Exam Questions 312-50v10

Certified Ethical Hacker v10

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

NEW QUESTION 1
- (Exam Topic 1)
What does the -oX flag do in an Nmap scan?

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

Answer: D

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

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.
Which type of virus detection method did Chandler use in this context?

A. Heuristic Analysis
B. Code Emulation
C. Integrity checking
D. Scanning

Answer: B

NEW QUESTION 4
- (Exam Topic 1)
If an attacker uses the command SELECT*FROM user WHERE name = 'x' AND userid IS NULL; --'; which type of SQL injection attack is the attacker performing?

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

Answer: D

NEW QUESTION 5
- (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 6
- (Exam Topic 1)
Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet?

A. ICMP Echo scanning
B. SYN/FIN scanning using IP fragments
C. ACK flag probe scanning
D. IPID scanning

Answer: B

NEW QUESTION 7
- (Exam Topic 1)
Which of the following attacks exploits web age vulnerabilities that allow an attacker to force an unsuspecting user's browser to send malicious requests they did

not intend?

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

Answer: C

NEW QUESTION 8
- (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 9
- (Exam Topic 1)
You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

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

Answer: A

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

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

Answer: D

NEW QUESTION 10
- (Exam Topic 1)
The collection of potentially actionable, overt, and publicly available information is known as

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

Answer: A

NEW QUESTION 15
- (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 17
- (Exam Topic 1)
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router, nobody can access to the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

```
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
```

A. The ACL 104 needs to be first because is UDP
B. The ACL 110 needs to be changed to port 80
C. The ACL for FTP must be before the ACL 110
D. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

Answer: D

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 23
- (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 26
- (Exam Topic 1)
An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?

A. Reverse Social Engineering
B. Tailgating
C. Piggybacking
D. Announced

Answer: B

NEW QUESTION 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)
What is the minimum number of network connections in a multi homed firewall?

A. 3
B. 5
C. 4
D. 2

Answer: A

NEW QUESTION 42

- (Exam Topic 1)
Sam is working as s 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 43

- (Exam Topic 1)
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?

A. Leave it as it Is and contact the incident response te3m right away
B. Block the connection to the suspicious IP Address from the firewall
C. Disconnect the email server from the network
D. Migrate the connection to the backup email server

Answer: C

NEW QUESTION 44

- (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 49

- (Exam Topic 1)
What is the least important information when you analyze a public IP address in a security alert?

A. ARP
B. Whois
C. DNS
D. Geolocation

Answer: A

NEW QUESTION 52

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

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

Answer: D

NEW QUESTION 55

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

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

Answer: B

NEW QUESTION 58
- (Exam Topic 1)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
What kind of Web application vulnerability likely exists in their software?

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

Answer: C

NEW QUESTION 61
- (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 66
- (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 71
- (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 76
- (Exam Topic 1)
Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to ""know"" to prove yourself that it was Bob who had send a mail?

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

Answer: D

NEW QUESTION 77
- (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 82
- (Exam Topic 1)
What is one of the advantages of using both symmetric and asymmetric cryptography in SSL/TLS?

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

Answer: D

NEW QUESTION 85
- (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 89
- (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 93
- (Exam Topic 1)
The network team has well-established procedures to follow for creating new rules on the firewall. This includes having approval from a manager prior to implementing any new rules. While reviewing the firewall configuration, you notice a recently implemented rule but cannot locate manager approval for it. What would be a good step to have in the procedures for a situation like this?

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

Answer: D

NEW QUESTION 98
- (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 100
- (Exam Topic 1)
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?

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

Answer: C

NEW QUESTION 104
- (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 106
- (Exam Topic 1)

```
ping -* 6 192.168.0.101

output

Pinging 192.168.0.101 with 32 bytes of data:
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Reply from 192.168.0.101: bytes=32 time<1ms TTL=128
Ping statistics for 192.168.0.101:
Packets: Sent=6, Received=6, Lost=0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum=0ms, Maximum=0ms, Average=0ms
```

What does the option * indicate?

