

Exam Questions 312-50v10

Certified Ethical Hacker v10

<https://www.2passeasy.com/dumps/312-50v10/>



NEW QUESTION 1

- (Exam Topic 1)

What would you enter, if you wanted to perform a stealth scan using Nmap?

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

Answer: B

NEW QUESTION 2

- (Exam Topic 1)

The Payment Card Industry Data Security Standard (PCI DSS) contains six different categories of control objectives. Each objective contains one or more requirements, which must be followed in order to achieve compliance. Which of the following requirements would best fit under the objective, "Implement strong access control measures"?

- A. Regularly test security systems and processes.
- B. Encrypt transmission of cardholder data across open, public networks.
- C. Assign a unique ID to each person with computer access.
- D. Use and regularly update anti-virus software on all systems commonly affected by malware.

Answer: C

NEW QUESTION 3

- (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 4

- (Exam Topic 1)

Which of the below hashing functions are not recommended for use?

- A. SHA-1.ECC
- B. MD5, SHA-1
- C. SHA-2. SHA-3
- D. MD5. SHA-5

Answer: A

NEW QUESTION 5

- (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 6

- (Exam Topic 1)

Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.

A camera captures people walking and identifies the individuals using Steve's approach.

After that, people must approximate their RFID badges. Both the identifications are required to open the door.

In this case, we can say:

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

Answer: B

NEW QUESTION 7

- (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 8

- (Exam Topic 1)

Which of the following is considered as one of the most reliable forms of TCP scanning?

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

Answer: A

NEW QUESTION 9

- (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 10

- (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 10

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 14

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 16

- (Exam Topic 1)

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

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

Answer: B

NEW QUESTION 17

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 19

- (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 22

- (Exam Topic 1)

What is the main security service a cryptographic hash provides?

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

Answer: D

NEW QUESTION 27

- (Exam Topic 1)

Which protocol is used for setting up secure channels between two devices, typically in VPNs?

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

Answer: B

NEW QUESTION 30

- (Exam Topic 1)

Which of the following provides a security professional with most information about the system's security posture?

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

Answer: D

NEW QUESTION 34

- (Exam Topic 1)

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

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

Answer: A

NEW QUESTION 37

- (Exam Topic 1)

Which of the following is the best countermeasure to encrypting ransomwares?

- A. Use multiple antivirus softwares
- B. Keep some generation of off-line backup
- C. Analyze the ransomware to get decryption key of encrypted data
- D. Pay a ransom

Answer: B

NEW QUESTION 41

- (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 42

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 47

- (Exam Topic 1)

Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.

Suppose a malicious user Rob tries to get access to the account of a benign user Ned.

Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

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

Answer: B

NEW QUESTION 52

- (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 57

- (Exam Topic 1)

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

#nmap -sX host.domain.com

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

Answer: C

NEW QUESTION 60

- (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 62

- (Exam Topic 1)

What is the purpose of a demilitarized zone on a network?

- A. To scan all traffic coming through the DMZ to the internal network
- B. To only provide direct access to the nodes within the DMZ and protect the network behind it
- C. To provide a place to put the honeypot
- D. To contain the network devices you wish to protect

Answer: B

NEW QUESTION 63

- (Exam Topic 1)

How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?

- A. Hash value
- B. Private key
- C. Digital signature
- D. Digital certificate

Answer: D

NEW QUESTION 64

- (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 69

- (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 74

- (Exam Topic 1)

A virus that attempts to install itself inside the file it is infecting is called?

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

Answer: B

NEW QUESTION 76

- (Exam Topic 1)

Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

- A. 123
- B. 161
- C. 69
- D. 113

Answer: A

NEW QUESTION 78

- (Exam Topic 1)

If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

- A. -sP
- B. -P
- C. -r
- D. -F

Answer: B

NEW QUESTION 79

- (Exam Topic 1)

Which of the following statements is TRUE?

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

Answer: A

NEW QUESTION 84

- (Exam Topic 1)

In the field of cryptanalysis, what is meant by a “rubber-hose” attack?

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

Answer: B

NEW QUESTION 86

- (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 91

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 93

- (Exam Topic 1)

Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?

- A. Hire a security consultant to provide direction.
- B. Do not back up either the credit card numbers or then hashes.

