activity in connection with Computers
- D. 18 U.S.
- E. pa
- F. 1029 Fraud and Related activity in connection with Access Devices
- G. 18 U.S.
- H. pa
- I. 1362 Communication Lines, Stations, or Systems
- J. 18 U.S.
- K. pa
- L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 614

- (Exam Topic 7)

Which of the following tools are used for enumeration? (Choose three.)

- A. SolarWinds
- B. USER2SID
- C. Cheops
- D. SID2USER
- E. DumpSec

Answer: BDE

NEW QUESTION 617

- (Exam Topic 7)

How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

- A. There is no way to tell because a hash cannot be reversed
- B. The right most portion of the hash is always the same
- C. The hash always starts with AB923D
- D. The left most portion of the hash is always the same
- E. A portion of the hash will be all 0's

Answer: B

NEW QUESTION 621

- (Exam Topic 7)

One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

- A. 200303028
- B. 3600
- C. 604800
- D. 2400
- E. 60
- F. 4800

Answer: A

NEW QUESTION 623

- (Exam Topic 7)

You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:

- A. user.log
- B. auth.fesg
- C. wtmp
- D. btmp

Answer: C

NEW QUESTION 626

- (Exam Topic 7)

What is the following command used for? net use \targetipc\$ "" /u:""

- A. Grabbing the etc/passwd file
- B. Grabbing the SAM
- C. Connecting to a Linux computer through Samba.
- D. This command is used to connect as a null session
- E. Enumeration of Cisco routers

Answer: D

NEW QUESTION 627

- (Exam Topic 7)

Which utility will tell you in real time which ports are listening or in another state?

- A. Netstat
- B. TCPView
- C. Nmap
- D. Loki

Answer: B

NEW QUESTION 628

- (Exam Topic 7)

Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

- A. Nikto
- B. Nmap
- C. Metasploit
- D. Armitage

Answer: B

NEW QUESTION 633

- (Exam Topic 7)

If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

- A. Birthday
- B. Brute force
- C. Man-in-the-middle
- D. Smurf

Answer: B

NEW QUESTION 635

- (Exam Topic 7)

Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

```
s-1-5-21-1125394485-807628933-54978560-100Johns
s-1-5-21-1125394485-807628933-54978560-652Rebecca
s-1-5-21-1125394485-807628933-54978560-412Sheela
s-1-5-21-1125394485-807628933-54978560-999Shawn
s-1-5-21-1125394485-807628933-54978560-777Somia
s-1-5-21-1125394485-807628933-54978560-500chang
s-1-5-21-1125394485-807628933-54978560-555Micah
```

From the above list identify the user account with System Administrator privileges.

- A. John
- B. Rebecca
- C. Sheela
- D. Shawn
- E. Somia
- F. Chang
- G. Micah

Answer: F

NEW QUESTION 638

- (Exam Topic 7)

You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 641

- (Exam Topic 7)

What is the purpose of DNS AAAA record?

- A. Authorization, Authentication and Auditing record
- B. Address prefix record
- C. Address database record
- D. IPv6 address resolution record

Answer: D

NEW QUESTION 645

- (Exam Topic 7)

A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.

However, he is unable to capture any logons though he knows that other users are logging in. What do you think is the most likely reason behind this?

- A. There is a NIDS present on that segment.
- B. Kerberos is preventing it.
- C. Windows logons cannot be sniffed.
- D. L0phtcrack only sniffs logons to web servers.

Answer: B

NEW QUESTION 647

- (Exam Topic 7)

What hacking attack is challenge/response authentication used to prevent?

- A. Replay attacks
- B. Scanning attacks
- C. Session hijacking attacks
- D. Password cracking attacks

Answer: A

NEW QUESTION 650

- (Exam Topic 7)

Study the following log extract and identify the attack.

```
12/26-07:06:22:31.167035 207.219.207.240:1882 -> 172.16.1.106:80
TCP TTL:13 TTL:50 TOS:0x0 IP:53476 DFF
***AP*** Seq: 0x2BDC107 Ack: 0x1CB9F186 Win: 0x2238 TcpLen: 20
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E C0 AF 2E GET /msadc/.....
2E 2F 2E 2E C0 AF 2E 2E 2F 2E 2E C0 AF 2E 2E 2F ./...../...../
77 69 6E 6E 74 2F 73 79 73 74 65 6D 33 32 2F 63 winnt/system32/c
6D 64 2E 65 78 65 3F 2F 63 2B 64 69 72 2B 63 3A md.exe?/c+dir+c:
5C 20 48 54 54 50 2F 31 2E 31 0D 0A 41 63 63 65 \ HTTP/1.1..Acce
70 74 3A 20 69 6D 61 67 65 2F 67 69 66 2C 20 69 pt: image/gif, i
6D 61 67 65 2F 78 2D 78 62 69 74 6D 61 70 2C 20 mage/x-xbitmap
69 6D 61 67 65 2F 6A 70 65 67 2C 20 69 6D 61 67 image/jpeg, imag
65 2F 70 6A 70 65 67 2C 20 61 70 70 6C 69 63 61 e/jpeg, applica
74 69 6F 6E 2F 76 6E 64 2E 6D 73 2D 65 78 63 65 tion/vnd.ms-exce
6C 2C 20 61 70 70 6C 69 63 61 74 69 6F 6E 2F 6D l, application/m
73 77 6F 72 64 2C 20 61 70 70 6C 69 63 61 74 69 sword, applicati
6F 6E 2F 76 6E 64 2E 6D 73 2D 70 6F 77 65 72 70 on/vnd.ms-powerp
6F 69 6E 74 2C 20 2A 2F 2A 0D 0A 41 63 63 65 70 oint, =/..Accep
74 2D 4C 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/age: en-v
73 0D 0A 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible;pt-EncodD
6E 67 3A 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A l; Windo, deflat
65 0D 0A 55 73 65 72 2D 41 67 65 6E 74 3A 20 4D e..User-Agent: M
6F 7A 69 6C 6C 61 2F 34 2E 30 20 28 63 6F 6D 70 ozilla/4.0 (comp
61 74 69 62 6C 65 3B 20 4D 53 49 45 20 35 2E 30 atible; MSIE 5.0
31 3B 20 57 69 6E 64 6F 77 73 20 39 35 29 0D 0A l; Windows 95)..
48 6F 73 74 3A 20 6C 61 62 2E 77 69 72 65 74 72 Host: lib.bvxttr
69 70 2E 6E 65 74 0D 0A 43 6F 6E 6E 65 63 74 69 ip.org..Connecti
6F 6E 3A 20 4B 65 65 70 2D 41 6C 69 76 65 0D 0A on: Keep-Alive..
43 6F 6F 68 69 65 3A 20 41 53 50 53 45 53 53 49 Cookie: ASPSESSI
4F 4E 49 44 47 51 51 51 51 51 5A 55 3D 4B 4E 4F ONIDGQQQQZU=KNO
48 4D 4F 4A 41 4B 50 46 4F 50 48 4D 4C 41 50 4E HMOJAKPFOPHMLAPN
49 46 49 46 42 0D 0A 0D 0A 41 50 4E 49 46 49 46 IFIFB....APNIFIF
42 0D 0A 0D 0A B....
```

