312-50v10 Dumps

Certified Ethical Hacker v10

https://www.certleader.com/312-50v10-dumps.html

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

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

Answer: D

NEW QUESTION 2
- (Exam Topic 1)
What would you enter, if you wanted to perform a stealth scan using Nmap?

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

Answer: B

NEW QUESTION 3
- (Exam Topic 1)
You are a security officer of a company. You had an alert from IDS that indicates that one PC on your Intranet is connected to a blacklisted IP address (C2 Server) on the Internet. The IP address was blacklisted just before the alert. You are staring an investigation to roughly analyze the severity of the situation. Which of the following is appropriate to analyze?

A. Event logs on the PC
B. Internet Firewall/Proxy log
C. IDS log
D. Event logs on domain controller

Answer: B

NEW QUESTION 4
- (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 5
- (Exam Topic 1)
Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets
the password to an encrypted file) from a person by a coercion or torture?

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

Answer: D

NEW QUESTION 6
- (Exam Topic 1)
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?

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

Answer: C

NEW QUESTION 7
- (Exam Topic 1)
Vlady works in a fishing company where the majority of the employees have very little understanding of IT let alone IT Security. Several information security issues

that Vlady often found includes, employees sharing password, writing his/her password on a post it note and stick it to his/her desk, leaving the computer unlocked, didn't log out from emails or other social media accounts, and etc.

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

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

Answer: A

NEW QUESTION 8
- (Exam Topic 1)
Which of the below hashing functions are not recommended for use?

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

Answer: A

NEW QUESTION 9
- (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 10
- (Exam Topic 1)
Which of the following act requires employer's standard national numbers to identify them on standard transactions?

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

Answer: B

NEW QUESTION 10
- (Exam Topic 1)
Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

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

Answer: C

NEW QUESTION 11
- (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 15
- (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 17
- (Exam Topic 1)
Which is the first step followed by Vulnerability Scanners for scanning a network?

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

Answer: D

NEW QUESTION 18
- (Exam Topic 1)
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 21
- (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 23
- (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 25
- (Exam Topic 1)
Which protocol is used for setting up secure channels between two devices, typically in VPNs?

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

Answer: B

NEW QUESTION 26
- (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 28

- (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 30
- (Exam Topic 1)
You are monitoring the network of your organizations. You notice that: Which of the following solution will you suggest?

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

Answer: D

NEW QUESTION 33
- (Exam Topic 1)
Which of the following is the best countermeasure to encrypting ransomwares?

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

Answer: B

NEW QUESTION 34
- (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 35
- (Exam Topic 1)
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

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

Answer: D

NEW QUESTION 40
- (Exam Topic 1)
Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key.
Suppose a malicious user Rob tries to get access to the account of a benign user Ned.
Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability?

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
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 45
- (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 48
- (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 53
- (Exam Topic 1)
Email is transmitted across the Internet using the Simple Mail Transport Protocol. SMTP does not encrypt email, leaving the information in the message vulnerable to being read by an unauthorized person. SMTP can upgrade a connection between two mail servers to use TLS. Email transmitted by SMTP over TLS is encrypted. What is the name of the command used by SMTP to transmit email over TLS?

A. OPPORTUNISTICTLS STARTTLS
B. FORCETLS
C. UPGRADETLS

Answer: B

NEW QUESTION 54
- (Exam Topic 1)
You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?

A. All three servers need to be placed internally
B. A web server facing the Internet, an application server on the internal network, a database server on the internal network
C. A web server and the database server facing the Internet, an application server on the internal network
D. All three servers need to face the Internet so that they can communicate between themselves

Answer: B

NEW QUESTION 59
- (Exam Topic 1)
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?

A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing

Answer: C

NEW QUESTION 61
- (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 62
- (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 66
- (Exam Topic 1)
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?

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

Answer: B

NEW QUESTION 70
- (Exam Topic 1)
A pen tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscuous mode?

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

Answer: D

NEW QUESTION 72
- (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 76
- (Exam Topic 1)
Darius is analysing logs from IDS. He want to understand what have triggered one alert and verify if it's true positive or false positive. Looking at the logs he copy and paste basic details like below:
source IP: 192.168.21.100
source port: 80
destination IP: 192.168.10.23
destination port: 63221
What is the most proper answer.

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

Answer: A

NEW QUESTION 77
- (Exam Topic 1)
A company's policy requires employees to perform file transfers using protocols which encrypt traffic. You suspect some employees are still performing file transfers using unencrypted protocols because the employees do not like changes. You have positioned a network sniffer to capture traffic from the laptops used by employees in the data ingest department. Using Wire shark to examine the captured traffic, which command can be used as a display filter to find unencrypted file transfers?