A. s
B. t
C. n
D. a

Answer: C

NEW QUESTION 111
- (Exam Topic 1)
These hackers have limited or no training and know how to use only basic techniques or tools. What kind of hackers are we talking about?

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

Answer: C

NEW QUESTION 113
- (Exam Topic 1)
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?

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

Answer: B

NEW QUESTION 114
- (Exam Topic 1)
Cross-site request forgery involves:

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

Answer: C

NEW QUESTION 118

- (Exam Topic 1)
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?

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

Answer: D

NEW QUESTION 121
- (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 122
- (Exam Topic 1)
A hacker named Jack is trying to compromise a bank's computer system. He needs to know the operating
system of that computer to launch further attacks. What process would help him?

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

Answer: A

NEW QUESTION 126
- (Exam Topic 1)
In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?

A. Chosen-plaintext attack
B. Ciphertext-only attack
C. Adaptive chosen-plaintext attack
D. Known-plaintext attack

Answer: A

NEW QUESTION 127
- (Exam Topic 1)
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. –T0
B. –T5
C. -O
D. -A

Answer: B

NEW QUESTION 132
- (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 136
- (Exam Topic 2)
Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment
B. Penetration testing

C. Risk assessment
D. Security auditing

Answer: D

NEW QUESTION 138
- (Exam Topic 2)
On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

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

Answer: C

NEW QUESTION 140
- (Exam Topic 2)
From the two screenshots below, which of the following is occurring?

First one:
```
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399
seconds
```

Second one:
```
1 [10.0.0.252]# nmap -sO 10.0.0.2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds
1 [10.0.0.253]# nmap -sP
1 [10.0.0.253]# nmap -sP
```

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

Answer: A

NEW QUESTION 145
- (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 147
- (Exam Topic 2)
Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

Answer: D

NEW QUESTION 150
- (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 151
- (Exam Topic 2)
What are the three types of authentication?

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

Answer: B

NEW QUESTION 154
- (Exam Topic 2)
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

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

Answer: A

NEW QUESTION 159
- (Exam Topic 2)
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

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

Answer: C

NEW QUESTION 163
- (Exam Topic 2)
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

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

Answer: B

NEW QUESTION 164
- (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 168
- (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 169
- (Exam Topic 2)
WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

Answer: C

NEW QUESTION 174
- (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 179
- (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 184
- (Exam Topic 2)
Which type of scan is used on the eye to measure the layer of blood vessels?

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

Answer: B

NEW QUESTION 187
- (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 188
- (Exam Topic 2)
Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 193
- (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 194
- (Exam Topic 2)
A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

Answer: C

NEW QUESTION 198
- (Exam Topic 2)
At a Windows Server command prompt, which command could be used to list the running services?

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

Answer: C

NEW QUESTION 202
- (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 205
- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 207
- (Exam Topic 2)
A botnet can be managed through which of the following?

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

Answer: A

NEW QUESTION 208
- (Exam Topic 2)
What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

Answer: B

NEW QUESTION 210
- (Exam Topic 2)
Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

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

Answer: B

NEW QUESTION 214
- (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 218
- (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 222
- (Exam Topic 2)
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning
B. Banner grabbing

C. Injecting arbitrary data
D. Analyzing service response

Answer: D

NEW QUESTION 225
- (Exam Topic 2)
Which of the following describes the characteristics of a Boot Sector Virus?

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

Answer: B

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

NEW QUESTION 230
- (Exam Topic 2)
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

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

Answer: C

NEW QUESTION 234
- (Exam Topic 2)
How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80HEAD / HTTP/1.0
B. telnet webserverAddress 80PUT / HTTP/1.0
C. telnet webserverAddress 80HEAD / HTTP/2.0
D. telnet webserverAddress 80PUT / HTTP/2.0

Answer: A

NEW QUESTION 239
- (Exam Topic 2)
When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

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

Answer: A

NEW QUESTION 244
- (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 249
- (Exam Topic 2)
In the software security development life cycle process, threat modeling occurs in which phase?