- A. Hexcode Attack
- B. Cross Site Scripting

- C. Multiple Domain Traversal Attack
- D. Unicode Directory Traversal Attack

Answer: D

NEW QUESTION 653

- (Exam Topic 7)

Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message "Hacker Message: You are dead! Freaks!" From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using his dial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

```
H@cker Mess@ge:
Y0u @re De@d! Fre@ks!
```

After seeing the defaced Web site, he disconnected his dial-up line, reconnected to the internal network, and used Secure Shell (SSH) to log in directly to the Web server. He ran Tripwire against the entire Web site, and determined that every system file and all the Web content on the server were intact. How did the attacker accomplish this hack?

- A. ARP spoofing
- B. SQL injection
- C. DNS poisoning
- D. Routing table injection

Answer: C

NEW QUESTION 657

- (Exam Topic 7)

What is the algorithm used by LM for Windows2000 SAM?

- A. MD4
- B. DES
- C. SHA
- D. SSL

Answer: B

NEW QUESTION 658

- (Exam Topic 7)

This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

```
<ahref="http://foobar.com/index.html?id=%3Cscript%20src=%22
http://baddomain.com/badscript.js %22%3E%3C/script%3E">See foobar</a>
```

What is this attack?

- A. Cross-site-scripting attack
- B. SQL Injection
- C. URL Traversal attack
- D. Buffer Overflow attack

Answer: A

NEW QUESTION 661

- (Exam Topic 7)

You have the SOA presented below in your Zone.

Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

- A. One day
- B. One hour
- C. One week
- D. One month

Answer: C

NEW QUESTION 663

- (Exam Topic 7)

Which command can be used to show the current TCP/IP connections?

- A. Netsh

- B. Netstat
- C. Net use connection
- D. Net use

Answer: A

NEW QUESTION 667

- (Exam Topic 7)

The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

You are hired to conduct security testing on their network.

You successfully brute-force the SNMP community string using a SNMP crack tool.

The access-list configured at the router prevents you from establishing a successful connection.

You want to retrieve the Cisco configuration from the router. How would you proceed?

- A. Use the Cisco's TFTP default password to connect and download the configuration file
- B. Run a network sniffer and capture the returned traffic with the configuration file from the router
- C. Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
- D. Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0

Answer: BD

NEW QUESTION 670

- (Exam Topic 7)

Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

- A. har.txt
- B. SAM file
- C. wwwroot
- D. Repair file

Answer: B

NEW QUESTION 672

- (Exam Topic 7)

Which of the following statements is FALSE with respect to Intrusion Detection Systems?

- A. Intrusion Detection Systems can be configured to distinguish specific content in network packets
- B. Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
- C. Intrusion Detection Systems require constant update of the signature library
- D. Intrusion Detection Systems can examine the contents of the data in context of the network protocol

Answer: B

NEW QUESTION 676

- (Exam Topic 7)

While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: `nmap -Pn -p- -si kiosk.adobe.com www.riaa.com`. `kiosk.adobe.com` is the host with incremental IP ID sequence. What is the purpose of using "-si" with Nmap?

- A. Conduct stealth scan
- B. Conduct ICMP scan
- C. Conduct IDLE scan
- D. Conduct silent scan

Answer: A

NEW QUESTION 678

- (Exam Topic 7)

OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

- A. `openssl s_client -site www.website.com:443`
- B. `openssl_client -site www.website.com:443`
- C. `openssl s_client -connect www.website.com:443`
- D. `openssl_client -connect www.website.com:443`

Answer: C

NEW QUESTION 683

- (Exam Topic 7)

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

- A. 110
- B. 135
- C. 139
- D. 161
- E. 445
- F. 1024

Answer: BCE

NEW QUESTION 688

- (Exam Topic 7)

Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

- A. Install DNS logger and track vulnerable packets
- B. Disable DNS timeouts
- C. Install DNS Anti-spoofing
- D. Disable DNS Zone Transfer

Answer: C

NEW QUESTION 692

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

312-50v10 Practice Exam Features:

- * 312-50v10 Questions and Answers Updated Frequently
- * 312-50v10 Practice Questions Verified by Expert Senior Certified Staff
- * 312-50v10 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * 312-50v10 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The 312-50v10 Practice Test Here](#)