- C. Back up the hashes of the credit card numbers not the actual credit card numbers.
- D. Encrypt backup tapes that are sent off-site.

Answer: A

NEW QUESTION 94

- (Exam Topic 1)

When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?

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

Answer: B

NEW QUESTION 96

- (Exam Topic 1)

You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.

Which of the below scanning technique will you use?

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

Answer: C

NEW QUESTION 98

- (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 99

- (Exam Topic 2)

A circuit level gateway works at which of the following layers of the OSI Model?

- A. Layer 5 - Application
- B. Layer 4 – TCP
- C. Layer 3 – Internet protocol
- D. Layer 2 – Data link

Answer: B

NEW QUESTION 101

- (Exam Topic 2)

The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

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

Answer: B

NEW QUESTION 102

- (Exam Topic 2)

Which tool would be used to collect wireless packet data?

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

Answer: A

NEW QUESTION 105

- (Exam Topic 2)

A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.

The engineer receives this output:

```
HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
```

Which of the following is an example of what the engineer performed?

- A. Cross-site scripting
- B. Banner grabbing
- C. SQL injection
- D. Whois database query

Answer: B

NEW QUESTION 107

- (Exam Topic 2)

An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

- A. The wireless card was not turned on.
- B. The wrong network card drivers were in use by Wireshark.
- C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
- D. Certain operating systems and adapters do not collect the management or control packets.

Answer: D

NEW QUESTION 109

- (Exam Topic 2)

Which of the following is a preventive control?

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

Answer: A

NEW QUESTION 111

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 113

- (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 118

- (Exam Topic 2)

Which of the following is an application that requires a host application for replication?

- A. Micro
- B. Worm

C. Trojan
D. Virus

Answer: D

Explanation:

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

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

NEW QUESTION 120

- (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 125

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 127

- (Exam Topic 2)

Which type of access control is used on a router or firewall to limit network activity?

- A. Mandatory
- B. Discretionary
- C. Rule-based
- D. Role-based

Answer: C

NEW QUESTION 131

- (Exam Topic 2)

A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

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

Answer: A

NEW QUESTION 133

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 137

- (Exam Topic 2)

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

- A. IP Security (IPSEC)
- B. Multipurpose Internet Mail Extensions (MIME)
- C. Pretty Good Privacy (PGP)
- D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Answer: C

NEW QUESTION 138

- (Exam Topic 2)

Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

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

Answer: C

NEW QUESTION 142

- (Exam Topic 2)

During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

- A. The tester must capture the WPA2 authentication handshake and then crack it.
- B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
- C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
- D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

Answer: A

NEW QUESTION 144

- (Exam Topic 2)

The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

```
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103
Destination:192.168.1.106 Protocol:TCP
```

What type of activity has been logged?

- A. Port scan targeting 192.168.1.103
- B. Teardrop attack targeting 192.168.1.106
- C. Denial of service attack targeting 192.168.1.103
- D. Port scan targeting 192.168.1.106

Answer: D

NEW QUESTION 149

- (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 153

- (Exam Topic 2)

Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

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

D. Read the last 512 bytes of the tape.

Answer: B

Explanation:

A full restore is required.

NEW QUESTION 156

- (Exam Topic 2)

The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

- A. An attacker, working slowly enough, can evade detection by the IDS.
- B. Network packets are dropped if the volume exceeds the threshold.
- C. Thresholding interferes with the IDS' ability to reassemble fragmented packets.
- D. The IDS will not distinguish among packets originating from different sources.

Answer: A

NEW QUESTION 158

- (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 159

- (Exam Topic 2)

Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

- A. Detective
- B. Passive
- C. Intuitive
- D. Reactive

Answer: B

NEW QUESTION 161

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 163

- (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 166

- (Exam Topic 2)

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

- A. Injecting parameters into a connection string using semicolons as a separator
- B. Inserting malicious Javascript code into input parameters

- C. Setting a user's session identifier (SID) to an explicit known value
- D. Adding multiple parameters with the same name in HTTP requests

Answer: A

NEW QUESTION 169

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 171

- (Exam Topic 2)

Which security control role does encryption meet?

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

Answer: A

NEW QUESTION 175

- (Exam Topic 2)

How is sniffing broadly categorized?