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

Answer: A

NEW QUESTION 253
- (Exam Topic 2)
A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

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

Answer: A

NEW QUESTION 257
- (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 258
- (Exam Topic 2)
A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

A. Perform a dictionary attack.
B. Perform a brute force attack.
C. Perform an attack with a rainbow table.
D. Perform a hybrid attack.

Answer: C

NEW QUESTION 261
- (Exam Topic 2)
What is the best defense against privilege escalation vulnerability?

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

Answer: C

NEW QUESTION 262
- (Exam Topic 2)
Which security control role does encryption meet?

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

Answer: A

NEW QUESTION 265
- (Exam Topic 2)
Which type of antenna is used in wireless communication?

A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

Answer: A

NEW QUESTION 269
- (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 272
- (Exam Topic 2)
Which tool can be used to silently copy files from USB devices?

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

Answer: B

NEW QUESTION 273
- (Exam Topic 2)
A newly discovered flaw in a software application would be considered which kind of security vulnerability?

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

Answer: C

NEW QUESTION 278
- (Exam Topic 2)
What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

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

Answer: C

NEW QUESTION 280
- (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 285
- (Exam Topic 2)
An NMAP scan of a server shows port 25 is open. What risk could this pose?

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

Answer: D

NEW QUESTION 288
- (Exam Topic 2)
To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

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

Answer: B

NEW QUESTION 291
- (Exam Topic 2)
Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

Answer: D

NEW QUESTION 292
- (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 296
- (Exam Topic 2)
A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

Answer: B

NEW QUESTION 301
- (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 306
- (Exam Topic 2)
How does an operating system protect the passwords used for account logins?

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

Answer: A

NEW QUESTION 310
- (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 313
- (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 318
- (Exam Topic 2)
Which command line switch would be used in NMAP to perform operating system detection?

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

Answer: D

NEW QUESTION 323
- (Exam Topic 2)
Which of the following cryptography attack methods is usually performed without the use of a computer?

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

Answer: C

NEW QUESTION 324
- (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 327
- (Exam Topic 2)
Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

Answer: C

NEW QUESTION 329
- (Exam Topic 2)
Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl
B. C++
C. Python
D. Java

Answer: B

NEW QUESTION 334
- (Exam Topic 2)
Which of the following is a detective control?

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

Answer: C

NEW QUESTION 336
- (Exam Topic 2)
The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?

A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

Answer: B

NEW QUESTION 338
- (Exam Topic 2)
A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

Answer: C

NEW QUESTION 341
- (Exam Topic 2)
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

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

Answer: A

NEW QUESTION 346
- (Exam Topic 2)
Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain
B. John the Ripper
C. Nikto
D. Hping

Answer: A

NEW QUESTION 349
- (Exam Topic 2)
Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

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

Answer: B

NEW QUESTION 354
- (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 356
- (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 357
- (Exam Topic 2)
One way to defeat a multi-level security solution is to leak data via

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

Answer: C

NEW QUESTION 361
- (Exam Topic 2)
Which of the following items of a computer system will an anti-virus program scan for viruses?

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

Answer: A

NEW QUESTION 364
- (Exam Topic 2)
Which statement is TRUE regarding network firewalls preventing Web Application attacks?

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

Answer: B

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

NEW QUESTION 366
- (Exam Topic 2)
What is the broadcast address for the subnet 190.86.168.0/22?

A. 190.86.168.255
B. 190.86.255.255
C. 190.86.171.255
D. 190.86.169.255

Answer: C

NEW QUESTION 370
- (Exam Topic 2)
Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

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

Answer: D

NEW QUESTION 375
- (Exam Topic 2)
What information should an IT system analysis provide to the risk assessor?

A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis

Answer: C

NEW QUESTION 380
- (Exam Topic 2)
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy
C. BBCrack
D. Blooover

Answer: B

Explanation:
Blackberry users warned of hacking tool threat.
Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.
References:
http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

NEW QUESTION 382
- (Exam Topic 2)
Least privilege is a security concept that requires that a user is

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

Answer: A

NEW QUESTION 387
- (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 388
- (Exam Topic 2)
Which of the following is a symmetric cryptographic standard?

