**615 Questions - CEHv9**

[Q1] 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

[Q2] Which of the following is an application that requires a host application for replication?

A. Micro

B. Worm

C. Trojan

D. Virus

[Q3] 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

[Q4] Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

A. Restore a random file.

B. Perform a full restore.

C. Read the first 512 bytes of the tape.

D. Read the last 512 bytes of the tape.

[Q5] Which of the following describes the characteristics of a Boot Sector Virus?

A. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR

B. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR

C. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

D. Overwrites the original MBR and only executes the new virus code

[Q6] Which statement is TRUE regarding network firewalls preventing Web Application attacks?

A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.

B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.

C. Network firewalls can prevent attacks if they are properly configured.

D. Network firewalls cannot prevent attacks because they are too complex to configure.

[Q7] Which of the following programs is usually targeted at Microsoft Office products?

A. Polymorphic virus

B. Multipart virus

C. Macro virus

D. Stealth virus

[Q8] 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)

[Q9] In order to show improvement of security over time, what must be developed?

A. Reports

B. Testing tools

C. Metrics

D. Taxonomy of vulnerabilities

[Q10] Passive reconnaissance involves collecting information through which of the following?

A. Social engineering

B. Network traffic sniffing

C. Man in the middle attacks

D. Publicly accessible sources

[Q11] How can rainbow tables be defeated?

A. Password salting

B. Use of non-dictionary words

C. All uppercase character passwords

D. Lockout accounts under brute force password cracking attempts

[Q12] 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:

A. Ping sweep of the 192.168.1.106 network

B. Remote service brute force attempt

C. Port scan of 192.168.1.106

D. Denial of service attack on 192.168.1.106

[Q13] An NMAP scan of a server shows port 25 is open. What risk could this pose?

A. Open printer sharing

B. Web portal data leak

C. Clear text authentication

D. Active mail relay

[Q14] 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?

A. The host is likely a Windows machine.

B. The host is likely a Linux machine.

C. The host is likely a router.

D. The host is likely a printer.

[Q15] What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?

A. Passive

B. Reflective

C. Active

D. Distributive

[Q16] Which of the following lists are valid data-gathering activities associated with a risk assessment?

A. Threat identification, vulnerability identification, control analysis

B. Threat identification, response identification, mitigation identification

C. Attack profile, defense profile, loss profile

D. System profile, vulnerability identification, security determination

[Q17] A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems. What kind of test is being performed?

A. white box

B. grey box

C. red box

D. black box

[Q18] Which of the following is a detective control?

A. Smart card authentication

B. Security policy

C. Audit trail

D. Continuity of operations plan

[Q19] Which of the following is a component of a risk assessment?

A. Physical security

B. Administrative safeguards

C. DMZ

D. Logical interface

[Q20] When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

A. Vulnerability scanning

B. Social engineering

C. Application security testing

D. Network sniffing

[Q21] A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?

A. Reject all invalid email received via SMTP.

B. Allow full DNS zone transfers.

C. Remove A records for internal hosts.

D. Enable null session pipes.

[Q22] Which of the following techniques will identify if computer files have been changed?

A. Network sniffing

B. Permission sets

C. Integrity checking hashes

D. Firewall alerts

[Q23] Which system consists of a publicly available set of databases that contain domain name registration contact information?

A. WHOIS

B. IANA

C. CAPTCHA

D. IETF

[Q24] A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?

A. Information reporting

B. Vulnerability assessment

C. Active information gathering

D. Passive information gathering

[Q25] The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:

A. Port scan targeting 192.168.1.103

B. Teardrop attack targeting 192.168.1.106

C. Denial of service attack targeting 192.168.1.103

D. Port scan targeting 192.168.1.106

[Q26] 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:

A. Cross-site scripting

B. Banner grabbing

C. SQL injection

D. Whois database query

[Q27] An NMAP scan of a server shows port 69 is open. What risk could this pose?

A. Unauthenticated access

B. Weak SSL version

C. Cleartext login

D. Web portal data leak

[Q28] What information should an IT system analysis provide to the risk assessor?

A. Management buy-in

B. Threat statement

C. Security architecture

D. Impact analysis

[Q29] Which results will be returned with the following Google search query?

site:target.com -site:Marketing.target.com accounting

A. Results matching all words in the query

B. Results matching accounting in domain target.com but not on the site Marketing.target.com

C. Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting

D. Results for matches on target.com and Marketing.target.com that include the word accounting

[Q30] A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?

A. Perform a vulnerability scan of the system.

B. Determine the impact of enabling the audit feature.

C. Perform a cost/benefit analysis of the audit feature.

D. Allocate funds for staffing of audit log review.

[Q31] Which of the following is a preventive control?

A. Smart card authentication

B. Security policy

C. Audit trail

D. Continuity of operations plan

[Q32] Which of the following is considered an acceptable option when managing a risk?

A. Reject the risk.

B. Deny the risk.

C. Mitigate the risk.

D. Initiate the risk.

[Q33] Which security control role does encryption meet?

A. Preventative

B. Detective

C. Offensive

D. Defensive

[Q34] A covert channel is a channel that

A. transfers information over, within a computer system, or network that is outside of the security policy.

B. transfers information over, within a computer system, or network that is within the security policy.

C. transfers information via a communication path within a computer system, or network for transfer of data.

D. transfers information over, within a computer system, or network that is encrypted.

[Q35] 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

[Q36] 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.

[Q37] If the final set of security controls does not eliminate all risk in a system, what could be done next?

A. Continue to apply controls until there is zero risk.

B. Ignore any remaining risk.

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

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

[Q38] What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?

A. Proper testing

B. Secure coding principles

C. Systems security and architecture review

D. Analysis of interrupts within the software

[Q39] Which of the following examples best represents a logical or technical control?

A. Security tokens

B. Heating and air conditioning

C. Smoke and fire alarms

D. Corporate security policy

[Q40] Which type of access control is used on a router or firewall to limit network activity?

A. Mandatory

B. Discretionary

C. Rule-based

D. Role-based

[Q41] At a Windows Server command prompt, which command could be used to list the running services?

A. Sc query type= running

B. Sc query \servername

C. Sc query

D. Sc config

[Q42] Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?

A. Cross-site scripting

B. SQL injection

C. Missing patches

D. CRLF injection

[Q43] While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type of firewall is the tester trying to traverse?

A. Packet filtering firewall

B. Application-level firewall

C. Circuit-level gateway firewall

D. Stateful multilayer inspection firewall

[Q44] A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:

A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389

B. Permit 217.77.88.12 11.12.13.50 RDP 3389

C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389

D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

[Q45] A circuit level gateway works at which of the following layers of the OSI Model?

A. Layer 5 -Application

B. Layer 4 TCP

C. Layer 3 Internet protocol

D. Layer 2 Data link

[Q46] Which of the following is a symmetric cryptographic standard?

A. DSA

B. PKI

C. RSA

D. 3DES

[Q47] 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.

A. Man-in-the-middle attack

B. Brute-force attack

C. Dictionary attack

D. Session hijacking

[Q48] Which property ensures that a hash function will not produce the same hashed value for two different messages?

A. Collision resistance

B. Bit length

C. Key strength

D. Entropy

[Q49] How can telnet be used to fingerprint a web server?

A. telnet webserverAddress 80

HEAD / HTTP/1.0

B. telnet webserverAddress 80

PUT / HTTP/1.0

C. telnet webserverAddress 80

HEAD / HTTP/2.0

D. telnet webserverAddress 80

PUT / HTTP/2.0

[Q50] Low humidity in a data center can cause which of the following problems?

A. Heat

B. Corrosion

C. Static electricity

D. Airborne contamination

[Q51] A consultant is hired to do physical penetration testing at a large financial company. In the first day of his assessment, the consultant goes to the company`s building dressed like an electrician and waits in the lobby for an employee to pass through the main

access gate, then the consultant follows the employee behind to get into the restricted area. Which type of attack did the consultant perform?

A. Man trap

B. Tailgating

C. Shoulder surfing

D. Social engineering

[Q52] When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's computer to update the router configuration. What type of an alert is this?

A. False positive

B. False negative

C. True positve

D. True negative

[Q53] While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?

A. Validate web content input for query strings.

B. Validate web content input with scanning tools.

C. Validate web content input for type, length, and range.

D. Validate web content input for extraneous queries.

[Q54] A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?

A. Forensic attack

B. ARP spoofing attack

C. Social engineering attack

D. Scanning attack

[Q55] Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?

A. Metasploit scripting engine

B. Nessus scripting engine

C. NMAP scripting engine

D. SAINT scripting engine

[Q56] Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?

A. Microsoft Security Baseline Analyzer

B. Retina

C. Core Impact

D. Microsoft Baseline Security Analyzer

[Q57] 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. Firewall-management policy

B. Acceptable-use policy

C. Remote-access policy

D. Permissive policy

[Q58] When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?

A. A bottom-up approach

B. A top-down approach

C. A senior creation approach

D. An IT assurance approach

[Q59] Which of the following processes evaluates the adherence of an organization to its stated security policy?

A. Vulnerability assessment

B. Penetration testing

C. Risk assessment

D. Security auditing

[Q60] A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?

A. The consultant will ask for money on the bid because of great work.

B. The consultant may expose vulnerabilities of other companies.

C. The company accepting bids will want the same type of format of testing.

D. The company accepting bids will hire the consultant because of the great work performed.

[Q61] Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan

B. Retinal scan

C. Iris scan

D. Signature kinetics scan

[Q62] What is the main reason the use of a stored biometric is vulnerable to an attack?

A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.

B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.

C. A stored biometric is no longer "something you are" and instead becomes "something you have".

D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

[Q63] During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?

A. The tester must capture the WPA2 authentication handshake and then crack it.

B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.

C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.

D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

[Q64] Which type of antenna is used in wireless communication?

A. Omnidirectional

B. Parabolic

C. Uni-directional

D. Bi-directional

[Q65] What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?

A. Blue Book

B. ISO 26029

C. Common Criteria

D. The Wassenaar Agreement

[Q66] One way to defeat a multi-level security solution is to leak data via

A. a bypass regulator.

B. steganography.

C. a covert channel.

D. asymmetric routing.

[Q67] Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?

A. The victim user must open the malicious link with an Internet Explorer prior to version 8.

B. The session cookies generated by the application do not have the HttpOnly flag set.

C. The victim user must open the malicious link with a Firefox prior to version 3.

D. The web application should not use random tokens.

[Q68] What is the main difference between a Normal SQL Injection and a Blind SQL Injection vulnerability?

A. The request to the web server is not visible to the administrator of the vulnerable application.

B. The attack is called Blind because, although the application properly filters user input, it is still vulnerable to code injection.

C. The successful attack does not show an error message to the administrator of the affected application.

D. The vulnerable application does not display errors with information about the injection results to the attacker.

[Q69] During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?

A. Using the Metasploit psexec module setting the SA / Admin credential

B. Invoking the stored procedure xp\_shell to spawn a Windows command shell

C. Invoking the stored procedure cmd\_shell to spawn a Windows command shell

D. Invoking the stored procedure xp\_cmdshell to spawn a Windows command shell

[Q70] The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?

A. Physical

B. Procedural

C. Technical

D. Compliance

[Q71] A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?

A. Netsh firewall show config

B. WMIC firewall show config

C. Net firewall show config

D. Ipconfig firewall show config

[Q72] Which of the following types of firewall inspects only header information in network traffic?

A. Packet filter

B. Stateful inspection

C. Circuit-level gateway

D. Application-level gateway

[Q73] During a penetration test, the tester conducts an ACK scan using NMAP against the external interface of the DMZ firewall. NMAP reports that port 80 is unfiltered. Based on this response, which type of packet inspection is the firewall conducting?

A. Host

B. Stateful

C. Stateless

D. Application

[Q74] Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?

A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.

B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.

C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.

D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

[Q75] Which of the following is an example of an asymmetric encryption implementation?

A. SHA1

B. PGP

C. 3DES

D. MD5

[Q76] A hacker was able to sniff packets on a company's wireless network. The following information was discovered:

A. 00101000 11101110

B. 11010111 00010001

C. 00001101 10100100 D. 11110010 01011011

00001101 10100100

D. 11110010 01011011

[Q77] Which of the following cryptography attack methods is usually performed without the use of a computer?

A. Ciphertext-only attack

B. Chosen key attack

C. Rubber hose attack

D. Rainbow table attack

[Q78] Which of the following is a strong post designed to stop a car?

A. Gate

B. Fence

C. Bollard

D. Reinforced rebar

[Q79] A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.

A. Segregation of duties

B. Undue influence

C. Lack of experience

D. Inadequate disaster recovery plan

[Q80] What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?

A. Set a BIOS password.

B. Encrypt the data on the hard drive.

C. Use a strong logon password to the operating system.

D. Back up everything on the laptop and store the backup in a safe place.

[Q81] In the software security development life cycle process, threat modeling occurs in which phase?

A. Design

B. Requirements

C. Verification

D. Implementation

[Q82] 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 negatives

B. False negatives

C. True positives

D. False positives

[Q83] Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?

A. Port scanning

B. Banner grabbing

C. Injecting arbitrary data

D. Analyzing service response

[Q84] Which of the following business challenges could be solved by using a vulnerability scanner?

A. Auditors want to discover if all systems are following a standard naming convention.

B. A web server was compromised and management needs to know if any further systems were compromised.

C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.

D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

[Q85] A security policy will be more accepted by employees if it is consistent and has the support of

A. coworkers.

B. executive management.

C. the security officer.

D. a supervisor.

[Q86] A company has hired a security administrator to maintain and administer Linux and Windows-based systems. Written in the nightly report file is the following:

Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.

Which of the following actions should the security administrator take?

A. Log the event as suspicious activity and report this behavior to the incident response team immediately.

B. Log the event as suspicious activity, call a manager, and report this as soon as possible.

C. Run an anti-virus scan because it is likely the system is infected by malware.

D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

[Q87] Which type of scan measures a person's external features through a digital video camera?

A. Iris scan

B. Retinal scan

C. Facial recognition scan

D. Signature kinetics scan

[Q88] WPA2 uses AES for wireless data encryption at which of the following encryption levels?

A. 64 bit and CCMP

B. 128 bit and CRC

C. 128 bit and CCMP

D. 128 bit and TKIP

[Q89] An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?

A. Classified

B. Overt

C. Encrypted

D. Covert

[Q90] What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?

A. Injecting parameters into a connection string using semicolons as a separator

B. Inserting malicious Javascript code into input parameters

C. Setting a user's session identifier (SID) to an explicit known value

D. Adding multiple parameters with the same name in HTTP requests

[Q91] A newly discovered flaw in a software application would be considered which kind of security vulnerability?

A. Input validation flaw

B. HTTP header injection vulnerability

C. 0-day vulnerability

D. Time-to-check to time-to-use flaw

[Q92] During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?

A. The web application does not have the secure flag set.

B. The session cookies do not have the HttpOnly flag set.

C. The victim user should not have an endpoint security solution.

D. The victim's browser must have ActiveX technology enabled.

[Q93] The use of alert thresholding in an IDS can reduce the volume of repeated alerts, but introduces which of the following vulnerabilities?

A. An attacker, working slowly enough, can evade detection by the IDS.

B. Network packets are dropped if the volume exceeds the threshold.

C. Thresholding interferes with the IDS ability to reassemble fragmented packets.

D. The IDS will not distinguish among packets originating from different sources.

[Q94] What is the main advantage that a network-based IDS/IPS system has over a host-based solution?

A. They do not use host system resources.

B. They are placed at the boundary, allowing them to inspect all traffic.

C. They are easier to install and configure.

D. They will not interfere with user interfaces.

[Q95] The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?

A. Asymmetric

B. Confidential

C. Symmetric

D. Non-confidential

[Q96] When an alert rule is matched in a network-based IDS like snort, the IDS does which of the following?

A. Drops the packet and moves on to the next one

B. Continues to evaluate the packet until all rules are checked

C. Stops checking rules, sends an alert, and lets the packet continue

D. Blocks the connection with the source IP address in the packet

[Q97] Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?

A. Detective

B. Passive

C. Intuitive

D. Reactive

[Q98] An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?

A. The wireless card was not turned on.

B. The wrong network card drivers were in use by Wireshark.

C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.

D. Certain operating systems and adapters do not collect the management or control packets.

[Q99] From the two screenshots below, which of the following is occurring?

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

B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

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

D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

[Q100] Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?