- A. Active and passive
- B. Broadcast and unicast
- C. Unmanaged and managed
- D. Filtered and unfiltered

Answer: A

NEW QUESTION 178

- (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 183

- (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 186

- (Exam Topic 2)

Which of the following is a strong post designed to stop a car?

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

Answer: C

NEW QUESTION 189

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 192

- (Exam Topic 2)

Which of the following does proper basic configuration of snort as a network intrusion detection system require?

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

Answer: A

NEW QUESTION 195

- (Exam Topic 2)

During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

- A. Host
- B. Stateful
- C. Stateless
- D. Application

Answer: C

NEW QUESTION 197

- (Exam Topic 2)

What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

- A. Blue Book
- B. ISO 26029
- C. Common Criteria
- D. The Wassenaar Agreement

Answer: C

NEW QUESTION 198

- (Exam Topic 2)

How can rainbow tables be defeated?

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

Answer: A

NEW QUESTION 202

- (Exam Topic 2)

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

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

Answer: A

Explanation:

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

References:

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

NEW QUESTION 205

- (Exam Topic 2)

Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

- A. ping 192.168.2.
- B. ping 192.168.2.255

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

Answer: D

NEW QUESTION 209

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 214

- (Exam Topic 2)

What is the main difference between a "Normal" SQL Injection and a "Blind" SQL Injection vulnerability?

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

Answer: D

NEW QUESTION 219

- (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 223

- (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 228

- (Exam Topic 2)

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

Which of the following actions should the security administrator take?

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

Answer: D

NEW QUESTION 229

- (Exam Topic 2)

Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

- A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

Answer: D

NEW QUESTION 232

- (Exam Topic 2)

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

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

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

Answer: C

NEW QUESTION 236

- (Exam Topic 2)

Which of the following is considered an acceptable option when managing a risk?

- A. Reject the risk.
- B. Deny the risk.
- C. Mitigate the risk.
- D. Initiate the risk.

Answer: C

NEW QUESTION 237

- (Exam Topic 2)

ICMP ping and ping sweeps are used to check for active systems and to check

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

Answer: A

NEW QUESTION 238

- (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 239

- (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 244

- (Exam Topic 2)

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

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

Answer: C

Explanation:

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

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

NEW QUESTION 246

- (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 249

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 250

- (Exam Topic 2)

A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field:

```
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC"
originalPath="vbscript:msgbox ("Vulnerable");>"
```

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable". Which web applications vulnerability did the analyst discover?

- A. Cross-site request forgery
- B. Command injection
- C. Cross-site scripting
- D. SQL injection

Answer: C

NEW QUESTION 255

- (Exam Topic 2)

Which of the following is a symmetric cryptographic standard?

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

Answer: D

NEW QUESTION 257

- (Exam Topic 2)

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

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

Answer: B

Explanation:

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

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

NEW QUESTION 258

- (Exam Topic 2)

Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Answer: A

NEW QUESTION 262

- (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 263

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 268

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 269

- (Exam Topic 3)

When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

- A. OWASP is for web applications and OSSTMM does not include web applications.
- B. OSSTMM is gray box testing and OWASP is black box testing.
- C. OWASP addresses controls and OSSTMM does not.
- D. OSSTMM addresses controls and OWASP does not.

Answer: D

NEW QUESTION 272

- (Exam Topic 3)

To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

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

Answer: C

NEW QUESTION 277

- (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 281

- (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 283

- (Exam Topic 3)

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

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

Answer: C

NEW QUESTION 288

- (Exam Topic 3)

An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

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

Answer: D

NEW QUESTION 293

- (Exam Topic 3)

Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

- A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
- B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
- C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
- D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

Answer: A

NEW QUESTION 295

- (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 298

- (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 303

- (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 308

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 309

- (Exam Topic 3)

How do employers protect assets with security policies pertaining to employee surveillance activities?

- A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
- B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
- C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
- D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

Answer: D

NEW QUESTION 310

- (Exam Topic 3)

Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

- A. Sarbanes-Oxley Act (SOX)
- B. Gramm-Leach-Bliley Act (GLBA)
- C. Fair and Accurate Credit Transactions Act (FACTA)
- D. Federal Information Security Management Act (FISMA)

Answer: A

NEW QUESTION 312

- (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 313

- (Exam Topic 3)

Which of the following items is unique to the N-tier architecture method of designing software applications?

