# EC-COUNCIL.312-50v10.v2019-07-27.q180

| | |
|---|---|
| **Exam Code:** | 312-50v10 |
| **Exam Name:** | Certified Ethical Hacker Exam (CEH v10) |
| **Certification Provider:** | EC-COUNCIL |
| **Free Question Number:** | 180 |
| **Version:** | v2019-07-27 |
| **# of views:** | 4361 |
| **# of Questions views:** | 168597 |

https://www.freecram.com/torrent/EC-COUNCIL.312-50v10.v2019-07-27.q180.html

**NEW QUESTION: 1**
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.
Example:
allintitle: root passwd
**A.** Maintaining Access
**B.** Scanning and Enumeration
**C.** Reconnaissance
**D.** Gaining Access
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 2**
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
**A.** SQL injection vulnerability
**B.** Session management vulnerability
**C.** Cross-site Request Forgery vulnerability
**D.** Cross-site scripting vulnerability
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 3**
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?
**A.** Inherent risk
**B.** Residual risk
**C.** Deferred risk

**D.** Impact risk
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 4**
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.** IDS log
**B.** Event logs on domain controller
**C.** Event logs on the PC
**D.** Internet Firewall/Proxy log
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 5**
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
**A.** Double Hashing
**B.** Salting
**C.** Keyed Hashing
**D.** Key Stretching
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 6**
Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?
**A.** Role Based Access Control (RBAC)
**B.** Discretionary Access Control (DAC)
**C.** Windows authentication
**D.** Single sign-on
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 7**
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 promiscous mode?
**A.** Winpcap
**B.** Winpsw
**C.** Libpcap
**D.** Winprom
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 8**
When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.
What proxy tool will help you find web vulnerabilities?
**A.** Burpsuite
**B.** Proxychains
**C.** Dimitry
**D.** Maskgen
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 9**
The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. He also needs to permit all FTP traffic to the rest of the network and deny all other traffic.
After he applied his ACL configuration in the router, nobody can access to the ftp, and the permitted hosts cannot access the Internet. According to the next configuration, what is happening in the network?

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

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

**NEW QUESTION: 10**
When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation. What command will help you to search files using Google as a search engine?
**A.** site: target.com filetype:xls username password email
**B.** domain: target.com archieve:xls username password email
**C.** site: target.com file:xls username password email
**D.** inurl: target.com filename:xls username password email
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 11**
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?
**A.** Spoof Scan
**B.** TCP SYN
**C.** TCP Connect scan
**D.** Idle scan
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 12**
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?
**A.** At least twice a year or after any significant upgrade or modification
**B.** At least once every three years or after any significant upgrade or modification
**C.** At least once every two years and after any significant upgrade or modification
**D.** At least once a year and after any significant upgrade or modification
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
**A.** hping2 -set-ICMP host.domain.com
**B.** hping2 host.domain.com
**C.** hping2 -1 host.domain.com
**D.** hping2-i host.domain.com
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 14**
You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?
**A.** UPX
**B.** UPD
**C.** ICMP
**D.** TCP
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 15**
Which of the following will perform an Xmas scan using NMAP?
**A.** nmap -sV 192.168.1.254
**B.** nmap -sP 192.168.1.254
**C.** nmap -sA 192.168.1.254

**D.** nmap -sX 192.168.1.254
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 16**
Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?
**A.** [site:]
**B.** [cache:]
**C.** [inurl:]
**D.** [link:]
**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 17**
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
**A.** Armitage
**B.** Nmap
**C.** Metasploit
**D.** Nikto
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 18**
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.** Network sniffing
**B.** Man-in-the middle attack
**C.** Firewalking
**D.** Session hijacking
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 19**
>NMAP -sn 192.168.11.200-215 The NMAP command above performs which of the following?
**A.** A ping scan
**B.** A port scan
**C.** A trace sweep
**D.** An operating system detect
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 20**
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?
**A.** Hacking Active Directory
**B.** Port Scanning
**C.** Shoulder-Surfing
**D.** Privilege Escalation
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 21**
A virus that attempts to install itself inside the file it is infecting is called?
**A.** Polymorphic virus
**B.** Tunneling virus
**C.** Cavity virus
**D.** Stealth virus
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 22**
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
**A.** msfd
**B.** msfencode
**C.** msfpayload
**D.** msfcli
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 23**
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows

mobile phones, computers and other devices to connect and communicate using a short-range wireless connection. Which of the following terms best matches the definition?
**A.** Bluetooth
**B.** Radio-Frequency identification
**C.** WLAN
**D.** InfraRed
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 24**
Your company was hired by a small healthcare provider to perform a technician assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?
**A.** Create a disk image of a clean Windows installation
**B.** Use the built-in Windows Update tool
**C.** Check MITRE.org for the latest list of CVE findings
**D.** Use a scan tool like Nessus
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 25**
What is the correct process for the TCP three-way handshake connection establishment and connection termination?
**A.** Connection Establishment: ACK, ACK-SYN, SYN Connection Termination: FIN, ACK-FIN, ACK
**B.** Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: FIN, ACK-FIN, ACK
**C.** Connection Establishment: FIN, ACK-FIN, ACK Connection Termination: SYN, SYN-ACK, ACK
**D.** Connection Establishment: SYN, SYN-ACK, ACK Connection Termination: ACK, ACK-SYN, SYN
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 26**
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.** Copy the data to removable media and keep it in case you need it.
**B.** Ignore the data and continue the assessment until completed as agreed.
**C.** Confront the client in a respectful manner and ask her about the data.
**D.** Immediately stop work and contact the proper legal authorities.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 27**
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.** Defense in depth
**B.** Host-Based Intrusion Detection System
**C.** Security through obscurity
**D.** Network-Based Intrusion Detection System
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**
In order to have an anonymous Internet surf, which of the following is best choice?
**A.** Use shared WiFi
**B.** Use SSL sites when entering personal information
**C.** Use Tor network with multi-node
**D.** Use public VPN
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 29**
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.** Brute force login
**B.** File system permissions
**C.** Privilege escalation
**D.** Directory traversal
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 30**
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, Blackbox
**B.** Internal, Whitebox
**C.** External, Whitebox

**D.** External, Blackbox
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 31**
Which of the following is the best countermeasure to encrypting ransomwares?
**A.** Analyze the ransomware to get decryption key of encrypted data
**B.** Keep some generation of off-line backup
**C.** Use multiple antivirus softwares
**D.** Pay a ransom
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 32**
Due to a slowdown of normal network operations, the IT department decided to monitor internet traffic for all of the employees. From a legal standpoint, what would be troublesome to take this kind of measure?
**A.** Not informing the employees that they are going to be monitored could be an invasion of privacy.
**B.** All of the employees would stop normal work activities
**C.** IT department would be telling employees who the boss is
**D.** The network could still experience traffic slow down.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 33**
Which of the following is a low-tech way of gaining unauthorized access to systems?
**A.** Social Engineering
**B.** Sniffing
**C.** Enumeration
**D.** Scanning
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 34**

Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?
**A.** Network security policy
**B.** Remote access policy
**C.** Information protection policy
**D.** Access control policy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
**A.** Announced
**B.** Grey-box
**C.** White-box
**D.** Black-box
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 36**
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?
**A.** Verify acces right before allowing access to protected information and UI controls.
**B.** Use digital certificates to authenticate a server prior to sending data.
**C.** Use security policies and procedures to define and implement proper security settings.
**D.** Validate and escape all information sent to a server.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 37**
During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
**A.** Create a procedures document
**B.** Identify and evaluate existing practices
**C.** Terminate the audit
**D.** Conduct compliance testing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 38**
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.** Enumeration
**B.** Reconnaissance

**C.** Scanning
**D.** Escalation
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 39**
What two conditions must a digital signature meet?
**A.** Has to be legible and neat.
**B.** Must be unique and have special characters.
**C.** Has to be the same number of characters as a physical signature and must be unique.
**D.** Has to be unforgeable, and has to be authentic.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 40**
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.** Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server
**B.** SSH communications are encrypted it's impossible to know who is the client or 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 (LEAVE A REPLY)**

**NEW QUESTION: 41**
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.** Gray Hat
**B.** Black Hat
**C.** White Hat
**D.** Suicide Hacker
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 42**
Which of the following parameters describe LM Hash:
I - The maximum password length is 14 characters
II - There are no distinctions between uppercase and lowercase
III - The password is split into two 7-byte halves
**A.** I
**B.** I and II
**C.** II

**D.** I, II, and III
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 43**
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.** Host-based IDS
**B.** Open source-based IDS
**C.** Gateway-based IDS
**D.** Network-based IDS
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 44**
Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.
If a scanned port is open, what happens?
**A.** The port will send an RST.
**B.** The port will send an ACK.
**C.** The port will ignore the packets.
**D.** The port will send a SYN.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 45**
Why should the security analyst disable/remove unnecessary ISAPI filters?
**A.** To defend against wireless attacks
**B.** To defend against jailbreaking
**C.** To defend against webserver attacks
**D.** To defend against social engineering attacks
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 46**
Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming?
**A.** Bluesmacking
**B.** Bluesniffing
**C.** Bluesnarfing
**D.** Bluejacking

**Answer: D (LEAVE A REPLY)**



**NEW QUESTION: 47**
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.** TCP ping
**B.** Hping
**C.** Traceroute
**D.** Broadcast ping
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 48**
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?
**A.** Exclamation mark
**B.** Double quote
**C.** Semicolon
**D.** Single quote
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 49**
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.** Session hijacking
**B.** Dictionary-attack
**C.** Brute-force attack
**D.** Man-in-the-middle attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 50**
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?
**A.** Password protected files
**B.** Full Disk encryption
**C.** Hidden folders
**D.** BIOS password
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 51**
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.** Adaptive chosen-plaintext attack
**B.** Chosen-plaintext attack
**C.** Known-plaintext attack
**D.** Ciphertext-only attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 52**
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain. If the DNS server is at
192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
**A.** list domain=abccorp.local type=zone
**B.** ls -d accorp.local
**C.** lserver 192.168.10.2 -t all
**D.** list server=192.168.10.2 type=all
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 53**
John the Ripper is a technical assessment tool used to test the weakness of which of the following?
**A.** Usernames

**B.** File permissions
**C.** Firewall rulesets
**D.** Passwords
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 54**
The following is part of a log file taken from the machine on the network with the IP address of
192.168.0.110:

```
Time:June 16 17:30:15 Port:20 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:17 Port:21 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:19 Port:22 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:21 Port:23 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:22 Port:25 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:23 Port:80 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
Time:June 16 17:30:30 Port:443 Source:192.168.0.105 Destination:192.168.0.110 Protocol:TCP
```



What type of activity has been logged?
**A.** Denial of service attack targeting 192.168.0.105
**B.** Port scan targeting 192.168.0.105
**C.** Teardrop attack targeting 192.168.0.110
**D.** Port scan targeting 192.168.0.110
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 55**
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?
**A.** Bob can be right since DMZ does not make sense when combined with stateless firewalls
**B.** Bob is partially right. DMZ does not make sense when a stateless firewall is available
**C.** Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
**D.** Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 56**

Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?
**A.** A biometric system that bases authentication decisions on physical attributes.
**B.** An authentication system that uses passphrases that are converted into virtual passwords.
**C.** A biometric system that bases authentication decisions on behavioral attributes.
**D.** An authentication system that creates one-time passwords that are encrypted with secret keys.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 57**
Which of the following is a component of a risk assessment?
**A.** DMZ
**B.** Logical interface
**C.** Physical security
**D.** Administrative safeguards
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 58**
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?
**A.** -F
**B.** -P
**C.** -sP
**D.** -r
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 59**
Which of the following Linux commands will resolve a domain name into IP address?
**A.** >host-t a hackeddomain.com
**B.** >host -t soa hackeddomain.com
**C.** >host -t AXFR hackeddomain.com
**D.** >host-t ns hackeddomain.com
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 60**
Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.
**A.** nmap -p 445 -n -T4 -open 10.1.0.0/16
**B.** nmap -s 445 -sU -T5 10.1.0.0/16
**C.** nmap -sn -sF 10.1.0.0/16 445

**D.** nmap -p 445 -max -Pn 10.1.0.0/16
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 61**
Your business has decided to add credit card numbers to the data it backs up to tape. Which of the following represents the best practice your business should observe?
**A.** Back up the hashes of the credit card numbers not the actual credit card numbers.
**B.** Do not back up either the credit card numbers or their hashes.
**C.** Hire a security consultant to provide direction.
**D.** Encrypt backup tapes that are sent off-site.
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 62**
Which security strategy requires using several, varying methods to protect IT systems against attacks?
**A.** Three-way handshake
**B.** Defense in depth
**C.** Covert channels
**D.** Exponential backoff algorithm
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 63**
Which of the following statements is TRUE?
**A.** Sniffers operate on Layer 2 of the OSI model
**B.** Sniffers operate on the Layer 1 of the OSI model.
**C.** Sniffers operate on Layer 3 of the OSI model
**D.** Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 64**

Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by a coercion or torture?
**A.** Timing Attack
**B.** Chosen-Cipher text Attack
**C.** Ciphertext-only Attack
**D.** Rubber Hose Attack
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 65**
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.** Wi-Fi Protected Access (WPA)
**B.** Temporal Key Integrity Protocol (TKIP)
**C.** Wi-Fi Protected Access 2 (WPA2)
**D.** Wired Equivalent Privacy (WEP)
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 66**
What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?
**A.** Back up everything on the laptop and store the backup in a safe place.
**B.** Use a strong logon password to the operating system.
**C.** Encrypt the data on the hard drive.
**D.** Set a BIOS password
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 67**
Which of the following is the successor of SSL?
**A.** GRE
**B.** RSA
**C.** IPSec
**D.** TLS
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 68**
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.** Install a CCTV with cameras pointing to the entrance doors and the street.
**B.** Use an IDS in the entrance doors and install some of them near the corners.
**C.** Use fences in the entrance doors.
**D.** Use lights in all the entrance doors and along the company's perimeter.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 69**
In the field of cryptanalysis, what is meant by a "rubber-hose" attack?
**A.** Attempting to decrypt ciphertext by making logical assumptions about the contents of the original plaintext.
**B.** A backdoor placed into a cryptographic algorithm by its creator.
**C.** Forcing the targeted keystream through a hardware-accelerated device such as an ASIC.
**D.** Extraction of cryptographic secrets through coercion or torture.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 70**
You are monitoring the network of your organizations. You notice that:
1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication
Which of the following solution will you suggest?
**A.** Both B and C
**B.** Block the Blacklist IP's @ Firewall
**C.** Update the Latest Signatures on your IDS/IPS
**D.** Clean the Malware which are trying to Communicate with the External Blacklist IP's
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 71**
The collection of potentially actionable, overt, and publicly available information is known as
**A.** Open-source intelligence
**B.** Social intelligence
**C.** Real intelligence
**D.** Human intelligence
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 72**
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.** DynDNS
**B.** Split DNS
**C.** DNS Scheme
**D.** DNSSEC
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 73**
A new wireless client is configured to join an 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.** Client is configured for the wrong channel
**B.** The client cannot see the SSID of the wireless network
**C.** The WAP does not recognize the client's MAC address
**D.** The wireless client is not configured to use DHCP
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 74**
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?
**A.** Read the first 512 bytes of the tape
**B.** Perform a full restore
**C.** Restore a random file
**D.** Read the last 512 bytes of the tape
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 75**
PGP, SSL, and IKE are all examples of which type of cryptography?
**A.** Hash Algorithm
**B.** Secret Key
**C.** Public Key
**D.** Digest
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 76**
Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?
**A.** Requires vendor updates for a new threat
**B.** Can identify unknown attacks

**C.** Cannot deal with encrypted network traffic
**D.** Produces less false positives
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 77**
Which of the following statements regarding ethical hacking is incorrect?
**A.** An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services
**B.** Testing should be remotely performed offsite.
**C.** Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems
**D.** Ethical hacking should not involve writing to or modifying the target systems.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 78**
A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?
**A.** Remote-access policy
**B.** Acceptable-use policy
**C.** Firewall-management policy
**D.** Permissive policy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenarios will compromise the privacy of her data?
**A.** None of these scenarios compromise the privacy of Alice's data
**B.** Agent Andrew subpoenas Alice, forcing her to reveal her private key. However, the cloud server successfully resists Andrew's attempt to access the stored data

**C.** Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before
**D.** Hacker Harry breaks into the cloud server and steals the encrypted data
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 80**
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?
**A.** Inverse TCP flag scanning
**B.** TCP Scanning
**C.** IP Fragment Scanning
**D.** ACK flag scanning
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 81**
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?
**A.** Tailgating
**B.** Social engineering
**C.** Eavesdropping
**D.** Piggybacking
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 82**
What is the process of logging, recording, and resolving events that take place in an organization?
**A.** Internal Procedure
**B.** Metrics
**C.** Security Policy
**D.** Incident Management Process
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 83**

Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?
**A.** Wireshark
**B.** Cain & Abel
**C.** Metasploit
**D.** Maltego
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 84**
Which Intrusion Detection System is the best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?
**A.** Firewalls
**B.** Honeypots
**C.** Host-based intrusion detection system (HIDS)
**D.** Network-based intrusion detection system (NIDS)
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 85**
Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
**A.** John the Ripper
**B.** Dsniff
**C.** Nikto
**D.** Snort
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 86**
Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access.
A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door.
In this case, we can say:
**A.** Biological motion cannot be used to identify people
**B.** The solution will have a high level of false positives
**C.** Although the approach has two phases, it actually implements just one authentication factor
**D.** The solution implements the two authentication factors: physical object and physical characteristic