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

Answer: D

NEW QUESTION 78

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

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

Answer: B

NEW QUESTION 82
- (Exam Topic 1)
During the process of encryption and decryption, what keys are shared? During the process of encryption and decryption, what keys are shared?

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

Answer: C

NEW QUESTION 86
- (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 90
- (Exam Topic 1)
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

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

Answer: A

NEW QUESTION 95
- (Exam Topic 2)
The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

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

Answer: A

NEW QUESTION 97
- (Exam Topic 2)
The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

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

Answer: B

NEW QUESTION 102
- (Exam Topic 2)
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 106
- (Exam Topic 2)
Which of the following is a preventive control?

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

Answer: A

NEW QUESTION 111
- (Exam Topic 2)
Which of the following open source tools would be the best choice to scan a network for potential targets?

A. NMAP
B. NIKTO
C. CAIN
D. John the Ripper

Answer: A

NEW QUESTION 112
- (Exam Topic 2)
Which of the following examples best represents a logical or technical control?

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

Answer: A

NEW QUESTION 117
- (Exam Topic 2)
Which property ensures that a hash function will not produce the same hashed value for two different messages?

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

Answer: A

NEW QUESTION 121
- (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 125
- (Exam Topic 2)
Which of the following is an application that requires a host application for replication?

A. Micro
B. Worm
C. Trojan
D. Virus

Answer: D

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

NEW QUESTION 130
- (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 135
- (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 139
- (Exam Topic 2)
What is a successful method for protecting a router from potential smurf attacks?

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

Answer: D

NEW QUESTION 141
- (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 144
- (Exam Topic 2)
A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?

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

Answer: D

NEW QUESTION 149
- (Exam Topic 2)
Which of the following is a hashing algorithm?

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

Answer: A

NEW QUESTION 153
- (Exam Topic 2)
Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

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

Answer: C

NEW QUESTION 156

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

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

Answer: C

NEW QUESTION 161
- (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 164
- (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 165
- (Exam Topic 2)
A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

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

Answer: B

NEW QUESTION 166
- (Exam Topic 2)
Smart cards use which protocol to transfer the certificate in a secure manner?

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

Answer: A

NEW QUESTION 170
- (Exam Topic 2)
A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

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

Answer: B

NEW QUESTION 172
- (Exam Topic 2)
The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

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

Answer: A

NEW QUESTION 177
- (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 181
- (Exam Topic 2)
Which set of access control solutions implements two-factor authentication?

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

Answer: A

NEW QUESTION 186
- (Exam Topic 2)
When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

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

Answer: B

NEW QUESTION 191
- (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 195
- (Exam Topic 2)
Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. --
B. ||
C. %%
D. "

Answer: A

NEW QUESTION 197
- (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 199
- (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 204
- (Exam Topic 2)
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

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

Answer: C

NEW QUESTION 207
- (Exam Topic 2)
Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

Answer: B

NEW QUESTION 211
- (Exam Topic 2)
A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0.
How can NMAP be used to scan these adjacent Class C networks?

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

Answer: A

NEW QUESTION 212
- (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 216
- (Exam Topic 2)
A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

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

Answer: D

NEW QUESTION 220
- (Exam Topic 2)
Which security control role does encryption meet?

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

Answer: A

NEW QUESTION 223

- (Exam Topic 2)
In order to show improvement of security over time, what must be developed?

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

Answer: C

Explanation:
Today, management demands metrics to get a clearer view of security.
Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.
References:
http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html

NEW QUESTION 227
- (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 231
- (Exam Topic 2)
Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key
B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

Answer: C

NEW QUESTION 235
- (Exam Topic 2)
What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

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

Answer: D

NEW QUESTION 238
- (Exam Topic 2)
What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

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

Answer: C

NEW QUESTION 242
- (Exam Topic 2)
How can rainbow tables be defeated?

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

Answer: A

NEW QUESTION 246
- (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 249
- (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 252
- (Exam Topic 2)
Passive reconnaissance involves collecting information through which of the following?

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

Answer: D

NEW QUESTION 257
- (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 258
- (Exam Topic 2)
When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive
B. False negative
C. True positve
D. True negative

Answer: A

NEW QUESTION 259
- (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 261
- (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 266
- (Exam Topic 2)
What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

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

Answer: D

NEW QUESTION 268
- (Exam Topic 2)
A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

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

Answer: D

NEW QUESTION 269
- (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 270
- (Exam Topic 2)
Which of the following programs is usually targeted at Microsoft Office products?