A. Cain

B. John the Ripper

C. Nikto

D. Hping

[Q101] Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?

A. They are written in Java.

B. They send alerts to security monitors.

C. They use the same packet analysis engine.

D. They use the same packet capture utility.

[Q102] Which set of access control solutions implements two-factor authentication?

A. USB token and PIN

B. Fingerprint scanner and retina scanner

C. Password and PIN

D. Account and password

[Q103] A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the companys internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?

A. SSL

B. Mutual authentication

C. IPSec

D. Static IP addresses

[Q104] 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)

[Q105] To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?

A. Recipient's private key

B. Recipient's public key

C. Master encryption key

D. Sender's public key

[Q106] An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?

A. g++ hackersExploit.cpp -o calc.exe

B. g++ hackersExploit.py -o calc.exe

C. g++ -i hackersExploit.pl -o calc.exe

D. g++ –compile i hackersExploit.cpp -o calc.exe

[Q107] 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.

A. PHP

B. C#

C. Python

D. ASP.NET

[Q108] A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:

A. A buffer overflow exploit

B. A chained exploit

C. A SQL injection exploit

D. A denial of service exploit

[Q109] One advantage of an application-level firewall is the ability to

A. filter packets at the network level.

B. filter specific commands, such as http:post.

C. retain state information for each packet.

D. monitor tcp handshaking.

[Q110] Which of the statements concerning proxy firewalls is correct?

A. Proxy firewalls increase the speed and functionality of a network.

B. Firewall proxy servers decentralize all activity for an application.

C. Proxy firewalls block network packets from passing to and from a protected network.

D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

[Q111] Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?

A. NMAP -PN -A -O -sS 192.168.2.0/24

B. NMAP -P0 -A -O -p1-65535 192.168.0/24

C. NMAP -P0 -A -sT -p0-65535 192.168.0/16

D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

[Q112] While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?

A. 10.10.10.10

B. 127.0.0.1

C. 192.168.1.1

D. 192.168.168.168

[Q113] A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?

A. NMAP -P 192.168.1-5.

B. NMAP -P 192.168.0.0/16

C. NMAP -P 192.168.1.0,2.0,3.0,4.0,5.0

D. NMAP -P 192.168.1/17

[Q114] A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?

A. Spoofing an IP address

B. Tunneling scan over SSH

C. Tunneling over high port numbers

D. Scanning using fragmented IP packets

[Q115] A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?

A. -sO

B. -sP

C. -sS

D. -sU

[Q116] ICMP ping and ping sweeps are used to check for active systems and to check

A. if ICMP ping traverses a firewall.

B. the route that the ICMP ping took.

C. the location of the switchport in relation to the ICMP ping.

D. the number of hops an ICMP ping takes to reach a destination.

[Q117] Which command line switch would be used in NMAP to perform operating system detection?

A. -OS

B. -sO

C. -sP

D. -O

[Q118] A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?

A. Locate type=ns

B. Request type=ns

C. Set type=ns

D. Transfer type=ns

[Q119] A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?

A. Cupp

B. Nessus

C. Cain and Abel

D. John The Ripper Pro

[Q120] On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?

A. nessus +

B. nessus \*s

C. nessus &

D. nessus -d

[Q121] Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?

A. NMAP

B. Metasploit

C. Nessus

D. BeEF

[Q122] What is the best defense against privilege escalation vulnerability?

A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.

B. Run administrator and applications on least privileges and use a content registry for tracking.

C. Run services with least privileged accounts and implement multi-factor authentication and authorization.

D. Review user roles and administrator privileges for maximum utilization of automation services.

[Q123] How can a rootkit bypass Windows 7 operating systems 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

[Q124] Which of the following items of a computer system will an anti-virus program scan for viruses?

A. Boot Sector

B. Deleted Files

C. Windows Process List

D. Password Protected Files

[Q125] Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?

A. UDP 123

B. UDP 541

C. UDP 514

D. UDP 415

[Q126] A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?

A. Issue the pivot exploit and set the meterpreter.

B. Reconfigure the network settings in the meterpreter.

C. Set the payload to propagate through the meterpreter.

D. Create a route statement in the meterpreter.

[Q127] What is the outcome of the commnc -l -p 2222 | nc 10.1.0.43 1234"?

A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.

B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.

C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.

D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

[Q128] Which of the following is a client-server tool utilized to evade firewall inspection?

A. tcp-over-dns

B. kismet

C. nikto

D. hping

[Q129] Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?

A. DataThief

B. NetCat

C. Cain and Abel

D. SQLInjector

[Q130] A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database.

In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?

A. Semicolon

B. Single quote

C. Exclamation mark

D. Double quote

[Q131] Which of the following identifies the three modes in which Snort can be configured to run?

A. Sniffer, Packet Logger, and Network Intrusion Detection System

B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System

C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System

D. Sniffer, Packet Logger, and Host Intrusion Prevention System

[Q132] When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?

A. Network tap

B. Layer 3 switch

C. Network bridge

D. Application firewall

[Q133] Which of the following programming languages is most vulnerable to buffer overflow attacks?

A. Perl

B. C++

C. Python

D. Java

[Q134] Smart cards use which protocol to transfer the certificate in a secure manner?

A. Extensible Authentication Protocol (EAP)

B. Point to Point Protocol (PPP)

C. Point to Point Tunneling Protocol (PPTP)

D. Layer 2 Tunneling Protocol (L2TP)

[Q135] Which of the following is a hashing algorithm?

A. MD5

B. PGP

C. DES

D. ROT13

[Q136] Which of the following problems can be solved by using Wireshark?

A. Tracking version changes of source code

B. Checking creation dates on all webpages on a server

C. Resetting the administrator password on multiple systems

D. Troubleshooting communication resets between two systems

[Q137] What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?

A. tcp.src == 25 and ip.host == 192.168.0.125

B. host 192.168.0.125:25

C. port 25 and host 192.168.0.125

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

[Q138] Which tool would be used to collect wireless packet data?

A. NetStumbler

B. John the Ripper

C. Nessus

D. Netcat

[Q139] Which of the following is an example of two factor authentication?

A. PIN Number and Birth Date

B. Username and Password

C. Digital Certificate and Hardware Token

D. Fingerprint and Smartcard ID

[Q140] Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?

A. 768 bit key

B. 1025 bit key

C. 1536 bit key

D. 2048 bit key

[Q141] After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?

A. SHA1

B. Diffie-Helman

C. RSA

D. AES

[Q142] What statement is true regarding LM hashes?

A. LM hashes consist in 48 hexadecimal characters.

B. LM hashes are based on AES128 cryptographic standard.

C. Uppercase characters in the password are converted to lowercase.

D. LM hashes are not generated when the password length exceeds 15 characters.

[Q143] 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

[Q144] A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field:

A. Cross-site request forgery

B. Command injection

C. Cross-site scripting

D. SQL injection

[Q145] A security administrator notices that the log file of the companys webserver contains suspicious entries:

A. command injection.

B. SQL injection.

C. directory traversal.

D. LDAP injection.

[Q146] Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?

A. Firewall

B. Honeypot

C. Core server

D. Layer 4 switch

[Q147] Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?

A. ping 192.168.2.

B. ping 192.168.2.255

C. for %V in (1 1 255) do PING 192.168.2.%V

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

[Q148] What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?

A. A stealth scan, opening port 123 and 153

B. A stealth scan, checking open ports 123 to 153

C. A stealth scan, checking all open ports excluding ports 123 to 153

D. A stealth scan, determine operating system, and scanning ports 123 to 153

[Q149] Which of the following parameters enables NMAP's operating system detection feature?

A. NMAP -sV

B. NMAP -oS

C. NMAP -sR

D. NMAP -O

[Q150] Which of the following open source tools would be the best choice to scan a network for potential targets?

A. NMAP

B. NIKTO

C. CAIN

D. John the Ripper

[Q151] A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?

A. -sO

B. -sP

C. -sS

D. -sU

[Q152] A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?

A. Fraggle

B. MAC Flood

C. Smurf

D. Tear Drop

[Q153] Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?

A. Netstat WMI Scan

B. Silent Dependencies

C. Consider unscanned ports as closed

D. Reduce parallel connections on congestion

[Q154] How does an operating system protect the passwords used for account logins?

A. The operating system performs a one-way hash of the passwords.

B. The operating system stores the passwords in a secret file that users cannot find.

C. The operating system encrypts the passwords, and decrypts them when needed.

D. The operating system stores all passwords in a protected segment of non-volatile memory.

[Q155] Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

A. Cavity virus

B. Polymorphic virus

C. Tunneling virus

D. Stealth virus

[Q156] An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion

Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?

A. By using SQL injection

B. By changing hidden form values

C. By using cross site scripting

D. By utilizing a buffer overflow attack

[Q157] Which tool can be used to silently copy files from USB devices?

A. USB Grabber

B. USB Dumper

C. USB Sniffer

D. USB Snoopy

[Q158] Which of the following is used to indicate a single-line comment in structured query language (SQL)?

A. —

B. ||

C. %%

D. ''

[Q159] A security engineer is attempting to map a companys internal network. The engineer enters in the following NMAP command:

NMAP n sS P0 p 80 \*\*\*.\*\*\*.\*\*.\*\*

What type of scan is this?

A. Quick scan

B. Intense scan

C. Stealth scan

D. Comprehensive scan

[Q160] What is the broadcast address for the subnet 190.86.168.0/22?

A. 190.86.168.255

B. 190.86.255.255

C. 190.86.171.255

D. 190.86.169.255

[Q161] A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?

A. Perform a dictionary attack.

B. Perform a brute force attack.

C. Perform an attack with a rainbow table.

D. Perform a hybrid attack.

[Q162] Which of the following does proper basic configuration of snort as a network intrusion detection system require?

A. Limit the packets captured to the snort configuration file.

B. Capture every packet on the network segment.

C. Limit the packets captured to a single segment.

D. Limit the packets captured to the /var/log/snort directory.

[Q163] How is sniffing broadly categorized?

A. Active and passive

B. Broadcast and unicast

C. Unmanaged and managed

D. Filtered and unfiltered

[Q164] What are the three types of authentication?

A. Something you: know, remember, prove

B. Something you: have, know, are

C. Something you: show, prove, are

D. Something you: show, have, prove

[Q165] The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and

A. non-repudiation.

B. operability.

C. security.

D. usability.

[Q166] What is the main disadvantage of the scripting languages as opposed to compiled programming languages?

A. Scripting languages are hard to learn.

B. Scripting languages are not object-oriented.

C. Scripting languages cannot be used to create graphical user interfaces.

D. Scripting languages are slower because they require an interpreter to run the code.

[Q167] A botnet can be managed through which of the following?

A. IRC

B. E-Mail

C. Linkedin and Facebook

D. A vulnerable FTP server

[Q168] Fingerprinting VPN firewalls is possible with which of the following tools?

A. Angry IP

B. Nikto

C. Ike-scan

D. Arp-scan

[Q169] What is a successful method for protecting a router from potential smurf attacks?

A. Placing the router in broadcast mode

B. Enabling port forwarding on the router

C. Installing the router outside of the network's firewall

D. Disabling the router from accepting broadcast ping messages

[Q170] Which of the following is optimized for confidential communications, such as bidirectional voice and video?

A. RC4

B. RC5

C. MD4

D. MD5

[Q171] Advanced encryption standard is an algorithm used for which of the following?

A. Data integrity

B. Key discovery

C. Bulk data encryption

D. Key recovery

[Q172] The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?

A. Multiple keys for non-repudiation of bulk data

B. Different keys on both ends of the transport medium

C. Bulk encryption for data transmission over fiber

D. The same key on each end of the transmission medium

[Q173] An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?

A. Birthday attack

B. Plaintext attack

C. Meet in the middle attack

D. Chosen ciphertext attack

[Q174] What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?

A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.

B. To get messaging programs to function with this algorithm requires complex configurations.

C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.

D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

[Q175] A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?

A. Public key

B. Private key

C. Modulus length

D. Email server certificate

[Q176] When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?

A. The key entered is a symmetric key used to encrypt the wireless data.

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

C. The key entered is based on the Diffie-Hellman method.

D. The key is an RSA key used to encrypt the wireless data.

[Q177] An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?

A. Timing attack

B. Replay attack

C. Memory trade-off attack

D. Chosen plain-text attack

[Q178] 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 validation

C. Certificate cryptography

D. Certificate revocation

[Q179] Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?

A. Key registry

B. Recovery agent

C. Directory

D. Key escrow

[Q180] To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?

A. Harvesting

B. Windowing

C. Hardening

D. Stealthing

[Q181] Which of the following is a common Service Oriented Architecture (SOA) vulnerability?

A. Cross-site scripting

B. SQL injection

C. VPath injection

D. XML denial of service issues

[Q182] 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 maintenance schedule of the affected systems.

B. Investigate based on the service level agreements of the systems.

C. Investigate based on the potential effect of the incident.

D. Investigate based on the order that the alerts arrived in.

[Q183] An IT security engineer notices that the companys web server is currently being hacked. What should the engineer do next?

A. Unplug the network connection on the companys web server.

B. Determine the origin of the attack and launch a counterattack.

C. Record as much information as possible from the attack.

D. Perform a system restart on the companys web server.

[Q184] Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?

A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.

B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.

C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.

D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

[Q185] Which of the following items is unique to the N-tier architecture method of designing software applications?

A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.

B. It is compatible with various databases including Access, Oracle, and SQL.

C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.

D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

[Q186] If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?

A. Hping

B. Traceroute

C. TCP ping

D. Broadcast ping

[Q187] Which of the following descriptions is true about a static NAT?

A. A static NAT uses a many-to-many mapping.

B. A static NAT uses a one-to-many mapping.

C. A static NAT uses a many-to-one mapping.

D. A static NAT uses a one-to-one mapping.

[Q188] Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?

A. Teardrop

B. SYN flood

C. Smurf attack

D. Ping of death

[Q189] Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for www.eccouncil.org and receives an error message stating there is no response from the server. What should the administrator do next?

A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.

B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.

C. Configure the firewall to allow traffic on TCP port 53.

D. Configure the firewall to allow traffic on TCP port 8080.

[Q190] While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:

<script>alert(" Testing Testing Testing ")</script>

Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?

A. Buffer overflow

B. Cross-site request forgery

C. Distributed denial of service

D. Cross-site scripting

[Q191] Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?

A. They provide a repeatable framework.

B. Anyone can run the command line scripts.

C. They are available at low cost.

D. They are subject to government regulation.

[Q192] The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?

A. An extensible security framework named COBIT

B. A list of flaws and how to fix them

C. Web application patches

D. A security certification for hardened web applications

[Q193] In the OSI model, where does PPTP encryption take place?

A. Transport layer

B. Application layer

C. Data link layer

D. Network layer

[Q194] Which of the following is an example of IP spoofing?

A. SQL injections

B. Man-in-the-middle

C. Cross-site scripting

D. ARP poisoning

[Q195] For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?

A. Sender's public key

B. Receiver's private key

C. Receiver's public key

D. Sender's private key

[Q196] Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?

A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.

B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.

C. Hashing is faster compared to more traditional encryption algorithms.

D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

[Q197] Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?

A. Poly key exchange

B. Cross certification

C. Poly key reference

D. Cross-site exchange

[Q198] Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?

A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.

B. The root CA stores the user's hash value for safekeeping.

C. The CA is the trusted root that issues certificates.

D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

[Q199] A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?

A. Implementing server-side PKI certificates for all connections

B. Mandating only client-side PKI certificates for all connections

C. Requiring client and server PKI certificates for all connections

D. Requiring strong authentication for all DNS queries

[Q200] Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?

A. RSA 1024 bit strength

B. AES 1024 bit strength

C. RSA 512 bit strength

D. AES 512 bit strength

[Q201] Which of the following is a characteristic of Public Key Infrastructure (PKI)?

A. Public-key cryptosystems are faster than symmetric-key cryptosystems.

B. Public-key cryptosystems distribute public-keys within digital signatures.

C. Public-key cryptosystems do not require a secure key distribution channel.

D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

[Q202] Which security strategy requires using several, varying methods to protect IT systems against attacks?

A. Defense in depth

B. Three-way handshake

C. Covert channels

D. Exponential backoff algorithm

[Q203] SOAP services use which technology to format information?

A. SATA

B. PCI

C. XML

D. ISDN

[Q204] Which statement best describes a server type under an N-tier architecture?