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 87**
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.** ACK flag probe scanning
**B.** IPID scanning
**C.** ICMP Echo scanning
**D.** SYN/FIN scanning using IP fragments
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 88**
Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?
**A.** ESP transport mode
**B.** AH Tunnel mode
**C.** ESP confidential
**D.** AH promiscuous
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 89**
Which of the following act requires employer's standard national numbers to identify them on standard transactions?
**A.** PCI-DSS
**B.** SOX
**C.** DMCA
**D.** HIPAA
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 90**
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.** FORCELTS
**B.** UPGRADETLS
**C.** OPPORTUNISTICTLS
**D.** STARTTLS
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 91**
How can rainbow tables be defeated?
**A.** Password salting
**B.** All uppercase character passwords
**C.** Lockout accounts under brute force password cracking attempts
**D.** Use of non-dictionary words
**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 92**
Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make
$1000 in a day?'.
3. Victim clicks to the interesting and attractive content URL.
4. Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or UPL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
**A.** HTML Injection
**B.** Session Fixation
**C.** Clickjacking Attack
**D.** HTTP Parameter Pollution
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 93**
Emil uses nmap to scan two hosts using this command:
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:

```
Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

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



What is his conclusion?

**A.** He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7

**B.** Host 192.168.99.7 is down.

**C.** Host 192.168.99.1 is the host that he launched the scan from.

**D.** Host 192.168.99.7 is an iPad.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 94**

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.** All three servers need to face the Internet so that they can communicate between themselves

**C.** A web server and the database server facing the Internet, an application server on the internal network

**D.** A web server facing the Internet, an application server on the internal network, a database server on the internal network

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 95**

WPA2 uses AES for wireless data encryption at which of the following encryption levels?

**A.** 64 bit and CCMP

**B.** 128 bi and TKIP

**C.** 128 bit and CCMP
**D.** 128 bit and CRC
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 96**
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.** Both static routes indicate that the traffic is internal with different gateway.
**C.** 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.
**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 (LEAVE A REPLY)**

**NEW QUESTION: 97**
Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""1111111111111111111111111111"");
}
Output:
Segmentation fault
**A.** Java
**B.** C#
**C.** C++
**D.** Python
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 98**
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering and it will tell you the "landscape" looks like.

What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?
**A.** network mapping
**B.** escalating privileges
**C.** gaining access
**D.** footprinting
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 99**
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library?
This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
**A.** POODLE
**B.** SSL/TLS Renegotiation Vulnerability
**C.** Shellshock
**D.** Heartbleed Bug
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 100**
Which of the following tools is used to detect wireless LANs using the 802.11 a/b/g/n WLAN standards on a linux platform?
**A.** Kismet
**B.** Netstumbler
**C.** Nessus
**D.** Abel
**Answer: A (LEAVE A REPLY)**
Explanation/Reference:

**NEW QUESTION: 101**
Which of the following programs is usually targeted at Microsoft Office products?
**A.** Stealth virus
**B.** Polymorphic virus
**C.** Macro virus
**D.** Multipart virus
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 102**
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?
**A.** SOA

**B.** single sign on
**C.** PKI
**D.** biometrics
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 103**
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/\r\n\%00account%00Ned%00access HTTP/1.1 Host: westbank.com"
**B.** "GET/restricted/bank.getaccount('Ned') HTTP/1.1 Host: westbank.com"
**C.** "GET/restricted/accounts/?name=Ned HTTP/1.1 Host: westbank.com"
**D.** "GET/restricted/goldtransfer?to=Rob&from=1 or 1=1' HTTP/1.1Host: westbank.com"
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 104**
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?
**A.** He will repeat the same attack against all L2 switches of the network.
**B.** He will repeat this action so that is escalates to a DoS attack.
**C.** He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
**D.** He will activate OSPF on the spoofed root bridge.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 105**
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?
**A.** Discovery
**B.** Recovery
**C.** Eradication
**D.** Containment
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 106**
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.** Ransomware Trojans
**C.** Banking Trojans
**D.** Turtle Trojans
**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 107**
Which method of password cracking takes the most time and effort?
**A.** Brute force
**B.** Dictionary attack
**C.** Shoulder surfing
**D.** Rainbow tables
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 108**
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?
**A.** Cross Site Request Forgery
**B.** Cross Site Scripting
**C.** Path disclosure
**D.** Injection
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 109**
The "Gray-box testing" methodology enforces what kind of restriction?
**A.** The internal operation of a system is only partly accessible to the tester.
**B.** The internal operation of a system is completely known to the tester.
**C.** Only the internal operation of a system is known to the tester.
**D.** Only the external operation of a system is accessible to the tester.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 110**
Elliot is in the process of exploiting a web application that uses SQL as a back-end database. He is determined that the application is vulnerable to SQL injection and has introduced conditional timing delays into injected queries to determine whether they are successful. What type of SQL injection is Elliot most likely performing?
**A.** Error-based SQL injection
**B.** NoSQL injection
**C.** Blind SQL injection
**D.** Union-based SQL injection
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 111**
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?
**A.** nmap -A --host-timeout 99-T1
**B.** nmap -A - Pn
**C.** nmap -sT -O -T0
**D.** nmap -sP -p-65535-T5
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 112**
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?
**A.** Enumeration
**B.** Scanning
**C.** System Hacking
**D.** Footprinting
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 113**
Which service in a PKI will vouch for the identity of an individual or company?
**A.** CA
**B.** CBC
**C.** CR
**D.** KDC
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 114**

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

**A.** Cross-Site Request Forgery (CSRF)

**B.** SQL injection attack

**C.** LDAP Injection attack

**D.** Cross-Site Scripting (XSS)

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 115**

Risks=Threats x Vulnerabilities is referred to as the:

**A.** Risk equation

**B.** Disaster recovery formula

**C.** Threat assessment

**D.** BIA equation

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 116**

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

192.168.1.106:

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

What type of activity has been logged?

**A.** Denial of service attack targeting 192.168.1.103

**B.** Teardrop attack targeting 192.168.1.106

**C.** Port scan targeting 192.168.1.103

**D.** Port scan targeting 192.168.1.106

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 117**

During an Xmas scan, what indicates a port is closed?

**A.** ACK

**B.** RST

**C.** SYN

**D.** No return response

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 118**
A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?
**A.** Ignore it.
**B.** Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.
**C.** Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.
**D.** Try to sell the information to a well-paying party on the dark web.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 119**
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap -Pn -p -sl kiosk.adobe.com www.riaa.com kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-sl" with Nmap?
**A.** Conduct stealth scan
**B.** Conduct IDLE scan
**C.** Conduct ICMP scan
**D.** Conduct silent scan
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 120**
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.** He cannot read it because it is encrypted.
**B.** The password file does not contain the passwords themselves.
**C.** The file reveals the passwords to the root user only.
**D.** He can open it and read the user ids and corresponding passwords.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 121**
Why is a penetration test considered to be more thorough than vulnerability scan?
**A.** A penetration test actively exploits vulnerabilities in the targeted infrastructure, while a vulnerability scan does not typically involve active exploitation.
**B.** Vulnerability scans only do host discovery and port scanning by default.
**C.** It is not - a penetration test is often performed by an automated tool, while a vulnerability scan requires active engagement.
**D.** The tools used by penetration testers tend to have much more comprehensive vulnerability databases.

**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 122**
On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service. What is the name of the process by which you can determine those critical business?
**A.** Emergency Plan Response (EPR)
**B.** Risk Mitigation
**C.** Business Impact Analysis (BIA)
**D.** Disaster Recovery Planning (DRP)
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 123**
Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file named
"Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt". In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.
What type of malware has Jesse encountered?
**A.** Macro Virus
**B.** Key-Logger
**C.** Worm
**D.** Trojan
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 124**
Which of the following program infects the system boot sector and the executable files at the same time?
**A.** Stealth virus
**B.** Multipartite Virus

**C.** Macro virus
**D.** Polymorphic virus
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 125**
An IT employee got a call from one our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?
**A.** The employee should not provide any information without previous management authorization
**B.** The employee can not provide any information: but, anyway, he/she will provide the name of the person in charge
**C.** Since the company's policy is all about Customer Service. he/she will provide information
**D.** Disregarding the call, the employee should hang up
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 126**
Which type of security feature stops vehicles from crashing through the doors of a building?
**A.** Mantrap
**B.** Bollards
**C.** Turnstile
**D.** Receptionist
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 127**
Which protocol is used for setting up secure channels between two devices, typically in VPNs?
**A.** IPSEC
**B.** PPP
**C.** SET
**D.** PEM
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 128**
As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?
**A.** Service Level Agreement
**B.** Rules of Engagement
**C.** Non-Disclosure Agreement

**D.** Project Scope
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 129**
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet
10.1.4.0/23.
Which of the following IP addresses could be leased as a result of the new configuration?
**A.** 10.1.4.156
**B.** 10.1.5.200
**C.** 10.1.4.254
**D.** 10.1.255.200
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 130**
Cross-site request forgery involves:
**A.** A browser making a request to a server without the user's knowledge
**B.** A server making a request to another server without the user's knowledge
**C.** A request sent by a malicious user from a browser to a server
**D.** Modification of a request by a proxy between client and server
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 131**
Which of the following describes the characteristics of a Boot Sector Virus?
**A.** Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.
**B.** Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
**C.** Overwrites the original MBR and only executes the new virus code.
**D.** Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 132**
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 be either accepted or rejected from when an individual provides identification and authentication information
**B.** The amount of time and resources that are necessary to maintain a biometric system
**C.** How long it takes to setup individual user accounts
**D.** The amount of time it takes to convert biometric data into a template on a smart card

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 133**
An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?
**A.** Intrusion Prevention System (IPS)
**B.** Network sniffer
**C.** Vulnerability scanner
**D.** Protocol analyzer
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 134**
Hackers often raise the trust level of a phishing message by modeling the email to look similar to the internal email used by the target company. This includes using logos, formatting, and names of the target company. The phishing message will often use the name of the company CEO, President, or Managers.
The time a hacker spends performing research to locate this information about a company is known as?
**A.** Reconnaissance
**B.** Exploration
**C.** Enumeration
**D.** Investigation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 135**
What would you enter, if you wanted to perform a stealth scan using Nmap?
**A.** nmap -sU
**B.** nmap -sM
**C.** nmap -sT
**D.** nmap -sS
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 136**
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?
**A.** Snort
**B.** Cain & Abel
**C.** Nmap

**D.** Nessus
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 137**
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?
**A.** Bootrom Exploit
**B.** iBoot Exploit
**C.** Sandbox Exploit
**D.** Userland Exploit
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 138**
DHCP snooping is a great solution to prevent rogue DHCP servers on your network. Which security feature on switchers leverages the DHCP snooping database to help prevent man-in-the-middle attacks?
**A.** Dynamic ARP Inspection (DAI)
**B.** Layer 2 Attack Prevention Protocol (LAPP)
**C.** Port security
**D.** Spanning tree
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 139**
What is the difference between the AES and RSA algorithms?
**A.** RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data
**B.** Both are symmetric algorithms, but AES uses 256-bit keys
**C.** AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data
**D.** Both are asymmetric algorithms, but RSA uses 1024-bit keys
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 140**
Jim's company regularly performs backups of their critical servers. But the company cannot afford to send backup tapes to an off-site vendor for long-term storage and archiving. Instead, Jim's company keeps the backup tapes in a safe in the office. Jim's company is audited each year, and the results from this year's audit show a risk because backup tapes are not stored off-site. The Manager of Information Technology has a plan to take the backup tapes home with him and wants to know what two things he can do to secure the backup tapes while in transit?
**A.** Degauss the backup tapes and transport them in a lock box.
**B.** Encrypt the backup tapes and use a courier to transport them.
**C.** Encrypt the backup tapes and transport them in a lock box.
**D.** Hash the backup tapes and transport them in a lock box.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 141**
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities.
Which type of virus detection method did Chandler use in this context?
**A.** Scanning
**B.** Heuristic Analysis
**C.** Integrity checking
**D.** Code Emulation
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 142**
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?
**A.** SHA-3
**B.** SHA-0
**C.** SHA-2
**D.** SHA-1
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 143**
How does the Address Resolution Protocol (ARP) work?
**A.** It sends a request packet to all the network elements, asking for the MAC address from a specific IP.
**B.** It sends a reply packet for a specific IP, asking for the MAC address.

**C.** It sends a request packet to all the network elements, asking for the domain name from a specific IP.
**D.** It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 144**

```
#!/usr/bin/python
import socket
buffer=["A"]
counter=50
while len(buffer) <=100:
buffer.append("A"*counter)
counter=counter+50
com-
mands=["HELP", "STATS.", "RTIME.", "LTIME.", ":SRUN.", "TRUN.", "GMON.", "
GDOG.", "KSTET.", "GTER.", "HTER.", "LTER.", "KSTAN."]
for command in commands:
for buffstring in buffer:
print "Exploiting" +command +" "+str(len(buffstring))
s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
s.connect(('127.0.0.1',9999))
s.recv(50)
s.send(command+buffstring)
s.close()
```

What is the code written for?
**A.** Denial-of-service (DoS)
**B.** Buffer Overflow
**C.** Encryption
**D.** Bruteforce
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 145**
Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF?
**A.** Dipole antenna
**B.** Omnidirectional antenna
**C.** Parabolic grid antenna
**D.** Yagi antenna
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 146**
By using a smart card and pin, you are using a two-factor authentication that satisfies
**A.** Something you have and something you know

**B.** Something you are and something you remember
**C.** Something you know and something you are
**D.** Something you have and something you are
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 147**
Sam is working as s pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?
**A.** False Positive Generation
**B.** Denial-of-Service
**C.** Insertion Attack
**D.** Obfuscating
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 148**
Which of the following statements is FALSE with respect to Intrusion Detection Systems?
**A.** Intrusion Detection Systems can examine the contents of the data in context of the network protocol
**B.** Intrusion Detection Systems require constant update of the signature library
**C.** Intrusion Detection Systems can be configured to distinguish specific content in network packets
**D.** Intrusion Detection Systems can easily distinguish a malicious payload in an encrypted traffic
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 149**
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:
**A.** Just a network monitoring tool
**B.** A signature-based IDS
**C.** A behavior-based IDS
**D.** A hybrid IDS
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 150**
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:

Access List should be written between VLANs.

Port security should be enabled for the intranet.

A security solution which filters data packets should be set between intranet (LAN) and DMZ.

A WAF should be used in front of the web applications.

According to the section from the report, which of the following choice is true?

**A.** A stateful firewall can be used between intranet (LAN) and DMZ.

**B.** There is access control policy between VLANs.

**C.** MAC Spoof attacks cannot be performed.

**D.** Possibility of SQL Injection attack is eliminated.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 151**

What is a "Collision attack" in cryptography?

**A.** Collision attacks try to get the public key

**B.** Collision attacks try to find two inputs producing the same hash

**C.** Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key

**D.** Collision attacks try to break the hash into three parts to get the plaintext value

**Answer: (SHOW ANSWER)**



**NEW QUESTION: 152**

Suppose your company has just passed a security risk assessment exercise. The results display that the risk of the breach in the main company application is 50%. Security staff has taken some measures and implemented the necessary controls. After that, another security risk assessment was performed showing that risk has decreased to 10%. The risk threshold for the application is 20%. Which of the following risk decisions will be the best for the project in terms of its successful continuation with the most business profit?

**A.** Accept the risk

**B.** Mitigate the risk

**C.** Introduce more controls to bring risk to 0%
**D.** Avoid the risk
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 153**
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 of 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: (SHOW ANSWER)**

**NEW QUESTION: 154**
The purpose of a _____is to deny network access to local area networks and other information assets by unauthorized wireless devices.
**A.** Wireless Analyzer
**B.** Wireless Jammer
**C.** Wireless Access Control List
**D.** Wireless Access Point
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 155**
If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?
**A.** Civil
**B.** International
**C.** Criminal
**D.** Common
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 156**
Which results will be returned with the following Google search query? site:target.com site:Marketing.target.com accounting
**A.** Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
**B.** Results matching "accounting" in domain target.com but not on the site Marketing.target.com
**C.** Results matching all words in the query.

**D.** Results for matches on target.com and Marketing,target.com that include the word "accounting"
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 157**
Which of these is capable of searching for and locating rogue access points?
**A.** NIDS
**B.** HIDS
**C.** WISS
**D.** WIPS
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 158**
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux serves to synchronize the time has stopped working?
**A.** OSPF
**B.** TimeKeeper
**C.** NTP
**D.** PPP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 159**
When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server.
You can detect all these methods (GET, POST, HEAD, DELETE, TRACE) using NMAP script engine.
What Nmap script will help you with this task?
**A.** http-git
**B.** http-methods
**C.** http-headers
**D.** http enum
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 160**

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

**NEW QUESTION: 161**
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?
**A.** Only using OSPFv3 will mitigate this risk.
**B.** Make sure that legitimate network routers are configured to run routing protocols with authentication.
**C.** Redirection of the traffic cannot happen unless the admin allows it explicitly.
**D.** Disable all routing protocols and only use static routes
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 162**
What does the -oX flag do in an Nmap scan?
**A.** Output the results in truncated format to the screen
**B.** Perform an Xmas scan
**C.** Perform an eXpress scan
**D.** Output the results in XML format to a file
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 163**
What is not a PCI compliance recommendation?
**A.** Use encryption to protect all transmission of card holder data over any public network.
**B.** Limit access to card holder data to as few individuals as possible.
**C.** Rotate employees handling credit card transactions on a yearly basis to different departments.
**D.** Use a firewall between the public network and the payment card data.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 164**

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

**A.** Fuzzing Testing

**B.** Static Testing

**C.** Function Testing

**D.** Dynamic Testing

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 165**

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

**A.** The gateway and the computer are not on the same network.

**B.** The computer is using an invalid IP address.

**C.** The computer is not using a private IP address.

**D.** The gateway is not routing to a public IP address.

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 166**

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.** Do not report it and continue the penetration test.

**B.** Transfer money from the administrator's account to another account.

**C.** Report immediately to the administrator.

**D.** Do not transfer the money but steal the bitcoins.

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 167**
An attacker scans a host with the below command. Which three flags are set? (Choose three.)
#nmap -sX host.domain.com
**A.** This is SYN scan. SYN flag is set
**B.** This is Xmas scan. URG, PUSH and FIN are set
**C.** This is ACK scan. ACK flag is set
**D.** This is Xmas scan. SYN and ACK flags are set
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 168**
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?
**A.** Promiscuous mode
**B.** Port forwarding
**C.** WEM
**D.** Multi-cast mode
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 169**
When tuning security alerts, what is the best approach?
**A.** Decrease False negatives
**B.** Rise False positives Rise False Negatives
**C.** Decrease the false positives
**D.** Tune to avoid False positives and False Negatives
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 170**
An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections.
When users accessed any page, the applet ran and exploited many machines.
Which one of the following tools the hacker probably used to inject HTML code?
**A.** Wireshark
**B.** Tcpdump
**C.** Ettercap
**D.** Aircrack-ng

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 171**
Which of the following steps for risk assessment methodology refers to vulnerability identification?
**A.** Determines if any flaws exist in systems, policies, or procedures
**B.** Assigns values to risk probabilities; Impact values
**C.** Determines risk probability that vulnerability will be exploited (High, Medium, Low)
**D.** Identifies sources of harm to an IT system (Natural, Human, Environmental)
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 172**
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 whose credentials are known. It was written by sysinternals and has been integrated within the framework. The 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 used in the psexec module's 'smbpass' option?
**A.** LM:NT
**B.** NT:LM
**C.** LM:NTLM
**D.** NTLM:LM
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 173**
Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

```
[eve@localhost ~]$ john secret.txt
Loaded 2 password hashes with no different salts (LM[DES 128/128 SSE2-16])
Press 'q' or Ctrol-C to abort, almost any other key for status
0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO...SAMPLUI
0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4
0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837
0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 15917KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

**A.** She is encrypting the file.
**B.** She is using John the Ripper to crack the passwords in the secret.txt file
**C.** She is using ftp to transfer the file to another hacker named John.
**D.** She is using John the Ripper to view the contents of the file.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 174**
Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?
**A.** Oakley
**B.** IPsec Policy Agent
**C.** Internet Key Exchange (IKE)
**D.** IPsec driver
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 175**
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?
**A.** Kismet
**B.** Burp Suite
**C.** OpenVAS
**D.** tshark
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 176**
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the provider's environment.
**A.** Cloud based
**B.** Heuristics based
**C.** Behavioral based
**D.** Honypot based
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 177**
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?
**A.** openssl_client -connect www.website.com:443
**B.** openssl s_client -connect www.website.com:443
**C.** openssl_client -site www.website.com:443
**D.** openssl s_client -site www.website.com:443

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 178**
You are monitoring the network of your organizations. You notice that:
1. There are huge outbound connections from your Internal Network to External IPs
2. On further investigation, you see that the external IPs are blacklisted
3. Some connections are accepted, and some are dropped
4. You find that it is a CnC communication
Which of the following solution will you suggest?
**A.** Block the Blacklist IP's @ Firewall as well as Clean the Malware which are trying to Communicate with the External Blacklist IP's.
**B.** Update the Latest Signatures on your IDS/IPS
**C.** Block the Blacklist IP's @ Firewall
**D.** Clean the Malware which are trying to Communicate with the External Blacklist IP's
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 179**
The "white box testing" methodology enforces what kind of restriction?
**A.** The internal operation of a system is only partly accessible to the tester.
**B.** The internal operation of a system is completely known to the tester.
**C.** Only the internal operation of a system is known to the tester.
**D.** Only the external operation of a system is accessible to the tester.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 180**
An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.
In which order should he perform these steps?
**A.** The sequence does not matter. Both steps have to be performed against all hosts.
**B.** First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
**C.** First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
**D.** The port scan alone is adequate. This way he saves time.
**Answer: (SHOW ANSWER)**

# EC-COUNCIL.312-50v10.v2020-10-01.q260

| | |
|---|---|
| **Exam Code:** | 312-50v10 |
| **Exam Name:** | Certified Ethical Hacker Exam (CEH v10) |
| **Certification Provider:** | EC-COUNCIL |
| **Free Question Number:** | 260 |
| **Version:** | v2020-10-01 |
| **# of views:** | 878 |
| **# of Questions views:** | 37246 |

https://www.freecram.com/torrent/EC-COUNCIL.312-50v10.v2020-10-01.q260.html

**NEW QUESTION: 1**
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 (LEAVE A REPLY)**
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: 2**
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 can be prevented by blocking all inbound TCP port 53 connections
**C.** Zone transfers cannot occur on the Internet
**D.** A zone transfer passes all zone information that a nslookup server maintains
**E.** A zone transfer passes all zone information that a DNS server maintains
**F.** A zone transfer is accomplished with the nslookup service
**Answer: A,B,E (LEAVE A REPLY)**

**NEW QUESTION: 3**

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.
Which command would you use?
**A.** c:\compmgmt.msc
**B.** c:\services.msc
**C.** c:\ncpa.cp
**D.** c:\gpedit
**Answer: A (LEAVE A REPLY)**
Explanation
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.
References:
http://www.waynezim.com/tag/compmgmtmsc/

**NEW QUESTION: 4**
Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
**A.** LOGIN, USER
**B.** USER, PASS
**C.** LOGIN, NICK
**D.** USER, NICK
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 5**
Which command line switch would be used in NMAP to perform operating system detection?
**A.** -sO
**B.** -sP
**C.** -O
**D.** -OS
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 6**
How can telnet be used to fingerprint a web server?
**A.** telnet webserverAddress 80PUT / HTTP/1.0
**B.** telnet webserverAddress 80PUT / HTTP/2.0
**C.** telnet webserverAddress 80HEAD / HTTP/2.0
**D.** telnet webserverAddress 80HEAD / HTTP/1.0
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 7**

The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?
**A.** Investigate based on the service level agreements of the systems.
**B.** Investigate based on the potential effect of the incident.
**C.** Investigate based on the order that the alerts arrived in.
**D.** Investigate based on the maintenance schedule of the affected systems.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 8**
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?
**A.** PKI
**B.** single sign on
**C.** biometrics
**D.** SOA
**Answer: A (LEAVE A REPLY)**
Explanation
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates [1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.
References: https://en.wikipedia.org/wiki/Public_key_infrastructure

**NEW QUESTION: 9**
It is a short-range wireless communication technology that allows mobile phones, computers and other devices to connect and communicate. This technology intends to replace cables connecting portable devices with high regards to security.
**A.** WLAN
**B.** Radio-Frequency Identification
**C.** InfraRed
**D.** Bluetooth
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 10**
Look at the following output. What did the hacker accomplish?

```
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
domain.com. 600 IN A 192.168.1.102
domain.com. 600 IN A 192.168.1.105
domain.com. 3600 IN NS srv1.domain.com.
domain.com. 3600 IN NS srv2.domain.com.
vpn.domain.com. 3600 IN A 192.168.1.1
server.domain.com. 3600 IN A 192.168.1.3
office.domain.com. 3600 IN A 192.168.1.4
remote.domain.com. 3600 IN A 192.168. 1.48
support.domain.com. 3600 IN A 192.168.1.47
ns1.domain.com. 3600 IN A 192.168.1.41
ns2.domain.com. 3600 IN A 192.168.1.42
ns3.domain.com. 3600 IN A 192.168.1.34
ns4.domain.com. 3600 IN A 192.168.1.45
srv1.domain.com. 3600 IN A 192.168.1.102
srv2.domain.com. 1200 IN A 192.168.1.105
domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com.
131 900 600 86400 3600
;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)
```



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

**NEW QUESTION: 11**
When discussing passwords, what is considered a brute force attack?
**A.** You attempt every single possibility until you exhaust all possible combinations or discover the password
**B.** You threaten to use the rubber hose on someone unless they reveal their password
**C.** You wait until the password expires
**D.** You create hashes of a large number of words and compare it with the encrypted passwords
**E.** You load a dictionary of words into your cracking program
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 12**

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

**A.** 10.10.10.10

**B.** 192.168.168.168

**C.** 127.0.0.1

**D.** 192.168.1.1

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 13**

Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

**A.** Cain & Abel

**B.** Wireshark

**C.** Maltego

**D.** Metasploit

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 14**

While reviewing the result of scanning run against a target network you come across the following:

```
system.sysDescr.0 : DISPLAY STRING- (ascii): Cisco Internetwork Operating
System Software
IOS (tm) 4500 Software (C4500-IS-M), Version 12.0(9), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by Cisco Systems, Inc.
Compiled Tue 25-Jan-00 04:28 by bettyl
system.sysObjectID.0 : OBJECT IDENTIFIER:
.iso.org.dod.internet.Private.enter [redacted].Cisco.[redacted].Cisco4700
system.sysUpTime.0 : Timeticks: (1563980[redacted] 18 days, 2:26:20.17
system.sysContact.0 : DISPLAY STRING- (ascii):
system.sysName.0 : DISPLAY STRING- (ascii): somerroutername
system.sysLocation.0 : DISPLAY STRING- (ascii):
system.sysServices.0 : INTEGER: 6
system.sysORLastChange.0 : Timeticks: (0) 0:00:00.00
```

Which among the following can be used to get this output?

**A.** nmap protocol scan

**B.** A Bo2k system query.

**C.** An SNMP walk

**D.** A sniffer

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 15**

Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?
**A.** The CA is the trusted root that issues certificates.
**B.** The root CA stores the user's hash value for safekeeping.
**C.** The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
**D.** The root CA is used to encrypt email messages to prevent unintended disclosure of data.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 16**
What is the minimum number of network connections in a multi homed firewall?
**A.** 3
**B.** 5
**C.** 2
**D.** 4
**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 17**
Which of the following is used to indicate a single-line comment in structured query language (SQL)?
**A.** %%
**B.** --
**C.** "
**D.** ||
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 18**
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the
192.168.1.0/24. Which of the following has occurred?
**A.** The computer is not using a private IP address.

**B.** The computer is using an invalid IP address.
**C.** The gateway is not routing to a public IP address.
**D.** The gateway and the computer are not on the same network.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 19**
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.** Mitigate
**B.** Avoid
**C.** Delegate
**D.** Accept
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 20**
The security concept of "separation of duties" is most similar to the operation of which type of security device?
**A.** Firewall
**B.** Bastion host
**C.** Intrusion Detection System
**D.** Honeypot
**Answer: (SHOW ANSWER)**
Explanation
In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.
References:
http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-du

**NEW QUESTION: 21**
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
**A.** msfcli
**B.** msfpayload
**C.** msfencode
**D.** msfd
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 22**
What are the three types of authentication?