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

Answer: D

NEW QUESTION 393
- (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 398
- (Exam Topic 2)
A security administrator notices that the log file of the company's webserver contains suspicious entries:

```
\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978
```

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to

A. command injection.
B. SQL injection.
C. directory traversal.
D. LDAP injection.

Answer: B

NEW QUESTION 403
- (Exam Topic 2)
Which of the following identifies the three modes in which Snort can be configured to run?

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

Answer: A

NEW QUESTION 405
- (Exam Topic 2)
When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

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

Answer: B

NEW QUESTION 410
- (Exam Topic 2)
What statement is true regarding LM hashes?

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

Answer: D

NEW QUESTION 412
- (Exam Topic 3)
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification
B. At least once every three years or after any significant upgrade or modification
C. At least twice a year or after any significant upgrade or modification
D. At least once every two years and after any significant upgrade or modification

Answer: A

NEW QUESTION 413
- (Exam Topic 3)
Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

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

Answer: A

NEW QUESTION 418
- (Exam Topic 3)
If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

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

Answer: D

NEW QUESTION 422
- (Exam Topic 3)
The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

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

Answer: B

NEW QUESTION 423
- (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 428
- (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 430
- (Exam Topic 3)
Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

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

Answer: D

NEW QUESTION 432
- (Exam Topic 3)
For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

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

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

Answer: D

NEW QUESTION 436
- (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 440
- (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 442
- (Exam Topic 3)
A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

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

Answer: B

NEW QUESTION 444
- (Exam Topic 3)
Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

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

Answer: A

NEW QUESTION 446
- (Exam Topic 3)
Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

Answer: C

NEW QUESTION 449
- (Exam Topic 3)
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

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

Answer: A

NEW QUESTION 451

- (Exam Topic 3)
Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

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

Answer: C

NEW QUESTION 453
- (Exam Topic 3)
Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

Answer: A

NEW QUESTION 457
- (Exam Topic 3)
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

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

Answer: A

NEW QUESTION 460
- (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 462
- (Exam Topic 3)
An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

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

Answer: D

NEW QUESTION 467
- (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 472
- (Exam Topic 3)
Which statement best describes a server type under an N-tier architecture?

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

Answer: C

NEW QUESTION 473
- (Exam Topic 3)
What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

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

Answer: D

NEW QUESTION 478
- (Exam Topic 3)
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

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

Answer: A

NEW QUESTION 482
- (Exam Topic 3)
Which type of security document is written with specific step-by-step details?

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

Answer: B

NEW QUESTION 486
- (Exam Topic 3)
Advanced encryption standard is an algorithm used for which of the following?

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

Answer: C

NEW QUESTION 489
- (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 490
- (Exam Topic 3)
Which of the following is an example of IP spoofing?

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

Answer: B

NEW QUESTION 493
- (Exam Topic 3)
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.

C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

Answer: A

NEW QUESTION 494
- (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 497
- (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 501
- (Exam Topic 4)
You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.
What tool will help you with the task?

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

Answer: A

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

NEW QUESTION 502
- (Exam Topic 4)
Perspective clients want to see sample reports from previous penetration tests. What should you do next?

A. Decline but, provide references.
B. Share full reports, not redacted.
C. Share full reports with redactions.
D. Share reports, after NDA is signed.

Answer: A

Explanation:
Penetration tests data should not be disclosed to third parties.

NEW QUESTION 504

- (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 507
- (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 509
- (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 512
- (Exam Topic 4)
The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

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

Answer: A

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

NEW QUESTION 516
- (Exam Topic 4)
How does the Address Resolution Protocol (ARP) work?

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

Answer: A

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

NEW QUESTION 517
- (Exam Topic 4)
What is the benefit of performing an unannounced Penetration Testing?

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

Answer: A

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

NEW QUESTION 520
- (Exam Topic 4)
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

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

Answer: A

Explanation:
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.
An attack may also reveal private keys of compromised parties. References: https://en.wikipedia.org/wiki/Heartbleed

NEW QUESTION 522
- (Exam Topic 4)
You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.
What is happening?