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

Answer: A

NEW QUESTION 318

- (Exam Topic 3)

International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

- A. guidelines and practices for security controls.
- B. financial soundness and business viability metrics.
- C. standard best practice for configuration management.
- D. contract agreement writing standards.

Answer: A

NEW QUESTION 319

- (Exam Topic 3)

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

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

Answer: B

NEW QUESTION 321

- (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 325

- (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 329

- (Exam Topic 4)

Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?

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

Answer: A

Explanation:

There are two main types of biometric identifiers:

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.

References:

<http://searchsecurity.techtarget.com/definition/biometrics>

NEW QUESTION 332

- (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 333

- (Exam Topic 4)

You have successfully gained access to a Linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).

What is the best way to evade the NIDS?

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

Answer: A

Explanation:

When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.

References:

<http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/>

NEW QUESTION 336

- (Exam Topic 4)

What is a "Collision attack" in cryptography?

- A. Collision attacks try to find two inputs producing the same hash.
- B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
- C. Collision attacks try to get the public key.
- D. Collision attacks try to break the hash into three parts to get the plaintext value.

Answer: A

Explanation:

A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result. References: <https://learncryptography.com/hash-functions/hash-collision-attack>

NEW QUESTION 341

- (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 346

- (Exam Topic 4)

A common cryptographical tool is the use of XOR. XOR the following binary values:

10110001

00111010

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

Answer: A

Explanation:

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

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

NEW QUESTION 350

- (Exam Topic 4)

You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.

What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

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

Answer: A

Explanation:

We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: <https://wiki.wireshark.org/DisplayFilters>

NEW QUESTION 353

- (Exam Topic 4)

```
env x=`(){};};echo exploit` bash -c 'cat /etc/passwd'
```

What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

- A. Display passwd content to prompt

- B. Removes the passwd file
- C. Changes all passwords in passwd
- D. Add new user to the passwd file

Answer: A

Explanation:

To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:

() {::}; /bin/cat /etc/passwd

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

References: <https://blog.cloudflare.com/inside-shellshock/>

NEW QUESTION 357

- (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 358

- (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 363

- (Exam Topic 4)

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

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

Answer: A

Explanation:

chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

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

NEW QUESTION 365

- (Exam Topic 4)

A medium-sized healthcare IT business decides to implement a risk management strategy. Which of the following is NOT one of the five basic responses to risk?

- A. Delegate
- B. Avoid
- C. Mitigate
- D. Accept

Answer: A

Explanation:

There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References:

<http://www.dbpmanagement.com/15/5-ways-to-manage-risk>

NEW QUESTION 366

- (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 370

- (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 371

- (Exam Topic 4)

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

- A. Split DNS
- B. DNSSEC
- C. DynDNS
- D. DNS Scheme

Answer: A

Explanation:

In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

References:

http://www.webopedia.com/TERM/S/split_DNS.html

NEW QUESTION 375

- (Exam Topic 4)

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

- A. `c:\compmgmt.msc`
- B. `c:\services.msc`
- C. `c:\ncpa.cp`
- D. `c:\gpedit`

Answer: A

Explanation:

To start the Computer Management Console from command line just type `compmgmt.msc`

`/computer:computername` in your run box or at the command line and it should automatically open the Computer Management console.

References:

<http://www.waynezim.com/tag/compmgmtmsc/>

NEW QUESTION 379

- (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 382

- (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 385

- (Exam Topic 4)

Which of the following statements is TRUE?

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

Answer: A

Explanation:

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

NEW QUESTION 390

- (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 392

- (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
- 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 396

- (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 397

- (Exam Topic 4)

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

- A. PKI
- B. single sign on
- C. biometrics
- D. SOA

Answer: A

Explanation:

A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

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

NEW QUESTION 402

- (Exam Topic 4)

What is the process of logging, recording, and resolving events that take place in an organization?

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

Answer: A

Explanation:

The activities within the incident management process include:

References: [https://en.wikipedia.org/wiki/Incident_management_\(ITSM\)#Incident_management_procedure](https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure)

NEW QUESTION 403

- (Exam Topic 4)

Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

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

Answer: A

Explanation:

Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.

References: <https://technet.microsoft.com/en-us/library/bb490717.aspx>

NEW QUESTION 406

- (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 409

- (Exam Topic 4)

It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

Which of the following terms best matches the definition?