**A.** Something you: know, remember, prove
**B.** Something you: have, know, are
**C.** Something you: show, have, prove
**D.** Something you: show, prove, are
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 23**
You are tasked to configure the DHCP server to lease the last 100 usable IP addresses in subnet to. 1.4.0/23.
Which of the following IP addresses could be teased as a result of the new configuration?
**A.** 10.1.4.254
**B.** 10.1.4.156
**C.** 10..1.5.200
**D.** 210.1.55.200
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 24**
Which utility will tell you in real time which ports are listening or in another state?
**A.** Nmap
**B.** Loki
**C.** Netstat
**D.** TCPView
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 25**
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.** Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to 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.** Start by foot printing the network and mapping out a plan of attack.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 26**
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 (LEAVE A REPLY)**
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: 27**
Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.
What would Yancey be considered?
**A.** Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing
**B.** Since he does not care about going to jail, he would be considered a Black Hat
**C.** Because Yancey works for the company currently; he would be a White Hat
**D.** Yancey would be considered a Suicide Hacker
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 28**
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
**A.** Key Stretching
**B.** Salting
**C.** Double Hashing
**D.** Keyed Hashing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 29**
Which of the following is an example of two factor authentication?
**A.** Username and Password
**B.** Digital Certificate and Hardware Token
**C.** Fingerprint and Smartcard ID

**D.** PIN Number and Birth Date
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 30**
To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?
**A.** Harvesting
**B.** Stealthing
**C.** Windowing
**D.** Hardening
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 31**
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Which of the below scanning technique will you use?
**A.** Inverse TCP flag scanning
**B.** IP Fragment Scanning
**C.** ACK flag scanning
**D.** TCP Scanning
**Answer: B (LEAVE A REPLY)**



**NEW QUESTION: 32**
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 yes; the friend needs help to gather evidence.
**B.** Say no; make sure that the friend knows the risk she's asking the CEH to take.
**C.** Say yes; do the job for free.
**D.** Say no; the friend is not the owner of the account.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 33**
Which type of cryptography does SSL, IKE and PGP belongs to?
**A.** Public Key
**B.** Digest
**C.** Hash Algorithm
**D.** Secret Key
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 34**
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.** SQL injection
**B.** SDLC process
**C.** Trap door
**D.** Honey pot
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 35**
Which command can be used to show the current TCP/IP connections?
**A.** Netstat
**B.** Net use connection
**C.** Netsh
**D.** Net use
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 36**
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?
**A.** Eradication
**B.** Discovery
**C.** Containment
**D.** Recovery
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 37**
While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of

packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

**A.** Stateful multilayer inspection firewall

**B.** Application-level firewall

**C.** Packet filtering firewall

**D.** Circuit-level gateway firewall

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 38**

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: (SHOW ANSWER)**

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: 39**

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

**A.** CBC

**B.** KDC

**C.** CR

**D.** CA

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 40**

A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT     STATE     SERVICE
21/tcp     open      ftp
23/tcp     open      telnet
80/tcp     open      http
139/tcp    open      netbios-ssn
515/tcp    open
631/tcp    open      ipp
9100/tcp   open
MAC Address: 00:00:48:0D:EE:89
```



**A.** The host is likely a Linux machine.
**B.** The host is likely a printer.
**C.** The host is likely a router.
**D.** The host is likely a Windows machine.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 41**
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.** Strict, Abstract
**B.** Simple, Complex
**C.** Hierarchical, Relational
**D.** Relational, Hierarchical
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 42**
Which of the following types of firewall inspects only header information in network traffic?
**A.** Circuit-level gateway
**B.** Stateful inspection
**C.** Packet filter
**D.** Application-level gateway
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 43**
An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?
**A.** He will repeat the same attack against all L2 switches of the network.
**B.** He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.

**C.** He will repeat this action so that it escalates to a DoS attack.
**D.** He will activate OSPF on the spoofed root bridge.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 44**
Within the context of Computer Security, which of the following statements describes Social Engineering best?
**A.** Social Engineering is a training program within sociology studies
**B.** Social Engineering is the means put in place by human resource to perform time accounting
**C.** Social Engineering is the act of publicly disclosing information
**D.** Social Engineering is the act of getting needed information from a person rather than breaking into a system
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 45**
Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?
**A.** Ping of death
**B.** SYN flood
**C.** Smurf attack
**D.** Teardrop
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 46**
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
<iframe src="http://www.vulnweb.com/updateif.php" style="display:none"></iframe> What is this type of attack (that can use either HTTP GET or HTTP POST) called?
**A.** Cross-Site Request Forgery
**B.** Cross-Site Scripting
**C.** SQL Injection
**D.** Browser Hacking
**Answer: (SHOW ANSWER)**
Explanation
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.
References: https://en.wikipedia.org/wiki/Cross-site_request_forgery



**NEW QUESTION: 47**
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?
**A.** Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
**B.** Manipulate format strings in text fields
**C.** SSH
**D.** SYN Flood
**Answer: (SHOW ANSWER)**
Explanation
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell.
One specific exploitation vector of the Shellshock bug is CGI-based web servers.
Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.
References:
https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

**NEW QUESTION: 48**
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 (LEAVE A REPLY)**
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: 49**
Bluetooth uses which digital modulation technique to exchange information between paired devices?
**A.** PSK (phase-shift keying)
**B.** FSK (frequency-shift keying)
**C.** ASK (amplitude-shift keying)
**D.** QAM (quadrature amplitude modulation)
**Answer: A (LEAVE A REPLY)**
Explanation
Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK.
References:
http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php

**NEW QUESTION: 50**
Bob is acknowledged as a hacker of repute and is popular among visitors of "underground" sites.
Bob is willing to share his knowledge with those who are willing to learn, and many have expressed their interest in learning from him. However, this knowledge has a risk associated with it, as it can be used for malevolent attacks as well.
In this context, what would be the most effective method to bridge the knowledge gap between the "black" hats or crackers and the "white" hats or computer security professionals? (Choose the test answer.)
**A.** Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.
**B.** Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.
**C.** Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

**D.** Hire more computer security monitoring personnel to monitor computer systems and networks.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 51**
Matthew, a black hat, has managed to open a meterpreter session to one of the kiosk machines in Evil Corp's lobby. He checks his current SID, which is S-1-5-21-1223352397-1872883824-861252104-501. What needs to happen before Matthew has full administrator access?
**A.** He needs to gain physical access.
**B.** He needs to disable antivirus protection.
**C.** He must perform privilege escalation.
**D.** He already has admin privileges, as shown by the "501" at the end of the SID.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 52**
You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?
**A.** Scan servers with MBSA
**B.** Scan servers with Nmap
**C.** Telent to every port on each server
**D.** Physically go to each server
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 53**
Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library? This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
**A.** Heartbleed Bug
**B.** SSL/TLS Renegotiation Vulnerability
**C.** POODLE
**D.** Shellshock
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 54**
Which of the following is a strong post designed to stop a car?
**A.** Gate
**B.** Bollard
**C.** Fence
**D.** Reinforced rebar
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 55**
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?
**A.** At least twice a year or after any significant upgrade or modification
**B.** At least once a year and after any significant upgrade or modification
**C.** At least once every two years and after any significant upgrade or modification
**D.** At least once every three years or after any significant upgrade or modification
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 56**
Why should the security analyst disable/remove unnecessary ISAPI filters?
**A.** To defend against webserver attacks
**B.** To defend against wireless attacks
**C.** To defend against jailbreaking
**D.** To defend against social engineering attacks
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 57**
What is the known plaintext attack used against DES which gives the result that encrypting plaintext with one DES key followed by encrypting it with a second DES key is no more secure than using a single key?
**A.** Meet-in-the-middle attack
**B.** Traffic analysis attack
**C.** Man-in-the-middle attack
**D.** Replay attack
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 58**
Which of the following is an application that requires a host application for replication?
**A.** Micro
**B.** Worm
**C.** Trojan
**D.** Virus
**Answer: D (LEAVE A REPLY)**
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: 59**
Which of the following is a protocol specifically designed for transporting event messages?
**A.** SYSLOG
**B.** SMS
**C.** SNMP
**D.** ICMP
**Answer: A (LEAVE A REPLY)**
Explanation
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.
References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

**NEW QUESTION: 60**
Which element of Public Key Infrastructure (PKI) verifies the applicant?
**A.** Registration authority
**B.** Verification authority
**C.** Certificate authority
**D.** Validation authority
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 61**
Which of the following tools are used for enumeration? (Choose three.)
**A.** Cheops
**B.** USER2SID
**C.** SolarWinds
**D.** DumpSec
**E.** SID2USER
**Answer: B,D,E (LEAVE A REPLY)**

**NEW QUESTION: 62**

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

What does the option * indicate?

**A.** a

**B.** n

**C.** s

**D.** t

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 63**

From the following table, identify the wrong answer in terms of Range (ft).

| Standard | Range (ft) |
|---|---|
| 802.11a | 150-150 |
| 802.11b | 150-150 |
| 802.11g | 150-150 |
| 802.16(WiMax) | 30 miles |

**A.** 802.11g

**B.** 802.11b

**C.** 802.11a

**D.** 802.16(WiMax)

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 64**

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 SSH and 10.240.250.23 is the server and 10.249.253.15 is the server

**C.** Application is FTP 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 client and 10.249.253.15 is the server
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 65**
Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?
**A.** Full disk encryption.
**B.** Password protected files
**C.** Hidden folders
**D.** BIOS password
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 66**
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.** 604800
**C.** 3600
**D.** 60
**E.** 2400
**F.** 4800
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 67**
What is a successful method for protecting a router from potential smurf attacks?
**A.** Disabling the router from accepting broadcast ping messages
**B.** Placing the router in broadcast mode
**C.** Enabling port forwarding on the router
**D.** Installing the router outside of the network's firewall
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 68**
Take a look at the following attack on a Web Server using obstructed URL:

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



How would you protect from these attacks?

**A.** Configure the Web Server to deny requests involving "hex encoded" characters

**B.** Enable Active Scripts Detection at the firewall and routers

**C.** Create rules in IDS to alert on strange Unicode requests

**D.** Use SSL authentication on Web Servers

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 69**

What is the purpose of DNS AAAA record?

**A.** Authorization, Authentication and Auditing record

**B.** IPv6 address resolution record

**C.** Address database record

**D.** Address prefix record

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 70**

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

**A.** Force all connections to use a username and password.

**B.** Block port 25 at the firewall.

**C.** Shut off the SMTP service on the server.

**D.** Switch from Windows Exchange to UNIX Sendmail.

**E.** None of the above.

**Answer: E (LEAVE A REPLY)**

**NEW QUESTION: 71**

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 (LEAVE A REPLY)**

**NEW QUESTION: 72**
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.** Non-Disclosure Agreement
**B.** Terms of Engagement
**C.** Project Scope
**D.** Service Level Agreement
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 73**
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.** Network sniffer
**D.** Protocol analyzer
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 74**
You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.
Which port would you see listening on these Windows machines in the network?
**A.** 445
**B.** 3389
**C.** 161
**D.** 1433
**Answer: A (LEAVE A REPLY)**
Explanation
The following ports are associated with file sharing and server message block (SMB) communications:
References: https://support.microsoft.com/en-us/kb/298804

**NEW QUESTION: 75**

Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days. Bob denies that he had ever sent a mail. What do you want to
""know"" to prove yourself that it was Bob who had send a mail?
**A.** Authentication
**B.** Confidentiality
**C.** Integrity
**D.** Non-Repudiation
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 76**
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: (SHOW ANSWER)**
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: 77**
The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?
**A.** Non-confidential

**B.** Confidential
**C.** Symmetric
**D.** Asymmetric
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 78**
Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?
**A.** AES 1024 bit strength
**B.** RSA 1024 bit strength
**C.** AES 512 bit strength
**D.** RSA 512 bit strength
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 79**
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?
**A.** Bob is partially right. DMZ does not make sense when a stateless firewall is available
**B.** Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one
**C.** Bob can be right since DMZ does not make sense when combined with stateless firewalls
**D.** Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 80**
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 (LEAVE A REPLY)**
Explanation
To upload files the user must have proper write file permissions.
References:
http://codex.wordpress.org/Hardening_WordPress

**NEW QUESTION: 81**
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
**A.** Announced
**B.** Grey-box
**C.** White-box
**D.** Black-box
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 82**
What statement is true regarding LM hashes?
**A.** LM hashes are based on AES128 cryptographic standard.
**B.** Uppercase characters in the password are converted to lowercase.
**C.** LM hashes consist in 48 hexadecimal characters.
**D.** LM hashes are not generated when the password length exceeds 15 characters.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 83**
What is the process of logging, recording, and resolving events that take place in an organization?
**A.** Incident Management Process
**B.** Security Policy
**C.** Internal Procedure
**D.** Metrics
**Answer: A (LEAVE A REPLY)**
Explanation
The activities within the incident management process include:
References:
https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

**NEW QUESTION: 84**
Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students.
He identified this when the IDS alerted for malware activities in the network.

What should Bob do to avoid this problem?
**A.** Separate students in a different VLAN
**B.** Ask students to use the wireless network
**C.** Disable unused ports in the switches
**D.** Use the 802.1x protocol
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 85**
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 an attack with a rainbow table.
**B.** Perform a hybrid attack.
**C.** Perform a dictionary attack.
**D.** Perform a brute force attack.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 86**
The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?
**A.** ACK
**B.** RST
**C.** SYN-ACK
**D.** SYN
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 87**
You are monitoring the network of your organizations. You notice that:
1. There are huge outbound connections from your Internal Network to External IPs.
2. On further investigation, you see that the External IPs are blacklisted.
3. Some connections are accepted, and some are dropped.
4. You find that it is a CnC communication.
Which of the following solution will you suggest?
**A.** Both B and C
**B.** Block the Blacklist IP's @ Firewall
**C.** Clean the Malware which are trying to Communicate with the External Blacklist IP's
**D.** Update the Latest Signatures on your IDS/IPS
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 88**
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 be either accepted or rejected form when an individual provides Identification and authentication information.
**B.** The amount of time and resources that are necessary to maintain a biometric system.
**C.** The amount of time it takes to convert biometric data into a template on a smart card.
**D.** How long it takes to setup individual user accounts.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 89**
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 a SYN
**B.** The port will ignore the packets
**C.** The port will send an ACK
**D.** The port will send an RST
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 90**
The following are types of Bluetooth attack EXCEPT_____?
**A.** Bluedriving
**B.** Bluejacking
**C.** Bluesmaking
**D.** Bluesnarfing
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 91**
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.** UPGRADETLS
**B.** FORCETLS
**C.** OPPORTUNISTICTLS STARTTLS
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 92**
Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?
**A.** SYN flooding
**B.** Ping of death
**C.** TCP hijacking
**D.** Smurf attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 93**
You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?
**A.** >host -t a hackeddomain.com
**B.** >host -t soa hackeddomain.com
**C.** >host -t ns hackeddomain.com
**D.** >host -t AXFR hackeddomain.com
**Answer: A (LEAVE A REPLY)**
Explanation
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.
References: https://en.wikipedia.org/wiki/List_of_DNS_record_types

**NEW QUESTION: 94**
Fingerprinting VPN firewalls is possible with which of the following tools?
**A.** Angry IP
**B.** Arp-scan
**C.** Nikto
**D.** Ike-scan
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 95**
What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?
**A.** Adware
**B.** Riskware
**C.** Ransomware
**D.** Spyware

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 96**
Destination unreachable administratively prohibited messages can inform the hacker to what?
**A.** That the network is functioning normally
**B.** That the packets are being malformed by the scanning software
**C.** That a circuit level proxy has been installed and is filtering traffic
**D.** That a router or other packet-filtering device is blocking traffic
**E.** That his/her scans are being blocked by a honeypot or jail
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 97**
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 (LEAVE A REPLY)**
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: 98**
env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?
**A.** Display passwd content to prompt
**B.** Removes the passwd file
**C.** Changes all passwords in passwd
**D.** Add new user to the passwd file
**Answer: A (LEAVE A REPLY)**

Explanation
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:
() {:;}; /bin/cat /etc/passwd
That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.
References: https://blog.cloudflare.com/inside-shellshock/

**NEW QUESTION: 99**
What is the main security service a cryptographic hash provides?
**A.** Integrity and collision resistance
**B.** Message authentication and collision resistance
**C.** Integrity and ease of computation
**D.** Integrity and computational in-feasibility
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 100**
Which method of password cracking takes the most time and effort?
**A.** Brute force
**B.** Rainbow tables
**C.** Dictionary attack
**D.** Shoulder surfing
**Answer: A (LEAVE A REPLY)**
Explanation
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.
References: https://en.wikipedia.org/wiki/Password_cracking

**NEW QUESTION: 101**
Which of the following lists are valid data-gathering activities associated with a risk assessment?
**A.** Threat identification, response identification, mitigation identification
**B.** Threat identification, vulnerability identification, control analysis
**C.** Attack profile, defense profile, loss profile
**D.** System profile, vulnerability identification, security determination
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 102**

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

**A.** Intuitive

**B.** Passive

**C.** Reactive

**D.** Detective

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 103**

What is the role of test automation in security testing?

**A.** It is an option but it tends to be very expensive.

**B.** It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

**C.** Test automation is not usable in security due to the complexity of the tests.

**D.** It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies.

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 104**

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 (LEAVE A REPLY)**

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: 105**

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 415

**B.** UDP 123

**C.** UDP 514

**D.** UDP 541

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 106**
Which of the following examples best represents a logical or technical control?
**A.** Heating and air conditioning
**B.** Corporate security policy
**C.** Security tokens
**D.** Smoke and fire alarms
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 107**
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: (SHOW ANSWER)**
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: 108**
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the corporate network. What tool should the analyst use to perform a Blackjacking attack?

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

**NEW QUESTION: 109**
To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.
What term is commonly used when referring to this type of testing?
**A.** Fuzzing
**B.** Randomizing
**C.** Mutating
**D.** Bounding
**Answer: A (LEAVE A REPLY)**
Explanation
Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.
References: https://en.wikipedia.org/wiki/Fuzz_testing

**NEW QUESTION: 110**
You work for Acme Corporation as Sales Manager. The company has tight network security restrictions. You are trying to steal data from the company's Sales database (Sales.xls) and transfer them to your home computer. Your company filters and monitors traffic that leaves from the internal network to the Internet. How will you achieve this without raising suspicion?
**A.** Encrypt the Sales.xls using PGP and e-mail it to your personal gmail account
**B.** Package the Sales.xls using Trojan wrappers and telnet them back your home computer

**C.** You can conceal the Sales.xls database in another file like photo.jpg or other files and send it out in an innocent looking email or file transfer using Steganography techniques
**D.** Change the extension of Sales.xls to sales.txt and upload them as attachment to your hotmail account
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 111**
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 (LEAVE A REPLY)**
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: 112**
Fingerprinting an Operating System helps a cracker because:
**A.** It informs the cracker of which vulnerabilities he may be able to exploit on your system
**B.** It opens a security-delayed window based on the port being scanned
**C.** It defines exactly what software you have installed
**D.** It doesn't depend on the patches that have been applied to fix existing security holes
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 113**
You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
**A.** hping2 --set-ICMP host.domain.com
**B.** hping2 -1 host.domain.com
**C.** hping2 host.domain.com
**D.** hping2 -i host.domain.com
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 114**

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.** Chosen plain-text attack
**C.** Memory trade-off attack
**D.** Replay attack
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 115**
Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?
**A.** Injecting arbitrary data
**B.** Analyzing service response
**C.** Port scanning
**D.** Banner grabbing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 116**
Which of the following business challenges could be solved by using a vulnerability scanner?
**A.** There is a monthly requirement to test corporate compliance with host application usage and security policies.
**B.** Auditors want to discover if all systems are following a standard naming convention.
**C.** A web server was compromised and management needs to know if any further systems were compromised.
**D.** There is an emergency need to remove administrator access from multiple machines for an employee that quit.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 117**
What port number is used by LDAP protocol?
**A.** 110
**B.** 445
**C.** 464
**D.** 389
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 118**
What kind of detection techniques is being used in antivirus softwares that identifies malware by collecting data from multiple protected systems and instead of analyzing files locally it's made on the premiers environment-
**A.** VCloud based

**B.** Honypot based
**C.** Heuristics based
**D.** Behaviour based
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 119**
On performing a risk assessment, you need to determine the potential impacts when some of the critical business process of the company interrupt its service. What is the name of the process by which you can determine those critical business?
**A.** Emergency Plan Response (EPR)
**B.** Disaster Recovery Planning (DRP)
**C.** Risk Mitigation
**D.** Business Impact Analysis (BIA)
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 120**
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 (LEAVE A REPLY)**
Explanation
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.
A possible solution to this danger is to conduct intermittent "unannounced" penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with "announced" penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.
References:
http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

**NEW QUESTION: 121**
Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?
**A.** DataThief
**B.** Cain and Abel
**C.** SQLInjector

**D.** NetCat
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 122**
When tuning security alerts, what is the best approach?
**A.** Decrease the false positives
**B.** Decrease False negatives
**C.** Rise False positives Rise False Negatives
**D.** Tune to avoid False positives and False Negatives
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 123**
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.** Firewalls
**B.** Host-based intrusion detection system (HIDS)
**C.** Honeypots
**D.** Network-based intrusion detection system (NIDS)
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 124**
Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?
**A.** Rootshock
**B.** Rootshell
**C.** Shellbash
**D.** Shellshock
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 125**

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.** The IDS will not distinguish among packets originating from different sources.
**C.** Thresholding interferes with the IDS' ability to reassemble fragmented packets.
**D.** Network packets are dropped if the volume exceeds the threshold.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 126**
Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?
**A.** ARP Proxy
**B.** Interceptor
**C.** Man-in-the-middle
**D.** Poisoning Attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 127**
Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by a coercion or torture?
**A.** Chosen-Cipher text Attack
**B.** Rubber Hose Attack
**C.** Timing Attack
**D.** Ciphertext-only Attack
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 128**
The "black box testing" methodology enforces which kind of restriction?
**A.** Only the external operation of a system is accessible to the tester.
**B.** Only the internal operation of a system is known to the tester.
**C.** The internal operation of a system is only partly accessible to the tester.
**D.** The internal operation of a system is completely known to the tester.
**Answer: A (LEAVE A REPLY)**
Explanation
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.
References: https://en.wikipedia.org/wiki/Black-box_testing

**NEW QUESTION: 129**
Which of the below hashing functions are not recommended for use?
**A.** MD5. SHA-5
**B.** SHA-2. SHA-3
**C.** MD5, SHA-1
**D.** SHA-1.ECC
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 130**
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?
**A.** Nmap
**B.** Nikto
**C.** Armitage
**D.** Metasploit
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 131**
Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?
**A.** Containment phase
**B.** Identification phase
**C.** Recovery phase
**D.** Preparation phase
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 132**
Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?
**A.** Malicious code is attempting to execute instruction in a non-executable memory region.
**B.** A page fault is occurring, which forces the operating system to write data from the hard drive.
**C.** A race condition is being exploited, and the operating system is containing the malicious process.
**D.** Malware is executing in either ROM or a cache memory area.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 133**

Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning.
What should Bob recommend to deal with such a threat?
**A.** Client awareness
**B.** The use of security agents in clients' computers
**C.** The use of DNSSEC
**D.** The use of double-factor authentication
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 134**
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.** Single quotation
**B.** Semicolon
**C.** Backslash
**D.** Double quotation
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 135**
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80.
The engineer receives this output:

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

Which of the following is an example of what the engineer performed?
**A.** Cross-site scripting
**B.** SQL injection
**C.** Whois database query
**D.** Banner grabbing
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 136**
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 (LEAVE A REPLY)**
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: 137**
This phase will increase the odds of success in later phases of the penetration test. It is also the very first step in Information Gathering, and it will tell you what the "landscape" looks like. What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?
**A.** footprinting
**B.** network mapping
**C.** gaining access
**D.** escalating privileges
**Answer: A (LEAVE A REPLY)**
Explanation
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.
References:
http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

**NEW QUESTION: 138**
Which of the following Secure Hashing Algorithm (SHA) produces a 160-bit digest from a message with a maximum length of (264-1) bits and resembles the MD5 algorithm?
**A.** SHA-1

**B.** SHA-0
**C.** SHA-3
**D.** SHA-2
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 139**
Which of the following is designed to identify malicious attempts to penetrate systems?
**A.** Intrusion Detection System
**B.** Firewall
**C.** Proxy
**D.** Router
**Answer: (SHOW ANSWER)**
Explanation
An intrusion detection system (IDS) is a device or software application that monitors network or system activities for malicious activities or policy violations and produces electronic reports to a management station.
References: https://en.wikipedia.org/wiki/Intrusion_detection_system

**NEW QUESTION: 140**
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 (LEAVE A REPLY)**
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: 141**
Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.
If these switches' ARP cache is successfully flooded, what will be the result?
**A.** The switches will drop into hub mode if the ARP cache is successfully flooded.

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

**NEW QUESTION: 142**
A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.
In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?
**A.** Single quote
**B.** Semicolon
**C.** Double quote
**D.** Exclamation mark
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 143**
Which of the following is a component of a risk assessment?
**A.** Logical interface
**B.** DMZ
**C.** Administrative safeguards
**D.** Physical security
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 144**
The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.
What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?
**A.** Private
**B.** Public
**C.** Shared
**D.** Root
**Answer: (SHOW ANSWER)**
Explanation
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the

confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.
An attack may also reveal private keys of compromised parties.
References: https://en.wikipedia.org/wiki/Heartbleed

**NEW QUESTION: 145**
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-one mapping.
**C.** A static NAT uses a many-to-one mapping.
**D.** A static NAT uses a one-to-many mapping.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 146**
Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain?
**A.** [site:]
**B.** [link:]
**C.** [cache:]
**D.** [inurl:]
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 147**
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
**A.** Reload from a previous backup
**B.** Reload from known good media
**C.** Delete the files and try to determine the source
**D.** Perform a trap and trace
**E.** Copy the system files from a known good system
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 148**
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.** tracert
**B.** nmap
**C.** tcpdump
**D.** ping
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 149**
Every company needs a formal written document which spells out to employees precisely what they are allowed to use the company's systems for, what is prohibited, and what will happen to them if they break the rules. Two printed copies of the policy should be given to every employee as soon as possible after they join the organization. The employee should be asked to sign one copy, which should be safely filed by the company. No one should be allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?
**A.** Information Audit Policy (IAP)
**B.** Information Security Policy (ISP)
**C.** Company Compliance Policy (CCP)
**D.** Penetration Testing Policy (PTP)
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 150**
What is the algorithm used by LM for Windows2000 SAM?
**A.** MD4
**B.** SSL
**C.** SHA
**D.** DES
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 151**
When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?
**A.** The key entered is a hash that is used to prove the integrity of the wireless data.
**B.** The key entered is a symmetric key used to encrypt the wireless data.
**C.** The key entered is based on the Diffie-Hellman method.
**D.** The key is an RSA key used to encrypt the wireless data.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 152**
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 (LEAVE A REPLY)**
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: 153**
Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?
**A.** Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
**B.** Configure the firewall to allow traffic on TCP port 8080.
**C.** Configure the firewall to allow traffic on TCP port 53.
**D.** Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 154**
You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity, what tool would you most likely select?
**A.** Nmap
**B.** Nessus
**C.** Cain & Abel
**D.** Snort
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 155**
Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

**A.** SAINT scripting engine
**B.** Metasploit scripting engine
**C.** Nessus scripting engine
**D.** NMAP scripting engine
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 156**
A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?
**A.** Share full reports, not redacted
**B.** Share full reports with redactions
**C.** Decline but, provide references
**D.** Share reports, after NDA is signed
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 157**
A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.
Which of the following programming languages would most likely be used?
**A.** C#
**B.** Python
**C.** ASP.NET
**D.** PHP
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 158**
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?
**A.** TCP Connect scan
**B.** TCP SYN
**C.** Spoof Scan
**D.** Idle Scan
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 159**
The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk.

The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).
What is the closest approximate cost of this replacement and recovery operation per year?
**A.** $146
**B.** $1320
**C.** $440
**D.** $100
**Answer: (SHOW ANSWER)**
Explanation
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).
Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.
In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.
References: https://en.wikipedia.org/wiki/Annualized_loss_expectancy

**NEW QUESTION: 160**
Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?
**A.** Speed
**B.** Key distribution
**C.** Security
**D.** Scalability
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 161**
What would you enter, if you wanted to perform a stealth scan using Nmap?
**A.** nmap -sT
**B.** nmap -sS
**C.** nmap -sU
**D.** nmap -sM
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 162**
What is not a PCI compliance recommendation?
**A.** Use encryption to protect all transmission of card holder data over any public network.
**B.** Use a firewall between the public network and the payment card data.
**C.** Limit access to card holder data to as few individuals as possible.
**D.** Rotate employees handling credit card transactions on a yearly basis to different departments.

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 163**
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 *s
**B.** nessus +
**C.** nessus -d
**D.** nessus &
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 164**
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.** Brute-force attack
**B.** Dictionary attack
**C.** Man-in-the-middle attack
**D.** Session hijacking
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 165**
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed.
Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?