A. A group of servers at a specific layer

B. A single server with a specific role

C. A group of servers with a unique role

D. A single server at a specific layer

[Q205] If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?

A. SDLC process

B. Honey pot

C. SQL injection

D. Trap door

[Q206] A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

A. The gateway is not routing to a public IP address.

B. The computer is using an invalid IP address.

C. The gateway and the computer are not on the same network.

D. The computer is not using a private IP address.

[Q207] Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?

A. Ping of death

B. SYN flooding

C. TCP hijacking

D. Smurf attack

[Q208] Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the networks IDS?

A. Timing options to slow the speed that the port scan is conducted

B. Fingerprinting to identify which operating systems are running on the network

C. ICMP ping sweep to determine which hosts on the network are not available

D. Traceroute to control the path of the packets sent during the scan

[Q209] When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is

A. OWASP is for web applications and OSSTMM does not include web applications.

B. OSSTMM is gray box testing and OWASP is black box testing.

C. OWASP addresses controls and OSSTMM does not.

D. OSSTMM addresses controls and OWASP does not.

[Q210] Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?

A. WebBugs

B. WebGoat

C. VULN\_HTML

D. WebScarab

[Q211] What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?

A. Legal, performance, audit

B. Audit, standards based, regulatory

C. Contractual, regulatory, industry

D. Legislative, contractual, standards based

[Q212] Which of the following algorithms provides better protection against brute force attacks by using a 160-bit message digest?

A. MD5

B. SHA-1

C. RC4

D. MD4

[Q213] Which cipher encrypts the plain text digit (bit or byte) one by one?

A. Classical cipher

B. Block cipher

C. Modern cipher

D. Stream cipher

[Q214] Which of the following can take an arbitrary length of input and produce a message digest output of 160 bit?

A. SHA-1

B. MD5

C. HAVAL

D. MD4

[Q215] Which element of Public Key Infrastructure (PKI) verifies the applicant?

A. Certificate authority

B. Validation authority

C. Registration authority

D. Verification authority

[Q216] Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?

A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security

B. Maintenance of the nations Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure

C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors

D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

[Q217] How do employers protect assets with security policies pertaining to employee surveillance activities?

A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.

B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.

C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.

D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

[Q218] Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?

A. Regulatory compliance

B. Peer review

C. Change management

D. Penetration testing

[Q219] Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?

A. Truecrypt

B. Sub7

C. Nessus

D. Clamwin

[Q220] When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

A. At least once a year and after any significant upgrade or modification

B. At least once every three years or after any significant upgrade or modification

C. At least twice a year or after any significant upgrade or modification

D. At least once every two years and after any significant upgrade or modification

[Q221] Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?

A. Sarbanes-Oxley Act (SOX)

B. Gramm-Leach-Bliley Act (GLBA)

C. Fair and Accurate Credit Transactions Act (FACTA)

D. Federal Information Security Management Act (FISMA)

[Q222] How can a policy help improve an employee's security awareness?

A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security

B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees

C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line

D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

[Q223] Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?

A. Penetration testing

B. Social engineering

C. Vulnerability scanning

D. Access control list reviews

[Q224] Which of the following guidelines or standards is associated with the credit card industry?

A. Control Objectives for Information and Related Technology (COBIT)

B. Sarbanes-Oxley Act (SOX)

C. Health Insurance Portability and Accountability Act (HIPAA)

D. Payment Card Industry Data Security Standards (PCI DSS)

[Q225] International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining

A. guidelines and practices for security controls.

B. financial soundness and business viability metrics.

C. standard best practice for configuration management.

D. contract agreement writing standards.

[Q226] Which type of security document is written with specific step-by-step details?

A. Process

B. Procedure

C. Policy

D. Paradigm

[Q227] An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?

A. Start by foot printing the network and mapping out a plan of attack.

B. Ask the employer for authorization to perform the work outside the company.

C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.

D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

[Q228] A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?

A. Threaten to publish the penetration test results if not paid.

B. Follow proper legal procedures against the company to request payment.

C. Tell other customers of the financial problems with payments from this company.

D. Exploit some of the vulnerabilities found on the company webserver to deface it.

[Q229] Which initial procedure should an ethical hacker perform after being brought into an organization?

A. Begin security testing.

B. Turn over deliverables.

C. Sign a formal contract with non-disclosure.

D. Assess what the organization is trying to protect.

[Q230] A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer. What is the consultant's obligation to the financial organization?

A. Say nothing and continue with the security testing.

B. Stop work immediately and contact the authorities.

C. Delete the pornography, say nothing, and continue security testing.

D. Bring the discovery to the financial organization's human resource department.

[Q231] A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?

A. Ignore the problem completely and let someone else deal with it.

B. Create a document that will crash the computer when opened and send it to friends.

C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.

D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

[Q232] A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?

A. Say no; the friend is not the owner of the account.

B. Say yes; the friend needs help to gather evidence.

C. Say yes; do the job for free.

D. Say no; make sure that the friend knows the risk shes asking the CEH to take.

[Q233] It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.

Which of the following terms best matches the definition?

A. Threat

B. Attack

C. Vulnerability

D. Risk

[Q234] As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.

A. Terms of Engagement

B. Project Scope

C. Non-Disclosure Agreement

D. Service Level Agreement

[Q235] Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.

A. Watering Hole Attack

B. Heartbleed Attack

C. Shellshock Attack

D. Spear Phising Attack

[Q236] 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.

A. 445

B. 3389

C. 161

D. 1433

[Q237] 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 shortrange

wireless connection.

A. Bluetooth

B. Radio-Frequency Identification

C. WLAN

D. InfraRed

[Q238] 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.

A. Botnet Trojan

B. Turtle Trojans

C. Banking Trojans

D. Ransomware Trojans

[Q239] You have compromised a server and successfully gained a root access. You want to pivot and pass traffic undetected over the network and evade any possible Intrusion Detection System.

What is the best approach?

A. Install Cryptcat and encrypt outgoing packets from this server.

B. Install and use Telnet to encrypt all outgoing traffic from this server.

C. Use Alternate Data Streams to hide the outgoing packets from this server.

D. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

[Q240] 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.

A. Ransomware

B. Adware

C. Spyware

D. Riskware

[Q241] 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.

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

[Q242] You have compromised a server on a network and successfully opened a shell. You aimed to identify all operating systems running on the network. However, as you attempt to fingerprint all machines in the network using the nmap syntax below, it is not going through.

A. OS Scan requires root privileges.

B. The nmap syntax is wrong.

C. This is a common behavior for a corrupted nmap application.

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

[Q243] Which of the following statements is TRUE?

A. Sniffers operate on Layer 2 of the OSI model

B. Sniffers operate on Layer 3 of the OSI model

C. Sniffers operate on both Layer 2 & Layer 3 of the OSI model.

D. Sniffers operate on the Layer 1 of the OSI model.

[Q244] 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

[Q245] What is the best description of SQL Injection?

A. It is an attack used to gain unauthorized access to a database.

B. It is an attack used to modify code in an application.

C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.

D. It is a Denial of Service Attack.

[Q246] Which of the following is the BEST way to defend against network sniffing?

A. Using encryption protocols to secure network communications

B. Register all machines MAC Address in a Centralized Database

C. Restrict Physical Access to Server Rooms hosting Critical Servers

D. Use Static IP Address

[Q247] You have successfully gained access to a linux server and would like to ensure that the succeeding outgoing traffic from this server will not be caught by a Network Based Intrusion Detection Systems (NIDS).

What is the best way to evade the NIDS?

A. Encryption

B. Protocol Isolation

C. Alternate Data Streams

D. Out of band signalling

[Q248] You just set up a security system in your network. In what kind of system would you find the following string of characters used as a rule within its configuration?

alert tcp any any -> 192.168.100.0/24 21 (msg: "FTP on the network!";)

A. An Intrusion Detection System

B. A firewall IPTable

C. A Router IPTable

D. FTP Server rule

[Q249] 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.

[Q250] You have successfully compromised a machine on the network and found a server that is alive on the same network. You tried to ping it but you didn't get any response back.

A. ICMP could be disabled on the target server.

B. The ARP is disabled on the target server.

C. TCP/IP doesn't support ICMP.

D. You need to run the ping command with root privileges.

[Q251] Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pre-test state.

A. III

B. IV

C. III and IV

D. All should be included.

[Q252] It is a regulation that has a set of guidelines, which should be adhered to by anyone who handles any electronic medical data. These guidelines stipulate that all medical practices must ensure that all necessary measures are in place while saving, accessing, and sharing any electronic medical data to keep patient data secure.

A. HIPAA

B. ISO/IEC 27002

C. COBIT

D. FISMA

[Q253] Which of the following is a component of a risk assessment?

A. Administrative safeguards

B. Physical security

C. DMZ

D. Logical interface

[Q254] A medium-sized healthcare IT business decides to implement a risk management strategy.

A. Delegate

B. Avoid

C. Mitigate

D. Accept

[Q255] Your company was hired by a small healthcare provider to perform a technical assessment on the network.

A. Use a scan tool like Nessus

B. Use the built-in Windows Update tool

C. Check MITRE.org for the latest list of CVE findings

D. Create a disk image of a clean Windows installation

[Q256] Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability.

A. zero-day

B. zero-hour

C. zero-sum

D. no-day

[Q257] An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victims profile to a text file and then submit the data to the attackers database.

A. Cross-Site Request Forgery

B. Cross-Site Scripting

C. SQL Injection

D. Browser Hacking

[Q258] It is a vulnerability in GNU's bash shell, discovered in September of 2014, that gives attackers access to run remote commands on a vulnerable system. The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).

A. Shellshock

B. Rootshock

C. Rootshell

D. Shellbash

[Q259] When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it.

What should you do?

A. Forward the message to your companys security response team and permanently delete the message from your computer.

B. Reply to the sender and ask them for more information about the message contents.

C. Delete the email and pretend nothing happened

D. Forward the message to your supervisor and ask for her opinion on how to handle the situation

[Q260] The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesnt have time to perform the task.

A. Wireshark

B. Nessus

C. Netcat

D. Netstat

[Q261] 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.

A. Place a front-end web server in a demilitarized zone that only handles external web traffic

B. Require all employees to change their passwords immediately

C. Move the financial data to another server on the same IP subnet

D. Issue new certificates to the web servers from the root certificate authority

[Q262] Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system.

If a scanned port is open, what happens?

A. The port will ignore the packets.

B. The port will send an RST.

C. The port will send an ACK.

D. The port will send a SYN.

[Q263] 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

[Q264] This tool is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the PTW attack, thus making the attack much faster compared to other WEP cracking tools.

A. Aircrack-ng

B. Airguard

C. WLAN-crack

D. wificracker

[Q265] The Heartbleed bug was discovered in 2014 and is widely referred to under MITREs 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.

A. Private

B. Public

C. Shared

D. Root

[Q266] In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving.

Which Algorithm is this referring to?

A. Wired Equivalent Privacy (WEP)

B. Wi-Fi Protected Access (WPA)

C. Wi-Fi Protected Access 2 (WPA2)

D. Temporal Key Integrity Protocol (TKIP)

[Q267] 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.

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)

[Q268] Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved with human trafficking.

What should you do?

A. Immediately stop work and contact the proper legal authorities.

B. Copy the data to removable media and keep it in case you need it.

C. Confront the client in a respectful manner and ask her about the data.

D. Ignore the data and continue the assessment until completed as agreed.

[Q269] Jesse receives an email with an attachment labeled Court\_Notice\_21206.zip. Inside the zip file is a file named Court\_Notice\_21206.docx.exe disguised as a word document. Upon execution, a window appears stating, This word document is corrupt. In the background, the file copies itself to Jesse APPDATAlocal directory and begins to beacon to a C2 server to download additional malicious binaries.

A. Trojan

B. Worm

C. Macro Virus

D. Key-Logger

[Q270] 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

[Q271] While using your banks online servicing you notice the following string in the URL bar: http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21 You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

A. Web Parameter Tampering

B. Cookie Tampering

C. XSS Reflection

D. SQL injection

[Q272] Perspective clients want to see sample reports from previous penetration tests.

What should you do next?

A. Decline but, provide references.

B. Share full reports, not redacted.

C. Share full reports with redactions.

D. Share reports, after NDA is signed.

[Q273] During a blackbox pen test you attempt to pass IRC traffic over port 80/TCP from a compromised web enabled host. The traffic gets blocked; however, outbound HTTP traffic is unimpeded.

What type of firewall is inspecting outbound traffic?

A. Application

B. Circuit

C. Stateful

D. Packet Filtering

[Q274] Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tense conversation on his cell phone as an authorized employee badges in. Jimmy, while still on the phone, grabs the door as it begins to close.

What just happened?

A. Piggybacking

B. Masqurading

C. Phishing

D. Whaling

[Q275] You've gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your tool kit you have an Ubuntu 9.10 Linux LiveCD. Which Linux based tool has the ability to change any user's password or to activate disabled Windows accounts?

A. CHNTPW

B. Cain & Abel

C. SET

D. John the Ripper

[Q276] An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to "www.MyPersonalBank.com", that the user is directed to a phishing site.

Which file does the attacker need to modify?

A. Hosts

B. Sudoers

C. Boot.ini

D. Networks

[Q277] After trying multiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first?

A. Create User Account

B. Disable Key Services

C. Disable IPTables

D. Download and Install Netcat

[Q278] env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'

What is the Shellshock bash vulnerability attempting to do on an 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

[Q279] Using Windows CMD, how would an attacker list all the shares to which the current user context has access?

A. NET USE

B. NET CONFIG

C. NET FILE

D. NET VIEW

[Q280] A common cryptographical tool is the use of XOR. XOR the following binary values:

10110001

00111010

A. 10001011

B. 11011000

C. 10011101

D. 10111100

[Q281] Which of the following is the successor of SSL?

A. TLS

B. RSA

C. GRE

D. IPSec

[Q282] You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?

A. TCP

B. UPD

C. ICMP

D. UPX

[Q283] 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.

A. Reconnaissance

B. Enumeration

C. Scanning

D. Escalation

[Q284] Which regulation defines security and privacy controls for Federal information systems and organizations?

A. NIST-800-53

B. PCI-DSS

C. EU Safe Harbor

D. HIPAA

[Q285] 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.

[Q286] You are performing information gathering for an important penetration test. You have found pdf, doc, and images in your objective. You decide to extract metadata from these files and analyze it.

A. Metagoofil

B. Armitage

C. Dimitry

D. cdpsnarf

[Q287] 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.

A. site: target.com filetype:xls username password email

B. inurl: target.com filename:xls username password email

C. domain: target.com archive:xls username password email

D. site: target.com file:xls username password email

[Q288] What is a "Collision attack" in cryptography?

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

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

C. Collision attacks try to get the public key.

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

[Q289] 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.

A. Social engineering

B. Tailgating

C. Piggybacking

D. Eavesdropping

[Q290] When you are getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRACE) that are available because there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from the server. You can detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.

A. http-methods

B. http enum

C. http-headers

D. http-git

[Q291] 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.

A. Burpsuite

B. Maskgen

C. Dimitry

D. Proxychains

[Q292] You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine.

A. tcp.dstport==514 && ip.dst==192.168.0.150

B. tcp.srcport==514 && ip.src==192.168.0.99

C. tcp.dstport==514 && ip.dst==192.168.0.0/16

D. tcp.srcport==514 && ip.src==192.168.150

[Q293] This asymmetry cipher is based on factoring the product of two large prime numbers.

What cipher is described above?

A. RSA

B. SHA

C. RC5

D. MD5

[Q294] Which of the following parameters describe LM Hash (see exhibit):

Exhibit:

A. I, II, and III

B. I

C. II

D. IandII

[Q295] 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

[Q296] 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

[Q297] 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.

A. Report immediately to the administrator

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

C. Transfer money from the administrator's account to another account.

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

[Q298] 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

[Q299] You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions.

A. Grep

B. Notepad

C. MS Excel

D. Relational Database

[Q300] You've just been hired to perform a pen test on an organization that has been subjected to a large-scale attack. The CIO is concerned with mitigating threats and vulnerabilities to totally eliminate risk.

A. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.

B. Interview all employees in the company to rule out possible insider threats.

C. Establish attribution to suspected attackers.

D. Start the wireshark application to start sniffing network traffic.

[Q301] 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?

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.

[Q302] 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

[Q303] Which of the following is not a Bluetooth attack?