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

Answer: C

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

NEW QUESTION 273
- (Exam Topic 2)
Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns
B. kismet
C. nikto
D. hping

Answer: A

NEW QUESTION 275
- (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 280
- (Exam Topic 2)
Which of the statements concerning proxy firewalls is correct?

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

Answer: D

NEW QUESTION 281
- (Exam Topic 2)
Which of the following parameters enables NMAP's operating system detection feature?

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

Answer: D

NEW QUESTION 284
- (Exam Topic 2)
Which system consists of a publicly available set of databases that contain domain name registration contact information?

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

Answer: A

NEW QUESTION 285
- (Exam Topic 2)
Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

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

Answer: D

NEW QUESTION 288
- (Exam Topic 2)
A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.
Which cryptography attack is the student attempting?

A. Man-in-the-middle attack
B. Brute-force attack
C. Dictionary attack
D. Session hijacking

Answer: C

NEW QUESTION 292
- (Exam Topic 2)
While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

Answer: C

NEW QUESTION 297
- (Exam Topic 2)
A security policy will be more accepted by employees if it is consistent and has the support of

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

Answer: B

NEW QUESTION 299
- (Exam Topic 2)
A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

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

Answer: D

NEW QUESTION 302
- (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 306
- (Exam Topic 3)
A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

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

Answer: A

NEW QUESTION 311
- (Exam Topic 3)
An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

A. Start by foot printing the network and mapping out a plan of attack.
B. Ask the employer for authorization to perform the work outside the company.
C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

Answer: B

NEW QUESTION 313
- (Exam Topic 3)
Which of the following guidelines or standards is associated with the credit card industry?

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

Answer: D

NEW QUESTION 315
- (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 318
- (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 323
- (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 328
- (Exam Topic 3)
Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

Answer: D

NEW QUESTION 329
- (Exam Topic 3)
Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

Answer: A

NEW QUESTION 333
- (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 335
- (Exam Topic 3)
SOAP services use which technology to format information?

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

Answer: C

NEW QUESTION 340
- (Exam Topic 3)
Which security strategy requires using several, varying methods to protect IT systems against attacks?

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

Answer: A

NEW QUESTION 342
- (Exam Topic 3)
Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

Answer: B

NEW QUESTION 343
- (Exam Topic 3)
If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

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

Answer: A

NEW QUESTION 344
- (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 346
- (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 351
- (Exam Topic 3)
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

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

Answer: A

NEW QUESTION 354
- (Exam Topic 3)
An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

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

Answer: D

NEW QUESTION 357
- (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 359
- (Exam Topic 3)
Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

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

Answer: B

NEW QUESTION 360
- (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 362
- (Exam Topic 3)
An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?

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

Answer: C

NEW QUESTION 365
- (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 369
- (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 371
- (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 375
- (Exam Topic 3)
A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

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

Answer: B

NEW QUESTION 376
- (Exam Topic 3)
Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

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

Answer: C

NEW QUESTION 379
- (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 380
- (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 382
- (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 385
- (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 390
- (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 395
- (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 400
- (Exam Topic 4)
A common cryptographical tool is the use of XOR. XOR the following binary values:
10110001
00111010

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

Answer: A

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

NEW QUESTION 401
- (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 lackers 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 403
- (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 407
- (Exam Topic 4)
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.
Which sort of trojan infects this server?

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

Answer: A

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

NEW QUESTION 411
- (Exam Topic 4)
You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.
Which command-line utility are you most likely to use?

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

Answer: A

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

NEW QUESTION 415
- (Exam Topic 4)
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.
What should you do?

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

Answer: A

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

NEW QUESTION 418
- (Exam Topic 4)
Which of the following is not a Bluetooth attack?

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

Answer: A

NEW QUESTION 422
- (Exam Topic 4)
What is the best description of SQL Injection?

A. It is an attack used to gain unauthorized access to a database.
B. It is an attack used to modify code in an application.
C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
D. It is a Denial of Service Attack.

Answer: A

Explanation:
SQL injection is a code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
References: https://en.wikipedia.org/wiki/SQL_injection

NEW QUESTION 426
- (Exam Topic 4)
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

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

Answer: A

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

NEW QUESTION 428
- (Exam Topic 4)
During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.
What is this type of DNS configuration commonly called?