```
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT      STATE         SERVICE
21/tcp      open        ftp
23/tcp      open        telnet
80/tcp      open        http
139/tcp     open        netbios-ssn
515/tcp     open
631/tcp     open        ipp
9100/tcp    open
MAC Address: 00:00:48:0D:EE:89
```



**A.** The host is likely a printer.
**B.** The host is likely a Windows machine.
**C.** The host is likely a Linux machine.

**D.** The host is likely a router.

**Answer: A (LEAVE A REPLY)**

Explanation

The Internet Printing Protocol (IPP) uses port 631.

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

**NEW QUESTION: 166**

The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

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

What is most likely taking place?

**A.** Port scan of 192.168.1.106

**B.** Remote service brute force attempt

**C.** Denial of service attack on 192.168.1.106

**D.** Ping sweep of the 192.168.1.106 network

**Answer: B (LEAVE A REPLY)**



**NEW QUESTION: 167**

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.port == 25 and ip.host == 192.168.0.125

**B.** tcp.src == 25 and ip.host == 192.168.0.125

**C.** port 25 and host 192.168.0.125

**D.** host 192.168.0.125:25

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 168**

An NMAP scan of a server shows port 25 is open. What risk could this pose?
**A.** Clear text authentication
**B.** Web portal data leak
**C.** Active mail relay
**D.** Open printer sharing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 169**
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.** Passive information gathering
**C.** Vulnerability assessment
**D.** Active information gathering
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 170**
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 -sT -p0-65535 192.168.0/16
**C.** NMAP -P0 -A -O -p1-65535 192.168.0/24
**D.** NMAP -PN -O -sS -p 1-1024 192.168.0/8
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 171**
Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?
**A.** MD4
**B.** MD5
**C.** HAVAL
**D.** SHA-1
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 172**

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.** Nessus
**B.** Maltego
**C.** Metasploit
**D.** Wireshark
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 173**
What is the proper response for a NULL scan if the port is closed?

**A.** PSH
**B.** No response
**C.** FIN
**D.** ACK
**E.** SYN
**F.** RST
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 174**
Which is the first step followed by Vulnerability Scanners for scanning a network?

**A.** TCP/UDP Port scanning
**B.** Checking if the remote host is alive
**C.** Firewall detection
**D.** OS Detection
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 175**
This TCP flag instructs the sending system to transmit all buffered data immediately.

**A.** RST
**B.** PSH
**C.** SYN
**D.** FIN
**E.** URG
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 176**
You work as a Security Analyst for a retail organization. In securing the company's network, you set up a firewall and an IDS. However, hackers are able to attack the network. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

**A.** False Negative
**B.** False Positive
**C.** True Negative
**D.** True Positive
**Answer: (SHOW ANSWER)**
Explanation
A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.
References:
https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

**NEW QUESTION: 177**
The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?
**A.** Multiple keys for non-repudiation of bulk data
**B.** The same key on each end of the transmission medium
**C.** Bulk encryption for data transmission over fiber
**D.** Different keys on both ends of the transport medium
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 178**
Which of the following will perform an Xmas scan using NMAP?
**A.** nmap -sV 192.168.1.254
**B.** nmap -sA 192.168.1.254
**C.** nmap -sX 192.168.1.254
**D.** nmap -sP 192.168.1.254
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 179**
How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?
**A.** Defeating the scanner from detecting any code change at the kernel
**B.** Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
**C.** Performing common services for the application process and replacing real applications with fake ones
**D.** Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 180**
How does the Address Resolution Protocol (ARP) work?

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

**NEW QUESTION: 181**
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 negative
**B.** True negative
**C.** True positve
**D.** False positive
**Answer: D (LEAVE A REPLY)**



**NEW QUESTION: 182**

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

**NEW QUESTION: 183**
Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?
**A.** BeEF
**B.** NMAP
**C.** Metasploit
**D.** Nessus
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 184**
Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?
**A.** CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.
**B.** CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
**C.** CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
**D.** CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 185**
Which of the following steps for risk assessment methodology refers to vulnerability identification?
**A.** Identifies sources of harm to an IT system. (Natural, Human. Environmental)

**B.** Determines if any flaws exist in systems, policies, or procedures
**C.** Determines risk probability that vulnerability will be exploited (High. Medium, Low)
**D.** Assigns values to risk probabilities; Impact values.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 186**
What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?
**A.** All are tools that are only effective against Linux
**B.** All are tools that can be used not only by hackers, but also security personnel
**C.** All are hacking tools developed by the legion of doom
**D.** All are DDOS tools
**E.** All are tools that are only effective against Windows
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 187**
A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.
What kind of Web application vulnerability likely exists in their software?
**A.** Cross-site scripting vulnerability
**B.** Cross-site Request Forgery vulnerability
**C.** SQL injection vulnerability
**D.** Web site defacement vulnerability
**Answer: (SHOW ANSWER)**
Explanation
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as <b>very</b> large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.
References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

**NEW QUESTION: 188**
Which tool can be used to silently copy files from USB devices?
**A.** USB Dumper
**B.** USB Grabber
**C.** USB Sniffer

**D.** USB Snoopy
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 189**
Windows LAN Manager (LM) hashes are known to be weak.
Which of the following are known weaknesses of LM? (Choose three.)
**A.** Effective length is 7 characters.
**B.** Hashes are sent in clear text over the network.
**C.** Converts passwords to uppercase.
**D.** Makes use of only 32-bit encryption.
**Answer: A,B,C (LEAVE A REPLY)**

**NEW QUESTION: 190**
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.** Forcing the targeted key stream through a hardware-accelerated device such as an ASIC.
**C.** Extraction of cryptographic secrets through coercion or torture.
**D.** A backdoor placed into a cryptographic algorithm by its creator.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 191**
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 (LEAVE A REPLY)**
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: 192**

Least privilege is a security concept that requires that a user is
**A.** limited to those functions required to do the job.
**B.** given root or administrative privileges.
**C.** trusted to keep all data and access to that data under their sole control.
**D.** given privileges equal to everyone else in the department.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 193**
Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?
**A.** wwwroot
**B.** har.txt
**C.** SAM file
**D.** Repair file
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 194**
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.** Masquerading
**C.** Tailgating
**D.** Whaling
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 195**
Which cipher encrypts the plain text digit (bit or byte) one by one?
**A.** Block cipher
**B.** Stream cipher
**C.** Classical cipher
**D.** Modern cipher
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 196**
Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?
**A.** The attacker is trying to detect machines on the network which have SSL enabled
**B.** It is a worm that is malfunctioning or hardcoded to scan on port 500

**C.** The attacker is trying to determine the type of VPN implementation and checking for IPSec
**D.** It is a network fault and the originating machine is in a network loop
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 197**
A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?
**A.** Social engineering
**B.** Tailgating
**C.** Man trap
**D.** Shoulder surfing
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 198**
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.** Gray Hat
**B.** Black Hat
**C.** White Hat
**D.** Suicide Hacker
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 199**
What hacking attack is challenge/response authentication used to prevent?
**A.** Session hijacking attacks
**B.** Replay attacks
**C.** Scanning attacks

**D.** Password cracking attacks
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 200**
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 and Software Keyloggers.
**B.** Hardware, Software, and Sniffing.
**C.** Software only, they are the most effective.
**D.** Passwords are always best obtained using Hardware key loggers.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 201**
During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?
**A.** The tester must capture the WPA2 authentication handshake and then crack it.
**B.** The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.
**C.** The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
**D.** The tester must use the tool inSSIDer to crack it using the ESSID of the network.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 202**
A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?
**A.** Transfer type=ns
**B.** Set type=ns
**C.** Locate type=ns
**D.** Request type=ns
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 203**
Analyst is investigating proxy logs and found out that one of the internal user visited website storing suspicious Java scripts. After opening one of them, he noticed that it is very hard to

understand the code and that all codes differ from the typical Java script. What is the name of this technique to hide the code and extend analysis time?

**A.** Code encoding

**B.** Steganography

**C.** Encryption

**D.** Obfuscation

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 204**

What are two things that are possible when scanning UDP ports? (Choose two.)

**A.** The four-way handshake will not be completed

**B.** Nothing

**C.** A reset will be returned

**D.** An RFC 1294 message will be returned

**E.** An ICMP message will be returned

**Answer: B,E (LEAVE A REPLY)**

**NEW QUESTION: 205**

In the context of password security, a simple dictionary attack involves loading a dictionary file (a text file full of dictionary words) into a cracking application such as L0phtCrack or John the Ripper, and running it against user accounts located by the application. The larger the word and word fragment selection, the more effective the dictionary attack is. The brute force method is the most inclusive, although slow. It usually tries every possible letter and number combination in its automated exploration. If you would use both brute force and dictionary methods combined together to have variation of words, what would you call such an attack?

**A.** Full Blown

**B.** Hybrid

**C.** Thorough

**D.** BruteDics

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 206**

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.** 1025 bit key

**B.** 768 bit key

**C.** 1536 bit key

**D.** 2048 bit key

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 207**

An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?
**A.** Reverse Social Engineering
**B.** Announced
**C.** Piggybacking
**D.** Tailgating
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 208**
How do employers protect assets with security policies pertaining to employee surveillance activities?
**A.** Employers use informal verbal communication channels to explain employee monitoring activities to employees.
**B.** Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
**C.** Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.
**D.** Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 209**
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.** He needs to add the command ""ip address"" just before the IP address.
**B.** The network must be down and the nmap command and IP address are ok.
**C.** He needs to change the address to 192.168.1.0 with the same mask.
**D.** 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.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 210**
Which address translation scheme would allow a single public IP address to always correspond to a single machine on an internal network, allowing "server publishing"?
**A.** Overloading Port Address Translation
**B.** Dynamic Network Address Translation

**C.** Static Network Address Translation
**D.** Dynamic Port Address Translation
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 211**
Which of the following describes the characteristics of a Boot Sector Virus?
**A.** Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR
**B.** Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
**C.** Modifies directory table entries so that directory entries point to the virus code instead of the actual program
**D.** Overwrites the original MBR and only executes the new virus code
**Answer: (SHOW ANSWER)**
Explanation
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR). The virus moves the boot sector to another location on the hard drive.
References: https://www.techopedia.com/definition/26655/boot-sector-virus



**NEW QUESTION: 212**
"Testing the network using the same methodologies and tools employed by attackers"

Identify the correct terminology that defines the above statement.
**A.** Designing Network Security
**B.** Security Policy Implementation
**C.** Vulnerability Scanning
**D.** Penetration Testing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 213**
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 CONFIG
**B.** NET USE
**C.** NET VIEW
**D.** NET FILE
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 214**
It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.
Which of the following terms best matches the definition?
**A.** Bluetooth
**B.** Radio-Frequency Identification
**C.** WLAN
**D.** InfraRed
**Answer: A (LEAVE A REPLY)**
Explanation
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.
References:
http://www.bbc.co.uk/webwise/guides/about-bluetooth

**NEW QUESTION: 215**
A medium-sized healthcare IT business decides to implement a risk management strategy.
Which of the following is NOT one of the five basic responses to risk?
**A.** Delegate
**B.** Avoid
**C.** Mitigate
**D.** Accept
**Answer: A (LEAVE A REPLY)**
Explanation
There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.
References:
http://www.dbpmanagement.com/15/5-ways-to-manage-risk

**NEW QUESTION: 216**
How does a denial-of-service attack work?
**A.** A hacker tries to decipher a password by using a system, which subsequently crashes the network

**B.** A hacker attempts to imitate a legitimate user by confusing a computer or even another person
**C.** A hacker uses every character, word, or letter he or she can think of to defeat authentication
**D.** A hacker prevents a legitimate user (or group of users) from accessing a service
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 217**
When a security analyst prepares for the formal security assessment - what of the following should be done in order to determine inconsistencies in the secure assets database and verify that system is compliant to the minimum security baseline?
**A.** Source code review
**B.** Interviewing employees and network engineers
**C.** Reviewing the firewalls configuration
**D.** Data items and vulnerability scanning
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 218**
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?
**A.** Disable all routing protocols and only use static routes.
**B.** Make sure that legitimate network routers are configured to run routing protocols with authentication.
**C.** Redirection of the traffic cannot happen unless the admin allows it explicitly.
**D.** Only using OSPFv3 will mitigate this risk.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 219**
How can a policy help improve an employee's security awareness?
**A.** By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths
**B.** By implementing written security procedures, enabling employee security training, and promoting the benefits of security
**C.** By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
**D.** By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 220**

Which of the following DoS tools is used to attack target web applications by starvation of available sessions on the web server?
The tool keeps sessions at halt using never-ending POST transmissions and sending an arbitrarily large content-length header value.
**A.** LOIC
**B.** My Doom
**C.** R-U-Dead-Yet?(RUDY)
**D.** Astacheldraht
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 221**
Which of the following is considered as one of the most reliable forms of TCP scanning?
**A.** NULL Scan
**B.** Xmas Scan
**C.** Half-open Scan
**D.** TCP Connect/Full Open Scan
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 222**
Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?
**A.** He can send an IP packet with the SYN bit and the source address of his computer.
**B.** Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
**C.** Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
**D.** Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 223**
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 (LEAVE A REPLY)**

**NEW QUESTION: 224**

What kind of risk will remain even if all theoretically possible safety measures would be applied?

**A.** Deferred risk

**B.** Inherent risk

**C.** Residual risk

**D.** Impact risk

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 225**

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.** Classic SQLi

**C.** Compound SQLi

**D.** DMS-specific SQLi

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 226**

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

**A.** Trojan

**B.** Scanner

**C.** DoS tool

**D.** Backdoor

**E.** RootKit

**Answer: (SHOW ANSWER)**



**NEW QUESTION: 227**

Which security control role does encryption meet?

**A.** Detective

**B.** Preventative

**C.** Defensive

**D.** Offensive
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 228**
At a Windows Server command prompt, which command could be used to list the running services?
**A.** Sc query \\servername
**B.** Sc query type= running
**C.** Sc config
**D.** Sc query
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 229**
During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?
**A.** Invoking the stored procedure xp_shell to spawn a Windows command shell
**B.** Using the Metasploit psexec module setting the SA / Admin credential
**C.** Invoking the stored procedure cmd_shell to spawn a Windows command shell
**D.** Invoking the stored procedure xp_cmdshell to spawn a Windows command shell
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 230**
While performing ping scans into a target network you get a frantic call from the organization's security team.
They report that they are under a denial of service attack. When you stop your scan, the smurf attack event stops showing up on the organization's IDS monitor.
How can you modify your scan to prevent triggering this event in the IDS?
**A.** Spoof the source IP address.
**B.** Scan more slowly.
**C.** Do not scan the broadcast IP.
**D.** Only scan the Windows systems.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 231**
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.** Download and Install Netcat
**B.** Disable Key Services
**C.** Disable IPTables
**D.** Create User Account

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 232**
The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?
**A.** network Sniffer
**B.** Vulnerability Scanner
**C.** Security incident and event Monitoring
**D.** Intrusion prevention Server
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 233**
Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?
**A.** Validate and escape all information sent to a server
**B.** Use security policies and procedures to define and implement proper security settings
**C.** Verify access right before allowing access to protected information and UI controls
**D.** Use digital certificates to authenticate a server prior to sending data
**Answer: A (LEAVE A REPLY)**
Explanation
Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.
References:
https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

**NEW QUESTION: 234**
Which of the following is a preventive control?
**A.** Continuity of operations plan
**B.** Audit trail
**C.** Security policy
**D.** Smart card authentication
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 235**
Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?
**A.** Certificate issuance
**B.** Certificate revocation
**C.** Certificate cryptography

**D.** Certificate validation
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 236**
A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21.
During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?
**A.** True positives
**B.** False negatives
**C.** True negatives
**D.** False positives
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 237**
Which of the following is a hashing algorithm?
**A.** ROT13
**B.** DES
**C.** MD5
**D.** PGP
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 238**
Cross-site request forgery involves:
**A.** A server making a request to another server without the user's knowledge
**B.** A request sent by a malicious user from a browser to a server
**C.** Modification of a request by a proxy between client and server
**D.** A browser making a request to a server without the user's knowledge
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 239**
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 malware scanner
**C.** a vulnerability scanner
**D.** a virus scanner
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 240**

You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at
192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
**A.** list server=192.168.10.2 type=all
**B.** List domain=Abccorp.local type=zone
**C.** is-d abccorp.local
**D.** Iserver 192.168.10.2-t all
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 241**
The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?
**A.** Injection
**B.** Cross Site Scripting
**C.** Cross Site Request Forgery
**D.** Path disclosure
**Answer: A (LEAVE A REPLY)**
Explanation
The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.
Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
References: https://www.owasp.org/index.php/Top_10_2013-Top_10



**NEW QUESTION: 242**
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 (LEAVE A REPLY)**
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: 243**
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends "many" IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually:
**A.** A behavior-based IDS
**B.** A signature-based IDS
**C.** A hybrid IDS
**D.** Just a network monitoring tool
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 244**
What does a type 3 code 13 represent? (Choose two.)
**A.** Port unreachable
**B.** Network unreachable
**C.** Echo request
**D.** Administratively prohibited
**E.** Destination unreachable
**F.** Time exceeded
**Answer: D,E (LEAVE A REPLY)**

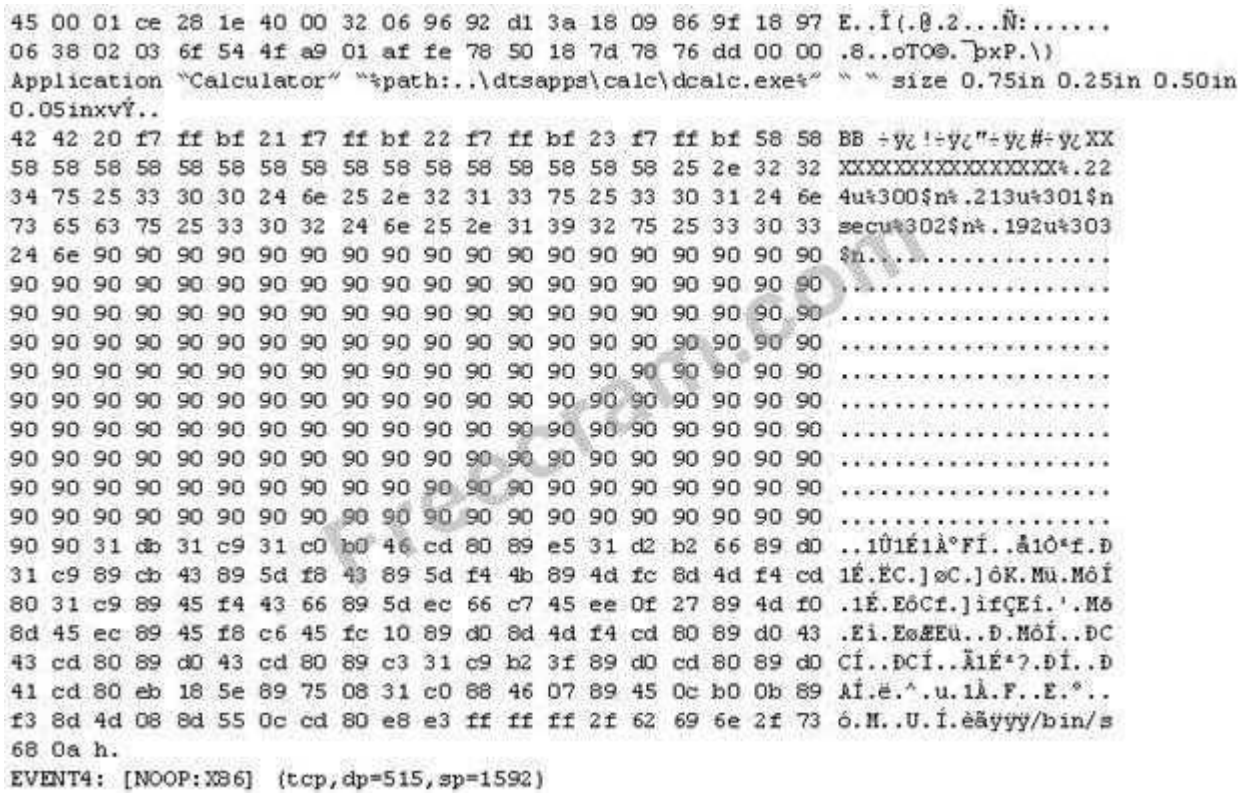
**NEW QUESTION: 245**
A person approaches a network administrator and wants advice on how to send encrypted email from home.
The end user does not want to have to pay for any license fees or manage server services.
Which of the following is the most secure encryption protocol that the network administrator should recommend?
**A.** IP Security (IPSEC)
**B.** Multipurpose Internet Mail Extensions (MIME)
**C.** Pretty Good Privacy (PGP)
**D.** Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 246**
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.** Traceroute
**B.** Hping
**C.** Broadcast ping
**D.** TCP ping
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 247**
Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?
**A.** Fast processor to help with network traffic analysis
**B.** They must be dual-homed
**C.** Similar RAM requirements
**D.** Fast network interface cards
**Answer: B (LEAVE A REPLY)**
Explanation
Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.
References: https://en.wikipedia.org/wiki/Dual-homed

**NEW QUESTION: 248**
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.
As an analyst what would you conclude about the attack?




**A.** The buffer overflow attack has been neutralized by the IDS

**B.** The attacker is attempting a buffer overflow attack and has succeeded

**C.** The attacker is attempting an exploit that launches a command-line shell

**D.** The attacker is creating a directory on the compromised machine

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 249**

Jack was attempting to fingerprint all machines in the network using the following Nmap syntax:

invictus@victim_server:~$ nmap -T4 -0 10.10.0.0/24

TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!

Obviously, it is not going through. What is the issue here?

**A.** The nmap syntax is wrong.

**B.** This is a common behavior for a corrupted nmap application

**C.** The outgoing TCP/IP fingerprinting is blocked by the host firewall

**D.** OS Scan requires root privileges

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 250**

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.** Bring the discovery to the financial organization's human resource department.
**C.** Stop work immediately and contact the authorities.
**D.** Delete the pornography, say nothing, and continue security testing.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 251**
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 (LEAVE A REPLY)**

**NEW QUESTION: 252**
Which of the following statements is TRUE?
**A.** Sniffers operate on Layer 3 of the OSI model
**B.** Sniffers operate on Layer 2 of the OSI model
**C.** Sniffers operate on both Layer 2 & Layer 3 of the OSI model.
**D.** Sniffers operate on the Layer 1 of the OSI model.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 253**
What is the following command used for?
net use \targetipc$ "" /u:""
**A.** This command is used to connect as a null session
**B.** Grabbing the SAM
**C.** Connecting to a Linux computer through Samba.
**D.** Grabbing the etc/passwd file
**E.** Enumeration of Cisco routers
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 254**
Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?
**A.** 161
**B.** 3389
**C.** 445
**D.** 1433
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 255**

If the final set of security controls does not eliminate all risk in a system, what could be done next?

**A.** If the residual risk is low enough, it can be accepted.

**B.** Continue to apply controls until there is zero risk.

**C.** Ignore any remaining risk.

**D.** Remove current controls since they are not completely effective.

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 256**

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

**A.** a bypass regulator.

**B.** a covert channel.

**C.** asymmetric routing.

**D.** steganography.

**Answer: (SHOW ANSWER)**



**NEW QUESTION: 257**

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

**A.** security.

**B.** operability.

**C.** non-repudiation.

**D.** usability.

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 258**

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

**A.** The internal operation of a system is only partly accessible to the tester.

**B.** The internal operation of a system is completely known to the tester.

**C.** Only the external operation of a system is accessible to the tester.

**D.** Only the internal operation of a system is known to the tester.

**Answer: A (LEAVE A REPLY)**

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

**NEW QUESTION: 259**
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.** Network-based IDS
**B.** Host-based IDS
**C.** Open source-based
**D.** Gateway-based IDS
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 260**
A zone file consists of which of the following Resource Records (RRs)?
**A.** SOA, NS, AXFR, and MX records
**B.** DNS, NS, PTR, and MX records
**C.** SOA, NS, A, and MX records
**D.** DNS, NS, AXFR, and MX records
**Answer: C (LEAVE A REPLY)**

# ECCouncil.312-50v11.v2021-04-21.q129

| | |
|---|---|
| **Exam Code:** | 312-50v11 |
| **Exam Name:** | Certified Ethical Hacker Exam |
| **Certification Provider:** | ECCouncil |
| **Free Question Number:** | 129 |
| **Version:** | v2021-04-21 |
| **# of views:** | 105 |
| **# of Questions views:** | 1327 |

https://www.freecram.com/torrent/ECCouncil.312-50v11.v2021-04-21.q129.html

**NEW QUESTION: 1**
Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?
**A.** 123
**B.** 113
**C.** 69
**D.** 161
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 2**
Which of the following tools are used for enumeration? (Choose three.)
**A.** USER2SID
**B.** DumpSec
**C.** Cheops
**D.** SID2USER
**E.** SolarWinds
**Answer: A,B,D (LEAVE A REPLY)**

**NEW QUESTION: 3**
Which of the following program infects the system boot sector and the executable files at the same time?
**A.** Polymorphic virus
**B.** Multipartite Virus
**C.** Stealth virus
**D.** Macro virus
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 4**
You receive an e-mail like the one shown below. When you click on the link contained in the mail, you are redirected to a website seeking you to download free Anti-Virus software.

Dear valued customers,
We are pleased to announce the newest version of Antivirus 2010 for Windows which will probe you with total security against the latest spyware, malware, viruses, Trojans and other online threats. Simply visit the link below and enter your antivirus code:



or you may contact us at the following address:
Media Internet Consultants, Edif. Neptuno, Planta
Baja, Ave. Ricardo J. Alfaro, Tumba Muerto, n/a Panama
How will you determine if this is Real Anti-Virus or Fake Anti-Virus website?
**A.** Connect to the site using SSL, if you are successful then the website is genuine
**B.** Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
**C.** Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site
**D.** Look at the website design, if it looks professional then it is a Real Anti-Virus website
**E.** Download and install Anti-Virus software from this suspicious looking site, your Windows 7 will prompt you and stop the installation if the downloaded file is a malware
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 5**
If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use?
**A.** -r
**B.** -F
**C.** -P
**D.** -sP
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 6**
Robin, a professional hacker, targeted an organization's network to sniff all the traffic. During this process.
Robin plugged in a rogue switch to an unused port in the LAN with a priority lower than any other switch in the network so that he could make it a root bridge that will later allow him to sniff all the traffic in the network.
What is the attack performed by Robin in the above scenario?
**A.** ARP spoofing attack

**B.** DNS poisoning attack
**C.** STP attack
**D.** VLAN hopping attack
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 7**
Your company was hired by a small healthcare provider to perform a technical assessment on the network.
What is the best approach for discovering vulnerabilities on a Windows-based computer?
**A.** Create a disk image of a clean Windows installation
**B.** Use a scan tool like Nessus
**C.** Check MITRE.org for the latest list of CVE findings
**D.** Use the built-in Windows Update tool
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 8**
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.** Client is configured for the wrong channel
**C.** The client cannot see the SSID of the wireless network
**D.** The wireless client is not configured to use DHCP
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 9**
What is the first step for a hacker conducting a DNS cache poisoning (DNS spoofing) attack against an organization?
**A.** The attacker queries a nameserver using the DNS resolver.
**B.** The attacker forges a reply from the DNS resolver.
**C.** The attacker makes a request to the DNS resolver.
**D.** The attacker uses TCP to poison the ONS resofver.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 10**
Eve is spending her day scanning the library computers. She notices that Alice is using a computer whose port
445 is active and listening. Eve uses the ENUM tool to enumerate Alice machine. From the command prompt, she types the following command.