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

Answer: A

Explanation:

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

References: [https://en.wikipedia.org/wiki/Threat_\(computer\)](https://en.wikipedia.org/wiki/Threat_(computer))

NEW QUESTION 410

- (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 413

- (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 415

- (Exam Topic 4)

It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all

medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

Which of the following regulations best matches the description?

- A. HIPAA
- B. ISO/IEC 27002
- C. COBIT
- D. FISMA

Answer: A

Explanation:

The HIPAA Privacy Rule regulates the use and disclosure of Protected Health Information (PHI) held by "covered entities" (generally, health care clearinghouses, employer sponsored health plans, health insurers, and medical service providers that engage in certain transactions.)[15] By regulation, the Department of Health and Human Services extended the HIPAA privacy rule to independent contractors of covered entities who fit within the definition of "business associates".

References: https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

NEW QUESTION 419

- (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 424

- (Exam Topic 4)

Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?

- A. Use a scan tool like Nessus
- B. Use the built-in Windows Update tool
- C. Check MITRE.org for the latest list of CVE findings
- D. Create a disk image of a clean Windows installation

Answer: A

Explanation:

Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.

Note: Significant capabilities of Nessus include: References: <http://searchnetworking.techtarget.com/definition/Nessus>

NEW QUESTION 429

- (Exam Topic 5)

Look at the following output. What did the hacker accomplish?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168.1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```

- A. The hacker used whois to gather publicly available records for the domain.
- B. The hacker used the "fierce" tool to brute force the list of available domains.
- C. The hacker listed DNS records on his own domain.
- D. The hacker successfully transferred the zone and enumerated the hosts.

Answer: D

NEW QUESTION 433

- (Exam Topic 5)

Risks = Threats x Vulnerabilities is referred to as the:

- A. Risk equation
- B. Threat assessment
- C. BIA equation
- D. Disaster recovery formula

Answer: A

Explanation:

The most effective way to define risk is with this simple equation: Risk = Threat x Vulnerability x Cost

This equation is fundamental to all information security. References: http://www.icharter.org/articles/risk_equation.html

NEW QUESTION 436

- (Exam Topic 5)

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What Web browser-based security vulnerability was exploited to compromise the user?

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

Answer: A

Explanation:

Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where

unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

NEW QUESTION 441

- (Exam Topic 5)

Which of the following is a protocol specifically designed for transporting event messages?

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

Answer: A

Explanation:

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

NEW QUESTION 442

- (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 444

- (Exam Topic 5)

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

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

Answer: A

Explanation:

The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References:

<http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html>

NEW QUESTION 446

- (Exam Topic 5)

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

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

Answer: A

NEW QUESTION 450

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 452

- (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 454

- (Exam Topic 5)

Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

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

Answer: B

NEW QUESTION 457

- (Exam Topic 5)

What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

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

Answer: A

Explanation:

Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell. One specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

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

NEW QUESTION 461

- (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 466

- (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 than 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 468

- (Exam Topic 5)

An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

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

Answer: A

Explanation:

The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

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

NEW QUESTION 469

- (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 472

- (Exam Topic 5)

Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

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

Answer: C

NEW QUESTION 474

- (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 478

- (Exam Topic 5)

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

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

Answer: A

Explanation:

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

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

NEW QUESTION 482

- (Exam Topic 5)

Which of the following security operations is used for determining the attack surface of an organization?

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

Answer: A

Explanation:

For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References:

<http://meisecurity.com/home/consulting/consulting-network-scanning/>

NEW QUESTION 487

- (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 491

- (Exam Topic 5)

If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

- A. Spoof Scan
- B. TCP Connect scan
- C. TCP SYN
- D. Idle Scan

Answer: C

NEW QUESTION 493

- (Exam Topic 5)

Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

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

Answer: D

NEW QUESTION 496

- (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 500

- (Exam Topic 5)

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

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

Answer: B

NEW QUESTION 504

- (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 505

- (Exam Topic 5)

Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

- A. Blind SQLi
- B. DMS-specific SQLi
- C. Classic SQLi
- D. Compound SQLi

Answer: A

NEW QUESTION 506

- (Exam Topic 5)

Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

```
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, "11111111111111111111111111111111");
}
```

Output: Segmentation fault

- A. C#
- B. Python
- C. Java
- D. C++

Answer: D

NEW QUESTION 507

- (Exam Topic 5)

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

- A. A biometric system that bases authentication decisions on behavioral attributes.
- B. A biometric system that bases authentication decisions on physical attributes.
- C. An authentication system that creates one-time passwords that are encrypted with secret keys.
- D. An authentication system that uses passphrases that are converted into virtual passwords.