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

Answer: A

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

NEW QUESTION 527
- (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 528
- (Exam Topic 4)
During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.
What type of firewall is inspecting outbound traffic?

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

Answer: A

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

NEW QUESTION 533
- (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 536
- (Exam Topic 4)
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?

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

Answer: A

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

NEW QUESTION 541
- (Exam Topic 4)
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

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

Answer: A

NEW QUESTION 543
- (Exam Topic 4)

This asymmetry cipher is based on factoring the product of two large prime numbers. What cipher is described above?

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

Answer: A

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

NEW QUESTION 545
- (Exam Topic 4)
Which of the following parameters describe LM Hash (see exhibit): Exhibit:

I - The maximum password length is 14 characters.

II - There are no distinctions between uppercase and lowercase.

III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I, II, and III
B. I
C. II
D. I and II

Answer: A

Explanation:
The LM hash is computed as follows:
1. The user's password is restricted to a maximum of fourteen characters.
2. The user's password is converted to uppercase. Etc.
14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds. References: https://en.wikipedia.org/wiki/LM_hash

NEW QUESTION 550
- (Exam Topic 4)
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like.
What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

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

Answer: A

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

NEW QUESTION 551
- (Exam Topic 4)
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?

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

Answer: A

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

NEW QUESTION 555
- (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 557
- (Exam Topic 4)
You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

```
invictus@victim_server:~$ nmap -T4 -O 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx.
QUITTING!
```

What seems to be wrong?

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

Answer: A

Explanation:
You requested a scan type which requires root privileges.
References:
http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

NEW QUESTION 558
- (Exam Topic 4)
Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.
Which of the following activities should not be included in this phase? (see exhibit) Exhibit:

I. Removing all files uploaded on the system

II. Cleaning all registry entries

III. Mapping of network state

IV. Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included.

Answer: A

Explanation:
The post-attack phase revolves around returning any modified system(s) to the pretest state. Examples of such activities:
References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

NEW QUESTION 560
- (Exam Topic 4)
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name.
What should be the first step in security testing the client?

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

Answer: A

Explanation:
 Phases of hacking
Phase 1—Reconnaissance Phase 2—Scanning
Phase 3—Gaining Access Phase 4—Maintaining Access Phase 5—Covering Tracks
Phase 1: Passive and Active Reconnaissance
References:
http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html

NEW QUESTION 564
- (Exam Topic 4)
Which of the following is assured by the use of a hash?

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

Answer: A

Explanation:
An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).
References: https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

NEW QUESTION 565
- (Exam Topic 4)
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

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

Answer: A

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

NEW QUESTION 569
- (Exam Topic 4)
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 unavailable during disaster recovery.
C. A backup is incomplete because no verification was performed.
D. An un-encrypted backup can be misplaced or stolen.

Answer: D

Explanation:
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.
References:
http://resources.infosecinstitute.com/backup-media-encryption/

NEW QUESTION 572
- (Exam Topic 4)
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in.
Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?

A. Piggybacking
B. Masqurading
C. Phishing
D. Whaling

Answer: A

Explanation:
In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.
References: https://en.wikipedia.org/wiki/Piggybacking_(security)

NEW QUESTION 573
- (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 576
- (Exam Topic 4)
Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.
What type of malware has Jesse encountered?

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

Answer: A

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

NEW QUESTION 579
- (Exam Topic 4)
It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?

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

Answer: A

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

NEW QUESTION 583
- (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 588
- (Exam Topic 4)
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.

What testing method did you use?

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

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

NEW QUESTION 589
- (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 591
- (Exam Topic 4)
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?

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

Answer: A

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

NEW QUESTION 596
- (Exam Topic 4)
The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?

A. Wireshark
B. Nessus
C. Netcat
D. Netstat

Answer: A

Explanation:
Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

NEW QUESTION 597
- (Exam Topic 4)
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?

A. promiscuous mode
B. port forwarding
C. multi-cast mode

D. WEM

Answer: A

Explanation:
Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.
References: https://www.tamos.com/htmlhelp/monitoring/

NEW QUESTION 598
- (Exam Topic 4)
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.
What should you do?