```
For /f "tokens=1 %%a in (hackfile.txt) do net use *
\\10.1.2.3\c$ /user:"Administrator" %%a
```

What is Eve trying to do?

**A.** Eve is trying to connect as a user with Administrator privileges

**B.** Eve is trying to enumerate all users with Administrative privileges

**C.** Eve is trying to carry out a password crack for user Administrator

**D.** Eve is trying to escalate privilege of the null user to that of Administrator

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 11**

What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

**A.** All are tools that are only effective against Windows

**B.** All are tools that are only effective against Linux

**C.** All are tools that can be used not only by hackers, but also security personnel

**D.** All are hacking tools developed by the legion of doom

**E.** All are DDOS tools

**Answer: E (LEAVE A REPLY)**

**NEW QUESTION: 12**

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

**A.** EU Safe Harbor

**B.** PCI-DSS

**C.** HIPAA

**D.** NIST-800-53

**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 13**

You have been authorized to perform a penetration test against a website. You want to use Google dorks to footprint the site but only want results that show file extensions. What Google dork operator would you use?

**A.** ext

**B.** site

**C.** filetype

**D.** inurl

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 14**

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

**A.** Net use

**B.** Netstat

**C.** Netsh
**D.** Net use connection
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 15**
You have successfully logged on a Linux system. You want to now cover your trade Your login attempt may be logged on several files located in /var/log. Which file does NOT belongs to the list:
**A.** user.log
**B.** auth.fesg
**C.** wtmp
**D.** btmp
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 16**
infecting a system with malware and using phishing to gain credentials to a system or web application are examples of which phase of the ethical hacking methodology?
**A.** Reconnaissance
**B.** Maintaining access
**C.** Scanning
**D.** Gaming access
**Answer: D (LEAVE A REPLY)**
Explanation
This phase having the hacker uses different techniques and tools to realize maximum data from the system.
they're -* Password cracking - Methods like Bruteforce, dictionary attack, rule-based attack, rainbow table are used. Bruteforce is trying all combinations of the password. Dictionary attack is trying an inventory of meaningful words until the password matches. Rainbow table takes the hash value of the password and compares with pre-computed hash values until a match is discovered.* Password attacks - Passive attacks like wire sniffing, replay attack. Active online attack like Trojans, keyloggers, hash injection, phishing. Offline attacks like pre-computed hash, distributed network and rainbow. Non electronic attack like shoulder surfing, social engineering and dumpster diving.

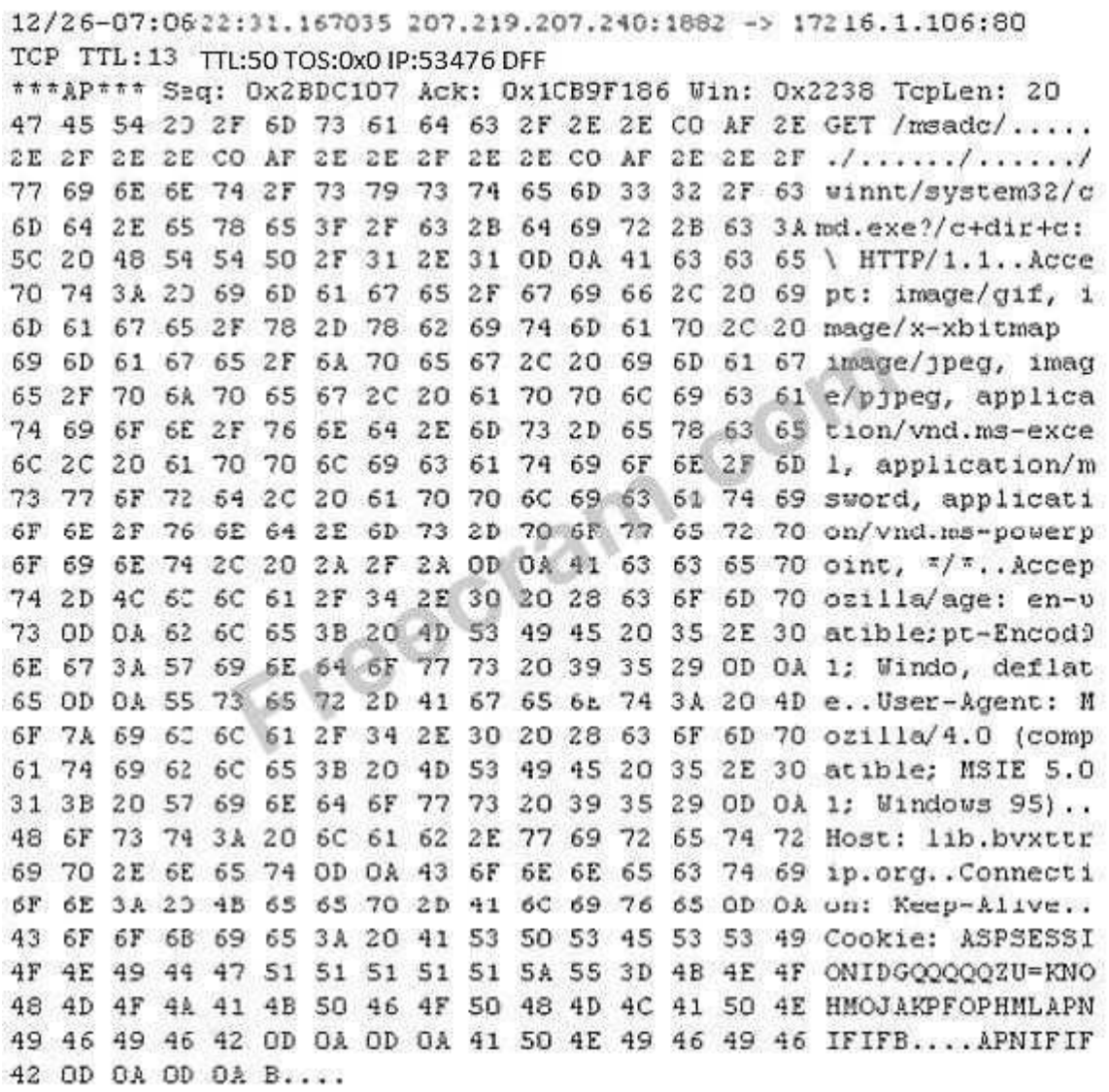
**NEW QUESTION: 17**
This form of encryption algorithm is asymmetric key block cipher that is characterized by a 128-bit block size, and its key size can be up to 256 bits. Which among the following is this encryption algorithm?
**A.** Twofish encryption algorithm
**B.** HMAC encryption algorithm
**C.** IDEA
**D.** Blowfish encryption algorithm
**Answer: (SHOW ANSWER)**
Explanation
Twofish is an encryption algorithm designed by Bruce Schneier. It's a symmetric key block cipher with a block size of 128 bits, with keys up to 256 bits. it's associated with AES (Advanced Encryption Standard) and an earlier block cipher called Blowfish. Twofish was actually a finalist to become the industry standard for encryption, but was ultimately beaten out by the present AES.Twofish has some distinctive features that set it aside from most other cryptographic protocols. For one, it uses pre-computed, key-dependent S-boxes. An S-box (substitution-box) may be a basic component of any symmetric key algorithm which performs substitution. within the context of Twofish's block cipher, the S-box works to obscure the connection of the key to the ciphertext. Twofish uses a pre-computed, key-dependent S-box which suggests that the S-box is already provided, but depends on the cipher key to decrypt the knowledge .
How Secure is Twofish?Twofish is seen as a really secure option as far as encryption protocols go. one among the explanations that it wasn't selected because the advanced encryption standard is thanks to its slower speed.
Any encryption standard that uses a 128-bit or higher key, is theoretically safe from brute force attacks.
Twofish is during this category.Because Twofish uses "pre-computed key-dependent S-boxes", it are often susceptible to side channel attacks. this is often thanks to the tables being pre-computed. However, making these tables key-dependent helps mitigate that risk. There are a couple of attacks on Twofish, but consistent with its creator, Bruce Schneier, it didn't constitute a real cryptanalysis. These attacks didn't constitue a practical break within the cipher.
Products That Use TwofishGnuPG: GnuPG may be a complete and free implementation of the OpenPGP standard as defined by RFC4880 (also referred to as PGP). GnuPG allows you to encrypt and sign your data and communications; it features a flexible key management system, along side access modules for all types of public key directories.KeePass: KeePass may be a password management tool that generates passwords with top-notch security. It's a free, open source, lightweight and easy-to-use

password manager with many extensions and plugins.Password Safe: Password Safe uses one master password to stay all of your passwords protected, almost like the functionality of most of the password managers on this list. It allows you to store all of your passwords during a single password database, or multiple databases for various purposes. Creating a database is straightforward , just create the database, set your master password.PGP (Pretty Good Privacy):
PGP is employed mostly for email encryption, it encrypts the content of the e-mail . However, Pretty Good Privacy doesn't encrypt the topic and sender of the e-mail , so make certain to never put sensitive information in these fields when using PGP.TrueCrypt:
TrueCrypt may be a software program that encrypts and protects files on your devices. With TrueCrypt the encryption is transparent to the user and is completed locally at the user's computer. this suggests you'll store a TrueCrypt file on a server and TrueCrypt will encrypt that file before it's sent over the network.

**NEW QUESTION: 18**
Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.
Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.
**A.** Solarwinds IP Network Browser
**B.** SNScan
**C.** NMap
**D.** SNMPScan
**E.** SNMPUtil
**Answer: A,B,E (LEAVE A REPLY)**

**NEW QUESTION: 19**
What is correct about digital signatures?
**A.** Digital signatures may be used in different documents of the same type.
**B.** 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.
**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: B (LEAVE A REPLY)**

**NEW QUESTION: 20**
Study the following log extract and identify the attack.




**A.** Hexcode Attack

**B.** Multiple Domain Traversal Attack

**C.** Unicode Directory Traversal Attack

**D.** Cross Site Scripting

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 21**

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.** Output the results in XML format to a file

**D.** Perform an Xmas scan

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 22**

In order to tailor your tests during a web-application scan, you decide to determine which web-server version is hosting the application. On using the sV flag with Nmap. you obtain the following response:
80/tcp open http-proxy Apache Server 7.1.6
what Information-gathering technique does this best describe?
**A.** Banner grabbing
**B.** WhOiS lookup
**C.** Dictionary attack
**D.** Brute forcing
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 23**
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.** Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
**B.** This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
**C.** This is probably a legitimate message as it comes from a respectable organization.
**D.** This is a scam because Bob does not know Scott.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 24**
Clark is a professional hacker. He created and configured multiple domains pointing to the same host to switch quickly between the domains and avoid detection.
Identify the behavior of the adversary In the above scenario.
**A.** Data staging
**B.** Unspecified proxy activities
**C.** Use of DNS tunneling
**D.** use of command-line interface
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 25**
When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN/ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN/ACK before the connection is established. This is referred to as the "TCP three-way handshake." While waiting for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue

typically empties quickly since the ACK is expected to arrive a few milliseconds after the SYN ACK.
How would an attacker exploit this design by launching TCP SYN attack?
**A.** Attacker generates TCP ACK packets with random source addresses towards a victim host
**B.** Attacker floods TCP SYN packets with random source addresses towards a victim host
**C.** Attacker generates TCP SYN packets with random destination addresses towards a victim host
**D.** Attacker generates TCP RST packets with random source addresses towards a victim host
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 26**
Allen, a professional pen tester, was hired by xpertTech solutWns to perform an attack simulation on the organization's network resources. To perform the attack, he took advantage of the NetBIOS API and targeted the NetBIOS service. B/enumerating NetBIOS, he found that port 139 was open and could see the resources that could be accessed or viewed on a remote system. He came across many NetBIOS codes during enumeration.
identify the NetBIOS code used for obtaining the messenger service running for the logged-in user?
**A.** <20>
**B.** C
<03>Windows Messenger administrationCourier administration is an organization based framework notice Windows administration by Microsoft that was remembered for some prior forms of Microsoft Windows.
This resigned innovation, despite the fact that it has a comparable name, isn't connected in any capacity to the later, Internet-based Microsoft Messenger administration for texting or to Windows Messenger and Windows Live Messenger (earlier named MSN Messenger) customer programming.
The Messenger Service was initially intended for use by framework managers to tell Windows clients about their networks.[1] It has been utilized malevolently to introduce spring up commercials to clients over the Internet (by utilizing mass-informing frameworks which sent an ideal message to a predetermined scope of IP addresses). Despite the fact that Windows XP incorporates a firewall, it isn't empowered naturally. Along these lines, numerous clients got such messages. Because of this maltreatment, the Messenger Service has been debilitated as a matter of course in Windows XP Service Pack 2.
**C.** <03>
**D.** <1B>
**E.** <00>
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 27**
The collection of potentially actionable, overt, and publicly available information is known as
**A.** Human intelligence
**B.** Social intelligence
**C.** Open-source intelligence
**D.** Real intelligence
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 28**
The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:
You are hired to conduct security testing on their network.
You successfully brute-force the SNMP community string using a SNMP crack tool.
The access-list configured at the router prevents you from establishing a successful connection.
You want to retrieve the Cisco configuration from the router. How would you proceed?
**A.** Use the Cisco's TFTP default password to connect and download the configuration file
**B.** Run a network sniffer and capture the returned traffic with the configuration file from the router
**C.** Run Generic Routing Encapsulation (GRE) tunneling protocol from your computer to the router masking your IP address
**D.** Send a customized SNMP set request with a spoofed source IP address in the range -192.168.1.0
**Answer: B,D (LEAVE A REPLY)**

**NEW QUESTION: 29**
An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?
**A.** Disable all routing protocols and only use static routes
**B.** Redirection of the traffic cannot happen unless the admin allows it explicitly.
**C.** Only using OSPFv3 will mitigate this risk.
**D.** Make sure that legitimate network routers are configured to run routing protocols with authentication.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 30**
How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

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

**NEW QUESTION: 31**
Taylor, a security professional, uses a tool to monitor her company's website, analyze the website's traffic, and track the geographical location of the users visiting the company's website. Which of the following tools did Taylor employ in the above scenario?
**A.** WebSite Watcher
**B.** web-Stat
**C.** Webroot
**D.** WAFW00F
**Answer: B (LEAVE A REPLY)**
Explanation
Increase your web site's performance and grow! Add Web-Stat to your site (it's free!) and watch individuals act together with your pages in real time.
Learn how individuals realize your web site. Get details concerning every visitor's path through your web site and track pages that flip browsers into consumers.
One-click install. observe locations, in operation systems, browsers and screen sizes and obtain alerts for new guests and conversions



**NEW QUESTION: 32**
The establishment of a TCP connection involves a negotiation called three-way handshake. What type of message does the client send to the server in order to begin this negotiation?
**A.** SYN
**B.** SYN-ACK
**C.** ACK
**D.** RST

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 33**
which of the following Bluetooth hacking techniques refers to the theft of information from a wireless device through Bluetooth?
**A.** Bluesmacking
**B.** Bluebugging
**C.** Bluejacking
**D.** Bluesnarfing
**Answer: (SHOW ANSWER)**
Explanation
Bluejacking is maybe the foremost common sort of Bluetooth hacking. This happens once a hacker searches for discoverable devices within the space and so sends spam within the sort of text messages to the devices.
this manner of hacking is very immature and harmless.
It was once used primarily to prank individuals within the past once mobile devices came with Bluetooth that was mechanically set to ascertainable. Bluejacking is employed nowadays for spam electronic communication and also the hackers World Health Organization use this bonk simply to frustrate others. the tactic doesn't offer hackers access to your phone or the knowledge on that.
The best thanks to alter Bluejacking is to ignore the messages if you receive them. If you retain your Bluetooth settings to "invisible" or "non-discoverable" you're not going to receive these messages. Also, keeping your smartphone or device set to "invisible" whereas you're in a very busy or open Wi-Fi space. this can forestall Bluejacking and also the next 2 well-liked styles of hacks.

**NEW QUESTION: 34**
You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories:
lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?
**A.** Dictionary Attack
**B.** Brute Force Attack
**C.** Hybrid Attack
**D.** Online Attack
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 35**
Ricardo has discovered the username for an application in his targets environment. As he has a limited amount of time, he decides to attempt to use a list of common passwords he found on the Internet. He compiles them into a list and then feeds that list as an argument into his password-cracking application, what type of attack is Ricardo performing?
**A.** Known plaintext
**B.** Password spraying
**C.** Brute force
**D.** Dictionary
**Answer: C (LEAVE A REPLY)**
Explanation
A brute force attack could be a popular cracking method: by some accounts, brute force attacks accounted for five% has a of confirmed security breaches. A brute force attack involves 'guessing' username and passwords to achieve unauthorized access to a system. Brute force could be a easy attack methodology and encompasses a high success rate.Some attackers use applications and scripts as brute force tools. These tools attempt various parole combos to bypass authentication processes. In different cases, attackers try and access net applications by sorting out the correct session ID. offender motivation might embody stealing data, infecting sites with malware, or disrupting service.While some attackers still perform brute force attacks manually, nowadays most brute force attacks nowadays area unit performed by bots. Attackers have lists of ordinarily used credentials, or real user credentials, obtained via security breaches or the dark net. Bots consistently attack websites and take a look at these lists of credentials, and apprize the offender after they gain access.
Types of Brute Force Attacks* Simple brute force attack-uses a scientific approach to 'guess' that doesn't believe outside logic.* Hybrid brute force attacks-starts from external logic to see that parole variation could also be presumably to succeed, then continues with the easy approach to undertake several potential variations.* Dictionary attacks-guesses username or passwords employing a wordbook of potential strings or phrases.* Rainbow table attacks-a rainbow table could be a precomputed table for reversing cryptologic hash functions. It may be wont to guess a perform up to a precise length consisting of a restricted set of characters.* Reverse brute force attack-uses a typical parole or assortment of passwords against several potential username . Targets a network of users that the attackers have antecedently obtained knowledge.* Credential stuffing-uses previously-known password-username pairs, attempting them against multiple websites. Exploits the actual fact that several users have an equivalent username and parole across totally different systems.
Hydra and different widespread Brute Force Attack ToolsSecurity analysts use the THC-Hydra tool to spot vulnerabilities in shopper systems. Hydra quickly runs through an outsized range of parole combos, either easy brute force or dictionary-based. It will attack

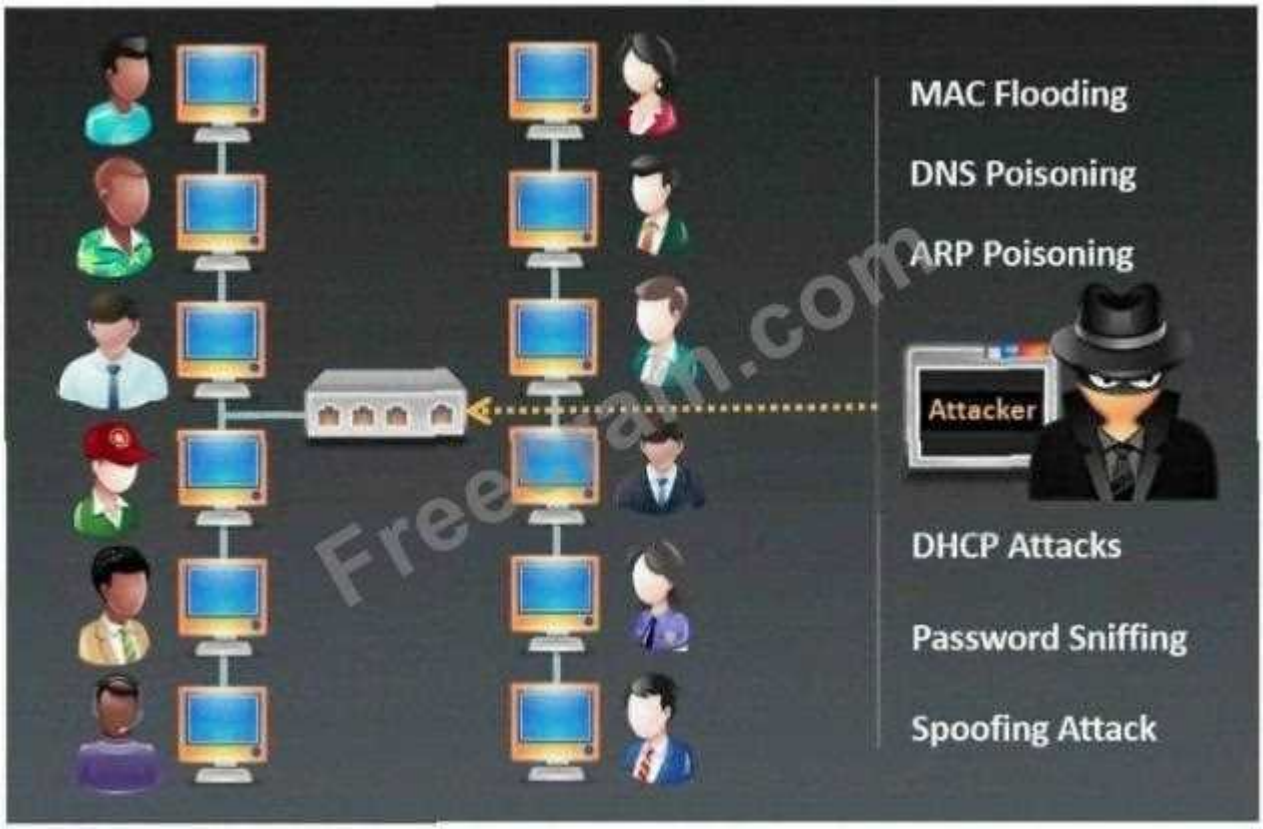
quite fifty protocols and multiple operational systems. Hydra is an open platform; the safety community and attackers perpetually develop new modules.
Other high brute force tools are:* Aircrack-ng-can be used on Windows, Linux, iOS, and golem. It uses a wordbook of wide used passwords to breach wireless networks.* John the Ripper-runs on fifteen totally different platforms as well as UNIX operating system, Windows, and OpenVMS. Tries all potential combos employing a dictionary of potential passwords.* L0phtCrack-a tool for cracking Windows passwords. It uses rainbow tables, dictionaries, and digital computer algorithms.* Hashcat-works on Windows, Linux, and Mac OS. will perform easy brute force, rule-based, and hybrid attacks.* DaveGrohl-an open-source tool for cracking mac OS. may be distributed across multiple computers.* Ncrack-a tool for cracking network authentication. It may be used on Windows, Linux, and BSD.

**NEW QUESTION: 36**
Widespread fraud ac Enron. WorldCom, and Tyco led to the creation of a law that was designed to improve the accuracy and accountability of corporate disclosures. It covers accounting firms and third parties that provide financial services to some organizations and came into effect in 2002. This law is known by what acronym?
**A.** Fed RAMP
**B.** PCIDSS
**C.** SOX
**D.** HIPAA
**Answer: C (LEAVE A REPLY)**
Explanation
The Sarbanes-Oxley Act of 2002 could be a law the U.S. Congress passed on July thirty of that year to assist defend investors from fallacious money coverage by companies.Also called the SOX Act of 2002 and also the company Responsibility Act of 2002, it mandated strict reforms to existing securities rules and obligatory powerful new penalties on law breakers.
The Sarbanes-Oxley law Act of 2002 came in response to money scandals within the early 2000s involving in public listed corporations like Enron Corporation, Tyco International plc, and WorldCom. The high-profile frauds cask capitalist confidence within the trustiness of company money statements Associate in Nursingd light-emitting diode several to demand an overhaul of decades-old restrictive standards.

**NEW QUESTION: 37**
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

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

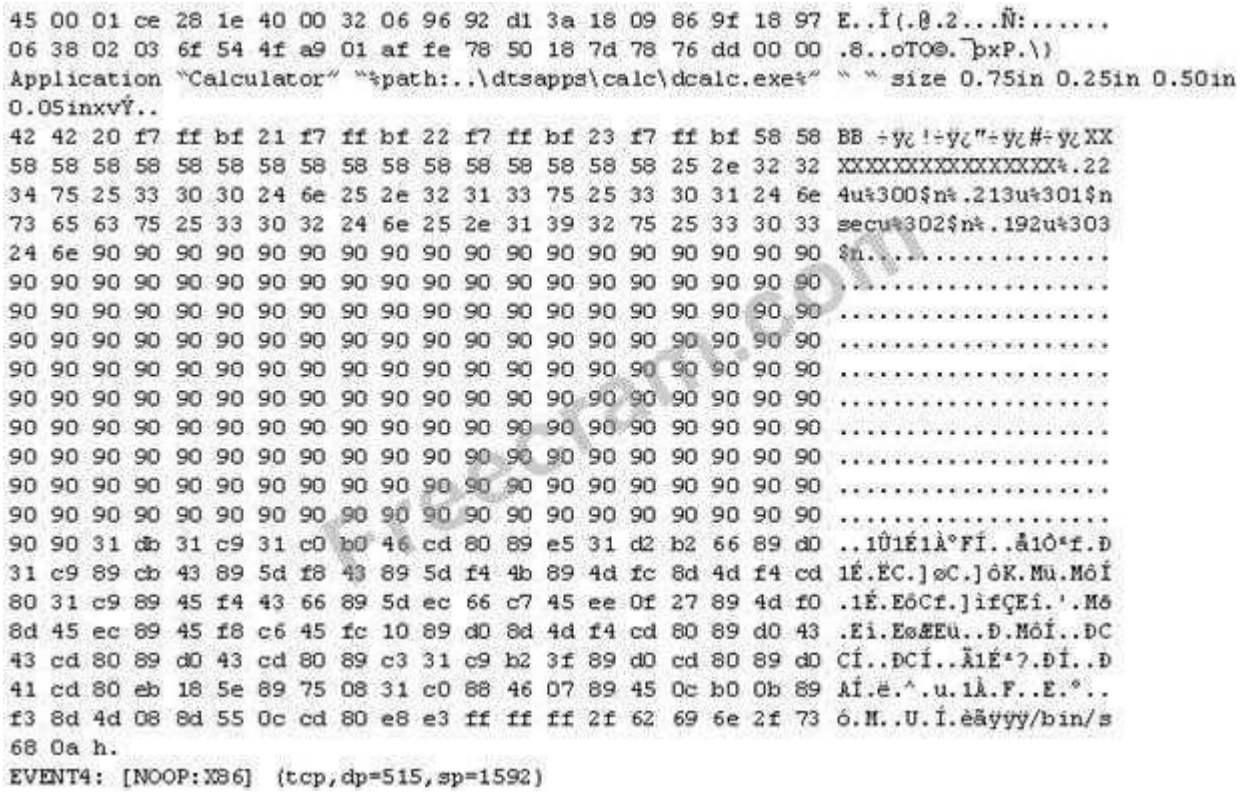
**NEW QUESTION: 38**
Which type of sniffing technique is generally referred as MiTM attack?




**A.** DHCP Sniffing
**B.** Password Sniffing
**C.** ARP Poisoning
**D.** Mac Flooding
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 39**
The following is an entry captured by a network IDS. You are assigned the task of analyzing this entry. You notice the value 0x90, which is the most common NOOP instruction for the Intel processor. You figure that the attacker is attempting a buffer overflow attack.
You also notice "/bin/sh" in the ASCII part of the output.

As an analyst what would you conclude about the attack?