A. Bluedriving

B. Bluejacking

C. Bluesmacking

D. Bluesnarfing

[Q304] 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

[Q305] The purpose of a \_\_\_\_\_\_\_\_\_\_ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A. Wireless Intrusion Prevention System

B. Wireless Access Point

C. Wireless Access Control List

D. Wireless Analyzer

[Q306] > NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

A. A ping scan

B. A trace sweep

C. An operating system detect

D. A port scan

[Q307] You are using NMAP to resolve domain names into IP addresses for a ping sweep later.

A. >host -t a hackeddomain.com

B. >host -t soa hackeddomain.com

C. >host -t ns hackeddomain.com

D. >host -t AXFR hackeddomain.com

[Q308] Which of the following is a command line packet analyzer similar to GUI-based Wireshark?

A. tcpdump

B. nessus

C. etherea

D. Jack the ripper

[Q309] The configuration allows a wired or wireless network interface controller to pass all traffic it receives to the central processing unit (CPU), rather than passing only the frames that the controller is intended to receive.

Which of the following is being described?

A. promiscuous mode

B. port forwarding

C. multi-cast mode

D. WEM

[Q310] Which of the following is an extremely common IDS evasion technique in the web world?

A. unicode characters

B. spyware

C. port knocking

D. subnetting

[Q311] 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

[Q312] 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

[Q313] Which mode of IPSec should you use to assure security and confidentiality of data within the same LAN?

A. ESP transport mode

B. AH permiscuous

C. ESP confidential

D. AH Tunnel mode

[Q314] Which of the following is assured by the use of a hash?

A. Integrity

B. Confidentiality

C. Authentication

D. Availability

[Q315] Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information.

B. A backup is unavailable during disaster recovery.

C. A backup is incomplete because no verification was performed.

D. An un-encrypted backup can be misplaced or stolen.

[Q316] An incident investigator asks to receive a copy of the event logs from all firewalls, proxy servers, and Intrusion Detection Systems (IDS) on the network of an organization that has experienced a possible breach of security. When the investigator attempts to correlate the information in all of the logs, the sequence of many of the logged events do not match up.

A. The network devices are not all synchronized.

B. Proper chain of custody was not observed while collecting the logs.

C. The attacker altered or erased events from the logs.

D. The security breach was a false positive.

[Q317] In Risk Management, how is the term "likelihood" related to the concept of "threat?"

A. Likelihood is the probability that a threat-source will exploit a vulnerability.

B. Likelihood is a possible threat-source that may exploit a vulnerability.

C. Likelihood is the likely source of a threat that could exploit a vulnerability.

D. Likelihood is the probability that a vulnerability is a threat-source.

[Q318] 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%).

A. $146

B. $1320

C. $440

D. $100

[Q319] 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.

A. File system permissions

B. Privilege escalation

C. Directory traversal

D. Brute force login

[Q320] 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.

A. Cross-Site Request Forgery

B. Cross-Site Scripting

C. Clickjacking

D. Web form input validation

[Q321] A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?

A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.

B. Attempts by attackers to access the user and password information stored in the company's SQL database.

C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.

D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

[Q322] 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.

A. Cross-site scripting vulnerability

B. Cross-site Request Forgery vulnerability

C. SQL injection vulnerability

D. Web site defacement vulnerability

[Q323] Which of the following is considered the best way to protect Personally Identifiable Information (PII) from Web application vulnerabilities?

A. Use cryptographic storage to store all PII

B. Use encrypted communications protocols to transmit PII

C. Use full disk encryption on all hard drives to protect PII

D. Use a security token to log into all Web applications that use PII

[Q324] 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

[Q325] 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+

[Q326] 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.

A. The WAP does not recognize the clients MAC address

B. The client cannot see the SSID of the wireless network

C. Client is configured for the wrong channel

D. The wireless client is not configured to use DHCP

[Q327] 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. Protocol analyzer

B. Intrusion Prevention System (IPS)

C. Network sniffer

D. Vulnerability scanner

[Q328] 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

[Q329] Which of the following is a protocol specifically designed for transporting event messages?

A. SYSLOG

B. SMS

C. SNMP

D. ICMP

[Q330] Which of the following security operations is used for determining the attack surface of an organization?

A. Running a network scan to detect network services in the corporate DMZ

B. Training employees on the security policy regarding social engineering

C. Reviewing the need for a security clearance for each employee

D. Using configuration management to determine when and where to apply security patches

[Q331] 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

[Q332] 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.

[Q333] 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.

[Q334] 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.

[Q335] 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

[Q336] To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which one of the following tools would most likely be used in such an audit?

A. Vulnerability scanner

B. Protocol analyzer

C. Port scanner

D. Intrusion Detection System

[Q337] Which of these options is the most secure procedure for storing backup tapes?

A. In a climate controlled facility offsite

B. On a different floor in the same building

C. Inside the data center for faster retrieval in a fireproof safe

D. In a cool dry environment

[Q338] What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Residual risk

B. Inherent risk

C. Deferred risk

D. Impact risk

[Q339] Risks = Threats x Vulnerabilities is referred to as the:

A. Risk equation

B. Threat assessment

C. BIA equation

D. Disaster recovery formula

[Q340] Which of the following is designed to identify malicious attempts to penetrate systems?

A. Intrusion Detection System

B. Firewall

C. Proxy

D. Router

[Q341] Which of the following is a low-tech way of gaining unauthorized access to systems?

A. Social Engineering

B. Sniffing

C. Eavesdropping

D. Scanning

[Q342] PGP, SSL, and IKE are all examples of which type of cryptography?

A. Public Key

B. Secret Key

C. Hash Algorithm

D. Digest

[Q343] Which method of password cracking takes the most time and effort?

A. Brute force

B. Rainbow tables

C. Dictionary attack

D. Shoulder surfing

[Q344] 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

[Q345] Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?

A. Nikto

B. Snort

C. John the Ripper

D. Dsniff

[Q346] Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?

A. tcptrace

B. tcptraceroute

C. Nessus

D. OpenVAS

[Q347] Which of the following tools is used to detect wireless LANs using the 802.11a/b/g/n WLAN standards on a linux platform?

A. Kismet

B. Nessus

C. Netstumbler

D. Abel

[Q348] Session splicing is an IDS evasion technique in which an attacker delivers data in multiple, smallsized packets to the target computer, making it very difficult for an IDS to detect the attack signatures.

Which tool can be used to perform session splicing attacks?

A. Whisker

B. tcpsplice

C. Burp

D. Hydra

[Q349] Which of the following tools can be used for passive OS fingerprinting?

A. tcpdump

B. nmap

C. ping

D. tracert

[Q350] You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?

A. Network-based IDS

B. Firewall

C. Proxy

D. Host-based IDS

[Q351] 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

[Q352] 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

[Q353] Which of the following types of firewalls ensures that the packets are part of the established session?

A. Stateful inspection firewall

B. Circuit-level firewall

C. Application-level firewall

D. Switch-level firewall

[Q354] Which of the following incident handling process phases is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an organization?

A. Preparation phase

B. Containment phase

C. Identification phase

D. Recovery phase

[Q355] Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'.

A. Steganography

B. Public-key cryptography

C. RSA algorithm

D. Encryption

[Q356] During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

A. Identify and evaluate existing practices

B. Create a procedures document

C. Conduct compliance testing

D. Terminate the audit

[Q357] Which of the following statements regarding ethical hacking is incorrect?

A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.

B. Testing should be remotely performed offsite.

C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.

D. Ethical hacking should not involve writing to or modifying the target systems.

[Q358] Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?

A. a port scanner

B. a vulnerability scanner

C. a virus scanner

D. a malware scanner

[Q359] What two conditions must a digital signature meet?

A. Has to be unforgeable, and has to be authentic.

B. Has to be legible and neat.

C. Must be unique and have special characters.

D. Has to be the same number of characters as a physical signature and must be unique.

[Q360] An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gains access to the DNS server and redirects the direction www.google.com to his own IP address. Now when the employees of the office want to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

A. ARP Poisoning

B. Smurf Attack

C. DNS spoofing

D. MAC Flooding

[Q361] 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

[Q362] What is the role of test automation in security testing?

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

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

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

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

[Q363] The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?

A. Hack attack

B. Sniffing

C. Dumpster diving

D. Spying

[Q364] The company ABC recently contracted a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?

A. The document can be sent to the accountant using an exclusive USB for that document.

B. The CFO can use a hash algorithm in the document once he approved the financial statements.

C. The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure it is the same document.

D. The CFO can use an excel file with a password.

[Q365] A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd. How can he use it?

A. The password file does not contain the passwords themselves.

B. He can open it and read the user ids and corresponding passwords.

C. The file reveals the passwords to the root user only.

D. He cannot read it because it is encrypted.

[Q366] Eve stole a file named secret.txt, transferred it to her computer and she just entered these commands:

A. She is encrypting the file.

B. She is using John the Ripper to view the contents of the file.

C. She is using ftp to transfer the file to another hacker named John.

D. She is using John the Ripper to crack the passwords in the secret.txt file.

[Q367] What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall.

A. Firewalking

B. Session hijacking

C. Network sniffing

D. Man-in-the-middle attack

[Q368] Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

A. Internal Whitebox

B. External, Whitebox

C. Internal, Blackbox

D. External, Blackbox

[Q369] Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?

A. Application Layer

B. Data tier

C. Presentation tier

D. Logic tier

[Q370] An attacker tries to do banner grabbing on a remote web server and executes the following command.

A. nmap can't retrieve the version number of any running remote service.

B. The hacker successfully completed the banner grabbing.

C. The hacker should've used nmap -O host.domain.com.

D. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.

[Q371] \_\_\_\_\_\_\_\_\_ is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.

A. DNSSEC

B. Zone transfer

C. Resource transfer

D. Resource records

[Q372] Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?

A. Fuzzy-testing the code

B. Third party running the code

C. Sandboxing the code

D. String validating the code

[Q373] An IT employee got a call from one of 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. Since the company's policy is all about Customer Service, he/she will provide information.

B. Disregarding the call, the employee should hang up.

C. The employee should not provide any information without previous management authorization.

D. The employees can not provide any information; but, anyway, he/she will provide the name of the person in charge.

[Q374] A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?

A. Ignore it.

B. Try to sell the information to a well-paying party on the dark web.

C. Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.

D. Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.

[Q375] In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?

A. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name.

B. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering.

C. Both pharming and phishing attacks are identical.

D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name.

[Q376] Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries.) More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and that are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

A. Algorithm is not the secret, key is the secret.

B. Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both encryption of plaintext and decryption of ciphertext.

C. Secure Sockets Layer (SSL) use the asymmetric encryption both (public/private key pair) to deliver the shared session key and to achieve a communication way.

D. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.

[Q377] Which of these is capable of searching for and locating rogue access points?

A. HIDS

B. WISS

C. WIPS

D. NIDS

[Q378] Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?

A. Wireshark

B. Maltego

C. Metasploit

D. Nessus

[Q379] Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?

A. Password protected files

B. Hidden folders

C. BIOS password

D. Full disk encryption.

[Q380] 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.

A. The network must be down and the nmap command and IP address are ok.

B. He needs to add the command ''''ip address'''' just before the IP address.

C. He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are not in that range.

D. He needs to change the address to 192.168.1.0 with the same mask.

[Q381] Bob learned that his username and password for a popular game has been compromised. He contacts the company and resets all the information. The company suggests he use two-factor authentication, which option below offers that?

A. A new username and password

B. A fingerprint scanner and his username and password.

C. Disable his username and use just a fingerprint scanner.

D. His username and a stronger password.

[Q382] 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. A race condition is being exploited, and the operating system is containing the malicious process.

B. A page fault is occurring, which forces the operating system to write data from the hard drive.

C. Malware is executing in either ROM or a cache memory area.

D. Malicious code is attempting to execute instruction in a non-executable memory region.

[Q383] Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?

A. Blind SQLi

B. DMS-specific SQLi

C. Classic SQLi

D. Compound SQLi

[Q384] In order to have an anonymous Internet surf, which of the following is best choice?

A. Use SSL sites when entering personal information

B. Use Tor network with multi-node

C. Use shared WiFi

D. Use public VPN

[Q385] 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:

A. MAC Spoof attacks cannot be performed.

B. Possibility of SQL Injection attack is eliminated.

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

D. There is access control policy between VLANs.

[Q386] Websites and web portals that provide web services commonly use the Simple Object Access Protocol SOAP. Which of the following is an incorrect definition or characteristics in the protocol?

A. Based on XML

B. Provides a structured model for messaging

C. Exchanges data between web services

D. Only compatible with the application protocol HTTP

[Q387] An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?

A. He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.

B. He will activate OSPF on the spoofed root bridge.

C. He will repeat the same attack against all L2 switches of the network.

D. He will repeat this action so that it escalates to a DoS attack.

[Q388] A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy

concerning this setup?

A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be performed.

B. As long as the physical access to the network elements is restricted, there is no need for additional measures.

C. There is no need for specific security measures on the network elements as long as firewalls and IPS systems exist.

D. The operator knows that attacks and down time are inevitable and should have a backup site.

[Q389] When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?

A. The amount of time it takes to convert biometric data into a template on a smart card.

B. The amount of time and resources that are necessary to maintain a biometric system.

C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.

D. How long it takes to setup individual user accounts.

[Q390] Due to a slow down of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A. All of the employees would stop normal work activities

B. IT department would be telling employees who the boss is

C. Not informing the employees that they are going to be monitored could be an invasion of privacy.

D. The network could still experience traffic slow down.

[Q391] In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types

of e-mails?

A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.

B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.

C. A blacklist of companies that have their mail server relays configured to be wide open.

D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

[Q392] 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.

A. Both static routes indicate that the traffic is external with different gateway.

B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.

C. Both static routes indicate that the traffic is internal with different gateway.

D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

[Q393]

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

A. Connection Establishment: FIN, ACK-FIN, ACK

Connection Termination: SYN, SYN-ACK, ACK

B. Connection Establishment: SYN, SYN-ACK, ACK

Connection Termination: ACK, ACK-SYN, SYN

C. Connection Establishment: ACK, ACK-SYN, SYN

Connection Termination: FIN, ACK-FIN, ACK

D. Connection Establishment: SYN, SYN-ACK, ACK

Connection Termination: FIN, ACK-FIN, ACK

[Q394] Emil uses nmap to scan two hosts using this command.

A. Host 192.168.99.7 is an iPad.

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

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

D. Host 192.168.99.7 is down.

[Q395] 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 Nmap

B. Physically go to each server

C. Scan servers with MBSA

D. Telent to every port on each server

[Q396] 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.

A. Phishing

B. Whaling

C. Tailgating

D. Masquerading

[Q397] Which protocol is used for setting up secured channels between two devices, typically in VPNs?

A. IPSEC

B. PEM

C. SET

D. PPP

[Q398] In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.

Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

A. NT:LM

B. LM:NT

C. LM:NTLM

D. NTLM:LM

[Q399] Which of the following Nmap commands will produce the following output?

A. nmap -sN -Ps -T4 192.168.1.1

B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1

C. nmap -sS -Pn 192.168.1.1

D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

[Q400] Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfpayload

B. msfcli

C. msfencode

D. msfd

[Q401] You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?

A. hping2 host.domain.com

B. hping2 –set-ICMP host.domain.com

C. hping2 -i host.domain.com

D. hping2 -1 host.domain.com

[Q402] Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

A. Burp Suite

B. OpenVAS

C. tshark

D. Kismet

[Q403] 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. RST

B. ACK

C. SYN-ACK

D. SYN

[Q404] Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Protect the payload and the headers

B. Authenticate

C. Encrypt

D. Work at the Data Link Layer

[Q405] Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?

A. A biometric system that bases authentication decisions on behavioral attributes.

B. A biometric system that bases authentication decisions on physical attributes.

C. An authentication system that creates one-time passwords that are encrypted with secret keys.

D. An authentication system that uses passphrases that are converted into virtual passwords.

[Q406] 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.

[Q407] Look at the following output. What did the hacker accomplish?

A. The hacker used whois to gather publicly available records for the domain.

B. The hacker used the "fierce" tool to brute force the list of available domains.

C. The hacker listed DNS records on his own domain.

D. The hacker successfully transfered the zone and enumerated the hosts.

[Q408] What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?

A. Security through obscurity

B. Host-Based Intrusion Detection System

C. Defense in depth

D. Network-Based Intrusion Detection System

[Q409] Scenario:

A. HTTP Parameter Pollution

B. HTML Injection

C. Session Fixation

D. ClickJacking Attack

[Q410] If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

A. Spoof Scan

B. TCP Connect scan

C. TCP SYN

D. Idle Scan

[Q411] What is correct about digital signatures?