Answer: C

NEW QUESTION 512

- (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 515

- (Exam Topic 5)

Which of the following types of firewalls ensures that the packets are part of the established session?

- A. Stateful inspection firewall
- B. Circuit-level firewall
- C. Application-level firewall
- D. Switch-level firewall

Answer: A

Explanation:

A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

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

NEW QUESTION 520

- (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 523

- (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 525

- (Exam Topic 5)

During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Answer: A

Explanation:

The auditor should first evaluate existing policies and practices to identify problem areas and opportunities.

NEW QUESTION 526

- (Exam Topic 5)

The security concept of "separation of duties" is most similar to the operation of which type of security device?

- A. Firewall
- B. Bastion host
- C. Intrusion Detection System
- D. Honeypot

Answer: A

Explanation:

In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References:

<http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-d>

NEW QUESTION 528

- (Exam Topic 5)

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

- A. Fuzzing
- B. Randomizing
- C. Mutating
- D. Bounding

Answer: A

Explanation:

Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

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

NEW QUESTION 532

- (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 536

- (Exam Topic 6)

Matthew received an email with an attachment named "YouWon\$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\local directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

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

Answer: B

NEW QUESTION 540

- (Exam Topic 6)

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

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

Answer: B

NEW QUESTION 544

- (Exam Topic 6)

Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

- A. It is a network fault and the originating machine is in a network loop
- B. It is a worm that is malfunctioning or hardcoded to scan on port 500
- C. The attacker is trying to detect machines on the network which have SSL enabled
- D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

Answer: D

NEW QUESTION 545

- (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 547

- (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 552

- (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 554

- (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 558

- (Exam Topic 6)

(Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.). Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

What is odd about this attack? Choose the best answer.

```
05/20-17:06:45.061034 192.160.13.4:31337 -> 172.16.1.101:1 TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
...
05/20-17:06:58.685879 192.160.13.4:31337 ->
172.16.1.101:1024
TCP TTL:44 TOS:0x10 ID:242
***FRP** Seq: OXA1D95 Ack: 0x53 Win: 0x400
```

- A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.
- B. This is back orifice activity as the scan comes from port 31337.
- C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.
- D. These packets were crafted by a tool, they were not created by a standard IP stack.

Answer: B

NEW QUESTION 560

- (Exam Topic 6)

What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

- A. c:\compmgmt.msc
- B. c:\gpedit
- C. c:\ncpa.cpl
- D. c:\services.msc

Answer: A

NEW QUESTION 562

- (Exam Topic 6)

Which of the following commands runs snort in packet logger mode?

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

Answer: B

NEW QUESTION 566

- (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 568

- (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 573

- (Exam Topic 6)

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

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

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

Answer: D

NEW QUESTION 574

- (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 576

- (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 577

- (Exam Topic 6)

In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

- A. Network layer headers and the session layer port numbers
- B. Presentation layer headers and the session layer port numbers
- C. Application layer port numbers and the transport layer headers
- D. Transport layer port numbers and application layer headers

Answer: D

NEW QUESTION 578

- (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 583

- (Exam Topic 6)

A distributed port scan operates by:

- A. Blocking access to the scanning clients by the targeted host
- B. Using denial-of-service software against a range of TCP ports
- C. Blocking access to the targeted host by each of the distributed scanning clients
- D. Having multiple computers each scan a small number of ports, then correlating the results

Answer: D

NEW QUESTION 588

- (Exam Topic 6)

Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

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

Answer: A

NEW QUESTION 590

- (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 591

- (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 593

- (Exam Topic 6)

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

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

Answer: C

NEW QUESTION 597

- (Exam Topic 6)

There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

- A. Collision
- B. Collusion
- C. Polymorphism
- D. Escrow

Answer: A

NEW QUESTION 598

- (Exam Topic 6)

Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

- A. SYN scan
- B. ACK scan
- C. RST scan
- D. Connect scan
- E. FIN scan

Answer: D

NEW QUESTION 603

- (Exam Topic 6)

Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

- A. Nothing, but suggest to him to change the network's SSID and password.
- B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
- C. Log onto to his network, after all it's his fault that you can get in.
- D. Only use his network when you have large downloads so you don't tax your own network.