```
45 00 01 ce 28 1e 40 00 32 06 96 92 d1 3a 18 09 86 9f 18 97 E..Î(.@.2...Ñ:.....
06 38 02 03 6f 54 4f a9 01 af fe 78 50 18 7d 78 76 dd 00 00 .8..oTO©.¯þxP.}xvÝ..
Application "Calculator" "%path:..\dtsapps\calc\dcalc.exe%" " " size 0.75in 0.25in 0.50in
0.05inxvÝ..
42 42 20 f7 ff bf 21 f7 ff bf 22 f7 ff bf 23 f7 ff bf 58 58 BB ÷ÿ¿!÷ÿ¿"÷ÿ¿#÷ÿ¿XX
58 58 58 58 58 58 58 58 58 58 58 58 58 58 25 2e 32 32 XXXXXXXXXXXXXX%.22
34 75 25 33 30 30 24 6e 25 2e 32 31 33 75 25 33 30 31 24 6e 4u%300$n%.213u%301$n
73 65 63 75 25 33 30 32 24 6e 25 2e 31 39 32 75 25 33 30 33 secu%302$n%.192u%303
24 6e 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 $n..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 ..................
90 90 31 db 31 c9 31 c0 b0 46 cd 80 89 e5 31 d2 b2 66 89 d0 ..1Û1É1À°FÍ..å1Ò²f.Ð
31 c9 89 cb 43 89 5d f8 43 89 5d f4 4b 89 4d fc 8d 4d f4 cd 1É.ËC.]øC.]ôK.Mü.MôÍ
80 31 c9 89 45 f4 43 66 89 5d ec 66 c7 45 ee 0f 27 89 4d f0 .1É.EôCf.]ìfÇEî.'.Mð
8d 45 ec 89 45 f8 c6 45 fc 10 89 d0 8d 4d f4 cd 80 89 d0 43 .Eì.EøÆEü..Ð.MôÍ..ÐC
43 cd 80 89 d0 43 cd 80 89 c3 31 c9 b2 3f 89 d0 cd 80 89 d0 CÍ..ÐCÍ..Ã1É²?.ÐÍ..Ð
41 cd 80 eb 18 5e 89 75 08 31 c0 88 46 07 89 45 0c b0 0b 89 AÍ.ë.^.u.1À.F..E.°..
f3 8d 4d 08 8d 55 0c cd 80 e8 e3 ff ff ff 2f 62 69 6e 2f 73 ó.M..U.Í.èãÿÿÿ/bin/s
68 0a h.
EVENT4: [NOOP:X86] (tcp,dp=515,sp=1592)
```

**A.** The attacker is attempting a buffer overflow attack and has succeeded

**B.** The attacker is attempting an exploit that launches a command-line shell

**C.** The buffer overflow attack has been neutralized by the IDS

**D.** The attacker is creating a directory on the compromised machine

**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 40**

What is the proper response for a NULL scan if the port is open?

**A.** SYN

**B.** FIN

**C.** RST

**D.** No response

**E.** PSH

**F.** ACK

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 41**

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

allowed to use the company's computer systems until they have signed the policy in acceptance of its terms.
What is this document called?
**A.** Company Compliance Policy (CCP)
**B.** Penetration Testing Policy (PTP)
**C.** Information Security Policy (ISP)
**D.** Information Audit Policy (IAP)
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 42**
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.** Immediately roll back the firewall rule until a manager can approve it
**B.** Monitor all traffic using the firewall rule until a manager can approve it.
**C.** Have the network team document the reason why the rule was implemented without prior manager approval.
**D.** 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.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 43**
What is the purpose of DNS AAAA record?
**A.** Authorization, Authentication and Auditing record
**B.** Address database record
**C.** IPv6 address resolution record
**D.** Address prefix record
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 44**
Richard, an attacker, aimed to hack loT devices connected to a target network. In this process. Richard recorded the frequency required to share information between connected devices. After obtaining the frequency, he captured the original data when commands were initiated by the connected devices. Once the original data were collected, he used free tools such as URH to segregate the command sequence.
Subsequently, he started injecting the segregated command sequence on the same frequency into the loT network, which repeats the captured signals of the devices. What Is the type of attack performed by Richard In the above scenario?
**A.** Side-channel attack

**B.** Replay attack
**C.** CrypTanalysis attack
**D.** Reconnaissance attack
**Answer: C (LEAVE A REPLY)**
Explanation
Cryptanalysis is that the science of cracking codes and secret writing secrets. it's accustomed violate authentication schemes, to interrupt scientific discipline protocols, and, additional benignantly, to seek out and proper weaknesses in coding algorithms.
It may be employed in IW applications - for instance, shaping Associate in Nursing encrypted signal to be accepted as authentic. Competitors UN agency are ready to discover the key can currently need to use it to their advantage, thus they're going to need to send phony encrypted messages to the supply so as to gain data or gain a bonus. It might even be used to pretend to be the supply so as to send phony data to others, UN agency currently can assume that it came from the official supply.
* Ciphertext solely attacks
* best-known plaintext attacks
* Chosen plaintext attacks
* Chosen ciphertext attacks
* Man-in-the-middle attacks
* aspect channel attacks
* Brute force attacks
* Birthday attacks
Among the kinds of attacks are:There are variety of different technical and non-technical cryptography attacks to that systems will fall victim. cryptographical attacks may be mounted not solely against coding algorithms, however conjointly against digital signature algorithms, MACing algorithms and pseudo-random variety generators.
Ciphertext solely AttackA ciphertext solely attack (COA) could be a case within which solely the encrypted message is accessible for attack, however as a result of the language is thought a frequency analysis may be tried. during this state of affairs the aggressor doesn't apprehend something concerning the contents of the message, and should work from ciphertext solely.

**NEW QUESTION: 45**
Dorian Is sending a digitally signed email to Polly, with which key is Dorian signing this message and how is Poly validating It?
**A.** Dorian is signing the message with his public key. and Poly will verify that the message came from Dorian by using Dorian's private key.
**B.** Dorian is signing the message with Polys private key. and Poly will verify mat the message came from Dorian by using Dorian's public key.
**C.** Dorian Is signing the message with Polys public key. and Poly will verify that the message came from Dorian by using Dorian's public key.

**D.** Dorian is signing the message with his private key. and Poly will verify that the message came from Dorian by using Dorian's public key.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 46**
What is the proper response for a NULL scan if the port is closed?
**A.** RST
**B.** ACK
**C.** PSH
**D.** No response
**E.** FIN
**F.** SYN
**Answer: A (LEAVE A REPLY)**



**NEW QUESTION: 47**
John, a professional hacker, decided to use DNS to perform data exfiltration on a target network, in this process, he embedded malicious data into the DNS protocol packets that even DNSSEC cannot detect. Using this technique. John successfully injected malware to bypass a firewall and maintained communication with the victim machine and C&C server. What is the technique employed by John to bypass the firewall?
**A.** DNS cache snooping
**B.** DNSSEC zone walking
**C.** DNS tunneling method
**D.** DNS enumeration
**Answer: (SHOW ANSWER)**
Explanation
DNS tunneling may be a method wont to send data over the DNS protocol, a protocol which has never been intended for data transfer. due to that, people tend to overlook it and it's become a well-liked but effective tool in many attacks.Most popular use case for DNS tunneling is obtaining free internet through bypassing captive portals at airports, hotels, or if you are feeling patient the not-so-cheap on the wing Wi-Fi.On those shared internet hotspots HTTP traffic is blocked until a username/password is provided, however DNS

traffic is usually still allowed within the background: we will encode our HTTP traffic over DNS and voila, we've internet access.This sounds fun but reality is, browsing anything on DNS tunneling is slow. Like, back to 1998 slow.Another more dangerous use of DNS tunneling would be bypassing network security devices (Firewalls, DLP appliances...) to line up an immediate and unmonitored communications channel on an organisation's network. Possibilities here are endless: Data exfiltration, fixing another penetration testing tool... you name it.To make it even more worrying, there's an outsized amount of easy to use DNS tunneling tools out there.There's even a minimum of one VPN over DNS protocol provider (warning: the planning of the web site is hideous, making me doubt on the legitimacy of it).As a pentester all this is often great, as a network admin not such a lot . How does it work:For those that ignoramus about DNS protocol but still made it here, i feel you deserve a really brief explanation on what DNS does: DNS is sort of a phonebook for the web , it translates URLs (human-friendly language, the person's name), into an IP address (machine-friendly language, the phone number). That helps us remember many websites, same as we will remember many people's names.For those that know what DNS is i might suggest looking here for a fast refresh on DNS protocol, but briefly what you would like to understand is:* A Record: Maps a website name to an IP address.example.com ? 12.34.52.67* NS Record (a.k.a. Nameserver record): Maps a website name to an inventory of DNS servers, just in case our website is hosted in multiple servers.example.com ? server1.example.com, server2.example.comWho is involved in DNS tunneling?* Client. Will launch DNS requests with data in them to a website .* One Domain that we will configure. So DNS servers will redirect its requests to an outlined server of our own.* Server. this is often the defined nameserver which can ultimately receive the DNS requests.The 6 Steps in DNS tunneling (simplified):1. The client encodes data during a DNS request. The way it does this is often by prepending a bit of knowledge within the domain of the request. for instance : mypieceofdata.server1.example.com2. The DNS request goes bent a DNS server.3. The DNS server finds out the A register of your domain with the IP address of your server.4. The request for mypieceofdata.server1.example.com is forwarded to the server.5. The server processes regardless of the mypieceofdata was alleged to do. Let's assume it had been an HTTP request.6. The server replies back over DNS and woop woop, we've got signal.

**NEW QUESTION: 48**

John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

**A.** Select someone else to check the procedures.

**B.** Read the incident manual every time it occurs.

**C.** Increase his technical skills.

**D.** Create an incident checklist.

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 49**
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?
**A.** Privilege Escalation
**B.** Port Scanning
**C.** Hacking Active Directory
**D.** Shoulder-Surfing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 50**
Peter is surfing the internet looking for information about DX Company. Which hacking process is Peter doing?
**A.** Footprinting
**B.** Scanning
**C.** Enumeration
**D.** System Hacking
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 51**
Internet Protocol Security IPsec is actually a suite pf protocols. Each protocol within the suite provides different functionality. Collective IPsec does everything except.
**A.** Protect the payload and the headers
**B.** Work at the Data Link Layer
**C.** Authenticate
**D.** Encrypt
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 52**
"Testing the network using the same methodologies and tools employed by attackers"

Identify the correct terminology that defines the above statement.
**A.** Vulnerability Scanning
**B.** Security Policy Implementation
**C.** Designing Network Security
**D.** Penetration Testing
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 53**

Yancey is a network security administrator for a large electric company. This company provides power for over 100, 000 people in Las Vegas. Yancey has worked for his company for over 15 years and has become very successful. One day, Yancey comes in to work and finds out that the company will be downsizing and he will be out of a job in two weeks. Yancey is very angry and decides to place logic bombs, viruses, Trojans, and backdoors all over the network to take down the company once he has left. Yancey does not care if his actions land him in jail for 30 or more years, he just wants the company to pay for what they are doing to him.
What would Yancey be considered?
**A.** Yancey is a Hacktivist Hacker since he is standing up to a company that is downsizing
**B.** Since he does not care about going to jail, he would be considered a Black Hat
**C.** Because Yancey works for the company currently; he would be a White Hat
**D.** Yancey would be considered a Suicide Hacker
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 54**
in an attempt to increase the security of your network, you Implement a solution that will help keep your wireless network undiscoverable and accessible only to those that know It.
How do you accomplish this?
**A.** Lock all users
**B.** Remove all passwords
**C.** Delete the wireless network
**D.** Disable SSID broadcasting
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 55**
Heather's company has decided to use a new customer relationship management tool. After performing the appropriate research, they decided to purchase a subscription to a cloud-hosted solution. The only administrative task that Heather will need to perform is the management of user accounts. The provider will take care of the hardware, operating system, and software administration including patching and monitoring.
Which of the following is this type of solution?
**A.** SaaS
**B.** IaaS
**C.** CaaS
**D.** PasS
**Answer: A (LEAVE A REPLY)**
Explanation
Software as a service (SaaS) allows users to attach to and use cloud-based apps over the web. Common examples ar email, calendaring and workplace tool (such as Microsoft workplace 365).

SaaS provides a whole software solution that you get on a pay-as-you-go basis from a cloud service provider.
You rent the use of an app for your organisation and your users connect with it over the web, typically with an internet browser. All of the underlying infrastructure, middleware, app software system and app knowledge ar located within the service provider's knowledge center. The service provider manages the hardware and software system and with the appropriate service agreement, can make sure the availability and also the security of the app and your data as well. SaaS allows your organisation to induce quickly up and running with an app at token upfront cost.
Common SaaS scenariosThis tool having used a web-based email service like Outlook, Hotmail or Yahoo!
Mail, then you have got already used a form of SaaS. With these services, you log into your account over the web, typically from an internet browser. the e-mail software system is found on the service provider's network and your messages ar hold on there moreover. you can access your email and hold on messages from an internet browser on any laptop or Internet-connected device.
The previous examples are free services for personal use. For organisational use, you can rent productivity apps, like email, collaboration and calendaring; and sophisticated business applications like client relationship management (CRM), enterprise resource coming up with (ERP) and document management. You buy the use of those apps by subscription or per the level of use.
Advantages of SaaSGain access to stylish applications. to supply SaaS apps to users, you don't ought to purchase, install, update or maintain any hardware, middleware or software system. SaaS makes even sophisticated enterprise applications, like ERP and CRM, affordable for organisations that lack the resources to shop for, deploy and manage the specified infrastructure and software system themselves.
Pay just for what you utilize. you furthermore may economize because the SaaS service automatically scales up and down per the level of usage.
Use free shopper software system. Users will run most SaaS apps directly from their web browser without needing to transfer and install any software system, though some apps need plugins. this suggests that you simply don't ought to purchase and install special software system for your users.
Mobilise your hands simply. SaaS makes it simple to "mobilise" your hands as a result of users will access SaaS apps and knowledge from any Internet-connected laptop or mobile device. You don't ought to worry concerning developing apps to run on differing types of computers and devices as a result of the service supplier has already done therefore. additionally, you don't ought to bring special experience aboard to manage the safety problems inherent in mobile computing. A fastidiously chosen service supplier can make sure the security of your knowledge, no matter the sort of device intense it.
Access app knowledge from anyplace. With knowledge hold on within the cloud, users will access their info from any Internet-connected laptop or mobile device. And once app

knowledge is hold on within the cloud, no knowledge is lost if a user's laptop or device fails.

**NEW QUESTION: 56**
Daniel Is a professional hacker who Is attempting to perform an SQL injection attack on a target website.
www.movlescope.com. During this process, he encountered an IDS that detects SQL Injection attempts based on predefined signatures. To evade any comparison statement, he attempted placing characters such as "or
'1'='1" In any bask injection statement such as "or 1=1." Identify the evasion technique used by Daniel in the above scenario.
**A.** IP fragmentation
**B.** Char encoding
**C.** Null byte
**D.** Variation
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 57**
Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting
**A.** Results for matches on target.com and Marketing.target.com that include the word "accounting"
**B.** Results matching "accounting" in domain target.com but not on the site Marketing.target.com
**C.** Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting.
**D.** Results matching all words in the query.
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 58**
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.** DynDNS
**B.** DNS Scheme
**C.** Split DNS
**D.** DNSSEC
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 59**

Which of the following represents the initial two commands that an IRC client sends to join an IRC network?
**A.** USER, NICK
**B.** USER, PASS
**C.** LOGIN, USER
**D.** LOGIN, NICK
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 60**
An organization is performing a vulnerability assessment tor mitigating threats. James, a pen tester, scanned the organization by building an inventory of the protocols found on the organization's machines to detect which ports are attached to services such as an email server, a web server or a database server. After identifying the services, he selected the vulnerabilities on each machine and started executing only the relevant tests. What is the type of vulnerability assessment solution that James employed in the above scenario?
**A.** Service-based solutions
**B.** Tree-based assessment
**C.** inference-based assessment
**D.** Product-based solutions
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 61**
Susan has attached to her company's network. She has managed to synchronize her boss's sessions with that of the file server. She then intercepted his traffic destined for the server, changed it the way she wanted to and then placed it on the server in his home directory.
What kind of attack is Susan carrying on?
**A.** A sniffing attack
**B.** A man in the middle attack
**C.** A spoofing attack
**D.** A denial of service attack
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 62**
Which definition among those given below best describes a covert channel?
**A.** It is the multiplexing taking place on a communication link.
**B.** A server program using a port that is not well known.
**C.** It is one of the weak channels used by WEP which makes it insecure
**D.** Making use of a protocol in a way it is not intended to be used.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 63**
Which of the following Linux commands will resolve a domain name into IP address?
**A.** >host -t AXFR hackeddomain.com
**B.** >host -t soa hackeddomain.com
**C.** >host-t ns hackeddomain.com
**D.** >host-t a hackeddomain.com
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 64**
Johnson, an attacker, performed online research for the contact details of reputed cybersecurity firms. He found the contact number of sibertech.org and dialed the number, claiming himself to represent a technical support team from a vendor. He warned that a specific server is about to be compromised and requested sibertech.org to follow the provided instructions. Consequently, he prompted the victim to execute unusual commands and install malicious files, which were then used to collect and pass critical Information to Johnson's machine. What is the social engineering technique Steve employed in the above scenario?
**A.** Phishing
**B.** Quid pro quo
**C.** Diversion theft
**D.** Elicitatiom
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 65**
John, a professional hacker, performs a network attack on a renowned organization and gains unauthorized access to the target network. He remains in the network without being detected for a long time and obtains sensitive information without sabotaging the organization. Which of the following attack techniques is used by John?
**A.** Advanced persistent
**B.** threat Diversion theft

**C.** Spear-phishing sites
**D.** insider threat
**Answer: A (LEAVE A REPLY)**
Explanation
An advanced persistent threat (APT) may be a broad term wont to describe AN attack campaign within which an intruder, or team of intruders, establishes a bootleg, long presence on a network so as to mine sensitive knowledge.
The targets of those assaults, that square measure terribly fastidiously chosen and researched, usually embrace massive enterprises or governmental networks. the implications of such intrusions square measure huge, and include:
* Intellectual property thieving (e.g., trade secrets or patents)
* Compromised sensitive info (e.g., worker and user personal data)
* The sabotaging of essential structure infrastructures (e.g., information deletion)
* Total website takeovers
Executing an APT assault needs additional resources than a regular internet application attack. The perpetrators square measure typically groups of intimate cybercriminals having substantial resource. Some APT attacks square measure government-funded and used as cyber warfare weapons.
APT attacks dissent from ancient internet application threats, in that:
* They're considerably additional advanced.
* They're not hit and run attacks-once a network is infiltrated, the culprit remains so as to realize the maximum amount info as potential.
* They're manually dead (not automated) against a selected mark and indiscriminately launched against an outsized pool of targets.
* They typically aim to infiltrate a complete network, as opposition one specific half.
More common attacks, like remote file inclusion (RFI), SQL injection and cross-site scripting (XSS), square measure oftentimes employed by perpetrators to ascertain a footing in a very targeted network. Next, Trojans and backdoor shells square measure typically wont to expand that foothold and make a persistent presence inside the targeted perimeter.

**NEW QUESTION: 66**
Annie, a cloud security engineer, uses the Docker architecture to employ a client/server model in the application she is working on. She utilizes a component that can process API requests and handle various Docker objects, such as containers, volumes. Images, and networks. What is the component of the Docker architecture used by Annie in the above scenario?
**A.** Docker client
**B.** Docker objects
**C.** Docker daemon
**D.** Docker registries

**Answer: B (LEAVE A REPLY)**

Explanation

When you use docker, you're making and using pictures, containers, networks, volumes, plugins, and alternative objects. This section could be a brief summary of some of those objects.

IMAGESAn image is a read-only template with instructions for making a docker container. Often, a picture relies on another image, with some further customization. for instance, you'll build a picture that relies on the ubuntu image, however installs the Apache internet server and your application, still because the configuration details required to create your application run.

You may produce your own pictures otherwise you might solely use those created by others and printed in a registry. to create your own image, you produce a Dockerfile with a simple syntax for defining the steps needed to make the image and run it. every instruction in a Dockerfile creates a layer within the image. once you change the Dockerfile and rebuild the image, solely those layers that have modified square measure remodeled. this is often a part of what makes pictures therefore light-weight, small, and fast, when put next to alternative virtualization technologies.

CONTAINERSA instrumentality could be a runnable instance of a picture. you'll produce, start, stop, move, or delete a instrumentality victimization the docker API or user interface. you'll connect a instrumentality to at least one or a lot of networks, attach storage to that, or perhaps produce a brand new image supported its current state.

By default, a container is relatively well isolated from alternative containers and its host machine. you'll management however isolated a container's network, storage, or alternative underlying subsystems square measure from alternative containers or from the host machine.

A instrumentality is outlined by its image still as any configuration choices you offer to that once you produce or begin it. once a instrumentality is removed, any changes to its state that aren't hold on in persistent storage disappear.

Example docker run commandThe following command runs an ubuntu container, attaches interactively to your native command-line session, and runs /bin/bash.

$ docker run -i -t ubuntu /bin/bash

When you run this command, the subsequent happens (assuming you're victimization the default written account configuration):

* If you are doing not have the ubuntu image locally, docker pulls it from your designed registry, like you had run docker pull ubuntu manually.
* docker creates a new container, like you had run a docker container create command manually.
* docker allocates a read-write filesystem to the container, as its final layer. this permits a running container to make or modify files and directories in its native filesystem.
* dock-walloper creates a network interface to attach the docker to the default network, since you did not specify any networking choices. This includes assigning an IP address to

the instrumentality. By default, containers will connect with external networks victimization the host machine's network connection.
* docker starts the container and executes /bin/bash. as a result of the container is running interactively and connected to your terminal (due to the -i and -t flags), you'll offer input using your keyboard whereas the output is logged to your terminal.
* when you type exit to terminate the /bin/bash command, the container stops however isn't removed.
you'll begin it once more or take away it.
SERVICESServices permit you to scale containers across multiple docker daemons, that all work along as a swarm with multiple managers and employees. every member of a swarm could be a docker daemon, and every one the daemons communicate victimization the docker API. A service permits you to outline the desired state, like the quantity of replicas of the service that has to be offered at any given time. By default, the service is load-balanced across all employee nodes. To the consumer, the docker API service seems to be one application. docker Engine supports swarm mode in docker one.12 and better.

**NEW QUESTION: 67**
To reach a bank web site, the traffic from workstations must pass through a firewall. You have been asked to review the firewall configuration to ensure that workstations in network 10.10.10.0/24 can only reach the bank web site 10.20.20.1 using https. Which of the following firewall rules meets this requirement?
**A.** If (source matches 10.10.10.0 and destination matches 10.20.20.1 and port matches 443) then permit
**B.** If (source matches 10.20.20.1 and destination matches 10.10.10.0/24 and port matches 443) then permit
**C.** If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 80 or 443) then permit
**D.** If (source matches 10.10.10.0/24 and destination matches 10.20.20.1 and port matches 443) then permit
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 68**
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?
**A.** Cain & Abel
**B.** SET
**C.** CHNTPW
**D.** John the Ripper
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 69**
Alice needs to send a confidential document to her coworker. Bryan. Their company has public key infrastructure set up. Therefore. Alice both encrypts the message and digitally signs it. Alice uses_____to encrypt the message, and Bryan uses_____to confirm the digital signature.
**A.** Bryan's public key; Bryan's public key
**B.** Bryan's public key; Alice's public key
**C.** Alice's public key; Alice's public key
**D.** Bryan's private key; Alice's public key
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 70**
Wilson, a professional hacker, targets an organization for financial benefit and plans to compromise its systems by sending malicious emails. For this purpose, he uses a tool to track the emails of the target and extracts information such as sender identities, mall servers, sender IP addresses, and sender locations from different public sources. He also checks if an email address was leaked using the haveibeenpwned.com API.
Which of the following tools is used by Wilson in the above scenario?
**A.** infoga
**B.** Factiva
**C.** Zoominfo
**D.** Netcraft
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 71**
While browsing his Facebook teed, Matt sees a picture one of his friends posted with the caption. "Learn more about your friends!", as well as a number of personal questions. Matt is suspicious and texts his friend, who confirms that he did indeed post it. With assurance that the post is legitimate. Matt responds to the questions on the post, a few days later. Mates bank account has been accessed, and the password has been changed.
What most likely happened?
**A.** Matt inadvertently provided the answers to his security questions when responding to the post.
**B.** Matt's bank-account login information was brute forced.
**C.** Matt Inadvertently provided his password when responding to the post.
**D.** Matt's computer was infected with a keylogger.
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 72**

The network users are complaining because their system are slowing down. Further, every time they attempt to go a website, they receive a series of pop-ups with advertisements. What types of malware have the system been infected with?

**A.** Virus

**B.** Spyware

**C.** Trojan

**D.** Adware

**Answer: (SHOW ANSWER)**

Explanation

Adware, or advertising supported computer code, is computer code that displays unwanted advertisements on your pc. Adware programs can tend to serve you pop-up ads, will modification your browser's homepage, add spyware and simply bombard your device with advertisements. Adware may be a additional summary name for doubtless unwanted programs. It's roughly a virulent disease and it's going to not be as clearly malicious as a great deal of different problematic code floating around on the net. create no mistake concerning it, though, that adware has to return off of no matter machine it's on. Not solely will adware be extremely annoying whenever you utilize your machine, it might additionally cause semipermanent problems for your device.

Adware a network users the browser to gather your internet browsing history so as to 'target' advertisements that appear tailored to your interests. At their most innocuous, adware infections square measure simply annoying. as an example, adware barrages you with pop-up ads that may create your net expertise markedly slower and additional labor intensive.

**NEW QUESTION: 73**

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

**A.** tracert

**B.** tcpdump

**C.** nmap

**D.** ping

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 74**

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

**A.** B757BF5C0D87772FAAD3B435B51404EE

**B.** BA810DBA98995F1817306D272A9441BB

**C.** 0182BD0BD4444BF836077A718CCDF409

**D.** 44EFCE164AB921CQAAD3B435B51404EE

**E.** CEC52EB9C8E3455DC2265B23734E0DAC

**F.** E52CAC67419A9A224A3B108F3FA6CB6D

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 75**
There have been concerns in your network that the wireless network component is not sufficiently secure. You perform a vulnerability scan of the wireless network and find that it is using an old encryption protocol that was designed to mimic wired encryption, what encryption protocol is being used?
**A.** WEP
**B.** RADIUS
**C.** WPA
**D.** WPA3
**Answer: (SHOW ANSWER)**
Explanation
Wi-Fi Protected Access (WPA), Wi-Fi Protected Access II (WPA2), and Wi-Fi Protected Access 3 (WPA3) are the three security and security certification programs developed by the Wi-Fi Alliance to secure wireless computer networks. The Alliance defined these in response to serious weaknesses researchers had found within the previous system, Wired Equivalent Privacy (WEP).WPA (sometimes mentioned because the draft IEEE 802.11i standard) became available in 2003. The Wi-Fi Alliance intended it as an intermediate measure in anticipation of the supply of the safer and sophisticated WPA2, which became available in 2004 and may be a common shorthand for the complete IEEE 802.11i (or IEEE 802.11i-2004) standard.In January 2018, Wi-Fi Alliance announced the discharge of WPA3 with several security improvements over WPA2.The Wi-Fi Alliance intended WPA as an intermediate measure to require the place of WEP pending the supply of the complete IEEE 802.11i standard. WPA might be implemented through firmware upgrades on wireless network interface cards designed for WEP that began shipping as far back as 1999. However, since the changes required within the wireless access points (APs) were more extensive than those needed on the network cards, most pre-2003 APs couldn't be upgraded to support WPA.The WPA protocol implements much of the IEEE 802.11i standard. Specifically, the Temporal Key Integrity Protocol (TKIP) was adopted for WPA. WEP used a 64-bit or 128-bit encryption key that has got to be manually entered on wireless access points and devices and doesn't change. TKIP employs a per-packet key, meaning that it dynamically generates a replacement