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

Answer: A

NEW QUESTION 603
- (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 608
- (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 611
- (Exam Topic 5)
A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.
What is a possible source of this problem?

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

Answer: A

Explanation:
MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.
References: https://en.wikipedia.org/wiki/MAC_filtering

NEW QUESTION 614
- (Exam Topic 5)
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

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

Answer: A

NEW QUESTION 616
- (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 619
- (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 623
- (Exam Topic 5)
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-
16])
Press 'q' or Ctrl-C to abort. almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

A. She is encrypting the file.
B. She is using John the Ripper to view the contents of the file.
C. She is using ftp to transfer the file to another hacker named John.
D. She is using John the Ripper to crack the passwords in the secret.txt file.

Answer: D

NEW QUESTION 628
- (Exam Topic 5)
What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

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

Answer: C

NEW QUESTION 632
- (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 634
- (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 638
- (Exam Topic 5)
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?

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

Answer: A

Explanation:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the

browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

NEW QUESTION 642
- (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 644
- (Exam Topic 5)
An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.
What is the most likely cause?

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

Answer: A

Explanation:
Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.
References:
http://ieeexplore.ieee.org/xpl/login.jsp?tp=
&arnumber=5619315&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D561

NEW QUESTION 646
- (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 648
- (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 653
- (Exam Topic 5)

In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
B. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.
C. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering.
D. Both pharming and phishing attacks are identical.
E. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DN
F. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name.

Answer: A

NEW QUESTION 656
- (Exam Topic 5)
Which protocol is used for setting up secured channels between two devices, typically in VPNs?

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

Answer: A

NEW QUESTION 659
- (Exam Topic 5)
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1 What is the main purpose of those static routes?

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

Answer: D

NEW QUESTION 664
- (Exam Topic 5)
Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.
Which tool can be used to perform session splicing attacks?

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

Answer: A

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

NEW QUESTION 669
- (Exam Topic 5)
A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?

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

Answer: A

NEW QUESTION 673
- (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)

NEW QUESTION 675
- (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 676
- (Exam Topic 5)
By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you know and something you are
B. Something you have and something you know
C. Something you have and something you are
D. Something you are and something you remember

Answer: B

NEW QUESTION 677
- (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 682
- (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 687
- (Exam Topic 5)
Emil uses nmap to scan two hosts using this command. nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT    STATE  SERVICE
21/tcp  open   ftp
23/tcp  open   telnet
53/tcp  open   domain
80/tcp  open   http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)

Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
```

What is his conclusion?

A. Host 192.168.99.7 is an iPad.
B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
C. Host 192.168.99.1 is the host that he launched the scan fro
D. Host 192.168.99.7 is down.

Answer: B

NEW QUESTION 688
- (Exam Topic 5)
The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

A. The document can be sent to the accountant using an exclusive USB for that document.
B. The CFO can use a hash algorithm in the document once he approved the financial statements.
C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.
D. The CFO can use an excel file with a password.

Answer: B

NEW QUESTION 690
- (Exam Topic 5)
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

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

Answer: D

NEW QUESTION 694
- (Exam Topic 5)
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?

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

Answer: C

NEW QUESTION 697
- (Exam Topic 5)
_____ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

A. DNSSEC

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

Answer: A

NEW QUESTION 702
- (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 703
- (Exam Topic 5)
Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

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

Answer: A

NEW QUESTION 708
- (Exam Topic 5)
Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

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

Answer: A

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

NEW QUESTION 711
- (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 712
- (Exam Topic 5)
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:
According to the section from the report, which of the following choice is true?

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

Answer: C

NEW QUESTION 713
- (Exam Topic 5)
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

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

Answer: C

NEW QUESTION 714
- (Exam Topic 5)
In order to have an anonymous Internet surf, which of the following is best choice?

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

Answer: B

NEW QUESTION 718
- (Exam Topic 5)
What is correct about digital signatures?

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

Answer: A

NEW QUESTION 720
- (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 723
- (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 728
......

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