A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.

B. Digital signatures may be used in different documents of the same type.

C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.

D. Digital signatures are issued once for each user and can be used everywhere until they expire.

[Q412] What is not a PCI compliance recommendation?

A. Limit access to card holder data to as few individuals as possible.

B. Use encryption to protect all transmission of card holder data over any public network.

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.

[Q413] Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?

A. Network-based intrusion detection system (NIDS)

B. Host-based intrusion detection system (HIDS)

C. Firewalls

D. Honeypots

[Q414] 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.

[Q415] What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?

A. User Access Control (UAC)

B. Data Execution Prevention (DEP)

C. Address Space Layout Randomization (ASLR)

D. Windows firewall

[Q416] Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?

A. Scalability

B. Speed

C. Key distribution

D. Security

[Q417] By using a smart card and pin, you are using a two-factor authentication that satisfies

A. Something you know and something you are

B. Something you have and something you know

C. Something you have and something you are

D. Something you are and something you remember

[Q418] What is the difference between the AES and RSA algorithms?

A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.

B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.

C. Both are symmetric algorithms, but AES uses 256-bit keys.

D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

[Q419] Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?

A. C#

B. Python

C. Java

D. C++

[Q420] 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. Also he 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 to the Internet. According to the next configuration what is happening in the network?

A. The ACL 110 needs to be changed to port 80

B. The ACL for FTP must be before the ACL 110

C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router

D. The ACL 104 needs to be first because is UDP

[Q421] Bob received this text message on his mobile phone: Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com. Which statement below is true?

A. This is probably a legitimate message as it comes from a respectable organization.

B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.

C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.

D. This is a scam because Bob does not know Scott.

[Q422] In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Port Scanning

B. Hacking Active Directory

C. Privilege Escalation

D. Shoulder-Surfing

[Q423] Which of the following will perform an Xmas scan using NMAP?

A. nmap -sA 192.168.1.254

B. nmap -sP 192.168.1.254

C. nmap -sX 192.168.1.254

D. nmap -sV 192.168.1.254

[Q424] As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?

A. request smtp 25

B. tcp.port eq 25

C. smtp port

D. tcp.contains port 25

[Q425] Which service in a PKI will vouch for the identity of an individual or company?

A. KDC

B. CA

C. CR

D. CBC

[Q426] In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?

A. Implementing IPv4 security in a dual-stack network offers protection from IPv6 attacks too.

B. Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.

C. Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addresses.

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

[Q427] 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.

A. Maintaining Access

B. Gaining Access

C. Reconnaissance

D. Scanning and Enumeration

[Q428] Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile

B. Bollards

C. Mantrap

D. Receptionist

[Q429] ……..is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless

users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting

up a fraudulent web site and luring people there.

A. Collision Attack

B. Evil Twin Attack

C. Sinkhole Attack

D. Signal Jamming Attack

[Q430] 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

[Q431] What attack is used to crack passwords by using a precomputed table of hashed passwords?

A. Brute Force Attack

B. Hybrid Attack

C. Rainbow Table Attack

D. Dictionary Attack

[Q432] Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?

A. Nothing, but suggest to him to change the network's SSID and password.

B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.

C. Log onto to his network, after all it's his fault that you can get in.

D. Only use his network when you have large downloads so you don't tax your own network.

[Q433] Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet-facing services, which OS did it not directly affect?

A. Windows

B. Unix

C. Linux

D. OSX

[Q434] You want to analyze packets on your wireless network. Which program would you use?

A. Wireshark with Airpcap

B. Airsnort with Airpcap

C. Wireshark with Winpcap

D. Ethereal with Winpcap

[Q435] 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. Containment

B. Eradication

C. Recovery

D. Discovery

[Q436] What is the code written for?

A. Buffer Overflow

B. Encryption

C. Bruteforce

D. Denial-of-service (Dos)

[Q437] An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?

A. Use fences in the entrance doors.

B. Install a CCTV with cameras pointing to the entrance doors and the street.

C. Use an IDS in the entrance doors and install some of them near the corners.

D. Use lights in all the entrance doors and along the company's perimeter.

[Q438] Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.

A. Heartbleed Bug

B. POODLE

C. SSL/TLS Renegotiation Vulnerability

D. Shellshock

[Q439] There are several ways to gain insight on how a cryptosystem works with the goal of reverse engineering the process. A term describes when two pieces of data result in the same value is?

A. Collision

B. Collusion

C. Polymorphism

D. Escrow

[Q440] 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

[Q441] One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?

A. Interview all employees in the company to rule out possible insider threats.

B. Establish attribution to suspected attackers.

C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.

D. Start the Wireshark application to start sniffing network traffic.

[Q442] Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?

A. http-git

B. http-headers

C. http enum

D. http-methods

[Q443] Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?

A. Gaining access

B. Escalating privileges

C. Network mapping

D. Footprinting

[Q444] 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. Bluetooth

B. Radio-Frequency Identification

C. WLAN

D. InfraRed

[Q445] Matthew received an email with an attachment named YouWon$10Grand.zip. The zip file contains a file named HowToClaimYourPrize.docx.exe. Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to

Matthews APPDATAIocaI directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?

A. Key-logger

B. Trojan

C. Worm

D. Macro Virus

[Q446] Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?

A. NET FILE

B. NET USE

C. NET CONFIG

D. NET VIEW

[Q447] What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the

database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

A. $440

B. $100

C. $1320

D. $146

[Q448] Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?

A. In a cool dry environment

B. Inside the data center for faster retrieval in a fireproof safe

C. In a climate controlled facility offsite

D. On a different floor in the same building

[Q449] Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?

A. Intrusion Detection System

B. Vulnerability scanner

C. Port scanner

D. Protocol analyzer

[Q450] Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?

A. NIST SP 800-53

B. PCI-DSS

C. EU Safe Harbor

D. HIPAA

[Q451] 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 reports, after NDA is signed

B. Share full reports, not redacted

C. Decline but, provide references

D. Share full reports with redactions

[Q452] 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 banks interest and your liabilities as a tester?

A. Service Level Agreement

B. Non-Disclosure Agreement

C. Terms of Engagement

D. Project Scope

[Q453] The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?

A. Accept

B. Mitigate

C. Delegate

D. Avoid

[Q454] A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?

A. Scanning

B. Reconnaissance

C. Escalation

D. Enumeration

[Q455] TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?

A. nmap

B. ping

C. tracert

D. tcpdump

[Q456] The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).

A. $62.5

B. $250

C. $125 D. $65.2

$125

D. $65.2

[Q457] Backing up data is a security must. However, it also have certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?

A. A backup is the source of Malware or illicit information

B. A backup is incomplete because no verification was performed

C. A backup is unavailable during disaster recovery

D. An unencrypted backup can be misplaced or stolen

[Q458] What kind of risk will remain even if all theoretically possible safety measures would be applied?

A. Residual risk

B. Inherent risk

C. Impact risk

D. Deferred risk

[Q459] While doing a Black box pen test via the TCP port (80), you noticed that the traffic gets blocked when you tried to pass IRC traffic from a web enabled host. However, you also noticed that outbound HTTP traffic is being allowed. What type of firewall is being utilized for the outbound traffic?

A. Stateful

B. Application

C. Circuit

D. Packet Filtering

[Q460] It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages.

Which of the following is being described?

A. SNMP

B. ICMP

C. SYSLOG

D. SMS

[Q461] While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?

A. The port will send an ACK

B. The port will send a SYN

C. The port will ignore the packets

D. The port will send an RST

[Q462] Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?

A. Metasploit

B. Wireshark

C. Maltego

D. Cain & Abel

[Q463] If you are to determine the attack surface of an organization, which of the following is the BEST thing to do?

A. Running a network scan to detect network services in the corporate DMZ

B. Reviewing the need for a security clearance for each employee

C. Using configuration management to determine when and where to apply security patches

D. Training employees on the security policy regarding social engineering

[Q464] What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?

A. nmap -T4 -F 10.10.0.0/24

B. nmap -T4 -q 10.10.0.0/24

C. nmap -T4 -O 10.10.0.0/24

D. nmap -T4 -r 10.10.1.0/24

[Q465] Youve just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?

A. TCP/IP doesnt support ICMP

B. ARP is disabled on the target server

C. ICMP could be disabled on the target server

D. You need to run the ping command with root privileges

[Q466] What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?

A. Armitage

B. Dimitry

C. Metagoofil

D. cdpsnarf

[Q467] Which of the following is NOT an ideal choice for biometric controls?

A. Iris patterns

B. Fingerprints

C. Height and weight

D. Voice

[Q468] While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?

A. Immediately stop work and contact the proper legal authorities

B. Ignore the data and continue the assessment until completed as agreed

C. Confront the client in a respectful manner and ask her about the data

D. Copy the data to removable media and keep it in case you need it

[Q469] In order to prevent particular ports and applications from getting packets into an organization, what does a firewall check?

A. Network layer headers and the session layer port numbers

B. Presentation layer headers and the session layer port numbers

C. Application layer port numbers and the transport layer headers

D. Transport layer port numbers and application layer headers

[Q470] Suppose youve gained access to your clients hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?

A. 1433

B. 161

C. 445

D. 3389

[Q471] Which of the following BEST describes the mechanism 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

[Q472] What is the term coined for logging, recording and resolving events in a company?

A. Internal Procedure

B. Security Policy

C. Incident Management Process

D. Metrics

[Q473] XOR is a common cryptographic tool. 10110001 XOR 00111010 is?

A. 10111100

B. 11011000

C. 10011101

D. 10001011

[Q474] A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?

A. Turtle Trojans

B. Ransomware Trojans

C. Botnet Trojan

D. Banking Trojans

[Q475] First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?

A. Delete the email and pretend nothing happened.

B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.

C. Forward the message to your companys security response team and permanently delete the message from your computer.

D. Reply to the sender and ask them for more information about the message contents.

[Q476] LM hash is a compromised password hashing function. 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 Its a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I

B. I, II, and III

C. II

D. IandII

[Q477] Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?

A. Preparation phase

B. Containment phase

C. Recovery phase

D. Identification phase

[Q478] Which of the following BEST describes how Address Resolution Protocol (ARP) works?

A. It sends a reply packet for a specific IP, asking for the MAC address

B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP

C. It sends a request packet to all the network elements, asking for the domain name from a specific IP

D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP

[Q479] Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?

A. Social Engineering

B. Piggybacking

C. Tailgating

D. Eavesdropping

[Q480] What tool and process are you going to use in order to remain undetected by an IDS while pivoting and passing traffic over a server youve compromised and gained root access to?

A. Install and use Telnet to encrypt all outgoing traffic from this server.

B. Install Cryptcat and encrypt outgoing packets from this server.

C. Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

D. Use Alternate Data Streams to hide the outgoing packets from this server.

[Q481] Youve just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?

A. Disable Key Services

B. Create User Account

C. Download and Install Netcat

D. Disable IPTables

[Q482] 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. Ransomware

B. Riskware

C. Adware

D. Spyware

[Q483] The following are types of Bluetooth attack EXCEPT\_\_\_\_\_?

A. Bluejacking

B. Bluesmaking

C. Bluesnarfing

D. Bluedriving

[Q484] Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?

A. Use digital certificates to authenticate a server prior to sending data.

B. Verify access right before allowing access to protected information and UI controls.

C. Verify access right before allowing access to protected information and UI controls.

D. Validate and escape all information sent to a server.

[Q485] A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether this packets are indeed malicious.

What tool are you going to use?

A. Intrusion Prevention System (IPS)

B. Vulnerability scanner

C. Protocol analyzer

D. Network sniffer

[Q486] Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?

A. Use cryptographic storage to store all PII

B. Use full disk encryption on all hard drives to protect PII

C. Use encrypted communications protocols to transmit PII

D. Use a security token to log into all Web applications that use PII

[Q487] A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?

A. The client cannot see the SSID of the wireless network

B. The WAP does not recognize the clients MAC address.

C. The wireless client is not configured to use DHCP.

D. Client is configured for the wrong channel

[Q488] This configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive. Select the option that BEST describes the above statement.

A. Multi-cast mode

B. WEM

C. Promiscuous mode

D. Port forwarding

[Q489] Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?

A. SOA

B. Single-Sign On

C. PKI

D. Biometrics

[Q490] A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?

A. Mutating

B. Randomizing

C. Fuzzing

D. Bounding

[Q491] What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?

A. c:compmgmt.msc

B. c:gpedit

C. c:ncpa.cpl

D. c:services.msc

[Q492] Which of the following is a wireless network detector that is commonly found on Linux?

A. Kismet

B. Abel

C. Netstumbler

D. Nessus

[Q493] Which specific element of security testing is being assured by using hash?

A. Authentication

B. Integrity

C. Confidentiality

D. Availability

[Q494] 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

[Q495] Which of the following is a vulnerability in GNUs bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system?

A. Shellshock

B. Rootshell

C. Rootshock

D. Shellbash

[Q496] When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?

A. AH Tunnel mode

B. AH promiscuous

C. ESP transport mode

D. ESP confidential

[Q497] 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. OS Scan requires root privileges

B. The nmap syntax is wrong.

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

D. This is a common behavior for a corrupted nmap application

[Q498] While performing online banking using a Web browser, Kyle receives an email that contains an image of a well-crafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?

A. Clickjacking

B. Web Form Input Validation

C. Cross-Site Request Forgery

D. Cross-Site Scripting

[Q499] A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?

A. Insufficient security management

B. Insufficient database hardening

C. Insufficient input validation

D. Insufficient exception handling

[Q500] Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network. Which AAA protocol would you implement?

A. TACACS+

B. DIAMETER

C. Kerberos

D. RADIUS

[Q501] Which type of cryptography does SSL, IKE and PGP belongs to?

A. Secret Key

B. Hash Algorithm

C. Digest

D. Public Key

[Q502] A recent security audit revealed that there were indeed several occasions that the companys network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?

A. True Positive

B. False Negative

C. False Positive

D. False Positive

[Q503] What are two things that are possible when scanning UDP ports? (Choose two.)

A. A reset will be returned

B. An ICMP message will be returned

C. The four-way handshake will not be completed

D. An RFC 1294 message will be returned E. Nothing

[Q504] What does a type 3 code 13 represent? (Choose two.)

A. Echo request

B. Destination unreachable

C. Network unreachable

D. Administratively prohibited E. Port unreachable F. Time exceeded

[Q505] Destination unreachable administratively prohibited messages can inform the hacker to what?

A. That a circuit level proxy has been installed and is filtering traffic

B. That his/her scans are being blocked by a honeypot or jail

C. That the packets are being malformed by the scanning software

D. That a router or other packet-filtering device is blocking traffic E. That the network is functioning normally

[Q506] Which of the following Nmap commands would be used to perform a stack fingerprinting?

A. Nmap -O -p80 <host(s.>

B. Nmap -hU -Q<host(s.>

C. Nmap -sT -p <host(s.>

D. Nmap -u -o -w2 <host> E. Nmap -sS -0p targe

[Q507] (Note: the student is being tested on concepts learnt during passive OS fingerprinting, basic TCP/IP connection concepts and the ability to read packet signatures from a sniff dump.). Snort has been used to capture packets on the network. On studying the packets, the penetration tester finds it to be abnormal. If you were the penetration tester, why would you find this abnormal?

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

A. This is not a spoofed packet as the IP stack has increasing numbers for the three flags.

B. This is back orifice activity as the scan comes from port 31337.

C. The attacker wants to avoid creating a sub-carries connection that is not normally valid.

D. These packets were crafted by a tool, they were not created by a standard IP stack.

[Q508] Which type of Nmap scan is the most reliable, but also the most visible, and likely to be picked up by and IDS?

A. SYN scan

B. ACK scan

C. RST scan

D. Connect scan E. FIN scan

[Q509] Name two software tools used for OS guessing? (Choose two.)

A. Nmap

B. Snadboy

C. Queso

D. UserInfo E. NetBus

[Q510] Sandra is the security administrator of XYZ.com. One day she notices that the XYZ.com Oracle database server has been compromised and customer information along with financial data has been stolen. The financial loss will be estimated in millions of dollars if the database gets into the hands of competitors. Sandra wants to report this crime to the law enforcement agencies immediately. Which organization coordinates computer crime investigations throughout the United States?