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

Answer: A

Explanation:
In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.
References:
http://www.webopedia.com/TERM/S/split_DNS.html

NEW QUESTION 432
- (Exam Topic 4)
Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

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

Answer: A

Explanation:
A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.
References: https://en.wikipedia.org/wiki/Service-oriented_architecture

NEW QUESTION 435
- (Exam Topic 4)
In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.
Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)
B. Wi-Fi Protected Access (WPA)
C. Wi-Fi Protected Access 2 (WPA2)
D. Temporal Key Integrity Protocol (TKIP)

Answer: A

Explanation:
WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.
Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).
References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

NEW QUESTION 440
- (Exam Topic 4)
After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

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

Answer: A

NEW QUESTION 442
- (Exam Topic 4)
Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.
What is this style of attack called?

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

Answer: A

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

NEW QUESTION 444
- (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 449
- (Exam Topic 4)
This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.
Which of the following tools is being described?

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

Answer: A

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

NEW QUESTION 452
- (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 455
- (Exam Topic 4)
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

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

Answer: A

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

NEW QUESTION 456
- (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 457
- (Exam Topic 4)
A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?

A. Place a front-end web server in a demilitarized zone that only handles external web traffic
B. Require all employees to change their passwords immediately
C. Move the financial data to another server on the same IP subnet
D. Issue new certificates to the web servers from the root certificate authority

Answer: A

Explanation:
A DMZ or demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to a larger and untrusted network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external network node only has direct access to equipment in the DMZ, rather than any other part of the network.
References: https://en.wikipedia.org/wiki/DMZ_(computing)

NEW QUESTION 461
- (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 465
- (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 467
- (Exam Topic 4)
It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.
Which of the following terms best matches the definition?

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

Answer: A

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

NEW QUESTION 470
- (Exam Topic 4)
While using your bank's online servicing you notice the following string in the URL bar: "http://www.MyPersonalBank.com/account?id=368940911028389 &Damount=10980&Camount=21"
You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.
Which type of vulnerability is present on this site?

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

Answer: A

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

NEW QUESTION 472
- (Exam Topic 4)
It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.
Which of the following regulations best matches the description?

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

Answer: A

Explanation:

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

NEW QUESTION 476
- (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 481
- (Exam Topic 4)
Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.
What should you do?

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

Answer: A

NEW QUESTION 483
- (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 488
- (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 489
- (Exam Topic 5)
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

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

Answer: B

NEW QUESTION 493
- (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 496
- (Exam Topic 5)
Which of the following tools can be used for passive OS fingerprinting?

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

Answer: A

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

NEW QUESTION 498
- (Exam Topic 5)
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.
What kind of vulnerability must be present to make this remote attack possible?

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

Answer: A

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

NEW QUESTION 503
- (Exam Topic 5)
What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall?

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

Answer: A

NEW QUESTION 508
- (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 511
- (Exam Topic 5)
PGP, SSL, and IKE are all examples of which type of cryptography?

A. Public Key
B. Secret Key
C. Hash Algorithm

D. Digest

Answer: A

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

NEW QUESTION 516
- (Exam Topic 5)
Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol?

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

Answer: D

NEW QUESTION 519
- (Exam Topic 5)
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.
Which of the following is true hash type and sort order that is using in the psexec module's 'smbpass'?

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

Answer: B

NEW QUESTION 520
- (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 525
- (Exam Topic 5)
What two conditions must a digital signature meet?

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

Answer: A

NEW QUESTION 527
- (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 531
- (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 535
- (Exam Topic 5)
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

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

Answer: C

NEW QUESTION 536
- (Exam Topic 5)
You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

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

Answer: A

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

NEW QUESTION 541
- (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 546
- (Exam Topic 5)
Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace
B. tcptraceroute
C. Nessus
D. OpenVAS

Answer: A

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

NEW QUESTION 550
- (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 552
- (Exam Topic 5)
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

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

Answer: D

NEW QUESTION 557
- (Exam Topic 5)
Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

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

Answer: A

Explanation:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one's ability to handle an incident. For the sake of brevity, the following should be performed:
References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

NEW QUESTION 561
- (Exam Topic 5)
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28.
Why he cannot see the servers?

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

Answer: C

NEW QUESTION 565
- (Exam Topic 5)
Which of the following statements regarding ethical hacking is incorrect?

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

Answer: A

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

NEW QUESTION 568
- (Exam Topic 5)
What does a firewall check to prevent particular ports and applications from getting packets into an organization?