128-bit key for every packet and thus prevents the kinds of attacks that compromised WEP.WPA also includes a Message Integrity Check, which is meant to stop an attacker from altering and resending data packets. This replaces the cyclic redundancy check (CRC) that was employed by the WEP standard. CRC's main flaw was that it didn't provide a sufficiently strong data integrity guarantee for the packets it handled. Well-tested message authentication codes existed to unravel these problems, but they required an excessive amount of computation to be used on old network cards. WPA uses a message integrity check algorithm called TKIP to verify the integrity of the packets. TKIP is far

stronger than a CRC, but not as strong because the algorithm utilized in WPA2. Researchers have since discovered a flaw in WPA that relied on older weaknesses in WEP and therefore the limitations of the message integrity code hash function, named Michael, to retrieve the keystream from short packets to use for re-injection and spoofing.

**NEW QUESTION: 76**
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.** White Hat
**B.** Black Hat
**C.** Gray Hat
**D.** Suicide Hacker
**Answer: C (LEAVE A REPLY)**



**NEW QUESTION: 77**
Bob was recently hired by a medical company after it experienced a major cyber security breach. Many patients are complaining that their personal medical records are fully exposed on the Internet and someone can find them with a simple Google search. Bob's boss is very worried because of regulations that protect those data. Which of the following regulations is mostly violated?
**A.** PCIDSS
**B.** PII
**C.** HIPPA/PHI
**D.** ISO 2002
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 78**
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.** Gray-Hat Hacker
**B.** Black-Hat Hackers A
**C.** White-Hat Hackers
**D.** Script Kiddies
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 79**
What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?
**A.** Delete the files and try to determine the source
**B.** Copy the system files from a known good system
**C.** Perform a trap and trace
**D.** Reload from a previous backup
**E.** Reload from known good media
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 80**
What is a NULL scan?
**A.** A scan in which certain flags are off
**B.** A scan with an illegal packet size
**C.** A scan in which all flags are turned off
**D.** A scan in which all flags are on
**E.** A scan in which the packet size is set to zero
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 81**
in this form of encryption algorithm, every Individual block contains 64-bit data, and three keys are used, where each key consists of 56 bits. Which is this encryption algorithm?
**A.** IDEA
**B.** Triple Data Encryption standard
**C.** MDS encryption algorithm
**D.** AES
**Answer: (SHOW ANSWER)**
Explanation
Triple DES is another mode of DES operation. It takes three 64-bit keys, for an overall key length of 192 bits.
In Stealth, you merely type within the entire 192-bit (24 character) key instead of entering each of the three keys individually. The Triple DES DLL then breaks the user-provided key into three subkeys, padding the keys if necessary in order that they are each 64 bits long. The procedure for encryption is strictly an equivalent as regular DES, but it's repeated 3

times , hence the name Triple DES. the info is encrypted with the primary key, decrypted with the second key, and eventually encrypted again with the third key.Triple DES runs 3 times slower than DES, but is far safer if used properly. The procedure for decrypting something is that the same because the procedure for encryption, except it's executed in reverse. Like DES, data is encrypted and decrypted in 64-bit chunks. Although the input key for DES is 64 bits long, the particular key employed by DES is merely 56 bits long . the smallest amount significant (right-most) bit in each byte may be a parity , and will be set in order that there are always an odd number of 1s in every byte. These parity bits are ignored, so only the seven most vital bits of every byte are used, leading to a key length of 56 bits. this suggests that the effective key strength for Triple DES is really 168 bits because each of the three keys contains 8 parity bits that aren't used during the encryption process.Triple DES ModesTriple ECB (Electronic Code Book)* This variant of Triple DES works precisely the same way because the ECB mode of DES.* this is often the foremost commonly used mode of operation.Triple CBC (Cipher Block Chaining)* This method is extremely almost like the quality DES CBC mode.* like Triple ECB, the effective key length is 168 bits and keys are utilized in an equivalent manner, as described above, but the chaining features of CBC mode also are employed.* the primary 64-bit key acts because the Initialization Vector to DES.* Triple ECB is then executed for one 64-bit block of plaintext.* The resulting ciphertext is then XORed with subsequent plaintext block to be encrypted, and therefore the procedure is repeated.* This method adds an additional layer of security to Triple DES and is therefore safer than Triple ECB, although it's not used as widely as Triple ECB.

**NEW QUESTION: 82**
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.** How long it takes to setup individual user accounts
**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 from when an individual provides identification and authentication information
**D.** The amount of time it takes to convert biometric data into a template on a smart card
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 83**
jane, an ethical hacker. Is testing a target organization's web server and website to identity security loopholes.
In this process, she copied the entire website and its content on a local drive to view the complete profile of the site's directory structure, file structure, external links, images, web pages, and so on. This information helps jane map the website's directories and gain

valuable information. What is the attack technique employed by Jane in the above scenario?

**A.** website mirroring

**B.** Session hijacking

**C.** Web cache poisoning

**D.** Website defacement

**Answer: (SHOW ANSWER)**

Explanation

Web cache poisoning is a complicated technique whereby an attacker exploits the behavior of an internet server and cache in order that a harmful HTTP response is served to other users.Fundamentally, web cache poisoning involves two phases. First, the attacker must compute the way to elicit a response from the back-end server that inadvertently contains some quite dangerous payload. Once successful, they have to form sure that their response is cached and subsequently served to the intended victims.A poisoned web cache can potentially be a devastating means of distributing numerous different attacks, exploiting vulnerabilities like XSS, JavaScript injection, open redirection, and so on.

How does an internet cache work?To understand how web cache poisoning vulnerabilities arise, it's important to possess a basic understanding of how web caches work.If a server had to send a replacement response to each single HTTP request separately, this is able to likely overload the server, leading to latency issues and a poor user experience, especially during busy periods. Caching is primarily a way of reducing such issues.The cache sits between the server and therefore the user, where it saves (caches) the responses to particular requests, usually for a hard and fast amount of your time . If another user then sends the same request, the cache simply serves a replica of the cached response on to the user, with none interaction from the back-end.

This greatly eases the load on the server by reducing the amount of duplicate requests it's to handle.

Cache keysWhen the cache receives an HTTP request, it first has got to determine whether there's a cached response that it can serve directly, or whether it's to forward the request for handling by the back-end server.

Caches identify equivalent requests by comparing a predefined subset of the request's components, known collectively because the "cache key". Typically, this is able to contain the request line and Host header.

Components of the request that aren't included within the cache key are said to be "unkeyed".If the cache key of an incoming request matches the key of a previous request, then the cache considers them to be equivalent.

As a result, it'll serve a replica of the cached response that was generated for the first request. this is applicable to all or any subsequent requests with the matching cache key, until the cached response expires.Crucially, the opposite components of the request are

ignored altogether by the cache. We'll explore the impact of this behavior in additional detail later.
What is the impact of an internet cache poisoning attack?The impact of web cache poisoning is heavily hooked in to two key factors:* What precisely the attacker can successfully get cachedAs the poisoned cache is more a way of distribution than a standalone attack, the impact of web cache poisoning is inextricably linked to how harmful the injected payload is. like most sorts of attack, web cache poisoning also can be utilized in combination with other attacks to escalate the potential impact even further.* The quantity of traffic on the affected pageThe poisoned response will only be served to users who visit the affected page while the cache is poisoned. As a result, the impact can range from non-existent to massive counting on whether the page is popular or not. If an attacker managed to poison a cached response on the house page of a serious website, for instance , the attack could affect thousands of users with none subsequent interaction from the attacker.Note that the duration of a cache entry doesn't necessarily affect the impact of web cache poisoning. An attack can usually be scripted in such how that it re-poisons the cache indefinitely.

**NEW QUESTION: 84**
Kevin, a professional hacker, wants to penetrate CyberTech Inc.'s network. He employed a technique, using which he encoded packets with Unicode characters. The company's IDS cannot recognize the packet, but the target web server can decode them.
What is the technique used by Kevin to evade the IDS system?
**A.** Desynchronization
**B.** Obfuscating
**C.** Session splicing
**D.** Urgency flag
**Answer: B (LEAVE A REPLY)**
Explanation
Adversaries could decide to build an possible or file difficult to find or analyze by encrypting, encoding, or otherwise obfuscating its contents on the system or in transit. this is often common behavior which will be used across totally different platforms and therefore the network to evade defenses.
Payloads may be compressed, archived, or encrypted so as to avoid detection. These payloads may be used throughout Initial Access or later to mitigate detection. typically a user's action could also be needed to open and Deobfuscate/Decode Files or info for User Execution. The user can also be needed to input a parole to open a parole protected compressed/encrypted file that was provided by the mortal. Adversaries can also used compressed or archived scripts, like JavaScript.
Portions of files can even be encoded to cover the plain-text strings that will otherwise facilitate defenders with discovery. Payloads can also be split into separate, ostensibly benign files that solely reveal malicious practicality once reassembled.

Adversaries can also modify commands dead from payloads or directly via a Command and Scripting Interpreter. surroundings variables, aliases, characters, and different platform/language specific linguistics may be wont to evade signature based mostly detections and application management mechanisms.

**NEW QUESTION: 85**
Fred is the network administrator for his company. Fred is testing an internal switch.
From an external IP address, Fred wants to try and trick this switch into thinking it already has established a session with his computer. How can Fred accomplish this?
**A.** He can send an IP packet with the SYN bit and the source address of his computer.
**B.** Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.
**C.** Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.
**D.** Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 86**
You start performing a penetration test against a specific website and have decided to start from grabbing all the links from the main page.
What Is the best Linux pipe to achieve your milestone?
**A.** wgethttps://site.com | cut-d"http-
**B.** wget https://stte.com | grep "< a href=*http" | grep "site.com"
**C.** dirb https://site.com | grep "site"
**D.** curl -s https://sile.com | grep "< a href-\'http" | grep "Site-com- | cut -d "V" -f 2
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 87**
An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to
"www.MyPersonalBank.com", the user is directed to a phishing site.
Which file does the attacker need to modify?
**A.** Networks
**B.** Sudoers
**C.** Boot.ini
**D.** Hosts
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 88**

Abel, a cloud architect, uses container technology to deploy applications/software including all its dependencies, such as libraries and configuration files, binaries, and other resources that run independently from other processes in the cloud environment. For the containerization of applications, he follows the five-tier container technology architecture. Currently. Abel is verifying and validating image contents, signing images, and sending them to the registries. Which of the following tiers of the container technology architecture Is Abel currently working in?

**A.** Tier-1: Developer machines

**B.** Tier-4: Orchestrators

**C.** Tier-3: Registries

**D.** Tier-2: Testing and accreditation systems

**Answer: D (LEAVE A REPLY)**

Explanation

The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.

formal declaration by a designated accrediting authority (DAA) or principal accrediting authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards. See authorization to operate (ATO).

Rationale: The Risk Management Framework uses a new term to refer to this concept, and it is called authorization.

Identifies the information resources covered by an accreditation decision, as distinguished from separately accredited information resources that are interconnected or with which information is exchanged via messaging. Synonymous with Security Perimeter.

For the purposes of identifying the Protection Level for confidentiality of a system to be accredited, the system has a conceptual boundary that extends to all intended users of the system, both directly and indirectly connected, who receive output from the system. See authorization boundary. Rationale: The Risk Management Framework uses a new term to refer to the concept of accreditation, and it is called authorization.

Extrapolating, the accreditation boundary would then be referred to as the authorization boundary.

**NEW QUESTION: 89**

Eric has discovered a fantastic package of tools named Dsniff on the Internet. He has learnt to use these tools in his lab and is now ready for real world exploitation. He was able to effectively intercept communications between the two entities and establish credentials with both sides of the connections. The two remote ends of the communication never notice that Eric is relaying the information between the two. What would you call this attack?

**A.** Interceptor
**B.** Poisoning Attack
**C.** Man-in-the-middle
**D.** ARP Proxy
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 90**
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed.
What command is used to determine if the entry is present in DNS cache?
**A.** dnsnooping -rt update.antivirus.com
**B.** dns --snoop update.antivirus.com
**C.** nslookup -norecursive update.antivirus.com
**D.** nslookup -fullrecursive update.antivirus.com
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 91**
Samuel, a professional hacker, monitored and Intercepted already established traffic between Bob and a host machine to predict Bob's ISN. Using this ISN, Samuel sent spoofed packets with Bob's IP address to the host machine. The host machine responded with <| packet having an Incremented ISN. Consequently. Bob's connection got hung, and Samuel was able to communicate with the host machine on behalf of Bob. What is the type of attack performed by Samuel in the above scenario?
**A.** UDP hijacking
**B.** Blind hijacking
**C.** TCP/IP hacking
**D.** Forbidden attack
**Answer: (SHOW ANSWER)**
Explanation
A TCP/IP hijack is an attack that spoofs a server into thinking it's talking with a sound client, once actually it's communication with an assaulter that has condemned (or hijacked) the tcp session. Assume that the client has administrator-level privileges, which the attacker needs to steal that authority so as to form a brand new account with root-level access of the server to be used afterward. A tcp Hijacking is sort of a two-phased man-in-the-middle attack. The man-in-the-middle assaulter lurks within the circuit between a shopper and a server so as to work out what port and sequence numbers are being employed for the conversation.
First, the attacker knocks out the client with an attack, like Ping of Death, or ties it up with some reasonably ICMP storm. This renders the client unable to transmit any packets to the

server. Then, with the client crashed, the attacker assumes the client's identity so as to talk with the server. By this suggests, the attacker gains administrator-level access to the server.
One of the most effective means of preventing a hijack attack is to want a secret, that's a shared secret between the shopper and also the server. looking on the strength of security desired, the key may be used for random exchanges. this is often once a client and server periodically challenge each other, or it will occur with each exchange, like Kerberos.



**NEW QUESTION: 92**
You are performing a penetration test for a client and have gained shell access to a Windows machine on the internal network. You intend to retrieve all DNS records for the internal domain, if the DNS server is at
192.168.10.2 and the domain name is abccorp.local, what command would you type at the nslookup prompt to attempt a zone transfer?
**A.** is-d abccorp.local
**B.** List domain=Abccorp.local type=zone
**C.** list server=192.168.10.2 type=all
**D.** Iserver 192.168.10.2-t all
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 93**
What is not a PCI compliance recommendation?
**A.** Use encryption to protect all transmission of card holder data over any public network.
**B.** Limit access to card holder data to as few individuals as possible.
**C.** Rotate employees handling credit card transactions on a yearly basis to different departments.
**D.** Use a firewall between the public network and the payment card data.
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 94**
what are common files on a web server that can be misconfigured and provide useful Information for a hacker such as verbose error messages?

**A.** httpd.conf
**B.** administration.config
**C.** idq.dll
**D.** php.ini
**Answer: (SHOW ANSWER)**
Explanation
idq.dll may be a library employed by ISAPI for indexing.idq.dll may be a system process that's needed for your PC to figure properly. It shouldn't be removed.The idq.dll is an executable file on your computer's disk drive . This file contains machine language . If you begin the software Microsoft Windows on your PC, the commands contained in idq.dll are going to be executed on your PC. For this purpose, the file is loaded into the most memory (RAM) and runs there as a Microsoft Indexing Service ISAPI Extension process (also called a task).
Is idq.dll harmful?This process is taken into account safe. it's unlikely to pose any harm to your system.
Can I stop or remove idq.dll?Since idq.dll may be a system process it shouldn't be stopped. the method is required for your PC to figure properly. Also the corresponding software Microsoft Windows shouldn't be uninstalled.
Is idq.dll CPU intensive?This process is taken into account to be CPU intensive. Without proper management, CPU intensive processes can manipulate system resources causing speed loss. Check the Microsoft Windows settings to ascertain if you'll close up unneeded modules or services.
Why is idq.dll giving me errors?System process issues are mainly a results of conflicting applications running on your PC. Consider uninstalling any applications you're not using. Then reboot your computer.

**NEW QUESTION: 95**
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 2011-03-15 11:06 NMAP scan report for 172.16.40.65 Host is up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn
515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8
**A.** The host is likely a Linux machine.
**B.** The host is likely a router.
**C.** The host is likely a Windows machine.
**D.** The host is likely a printer.
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 96**
Andrew is an Ethical Hacker who was assigned the task of discovering all the active devices hidden by a restrictive firewall in the IPv4 range in a given target network.
Which of the following host discovery techniques must he use to perform the given task?
**A.** ACK flag probe scan
**B.** TCP Maimon scan
**C.** UDP scan
**D.** app ping scan
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 97**
Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.


In MAC flooding attack, a switch is fed with many Ethernet frames, each containing different source MAC addresses, by the attacker. Switches have a limited memory for mapping various MAC addresses to physical ports. What happens when the CAM table becomes full?
**A.** Switch then acts as hub by broadcasting packets to all machines on the network
**B.** Every packet is dropped and the switch sends out SNMP alerts to the IDS port
**C.** The CAM overflow table will cause the switch to crash causing Denial of Service
**D.** The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 98**
User A is writing a sensitive email message to user B outside the local network. User A has chosen to use PKI to secure his message and ensure only user B can read the sensitive email. At what layer of the OSI layer does the encryption and decryption of the message take place?
**A.** Application
**B.** Transport

**C.** Presentation
**D.** Session
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 99**
_____ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.
**A.** Scanner
**B.** RootKit
**C.** Trojan
**D.** Backdoor
**E.** DoS tool
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 100**
what is the port to block first in case you are suspicious that an IoT device has been compromised?
**A.** 22
**B.** 443
**C.** 48101
**D.** 80
**Answer: B (LEAVE A REPLY)**
Explanation
You can perceive Port 443 as an online browsing port wont to secure browser communication or HTTPS services.
It will offer coding and transport over secure ports. Thus, the information you transfer across such connections are extremely proof against third-party eavesdropping and interruption.
Moreover, the identity of the server that you just connect remotely may be documented confidently.
Once the association is established, internet browsers can show signs sort of a padlock, Associate in Nursing unbroken key, etc. within the standing region of your window, informing you regarding the secured connections.
Though Port 443 is that the commonplace port for HTTPS traffic, HTTPS port 443 also can support HTTP sites. just in case the positioning uses HTTPS however is unable to load over port 443, port eighty that handles all unencrypted HTTP internet traffic can step in to load the HTTPS-enabled web site.

**NEW QUESTION: 101**

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.** Copy the data to removable media and keep it in case you need it.
**B.** Immediately stop work and contact the proper legal authorities.
**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: B (LEAVE A REPLY)**

**NEW QUESTION: 102**
You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL.
What may be the problem?
**A.** Traffic is Blocked on UDP Port 80
**B.** Traffic is Blocked on UDP Port 53
**C.** Traffic is Blocked on TCP Port 80
**D.** Traffic is Blocked on TCP Port 54
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 103**
Nedved is an IT Security Manager of a bank in his country. One day. he found out that there is a security breach to his company's email server based on analysis of a suspicious connection from the email server to an unknown IP Address.
What is the first thing that Nedved needs to do before contacting the incident response team?
**A.** Leave it as it Is and contact the incident response te3m right away
**B.** Migrate the connection to the backup email server
**C.** Disconnect the email server from the network
**D.** Block the connection to the suspicious IP Address from the firewall
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 104**
Susan, a software developer, wants her web API to update other applications with the latest information. For this purpose, she uses a user-defined HTTP tailback or push APIs that are raised based on trigger events: when invoked, this feature supplies data to other applications so that users can instantly receive real-time Information.
Which of the following techniques is employed by Susan?
**A.** SOAP API

**B.** REST API
**C.** Webhoos
**D.** web shells
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 105**
Ethical hacker jane Smith is attempting to perform an SQL injection attach. She wants to test the response time of a true or false response and wants to use a second command to determine whether the database will return true or false results for user IDs. which two SQL Injection types would give her the results she is looking for?
**A.** Out of band and boolean-based
**B.** Time-based and boolean-based
**C.** union-based and error-based
**D.** Time-based and union-based
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 106**
You are analysing traffic on the network with Wireshark. You want to routinely run a cron job which will run the capture against a specific set of IPs - 192.168.8.0/24. What command you would use?
**A.** wireshark --fetch "192.168.8*"
**B.** tshark -net 192.255.255.255 mask 192.168.8.0
**C.** sudo tshark -f"net 192 .68.8.0/24"
**D.** wireshark --capture --local masked 192.168.8.0 ---range 24
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 107**
Scenario1:
1.Victim opens the attacker's web site.
2.Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make
$1000 in a day?'.

3.Victim clicks to the interesting and attractive content URL.
4.Attacker creates a transparent 'iframe' in front of the URL which victim attempts to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' URL but actually he/she clicks to the content or URL that exists in the transparent 'iframe' which is setup by the attacker.
What is the name of the attack which is mentioned in the scenario?
**A.** HTTP Parameter Pollution
**B.** HTML Injection
**C.** Clickjacking Attack
**D.** Session Fixation
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 108**
Attacker Rony Installed a rogue access point within an organization's perimeter and attempted to Intrude into its internal network. Johnson, a security auditor, identified some unusual traffic in the internal network that is aimed at cracking the authentication mechanism. He immediately turned off the targeted network and tested for any weak and outdated security mechanisms that are open to attack. What is the type of vulnerability assessment performed by Johnson in the above scenario?
**A.** Distributed assessment
**B.** Wireless network assessment
**C.** Most-based assessment
**D.** Application assessment
**Answer: (SHOW ANSWER)**
Explanation
Expanding your network capabilities are often done well using wireless networks, but it also can be a source of harm to your data system . Deficiencies in its implementations or configurations can allow tip to be accessed in an unauthorized manner.This makes it imperative to closely monitor your wireless network while also conducting periodic Wireless Network assessment.It identifies flaws and provides an unadulterated view of exactly how vulnerable your systems are to malicious and unauthorized accesses.Identifying misconfigurations and inconsistencies in wireless implementations and rogue access points can improve your security posture and achieve compliance with regulatory frameworks.

**NEW QUESTION: 109**
Which type of security feature stops vehicles from crashing through the doors of a building?
**A.** Receptionist
**B.** Bollards
**C.** Mantrap

**D.** Turnstile
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 110**
After an audit, the auditors Inform you that there is a critical finding that you must tackle Immediately. You read the audit report, and the problem is the service running on port 369. Which service Is this and how can you tackle the problem?
**A.** The service is SMTP, and you must change it to SMIME. which is an encrypted way to send emails.
**B.** The service is NTP. and you have to change It from UDP to TCP in order to encrypt it
**C.** The service is LDAP. and you must change it to 636. which is LDPAPS.
**D.** The findings do not require immediate actions and are only suggestions.
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 111**
Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

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

From the above list identify the user account with System Administrator privileges.
**A.** Chang
**B.** Somia
**C.** Sheela
**D.** Rebecca
**E.** Shawn
**F.** Micah
**G.** John
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 112**
While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?

**A.** Web form input validation
**B.** Cross-Site Scripting
**C.** Clickjacking
**D.** Cross-Site Request Forgery
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 113**
Which service in a PKI will vouch for the identity of an individual or company?
**A.** KDC
**B.** CR
**C.** CA
**D.** CBC
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 114**
MX record priority increases as the number increases. (True/False.)
**A.** True
**B.** False
**Answer: B (LEAVE A REPLY)**

**NEW QUESTION: 115**
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing - Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?
**A.** BBProxy
**B.** BBCrack
**C.** Blooover
**D.** Paros Proxy
**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 116**
Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?
**A.** SOA
**B.** biometrics
**C.** single sign on
**D.** PKI
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 117**
This wireless security protocol allows 192-bit minimum-strength security protocols and cryptographic tools to protect sensitive data, such as GCMP-2S6. MMAC-SHA384, and ECDSA using a 384-bit elliptic curve.
Which is this wireless security protocol?
**A.** WPA2 Personal
**B.** WPA3-Personal
**C.** WPA2-Enterprise
**D.** WPA3-Enterprise
**Answer: (SHOW ANSWER)**
Explanation
Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise.
WPA3-Enterprise builds upon WPA2 and ensures the consistent application of security protocol across the network.WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to raised protect sensitive data:* Authenticated encryption: 256-bit Galois/Counter Mode Protocol (GCMP-256)* Key derivation and confirmation: 384-bit Hashed Message Authentication Mode (HMAC) with Secure Hash Algorithm (HMAC-SHA384)* Key establishment and authentication: Elliptic Curve Diffie-Hellman (ECDH) exchange and Elliptic Curve Digital Signature Algorithm (ECDSA) employing a 384-bit elliptic curve* Robust management frame protection: 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256)The 192-bit security mode offered by WPA3-Enterprise ensures the proper combination of cryptographic tools are used and sets a uniform baseline of security within a WPA3 network.

**NEW QUESTION: 118**
Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users.
**A.** SQL injection attack
**B.** LDAP Injection attack
**C.** Cross-Site Request Forgery (CSRF)
**D.** Cross-Site Scripting (XSS)
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 119**
How is the public key distributed in an orderly, controlled fashion so that the users can be sure of the sender's identity?
**A.** Hash value
**B.** Private key

**C.** Digital certificate
**D.** Digital signature
**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 120**
The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the Central Processing Unit (CPU), rather than passing only the frames that the controller is intended to receive.
Which of the following is being described?
**A.** WEM
**B.** Multi-cast mode
**C.** Port forwarding
**D.** Promiscuous mode
**Answer: D (LEAVE A REPLY)**

**NEW QUESTION: 121**
The tools which receive event logs from servers, network equipment, and applications, and perform analysis and correlation on those logs, and can generate alarms for security relevant issues, are known as what?
**A.** Intrusion prevention Server
**B.** Security incident and event Monitoring
**C.** network Sniffer
**D.** Vulnerability Scanner
**Answer: (SHOW ANSWER)**



**NEW QUESTION: 122**
Gilbert, a web developer, uses a centralized web API to reduce complexity and increase the Integrity of updating and changing data. For this purpose, he uses a web service that uses HTTP methods such as PUT.
POST. GET. and DELETE and can improve the overall performance, visibility, scalability, reliability, and portability of an application. What is the type of web-service API mentioned in the above scenario?

**A.** RESTful API
**B.** SOAP API
**C.** REST API
**D.** JSON-RPC
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 123**
You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