A. NDCA

B. NICP

C. CIRP

D. NPC E. CIA

[Q511] While reviewing the result of scanning run against a target network you come across the following:

A. A Bo2k system query.

B. nmap protocol scan

C. A sniffer

D. An SNMP walk

[Q512] You are manually conducting Idle Scanning using Hping2. During your scanning you notice that almost every query increments the IPID regardless of the port being queried. One or two of the queries cause the IPID to increment by more than one value. Why do you think this occurs?

A. The zombie you are using is not truly idle.

B. A stateful inspection firewall is resetting your queries.

C. Hping2 cannot be used for idle scanning.

D. These ports are actually open on the target system.

[Q513] 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.

A. Scan more slowly.

B. Do not scan the broadcast IP.

C. Spoof the source IP address.

D. Only scan the Windows systems.

[Q514] Neil notices that a single address is generating traffic from its port 500 to port 500 of several other machines on the network. This scan is eating up most of the network bandwidth and Neil is concerned. As a security professional, what would you infer from this scan?

A. It is a network fault and the originating machine is in a network loop

B. It is a worm that is malfunctioning or hardcoded to scan on port 500

C. The attacker is trying to detect machines on the network which have SSL enabled

D. The attacker is trying to determine the type of VPN implementation and checking for IPSec

[Q515] A distributed port scan operates by:

A. Blocking access to the scanning clients by the targeted host

B. Using denial-of-service software against a range of TCP ports

C. Blocking access to the targeted host by each of the distributed scanning clients

D. Having multiple computers each scan a small number of ports, then correlating the results

[Q516] An nmap command that includes the host specification of 202.176.56-57.\* will scan \_\_\_\_\_\_\_ number of hosts.

A. 2

B. 256

C. 512

D. Over 10, 000

[Q517] A specific site received 91 ICMP\_ECHO packets within 90 minutes from 47 different sites.

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

A. The packets were sent by a worm spoofing the IP addresses of 47 infected sites

B. ICMP ID and Seq numbers were most likely set by a tool and not by the operating system

C. All 77 packets came from the same LAN segment and hence had the same ICMP ID and Seq number

D. 13 packets were from an external network and probably behind a NAT, as they had an ICMP ID 0 and Seq 0

[Q518] Which of the following commands runs snort in packet logger mode?

A. ./snort -dev -h ./log

B. ./snort -dev -l ./log

C. ./snort -dev -o ./log

D. ./snort -dev -p ./log

[Q519] You have initiated an active operating system fingerprinting attempt with nmap against a target system:

A. Windows XP

B. Windows 98 SE

C. Windows NT4 Server

D. Windows 2000 Server

[Q520] Study the log below and identify the scan type.

A. nmap -sR 192.168.1.10

B. nmap -sS 192.168.1.10

C. nmap -sV 192.168.1.10

D. nmap -sO -T 192.168.1.10

[Q521] Which of the following command line switch would you use for OS detection in Nmap?

A. -D

B. -O

C. -P

D. X

[Q522] Why would an attacker want to perform a scan on port 137?

A. To discover proxy servers on a network

B. To disrupt the NetBIOS SMB service on the target host

C. To check for file and print sharing on Windows systems

D. To discover information about a target host using NBTSTAT

[Q523] Which Type of scan sends a packets with no flags set?

A. Open Scan

B. Null Scan

C. Xmas Scan

D. Half-Open Scan

[Q524] Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test.

While conducting a port scan she notices open ports in the range of 135 to 139.

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

A. Finger

B. FTP

C. Samba

D. SMB

[Q525] SNMP is a protocol used to query hosts, servers, and devices about performance or health status data. This protocol has long been used by hackers to gather great amount of information about remote hosts. Which of the following features makes this possible?

(Choose two.)

A. It used TCP as the underlying protocol.

B. It uses community string that is transmitted in clear text.

C. It is susceptible to sniffing.

D. It is used by all network devices on the market.

[Q526] 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. Educate everyone with books, articles and training on risk analysis, vulnerabilities and safeguards.

B. Hire more computer security monitoring personnel to monitor computer systems and networks.

C. Make obtaining either a computer security certification or accreditation easier to achieve so more individuals feel that they are a part of something larger than life.

D. Train more National Guard and reservist in the art of computer security to help out in times of emergency or crises.

[Q527] Peter extracts the SIDs list from Windows 2000 Server machine using the hacking tool "SIDExtractor". Here is the output of the SIDs:

A. John

B. Rebecca

C. Sheela

D. Shawn E. Somia F. Chang G. Micah

[Q528] 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 Port Address Translation

C. Dynamic Network Address Translation

D. Static Network Address Translation

[Q529] What is the following command used for?

A. Grabbing the etc/passwd file

B. Grabbing the SAM

C. Connecting to a Linux computer through Samba.

D. This command is used to connect as a null session E. Enumeration of Cisco routers

[Q530] What is the proper response for a NULL scan if the port is closed?

A. SYN

B. ACK

C. FIN

D. PSH E. RST F. No response

[Q531] One of your team members has asked you to analyze the following SOA record.

What is the TTL? Rutgers.edu.SOA NS1.Rutgers.edu ipad.college.edu (200302028 3600 3600 604800 2400.)

A. 200303028

B. 3600

C. 604800

D. 2400 E. 60 F. 4800

[Q532] One of your team members has asked you to analyze the following SOA record. What is the version?

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

A. 200303028

B. 3600

C. 604800

D. 2400 E. 60 F. 4800

[Q533] MX record priority increases as the number increases. (True/False.)

A. True

B. False

[Q534] Which of the following tools can be used to perform a zone transfer?

A. NSLookup

B. Finger

C. Dig

D. Sam Spade E. Host F. Netcat G. Neotrace

[Q535] Under what conditions does a secondary name server request a zone transfer from a primary name server?

A. When a primary SOA is higher that a secondary SOA

B. When a secondary SOA is higher that a primary SOA

C. When a primary name server has had its service restarted

D. When a secondary name server has had its service restarted E. When the TTL falls to zero

[Q536] What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

A. 110

B. 135

C. 139

D. 161 E. 445 F. 1024

[Q537] What is a NULL scan?

A. A scan in which all flags are turned off

B. A scan in which certain flags are off

C. A scan in which all flags are on

D. A scan in which the packet size is set to zero E. A scan with an illegal packet size

[Q538] What is the proper response for a NULL scan if the port is open?

A. SYN

B. ACK

C. FIN

D. PSH E. RST F. No response

[Q539] Which of the following statements about a zone transfer is correct? (Choose three.)

A. A zone transfer is accomplished with the DNS

B. A zone transfer is accomplished with the nslookup service

C. A zone transfer passes all zone information that a DNS server maintains

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

[Q540] You have the SOA presented below in your Zone.

Your secondary servers have not been able to contact your primary server to synchronize information. How long will the secondary servers attempt to contact the primary server before it considers that zone is dead and stops responding to queries?

collegae.edu.SOA, cikkye.edu ipad.college.edu. (200302028 3600 3600 604800 3600)

A. One day

B. One hour

C. One week

D. One month

[Q541] Tess King is using the nslookup command to craft queries to list all DNS information (such as Name Servers, host names, MX records, CNAME records, glue records (delegation for child Domains), zone serial number, TimeToLive (TTL) records, etc) for a Domain.

A. A zone harvesting

B. A zone transfer

C. A zone update

D. A zone estimate

[Q542] A zone file consists of which of the following Resource Records (RRs)?

A. DNS, NS, AXFR, and MX records

B. DNS, NS, PTR, and MX records

C. SOA, NS, AXFR, and MX records

D. SOA, NS, A, and MX records

[Q543] Let's imagine three companies (A, B and C), all competing in a challenging global environment. Company A and B are working together in developing a product that will generate a major competitive advantage for them. Company A has a secure DNS server while

company B has a DNS server vulnerable to spoofing. With a spoofing attack on the DNS server of company B, company C gains access to outgoing e-mails from company B. How do you prevent DNS spoofing?

A. Install DNS logger and track vulnerable packets

B. Disable DNS timeouts

C. Install DNS Anti-spoofing

D. Disable DNS Zone Transfer

[Q544] Which DNS resource record can indicate how long any "DNS poisoning" could last?

A. MX

B. SOA

C. NS

D. TIMEOUT

[Q545] Joseph was the Web site administrator for the Mason Insurance in New York, who's main Web site was located at www.masonins.com. Joseph uses his laptop computer regularly to administer the Web site. One night, Joseph received an urgent phone call from his friend, Smith. According to Smith, the main Mason Insurance web site had been vandalized! All of its normal content was removed and replaced with an attacker's message ''Hacker Message: You are dead! Freaks! From his office, which was directly connected to Mason Insurance's internal network, Joseph surfed to the Web site using his laptop. In his browser, the Web site looked completely intact.

No changes were apparent. Joseph called a friend of his at his home to help troubleshoot the problem. The Web site appeared defaced when his friend visited using his DSL connection. So, while Smith and his friend could see the defaced page, Joseph saw the intact Mason Insurance web site. To help make sense of this problem, Joseph decided to access the Web site using hisdial-up ISP. He disconnected his laptop from the corporate internal network and used his modem to dial up the same ISP used by Smith. After his modem connected, he quickly typed www.masonins.com in his browser to reveal the following web page:

A. ARP spoofing

B. SQL injection

C. DNS poisoning

D. Routing table injection

[Q546] Which of the following tools are used for enumeration? (Choose three.)

A. SolarWinds

B. USER2SID

C. Cheops

D. SID2USER E. DumpSec

[Q547] What did the following commands determine?

A. That the Joe account has a SID of 500

B. These commands demonstrate that the guest account has NOT been disabled

C. These commands demonstrate that the guest account has been disabled

D. That the true administrator is Joe E. Issued alone, these commands prove nothing

[Q548] Which definition among those given below best describes a covert channel?

A. A server program using a port that is not well known.

B. Making use of a protocol in a way it is not intended to be used.

C. It is the multiplexing taking place on a communication link.

D. It is one of the weak channels used by WEP which makes it insecure

[Q549] 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.

A. A sniffing attack

B. A spoofing attack

C. A man in the middle attack

D. A denial of service attack

[Q550] 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. Man-in-the-middle

C. ARP Proxy

D. Poisoning Attack

[Q551] 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.

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

[Q552] Which of the following represents the initial two commands that an IRC client sends to join an IRC network?

A. USER, NICK

B. LOGIN, NICK

C. USER, PASS

D. LOGIN, USER

[Q553] Study the following log extract and identify the attack.

A. Hexcode Attack

B. Cross Site Scripting

C. Multiple Domain Traversal Attack

D. Unicode Directory Traversal Attack

[Q554] Null sessions are un-authenticated connections (not using a username or password.) to an NT or 2000 system. Which TCP and UDP ports must you filter to check null sessions on your network?

A. 137 and 139

B. 137 and 443

C. 139 and 443

D. 139 and 445

[Q555] 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 creating a directory on the compromised machine

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

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

[Q556] Based on the following extract from the log of a compromised machine, what is the hacker really trying to steal?

A. har.txt

B. SAM file

C. wwwroot

D. Repair file

[Q557] As a securing consultant, what are some of the things you would recommend to a company to ensure DNS security?

A. Use the same machines for DNS and other applications

B. Harden DNS servers

C. Use split-horizon operation for DNS servers

D. Restrict Zone transfers E. Have subnet diversity between DNS servers

[Q558] Why would you consider sending an email to an address that you know does not exist within the company you are performing a Penetration Test for?

A. To determine who is the holder of the root account

B. To perform a DoS

C. To create needless SPAM

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

[Q559] What tool can crack Windows SMB passwords simply by listening to network traffic?

A. This is not possible

B. Netbus

C. NTFSDOS

D. L0phtcrack

[Q560] A network admin contacts you. He is concerned that ARP spoofing or poisoning might occur on his network. What are some things he can do to prevent it? Select the best answers.

A. Use port security on his switches.

B. Use a tool like ARPwatch to monitor for strange ARP activity.

C. Use a firewall between all LAN segments.

D. If you have a small network, use static ARP entries. E. Use only static IP addresses on all PC's.

[Q561] Peter, a Network Administrator, has come to you looking for advice on a tool that would help him perform SNMP enquires over the network.

Which of these tools would do the SNMP enumeration he is looking for? Select the best answers.

A. SNMPUtil

B. SNScan

C. SNMPScan

D. Solarwinds IP Network Browser E. NMap

[Q562] If a token and 4-digit personal identification number (PIN) are used to access a computer system and the token performs off-line checking for the correct PIN, what type of attack is possible?

A. Birthday

B. Brute force

C. Man-in-the-middle

D. Smurf

[Q563] Bob is doing a password assessment for one of his clients. Bob suspects that security policies are not in place. He also suspects that weak passwords are probably the norm throughout the company he is evaluating. Bob is familiar with password weaknesses and key loggers.

Which of the following options best represents the means that Bob can adopt to retrieve passwords from his clients hosts and servers?

A. Hardware, Software, and Sniffing.

B. Hardware and Software Keyloggers.

C. Passwords are always best obtained using Hardware key loggers.

D. Software only, they are the most effective.

[Q564] Study the snort rule given below:

A. WebDav

B. SQL Slammer

C. MS Blaster

D. MyDoom

[Q565] Which of the following algorithms can be used to guarantee the integrity of messages being sent, in transit, or stored?

A. symmetric algorithms

B. asymmetric algorithms

C. hashing algorithms

D. integrity algorithms

[Q566] A user on your Windows 2000 network has discovered that he can use L0phtcrack to sniff the SMB exchanges which carry user logons. The user is plugged into a hub with 23 other systems.

However, he is unable to capture any logons though he knows that other users are logging in.

What do you think is the most likely reason behind this?

A. There is a NIDS present on that segment.

B. Kerberos is preventing it.

C. Windows logons cannot be sniffed.

D. L0phtcrack only sniffs logons to web servers.

[Q567] You are attempting to crack LM Manager hashed from Windows 2000 SAM file. You will be using LM Brute force hacking tool for decryption. What encryption algorithm will you be decrypting?

A. MD4

B. DES

C. SHA

D. SSL

[Q568] 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. Thorough

C. Hybrid

D. BruteDics

[Q569] What is the algorithm used by LM for Windows2000 SAM?

A. MD4

B. DES

C. SHA

D. SSL

[Q570] E-mail scams and mail fraud are regulated by which of the following?

A. 18 U.S.C. par. 1030 Fraud and Related activity in connection with Computers

B. 18 U.S.C. par. 1029 Fraud and Related activity in connection with Access Devices C. 18 U.S.

C. par. 1362 Communication Lines, Stations, or Systems

D. 18 U.S.C. par. 2510 Wire and Electronic Communications Interception and Interception of Oral Communication

[Q571] Which of the following LM hashes represent a password of less than 8 characters? (Choose two.)

A. BA810DBA98995F1817306D272A9441BB

B. 44EFCE164AB921CQAAD3B435B51404EE

C. 0182BD0BD4444BF836077A718CCDF409

D. CEC52EB9C8E3455DC2265B23734E0DAC E. B757BF5C0D87772FAAD3B435B51404EE F. E52CAC67419A9A224A3B108F3FA6CB6D

[Q572] Which of the following is the primary objective of a rootkit?

A. It opens a port to provide an unauthorized service

B. It creates a buffer overflow

C. It replaces legitimate programs

D. It provides an undocumented opening in a program

[Q573] This kind of password cracking method uses word lists in combination with numbers and special characters:

A. Hybrid

B. Linear

C. Symmetric

D. Brute Force

[Q574] \_\_\_\_\_\_\_\_\_ is a tool that can hide processes from the process list, can hide files, registry entries, and intercept keystrokes.

A. Trojan

B. RootKit

C. DoS tool

D. Scanner E. Backdoor

[Q575] What is the BEST alternative if you discover that a rootkit has been installed on one of your computers?

A. Copy the system files from a known good system

B. Perform a trap and trace

C. Delete the files and try to determine the source

D. Reload from a previous backup E. Reload from known good media

[Q576] What do Trinoo, TFN2k, WinTrinoo, T-Sight, and Stracheldraht have in common?

A. All are hacking tools developed by the legion of doom

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

C. All are DDOS tools

D. All are tools that are only effective against Windows E. All are tools that are only effective against Linux

[Q577] How can you determine if an LM hash you extracted contains a password that is less than 8 characters long?