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

Answer: A

Explanation:

Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.
Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.
References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters
http://howdoesinternetwork.com/2012/application-layer-firewalls

NEW QUESTION 570
- (Exam Topic 5)
Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

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

Answer: B

NEW QUESTION 575
- (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 576
- (Exam Topic 5)
What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

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

Answer: B

NEW QUESTION 581
- (Exam Topic 5)
Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

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

Answer: A

NEW QUESTION 582
- (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 585
- (Exam Topic 5)
When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

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

Answer: C

NEW QUESTION 587
- (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 589
- (Exam Topic 5)
Scenario:
What is the name of the attack which is mentioned in the scenario?

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

Answer: D

NEW QUESTION 592
- (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 596
- (Exam Topic 5)
Which of the following is a low-tech way of gaining unauthorized access to systems?

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

Answer: A

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

NEW QUESTION 599
- (Exam Topic 5)
In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?

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

Answer: B

NEW QUESTION 603
- (Exam Topic 5)
The "white box testing" methodology enforces what kind of restriction?

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

Answer: A

Explanation:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests

internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.
References: https://en.wikipedia.org/wiki/White-box_testing

NEW QUESTION 605
- (Exam Topic 5)
An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.
Which AAA protocol is most likely able to handle this requirement?

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

Answer: A

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

NEW QUESTION 606
- (Exam Topic 5)
A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

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

Answer: C

NEW QUESTION 607
- (Exam Topic 5)
Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.
What just happened?

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

Answer: C

NEW QUESTION 609
- (Exam Topic 5)
A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

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

Answer: A

NEW QUESTION 614
- (Exam Topic 6)
Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network
B. To disrupt the NetBIOS SMB service on the target host
C. To check for file and print sharing on Windows systems
D. To discover information about a target host using NBTSTAT

Answer: D

NEW QUESTION 619
- (Exam Topic 6)
In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

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

E. Vulnerabilities in the application layer are greatly different from IPv4.

Answer: B

NEW QUESTION 623
- (Exam Topic 6)
Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

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

Answer: A

NEW QUESTION 625
- (Exam Topic 6)
Which of the following is a wireless network detector that is commonly found on Linux?

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

Answer: A

NEW QUESTION 627
- (Exam Topic 6)
You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

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

Answer: B

NEW QUESTION 630
- (Exam Topic 6)
........is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.
Fill in the blank with appropriate choice.

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

Answer: B

NEW QUESTION 634
- (Exam Topic 6)
What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

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

Answer: A

NEW QUESTION 638
- (Exam Topic 6)
SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible? (Choose two.)

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

Answer: BD

NEW QUESTION 643

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

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

Answer: D

NEW QUESTION 648
- (Exam Topic 6)
An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

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

Answer: B

NEW QUESTION 653
- (Exam Topic 6)
The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

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

Answer: C

NEW QUESTION 656
- (Exam Topic 6)
Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

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

Answer: A

NEW QUESTION 661
- (Exam Topic 6)
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

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

Answer: C

NEW QUESTION 664
- (Exam Topic 6)
Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

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

Answer: B

NEW QUESTION 667
- (Exam Topic 6)
You want to analyze packets on your wireless network. Which program would you use?

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

Answer: A

NEW QUESTION 671
- (Exam Topic 6)
Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in the range of 135 to 139.
What protocol is most likely to be listening on those ports?

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

Answer: D

NEW QUESTION 676
- (Exam Topic 6)
Which of the following is a restriction being enforced in "white box testing?"

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

Answer: B

NEW QUESTION 680
- (Exam Topic 6)
A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

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

Answer: B

NEW QUESTION 681
- (Exam Topic 6)
You are about to be hired by a well-known Bank to perform penetration tests. Which of the following documents describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?

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

Answer: C

NEW QUESTION 683
- (Exam Topic 6)
What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server you've compromised and gained root access to?

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

Answer: B

NEW QUESTION 685
- (Exam Topic 6)
Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>
B. Nmap -hU -Q<host(s.>
C. Nmap -sT -p <host(s.>
D. Nmap -u -o -w2 <host>
E. Nmap -sS -0p targe

Answer: B

NEW QUESTION 689
- (Exam Topic 6)

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

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

Answer: A

NEW QUESTION 693
- (Exam Topic 6)
It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?

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

Answer: C

NEW QUESTION 697
- (Exam Topic 6)
Which type of cryptography does SSL, IKE and PGP belongs to?

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

Answer: D

NEW QUESTION 698
- (Exam Topic 6)
What does a type 3 code 13 represent? (Choose two.)