Answer: A

NEW QUESTION 606

- (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 611

- (Exam Topic 6)

The following are types of Bluetooth attack EXCEPT ?

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

Answer: D

NEW QUESTION 616

- (Exam Topic 6)

First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?

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

Answer: C

NEW QUESTION 620

- (Exam Topic 6)

Sandra is the security administrator of XYZ.com. One day she notices that the XYZ.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crime investigations throughout the United States?

- A. NDCA
- B. NICP
- C. CIRP
- D. NPC
- E. CIA

Answer: D

NEW QUESTION 621

- (Exam Topic 6)

Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?

- A. Use cryptographic storage to store all PII

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

Answer: C

NEW QUESTION 624

- (Exam Topic 6)

Jack was attempting to fingerprint all machines in the network using the following Nmap syntax: `invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24`
TCP/IP fingerprinting (for OS scan) xxxxxxxx xxxxxx xxxxxxxxxx. QUITTING! Obviously, it is not going through. What is the issue here?

- A. OS Scan requires root privileges
- B. The nmap syntax is wrong.
- C. The outgoing TCP/IP fingerprinting is blocked by the host firewall
- D. This is a common behavior for a corrupted nmap application

Answer: A

NEW QUESTION 625

- (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 626

- (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 627

- (Exam Topic 6)

One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

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

Answer: C

NEW QUESTION 629

- (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 631

- (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 636

- (Exam Topic 6)

A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.

77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

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

Answer: B

NEW QUESTION 639

- (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 644

- (Exam Topic 6)

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

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

Answer: D

NEW QUESTION 646

- (Exam Topic 6)

What attack is used to crack passwords by using a precomputed table of hashed passwords?

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

Answer: C

NEW QUESTION 649

- (Exam Topic 7)

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

What is this document called?

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

Answer: B

NEW QUESTION 653

- (Exam Topic 7)

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

- A. 18 U.S.
- B. pa
- C. 1030 Fraud and Related activity in connection with Computers
- D. 18 U.S.
- E. pa
- F. 1029 Fraud and Related activity in connection with Access Devices
- G. 18 U.S.
- H. pa
- I. 1362 Communication Lines, Stations, or Systems
- J. 18 U.S.

K. pa
L. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

Answer: A

NEW QUESTION 657

- (Exam Topic 7)

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

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

Answer: BDE

NEW QUESTION 659

- (Exam Topic 7)

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

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

Answer: B

NEW QUESTION 664

- (Exam Topic 7)

In the context of Windows Security, what is a 'null' user?

- A. A user that has no skills
- B. An account that has been suspended by the admin
- C. A pseudo account that has no username and password
- D. A pseudo account that was created for security administration purpose

Answer: C

NEW QUESTION 665

- (Exam Topic 7)

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

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

Answer: A

NEW QUESTION 667

- (Exam Topic 7)

Take a look at the following attack on a Web Server using obstructed URL:

```
http://www.certifiedhacker.com/script.ext?
template=%2e%2e%2f%2e%2e%2f%2e%2e%2f%65%74%63%2f%70%61%73%73%77%64
This request is made up of:
%2e%2e%2f%2e%2f%2e%2e%2f = ../ ../ ../
%65%74%63 = etc
%2f = /
%70%61%73%73%77%64 = passwd
```

How would you protect from these attacks?

- A. Configure the Web Server to deny requests involving "hex encoded" characters
- B. Create rules in IDS to alert on strange Unicode requests
- C. Use SSL authentication on Web Servers
- D. Enable Active Scripts Detection at the firewall and routers

Answer: B

NEW QUESTION 669

- (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 674

- (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 675

- (Exam Topic 7)

You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?

- A. Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
- B. Package the Sales.xls using Trojan wrappers and telnet them back your home computer
- C. You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
- D. Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account

Answer: C

NEW QUESTION 680

.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 312-50v10 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 312-50v10 Product From:

<https://www.2passeasy.com/dumps/312-50v10/>

Money Back Guarantee

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