A. There is no way to tell because a hash cannot be reversed

B. The right most portion of the hash is always the same

C. The hash always starts with AB923D

D. The left most portion of the hash is always the same E. A portion of the hash will be all 0's

[Q578] 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 load a dictionary of words into your cracking program

D. You create hashes of a large number of words and compare it with the encrypted passwords E. You wait until the password expires

[Q579] Which of the following are well known password-cracking programs?

A. L0phtcrack

B. NetCat

C. Jack the Ripper

D. Netbus E. John the Ripper

[Q580] Password cracking programs reverse the hashing process to recover passwords. (True/False.)

A. True

B. False

[Q581] While examining audit logs, you discover that people are able to telnet into the SMTP server on port 25. You would like to block this, though you do not see any evidence of an attack or other wrong doing. However, you are concerned about affecting the normal functionality of the email server. From the following options choose how best you can achieve this objective?

A. Block port 25 at the firewall.

B. Shut off the SMTP service on the server.

C. Force all connections to use a username and password.

D. Switch from Windows Exchange to UNIX Sendmail. E. None of the above.

[Q582] Windows LAN Manager (LM) hashes are known to be weak.

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

A. Converts passwords to uppercase.

B. Hashes are sent in clear text over the network.

C. Makes use of only 32-bit encryption.

D. Effective length is 7 characters.

[Q583] You have retrieved the raw hash values from a Windows 2000 Domain Controller. Using social engineering, you come to know that they are enforcing strong passwords. You understand that all users are required to use passwords that are at least 8 characters in length. All passwords must also use 3 of the 4 following categories: lower case letters, capital letters, numbers and special characters. With your existing knowledge of users, likely user account names and the possibility that they will choose the easiest passwords possible, what would be the fastest type of password cracking attack you can run against these hash values and still get results?

A. Online Attack

B. Dictionary Attack

C. Brute Force Attack

D. Hybrid Attack

[Q584] An attacker runs netcat tool to transfer a secret file between two hosts.

A. Machine A: netcat -l -p -s password 1234 < testfile

Machine B: netcat <machine A IP> 1234

B. Machine A: netcat -l -e magickey -p 1234 < testfile

Machine B: netcat <machine A IP> 1234

C. Machine A: netcat -l -p 1234 < testfile -pw password

Machine B: netcat <machine A IP> 1234 -pw password

D. Use cryptcat instead of netcat

[Q585] What is GINA?

A. Gateway Interface Network Application

B. GUI Installed Network Application CLASS

C. Global Internet National Authority (G-USA)

D. Graphical Identification and Authentication DLL

[Q586] Fingerprinting an Operating System helps a cracker because:

A. It defines exactly what software you have installed

B. It opens a security-delayed window based on the port being scanned

C. It doesn't depend on the patches that have been applied to fix existing security holes

D. It informs the cracker of which vulnerabilities he may be able to exploit on your system

[Q587] In the context of Windows Security, what is a 'null' user?

A. A user that has no skills

B. An account that has been suspended by the admin

C. A pseudo account that has no username and password

D. A pseudo account that was created for security administration purpose

[Q588] What does the following command in netcat do?

A. logs the incoming connections to /etc/passwd file

B. loads the /etc/passwd file to the UDP port 55555

C. grabs the /etc/passwd file when connected to UDP port 55555

D. deletes the /etc/passwd file when connected to the UDP port 55555

[Q589] What hacking attack is challenge/response authentication used to prevent?

A. Replay attacks

B. Scanning attacks

C. Session hijacking attacks

D. Password cracking attacks

[Q590] In this attack, a victim receives an e-mail claiming from PayPal stating that their account has been disabled and confirmation is required before activation. The attackers then scam to collect not one but two credit card numbers, ATM PIN number and other personal details. Ignorant users usually fall prey to this scam.

Which of the following statement is incorrect related to this attack?

A. Do not reply to email messages or popup ads asking for personal or financial information

B. Do not trust telephone numbers in e-mails or popup ads

C. Review credit card and bank account statements regularly

D. Antivirus, anti-spyware, and firewall software can very easily detect these type of attacks E. Do not send credit card numbers, and personal or financial information via e-mail

[Q591] Bob is going to perform an active session hijack against Brownies Inc. He has found a target that allows session oriented connections (Telnet) and performs the sequence prediction on the target operating system. He manages to find an active session due to the high level of traffic on the network. What is Bob supposed to do next?

A. Take over the session

B. Reverse sequence prediction

C. Guess the sequence numbers

D. Take one of the parties offline

[Q592] ViruXine.W32 virus hides their presence by changing the underlying executable code.

This Virus code mutates while keeping the original algorithm intact, the code changes itself each time it runs, but the function of the code (its semantics) will not change at all.

A. Polymorphic Virus

B. Metamorphic Virus

C. Dravidic Virus

D. Stealth Virus

[Q593] Identify the correct terminology that defines the above statement.

A. Vulnerability Scanning

B. Penetration Testing

C. Security Policy Implementation

D. Designing Network Security

[Q594] Nathan is testing some of his network devices. Nathan is using Macof to try and flood the ARP cache of these switches.

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

A. The switches will drop into hub mode if the ARP cache is successfully flooded.

B. If the ARP cache is flooded, the switches will drop into pix mode making it less susceptible to attacks.

C. Depending on the switch manufacturer, the device will either delete every entry in its ARP cache or reroute packets to the nearest switch.

D. The switches will route all traffic to the broadcast address created collisions.

[Q595] You are programming a buffer overflow exploit and you want to create a NOP sled of 200 bytes in the program exploit.c

A. 0x60

B. 0x80

C. 0x70

D. 0x90

[Q596] This TCP flag instructs the sending system to transmit all buffered data immediately.

A. SYN

B. RST

C. PSH

D. URG E. FIN

[Q597] The network administrator at Spears Technology, Inc has configured the default gateway Cisco router's access-list as below:

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

[Q598] 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

[Q599] Study the snort rule given below and interpret the rule. alert tcp any any –> 192.168.1.0/24 111

(content:"|00 01 86 a5|"; msG. "mountd access";)

A. An alert is generated when a TCP packet is generated from any IP on the 192.168.1.0 subnet and destined to any IP on port 111

B. An alert is generated when any packet other than a TCP packet is seen on the network and destined for the 192.168.1.0 subnet

C. An alert is generated when a TCP packet is originated from port 111 of any IP address to the 192.168.1.0 subnet

D. An alert is generated when a TCP packet originating from any IP address is seen on the network and destined for any IP address on the 192.168.1.0 subnet on port 111

[Q600] What port number is used by LDAP protocol?

A. 110

B. 389

C. 464

D. 445

[Q601] Fred is the network administrator for his company. Fred is testing an internal switch.

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

A. Fred can accomplish this by sending an IP packet with the RST/SIN bit and the source address of his computer.

B. He can send an IP packet with the SYN bit and the source address of his computer.

C. Fred can send an IP packet with the ACK bit set to zero and the source address of the switch.

D. Fred can send an IP packet to the switch with the ACK bit and the source address of his machine.

[Q602] Within the context of Computer Security, which of the following statements describes Social Engineering best?

A. Social Engineering is the act of publicly disclosing information

B. Social Engineering is the means put in place by human resource to perform time accounting

C. Social Engineering is the act of getting needed information from a person rather than breaking into a system

D. Social Engineering is a training program within sociology studies

[Q603] In Trojan terminology, what is a covert channel?

A. A channel that transfers information within a computer system or network in a way that violates the security policy

B. A legitimate communication path within a computer system or network for transfer of data

C. It is a kernel operation that hides boot processes and services to mask detection

D. It is Reverse tunneling technique that uses HTTPS protocol instead of HTTP protocol to establish connections

[Q604] 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 SYN packets with random destination addresses towards a victim host

B. Attacker floods TCP SYN packets with random source addresses towards a victim host

C. Attacker generates TCP ACK packets with random source addresses towards a victim host

D. Attacker generates TCP RST packets with random source addresses towards a victim host

[Q605] 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.

A. Yancey would be considered a Suicide Hacker

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 is a Hacktivist Hacker since he is standing up to a company that is downsizing

[Q606] 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:

A. Look at the website design, if it looks professional then it is a Real Anti-Virus website

B. Connect to the site using SSL, if you are successful then the website is genuine

C. Search using the URL and Anti-Virus product name into Google and lookout for suspicious warnings against this site

D. 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 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

[Q607] 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.

A. Information Audit Policy (IAP)

B. Information Security Policy (ISP)

C. Penetration Testing Policy (PTP)

D. Company Compliance Policy (CCP)

[Q608] Take a look at the following attack on a Web Server using obstructed URL:

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

B. Create rules in IDS to alert on strange Unicode requests

C. Use SSL authentication on Web Servers

D. Enable Active Scripts Detection at the firewall and routers

[Q609] Which type of sniffing technique is generally referred as MiTM attack?

A. Password Sniffing

B. ARP Poisoning

C. Mac Flooding

D. DHCP Sniffing

[Q610] Switches maintain a CAM Table that maps individual MAC addresses on the network to physical ports on the switch.

A. Switch then acts as hub by broadcasting packets to all machines on the network

B. The CAM overflow table will cause the switch to crash causing Denial of Service

C. The switch replaces outgoing frame switch factory default MAC address of FF:FF:FF:FF:FF:FF

D. Every packet is dropped and the switch sends out SNMP alerts to the IDS port

[Q611] You went to great lengths to install all the necessary technologies to prevent hacking attacks, such as expensive firewalls, antivirus software, anti-spam systems and intrusion detection/prevention tools in your company's network. You have configured the most

secure policies and tightened every device on your network. You are confident that hackers will never be able to gain access to your network with complex security system in place.

Your peer, Peter Smith who works at the same department disagrees with you.

He says even the best network security technologies cannot prevent hackers gaining access to the network because of presence of "weakest link" in the security chain.

What is Peter Smith talking about?

A. Untrained staff or ignorant computer users who inadvertently become the weakest link in your security chain

B. "zero-day" exploits are the weakest link in the security chain since the IDS will not be able to detect these attacks

C. "Polymorphic viruses" are the weakest link in the security chain since the Anti-Virus scanners will not be able to detect these attacks

D. Continuous Spam e-mails cannot be blocked by your security system since spammers use different techniques to bypass the filters in your gateway

[Q612] How does a denial-of-service attack work?

A. A hacker prevents a legitimate user (or group of users) from accessing a service

B. A hacker uses every character, word, or letter he or she can think of to defeat authentication

C. A hacker tries to decipher a password by using a system, which subsequently crashes the network

D. A hacker attempts to imitate a legitimate user by confusing a computer or even another person

[Q613] You are trying to break into a highly classified top-secret mainframe computer with highest security system in place at Merclyn Barley Bank located in Los Angeles.

You know that conventional hacking doesn't work in this case, because organizations such as banks are generally tight and secure when it comes to protecting their systems.

In other words, you are trying to penetrate an otherwise impenetrable system.

How would you proceed?

A. Look for "zero-day" exploits at various underground hacker websites in Russia and China and buy the necessary exploits from these hackers and target the bank's network

B. Try to hang around the local pubs or restaurants near the bank, get talking to a poorly-paid or disgruntled employee, and offer them money if they'll abuse their access privileges by providing you with sensitive information

C. Launch DDOS attacks against Merclyn Barley Bank's routers and firewall systems using 100, 000 or more "zombies" and "bots"

D. Try to conduct Man-in-the-Middle (MiTM) attack and divert the network traffic going to the Merclyn Barley Bank's Webserver to that of your machine using DNS Cache Poisoning techniques

[Q614] This is an attack that takes advantage of a web site vulnerability in which the site displays content that includes un-sanitized user-provided data.