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

Answer: BD

NEW QUESTION 700
- (Exam Topic 6)
Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

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

Answer: A

NEW QUESTION 701
- (Exam Topic 6)
What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

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

Answer: C

NEW QUESTION 702
- (Exam Topic 6)
Name two software tools used for OS guessing? (Choose two.)

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

E. NetBus

Answer: AC

NEW QUESTION 706
- (Exam Topic 6)
Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

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

Answer: C

NEW QUESTION 710
- (Exam Topic 6)
A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious. What tool are you going to use?

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

Answer: C

NEW QUESTION 711
- (Exam Topic 6)
Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"". Which statement below is true?

A. This is probably a legitimate message as it comes from a respectable organization.
B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
D. This is a scam because Bob does not know Scott.

Answer: C

NEW QUESTION 713
- (Exam Topic 6)
Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

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

Answer: D

NEW QUESTION 714
- (Exam Topic 6)
Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

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

Answer: A

NEW QUESTION 718
- (Exam Topic 6)
The following are types of Bluetooth attack EXCEPT ?

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

Answer: D

NEW QUESTION 722

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

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

Answer: A

NEW QUESTION 724
- (Exam Topic 6)
A specific site received 91 ICMP_ECHO packets within 90 minutes from 47 different sites.
77 of the ICMP_ECHO packets had an ICMP ID:39612 and Seq:57072. 13 of the ICMP_ECHO packets had an ICMP ID:0 and Seq:0. What can you infer from this information?

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

Answer: B

NEW QUESTION 729
- (Exam Topic 6)
Which of the following command line switch would you use for OS detection in Nmap?

A. -D
B. -O
C. -P
D. –X

Answer: B

NEW QUESTION 734
- (Exam Topic 6)
While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

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

Answer: B

NEW QUESTION 739
- (Exam Topic 7)
Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.
What do you think Tess King is trying to accomplish? Select the best answer.

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

Answer: B

NEW QUESTION 743
- (Exam Topic 7)
What is the proper response for a NULL scan if the port is open?

A. SYN
B. ACK
C. FIN
D. PSH
E. RST
F. No response

Answer: F

NEW QUESTION 745
- (Exam Topic 7)
E- mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.

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

Answer: A

NEW QUESTION 746
- (Exam Topic 7)
Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.
Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.
B. Hardware and Software Keyloggers.
C. Passwords are always best obtained using Hardware key loggers.
D. Software only, they are the most effective.

Answer: A

NEW QUESTION 750
- (Exam Topic 7)
Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS
B. A zone transfer is accomplished with the nslookup service
C. A zone transfer passes all zone information that a DNS server maintains
D. A zone transfer passes all zone information that a nslookup server maintains
E. A zone transfer can be prevented by blocking all inbound TCP port 53 connections
F. Zone transfers cannot occur on the Internet

Answer: ACE

NEW QUESTION 754
- (Exam Topic 7)
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

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

Answer: B

NEW QUESTION 756
- (Exam Topic 7)
An LDAP directory can be used to store information similar to a SQL database. LDAP uses a database structure instead of SQL's structure. Because of this, LDAP has difficulty representing many-to-one relationships.

A. Relational, Hierarchical
B. Strict, Abstract
C. Hierarchical, Relational
D. Simple, Complex

Answer: C

NEW QUESTION 761
- (Exam Topic 7)
One of your team members has asked you to analyze the following SOA record. What is the version? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.) (Choose four.)

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

Answer: A

NEW QUESTION 766
- (Exam Topic 7)
What is GINA?

A. Gateway Interface Network Application
B. GUI Installed Network Application CLASS
C. Global Internet National Authority (G-USA)
D. Graphical Identification and Authentication DLL

Answer: D

NEW QUESTION 767
- (Exam Topic 7)
Tremp is an IT Security Manager, and he is planning to deploy an IDS in his small company. He is looking for an IDS with the following characteristics: - Verifies success or failure of an attack - Monitors system activities Detects attacks that a network-based IDS fails to detect - Near real-time detection and response - Does not require additional hardware - Lower entry cost Which type of IDS is best suited for Tremp's requirements?

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

Answer: C

NEW QUESTION 770
- (Exam Topic 7)
What is the following command used for? net use \targetipc$ "" /u:""

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

Answer: D

NEW QUESTION 772
- (Exam Topic 7)
If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

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

Answer: B

NEW QUESTION 773
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 312-50v10 Exam with Our Prep Materials Via below:

https://www.certleader.com/312-50v10-dumps.html