```
char shellcode[] =
"\x31\xc0\xb0\x46\x31\xdb\x31\xc9\xcd\x80\xeb\x16\x5b\x31\xc0"
"\x88\x43\x07\x89\x5b\x08\x89\x43\x0c\xb0\x0b\x8d\x4b\x08\x8d"
"\x53\x0c\xcd\x80\xe8\xe5\xff\xff\xff\x2f\x62\x69\x6e\x2f\x73"
"\x68";
```

What is the hexadecimal value of NOP instruction?
**A.** 0x80
**B.** 0x90
**C.** 0x70
**D.** 0x60
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 124**
You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration? alert tcp any any -> 192.168.100.0/24 21 (msg: ""FTP on the network!"";)
**A.** An Intrusion Detection System
**B.** A Router IPTable
**C.** FTP Server rule
**D.** A firewall IPTable
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 125**
What hacking attack is challenge/response authentication used to prevent?
**A.** Scanning attacks
**B.** Password cracking attacks
**C.** Session hijacking attacks
**D.** Replay attacks
**Answer: (SHOW ANSWER)**

**NEW QUESTION: 126**
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other

machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

**A.** The gateway and the computer are not on the same network.

**B.** The computer is using an invalid IP address.

**C.** The computer is not using a private IP address.

**D.** The gateway is not routing to a public IP address.

**Answer: (SHOW ANSWER)**

**NEW QUESTION: 127**

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.** Hierarchical, Relational

**B.** Simple, Complex

**C.** Strict, Abstract

**D.** Relational, Hierarchical

**Answer: A (LEAVE A REPLY)**

**NEW QUESTION: 128**

Morris, a professional hacker, performed a vulnerability scan on a target organization by sniffing the traffic on the network lo identify the active systems, network services, applications, and vulnerabilities. He also obtained the list of the users who are currently accessing the network. What is the type of vulnerability assessment that Morris performed on the target organization?

**A.** internal assessment

**B.** Passive assessment

**C.** Credentialed assessment

**D.** External assessment

**Answer: C (LEAVE A REPLY)**

**NEW QUESTION: 129**

Which of the following statements about a zone transfer is correct? (Choose three.)

**A.** A zone transfer can be prevented by blocking all inbound TCP port 53 connections

**B.** A zone transfer is accomplished with the DNS

**C.** A zone transfer passes all zone information that a nslookup server maintains

**D.** A zone transfer passes all zone information that a DNS server maintains

**E.** Zone transfers cannot occur on the Internet

**F.** A zone transfer is accomplished with the nslookup service

**Answer: A,B,D (LEAVE A REPLY)**

**Valid 312-50v11 Dumps** shared by Fast2test.com for Helping Passing 312-50v11 Exam! Fast2test.com now offer the **newest 312-50v11 exam dumps**, the Fast2test.com 312-50v11 exam **questions have been updated** and **answers have been corrected** get the **newest** Fast2test.com 312-50v11 dumps with Test Engine here: https://www.fast2test.com/312-50v11-premium-file.html (**375** Q&As Dumps, **40%OFF Special Discount: freecram**)