A. Cross-site-scripting attack

B. SQL Injection

C. URL Traversal attack

D. Buffer Overflow attack

**Answers**

[Q1] Correct Answer: B

[Q2] Correct Answer: D

[Q3] Correct Answer: B

[Q4] Correct Answer: B

[Q5] Correct Answer: B

[Q6] Correct Answer: B

[Q7] Correct Answer: C

[Q8] Correct Answer: A

[Q9] Correct Answer: C

[Q10] Correct Answer: D

[Q11] Correct Answer: A

[Q12] Correct Answer: B

[Q13] Correct Answer: D

[Q14] Correct Answer: D

[Q15] Correct Answer: C

[Q16] Correct Answer: A

[Q17] Correct Answer: D

[Q18] Correct Answer: C

[Q19] Correct Answer: B

[Q20] Correct Answer: B

[Q21] Correct Answer: C

[Q22] Correct Answer: C

[Q23] Correct Answer: A

[Q24] Correct Answer: D

[Q25] Correct Answer: D

[Q26] Correct Answer: B

[Q27] Correct Answer: A

[Q28] Correct Answer: C

[Q29] Correct Answer: B

[Q30] Correct Answer: B

[Q31] Correct Answer: A

[Q32] Correct Answer: C

[Q33] Correct Answer: A

[Q34] Correct Answer: A

[Q35] Correct Answer: D

[Q36] Correct Answer: A

[Q37] Correct Answer: C

[Q38] Correct Answer: D

[Q39] Correct Answer: A

[Q40] Correct Answer: C

[Q41] Correct Answer: C

[Q42] Correct Answer: C

[Q43] Correct Answer: C

[Q44] Correct Answer: B

[Q45] Correct Answer: B

[Q46] Correct Answer: D

[Q47] Correct Answer: C

[Q48] Correct Answer: A

[Q49] Correct Answer: A

[Q50] Correct Answer: C

[Q51] Correct Answer: B

[Q52] Correct Answer: A

[Q53] Correct Answer: C

[Q54] Correct Answer: C

[Q55] Correct Answer: C

[Q56] Correct Answer: D

[Q57] Correct Answer: C

[Q58] Correct Answer: B

[Q59] Correct Answer: D

[Q60] Correct Answer: B

[Q61] Correct Answer: B

[Q62] Correct Answer: D

[Q63] Correct Answer: A

[Q64] Correct Answer: A

[Q65] Correct Answer: C

[Q66] Correct Answer: C

[Q67] Correct Answer: D

[Q68] Correct Answer: D

[Q69] Correct Answer: D

[Q70] Correct Answer: B

[Q71] Correct Answer: A

[Q72] Correct Answer: A

[Q73] Correct Answer: C

[Q74] Correct Answer: C

[Q75] Correct Answer: B

[Q76] Correct Answer: B

[Q77] Correct Answer: C

[Q78] Correct Answer: C

[Q79] Correct Answer: A

[Q80] Correct Answer: B

[Q81] Correct Answer: A

[Q82] Correct Answer: D

[Q83] Correct Answer: D

[Q84] Correct Answer: D

[Q85] Correct Answer: B

[Q86] Correct Answer: D

[Q87] Correct Answer: C

[Q88] Correct Answer: C

[Q89] Correct Answer: D

[Q90] Correct Answer: A

[Q91] Correct Answer: C

[Q92] Correct Answer: B

[Q93] Correct Answer: A

[Q94] Correct Answer: A

[Q95] Correct Answer: A

[Q96] Correct Answer: B

[Q97] Correct Answer: B

[Q98] Correct Answer: D

[Q99] Correct Answer: A

[Q100] Correct Answer: A

[Q101] Correct Answer: D

[Q102] Correct Answer: A

[Q103] Correct Answer: C

[Q104] Correct Answer: C

[Q105] Correct Answer: B

[Q106] Correct Answer: A

[Q107] Correct Answer: C

[Q108] Correct Answer: B

[Q109] Correct Answer: B

[Q110] Correct Answer: D

[Q111] Correct Answer: B

[Q112] Correct Answer: B

[Q113] Correct Answer: A

[Q114] Correct Answer: B

[Q115] Correct Answer: A

[Q116] Correct Answer: A

[Q117] Correct Answer: D

[Q118] Correct Answer: C

[Q119] Correct Answer: C

[Q120] Correct Answer: C

[Q121] Correct Answer: C

[Q122] Correct Answer: C

[Q123] Correct Answer: D

[Q124] Correct Answer: A

[Q125] Correct Answer: C

[Q126] Correct Answer: D

[Q127] Correct Answer: B

[Q128] Correct Answer: A

[Q129] Correct Answer: A

[Q130] Correct Answer: B

[Q131] Correct Answer: A

[Q132] Correct Answer: A

[Q133] Correct Answer: B

[Q134] Correct Answer: A

[Q135] Correct Answer: A

[Q136] Correct Answer: D

[Q137] Correct Answer: D

[Q138] Correct Answer: A

[Q139] Correct Answer: D

[Q140] Correct Answer: C

[Q141] Correct Answer: A

[Q142] Correct Answer: D

[Q143] Correct Answer: D

[Q144] Correct Answer: C

[Q145] Correct Answer: B

[Q146] Correct Answer: B

[Q147] Correct Answer: D

[Q148] Correct Answer: D

[Q149] Correct Answer: D

[Q150] Correct Answer: A

[Q151] Correct Answer: B

[Q152] Correct Answer: B

[Q153] Correct Answer: D

[Q154] Correct Answer: A

[Q155] Correct Answer: D

[Q156] Correct Answer: B

[Q157] Correct Answer: B

[Q158] Correct Answer: A

[Q159] Correct Answer: C

[Q160] Correct Answer: C

[Q161] Correct Answer: C

[Q162] Correct Answer: A

[Q163] Correct Answer: A

[Q164] Correct Answer: B

[Q165] Correct Answer: A

[Q166] Correct Answer: D

[Q167] Correct Answer: A

[Q168] Correct Answer: C

[Q169] Correct Answer: D

[Q170] Correct Answer: A

[Q171] Correct Answer: C

[Q172] Correct Answer: D

[Q173] Correct Answer: D

[Q174] Correct Answer: D

[Q175] Correct Answer: B

[Q176] Correct Answer: A

[Q177] Correct Answer: D

[Q178] Correct Answer: B

[Q179] Correct Answer: D

[Q180] Correct Answer: C

[Q181] Correct Answer: D

[Q182] Correct Answer: C

[Q183] Correct Answer: C

[Q184] Correct Answer: A

[Q185] Correct Answer: A

[Q186] Correct Answer: A

[Q187] Correct Answer: D

[Q188] Correct Answer: A

[Q189] Correct Answer: A

[Q190] Correct Answer: D

[Q191] Correct Answer: A

[Q192] Correct Answer: B

[Q193] Correct Answer: C

[Q194] Correct Answer: B

[Q195] Correct Answer: D

[Q196] Correct Answer: D

[Q197] Correct Answer: B

[Q198] Correct Answer: C

[Q199] Correct Answer: C

[Q200] Correct Answer: A

[Q201] Correct Answer: B

[Q202] Correct Answer: A

[Q203] Correct Answer: C

[Q204] Correct Answer: C

[Q205] Correct Answer: D

[Q206] Correct Answer: A

[Q207] Correct Answer: A

[Q208] Correct Answer: A

[Q209] Correct Answer: D

[Q210] Correct Answer: B

[Q211] Correct Answer: D

[Q212] Correct Answer: B

[Q213] Correct Answer: D

[Q214] Correct Answer: A

[Q215] Correct Answer: C

[Q216] Correct Answer: A

[Q217] Correct Answer: D

[Q218] Correct Answer: C

[Q219] Correct Answer: C

[Q220] Correct Answer: A

[Q221] Correct Answer: A

[Q222] Correct Answer: A

[Q223] Correct Answer: A

[Q224] Correct Answer: D

[Q225] Correct Answer: A

[Q226] Correct Answer: B

[Q227] Correct Answer: B

[Q228] Correct Answer: B

[Q229] Correct Answer: C

[Q230] Correct Answer: B

[Q231] Correct Answer: D

[Q232] Correct Answer: A

[Q233] Correct Answer: A

[Q234] Correct Answer: A

[Q235] Correct Answer: A

[Q236] Correct Answer: A

[Q237] Correct Answer: A

[Q238] Correct Answer: A

[Q239] Correct Answer: A

[Q240] Correct Answer: A

[Q241] Correct Answer: A

[Q242] Correct Answer: A

[Q243] Correct Answer: A

[Q244] Correct Answer: A

[Q245] Correct Answer: A

[Q246] Correct Answer: A

[Q247] Correct Answer: A

[Q248] Correct Answer: A

[Q249] Correct Answer: A

[Q250] Correct Answer: A

[Q251] Correct Answer: A

[Q252] Correct Answer: A

[Q253] Correct Answer: A

[Q254] Correct Answer: A

[Q255] Correct Answer: A

[Q256] Correct Answer: A

[Q257] Correct Answer: A

[Q258] Correct Answer: A

[Q259] Correct Answer: A

[Q260] Correct Answer: A

[Q261] Correct Answer: A

[Q262] Correct Answer: A

[Q263] Correct Answer: A

[Q264] Correct Answer: A

[Q265] Correct Answer: A

[Q266] Correct Answer: A

[Q267] Correct Answer: A

[Q268] Correct Answer: A

[Q269] Correct Answer: A

[Q270] Correct Answer: A

[Q271] Correct Answer: A

[Q272] Correct Answer: A

[Q273] Correct Answer: A

[Q274] Correct Answer: A

[Q275] Correct Answer: A

[Q276] Correct Answer: A

[Q277] Correct Answer: A

[Q278] Correct Answer: A

[Q279] Correct Answer: A

[Q280] Correct Answer: A

[Q281] Correct Answer: A

[Q282] Correct Answer: A

[Q283] Correct Answer: A

[Q284] Correct Answer: A

[Q285] Correct Answer: A

[Q286] Correct Answer: A

[Q287] Correct Answer: A

[Q288] Correct Answer: A

[Q289] Correct Answer: A

[Q290] Correct Answer: A

[Q291] Correct Answer: A

[Q292] Correct Answer: A

[Q293] Correct Answer: A

[Q294] Correct Answer: A

[Q295] Correct Answer: A

[Q296] Correct Answer: A

[Q297] Correct Answer: A

[Q298] Correct Answer: A

[Q299] Correct Answer: A

[Q300] Correct Answer: A

[Q301] Correct Answer: A

[Q302] Correct Answer: A

[Q303] Correct Answer: A

[Q304] Correct Answer: A

[Q305] Correct Answer: A

[Q306] Correct Answer: A

[Q307] Correct Answer: A

[Q308] Correct Answer: A

[Q309] Correct Answer: A

[Q310] Correct Answer: A

[Q311] Correct Answer: A

[Q312] Correct Answer: A

[Q313] Correct Answer: A

[Q314] Correct Answer: A

[Q315] Correct Answer: D

[Q316] Correct Answer: A

[Q317] Correct Answer: A

[Q318] Correct Answer: A

[Q319] Correct Answer: A

[Q320] Correct Answer: A

[Q321] Correct Answer: A

[Q322] Correct Answer: A

[Q323] Correct Answer: A

[Q324] Correct Answer: A

[Q325] Correct Answer: A

[Q326] Correct Answer: A

[Q327] Correct Answer: A

[Q328] Correct Answer: A

[Q329] Correct Answer: A

[Q330] Correct Answer: A

[Q331] Correct Answer: A

[Q332] Correct Answer: A

[Q333] Correct Answer: A

[Q334] Correct Answer: A

[Q335] Correct Answer: A

[Q336] Correct Answer: A

[Q337] Correct Answer: A

[Q338] Correct Answer: A

[Q339] Correct Answer: A

[Q340] Correct Answer: A

[Q341] Correct Answer: A

[Q342] Correct Answer: A

[Q343] Correct Answer: A

[Q344] Correct Answer: A

[Q345] Correct Answer: A

[Q346] Correct Answer: A

[Q347] Correct Answer: A

[Q348] Correct Answer: A

[Q349] Correct Answer: A

[Q350] Correct Answer: A

[Q351] Correct Answer: A

[Q352] Correct Answer: A

[Q353] Correct Answer: A

[Q354] Correct Answer: A

[Q355] Correct Answer: A

[Q356] Correct Answer: A

[Q357] Correct Answer: A

[Q358] Correct Answer: B

[Q359] Correct Answer: A

[Q360] Correct Answer: C

[Q361] Correct Answer: A

[Q362] Correct Answer: A

[Q363] Correct Answer: C

[Q364] Correct Answer: B

[Q365] Correct Answer: A

[Q366] Correct Answer: D

[Q367] Correct Answer: A

[Q368] Correct Answer: C

[Q369] Correct Answer: D

[Q370] Correct Answer: B

[Q371] Correct Answer: A

[Q372] Correct Answer: A

[Q373] Correct Answer: C

[Q374] Correct Answer: C

[Q375] Correct Answer: A

[Q376] Correct Answer: C

[Q377] Correct Answer: C

[Q378] Correct Answer: C

[Q379] Correct Answer: D

[Q380] Correct Answer: C

[Q381] Correct Answer: B

[Q382] Correct Answer: D

[Q383] Correct Answer: A

[Q384] Correct Answer: B

[Q385] Correct Answer: C

[Q386] Correct Answer: D

[Q387] Correct Answer: A

[Q388] Correct Answer: A

[Q389] Correct Answer: C

[Q390] Correct Answer: C

[Q391] Correct Answer: B

[Q392] Correct Answer: D

[Q393] Correct Answer: D

[Q394] Correct Answer: B

[Q395] Correct Answer: A

[Q396] Correct Answer: C

[Q397] Correct Answer: A

[Q398] Correct Answer: B

[Q399] Correct Answer: D

[Q400] Correct Answer: C

[Q401] Correct Answer: D

[Q402] Correct Answer: D

[Q403] Correct Answer: D

[Q404] Correct Answer: D

[Q405] Correct Answer: C

[Q406] Correct Answer: B

[Q407] Correct Answer: D

[Q408] Correct Answer: C

[Q409] Correct Answer: D

[Q410] Correct Answer: C

[Q411] Correct Answer: A

[Q412] Correct Answer: C

[Q413] Correct Answer: A

[Q414] Correct Answer: C

[Q415] Correct Answer: B

[Q416] Correct Answer: B

[Q417] Correct Answer: B

[Q418] Correct Answer: B

[Q419] Correct Answer: D

[Q420] Correct Answer: C

[Q421] Correct Answer: C

[Q422] Correct Answer: C

[Q423] Correct Answer: C

[Q424] Correct Answer: B

[Q425] Correct Answer: B

[Q426] Correct Answer: B

[Q427] Correct Answer: C

[Q428] Correct Answer: B

[Q429] Correct Answer: B

[Q430] Correct Answer: D

[Q431] Correct Answer: C

[Q432] Correct Answer: A

[Q433] Correct Answer: A

[Q434] Correct Answer: A

[Q435] Correct Answer: A

[Q436] Correct Answer: A

[Q437] Correct Answer: B

[Q438] Correct Answer: A

[Q439] Correct Answer: A

[Q440] Correct Answer: B

[Q441] Correct Answer: C

[Q442] Correct Answer: D

[Q443] Correct Answer: D

[Q444] Correct Answer: A

[Q445] Correct Answer: B

[Q446] Correct Answer: B

[Q447] Correct Answer: D

[Q448] Correct Answer: C

[Q449] Correct Answer: B

[Q450] Correct Answer: A

[Q451] Correct Answer: C

[Q452] Correct Answer: C

[Q453] Correct Answer: C

[Q454] Correct Answer: B

[Q455] Correct Answer: D

[Q456] Correct Answer: A

[Q457] Correct Answer: D

[Q458] Correct Answer: A

[Q459] Correct Answer: B

[Q460] Correct Answer: C

[Q461] Correct Answer: C

[Q462] Correct Answer: C

[Q463] Correct Answer: A

[Q464] Correct Answer: A

[Q465] Correct Answer: C

[Q466] Correct Answer: C

[Q467] Correct Answer: C

[Q468] Correct Answer: A

[Q469] Correct Answer: D

[Q470] Correct Answer: C

[Q471] Correct Answer: A

[Q472] Correct Answer: C

[Q473] Correct Answer: D

[Q474] Correct Answer: C

[Q475] Correct Answer: C

[Q476] Correct Answer: B

[Q477] Correct Answer: A

[Q478] Correct Answer: D

[Q479] Correct Answer: A

[Q480] Correct Answer: B

[Q481] Correct Answer: B

[Q482] Correct Answer: A

[Q483] Correct Answer: D

[Q484] Correct Answer: D

[Q485] Correct Answer: C

[Q486] Correct Answer: C

[Q487] Correct Answer: B

[Q488] Correct Answer: C

[Q489] Correct Answer: C

[Q490] Correct Answer: C

[Q491] Correct Answer: A

[Q492] Correct Answer: A

[Q493] Correct Answer: B

[Q494] Correct Answer: B

[Q495] Correct Answer: A

[Q496] Correct Answer: C

[Q497] Correct Answer: A

[Q498] Correct Answer: C

[Q499] Correct Answer: B

[Q500] Correct Answer: D

[Q501] Correct Answer: D

[Q502] Correct Answer: B

[Q503] Correct Answer: BE

[Q504] Correct Answer: BD

[Q505] Correct Answer: D

[Q506] Correct Answer: B

[Q507] Correct Answer: B

[Q508] Correct Answer: D

[Q509] Correct Answer: AC

[Q510] Correct Answer: D

[Q511] Correct Answer: D

[Q512] Correct Answer: A

[Q513] Correct Answer: B

[Q514] Correct Answer: D

[Q515] Correct Answer: D

[Q516] Correct Answer: C

[Q517] Correct Answer: B

[Q518] Correct Answer: B

[Q519] Correct Answer: D

[Q520] Correct Answer: D

[Q521] Correct Answer: B

[Q522] Correct Answer: D

[Q523] Correct Answer: B

[Q524] Correct Answer: D

[Q525] Correct Answer: BD

[Q526] Correct Answer: A

[Q527] Correct Answer: F

[Q528] Correct Answer: D

[Q529] Correct Answer: D

[Q530] Correct Answer: E

[Q531] Correct Answer: D

[Q532] Correct Answer: A

[Q533] Correct Answer: B

[Q534] Correct Answer: ACDE

[Q535] Correct Answer: A

[Q536] Correct Answer: BCE

[Q537] Correct Answer: A

[Q538] Correct Answer: F

[Q539] Correct Answer: ACE

[Q540] Correct Answer: C

[Q541] Correct Answer: B

[Q542] Correct Answer: D

[Q543] Correct Answer: C

[Q544] Correct Answer: B

[Q545] Correct Answer: C

[Q546] Correct Answer: BDE

[Q547] Correct Answer: D

[Q548] Correct Answer: B

[Q549] Correct Answer: C

[Q550] Correct Answer: B

[Q551] Correct Answer: C

[Q552] Correct Answer: A

[Q553] Correct Answer: D

[Q554] Correct Answer: D

[Q555] Correct Answer: D

[Q556] Correct Answer: B

[Q557] Correct Answer: BCDE

[Q558] Correct Answer: D

[Q559] Correct Answer: D

[Q560] Correct Answer: ABD

[Q561] Correct Answer: ABD

[Q562] Correct Answer: B

[Q563] Correct Answer: A

[Q564] Correct Answer: C

[Q565] Correct Answer: C

[Q566] Correct Answer: B

[Q567] Correct Answer: B

[Q568] Correct Answer: C

[Q569] Correct Answer: B

[Q570] Correct Answer: A

[Q571] Correct Answer: BE

[Q572] Correct Answer: C

[Q573] Correct Answer: A

[Q574] Correct Answer: B

[Q575] Correct Answer: E

[Q576] Correct Answer: C

[Q577] Correct Answer: B

[Q578] Correct Answer: A

[Q579] Correct Answer: AE

[Q580] Correct Answer: B

[Q581] Correct Answer: E

[Q582] Correct Answer: ABD

[Q583] Correct Answer: D

[Q584] Correct Answer: D

[Q585] Correct Answer: D

[Q586] Correct Answer: D

[Q587] Correct Answer: C

[Q588] Correct Answer: C

[Q589] Correct Answer: A

[Q590] Correct Answer: D

[Q591] Correct Answer: C

[Q592] Correct Answer: A

[Q593] Correct Answer: B

[Q594] Correct Answer: A

[Q595] Correct Answer: D

[Q596] Correct Answer: C

[Q597] Correct Answer: BD

[Q598] Correct Answer: C

[Q599] Correct Answer: D

[Q600] Correct Answer: B

[Q601] Correct Answer: D

[Q602] Correct Answer: C

[Q603] Correct Answer: A

[Q604] Correct Answer: B

[Q605] Correct Answer: A

[Q606] Correct Answer: C

[Q607] Correct Answer: B

[Q608] Correct Answer: B

[Q609] Correct Answer: B

[Q610] Correct Answer: A

[Q611] Correct Answer: A

[Q612] Correct Answer: A

[Q613] Correct Answer: B

[Q614] Correct Answer: A