312-50v10.exam.110q

Number: 312-50v10
Passing Score: 800
Time Limit: 120 min

312-50v10

Certified Ethical Hacker v10 Exam

Exam A

QUESTION 1
Which tool allows analysts and pen testers to examine links between data using graphs and link analysis?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
Which of these is capable of searching for and locating rogue access points?

A. HIDS
B. NIDS
C. WISS
D. WIPS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 3
A hacker is an intelligent individual with excellent computer skills and the ability to explore a computer's software and hardware without the owner's permission.

Their intention can either be to simply gain knowledge or to illegally make changes.
Which of the following class of hacker refers to an individual who works both offensively and defensively at various times?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristics of the protocol?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You have gained physical access to a Windows 2008 R2 server which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?

A. John the Ripper
B. SET

C. CHNTPW
D. Cain & Abel

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 6
What type of vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8
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 tool could the tester use to get a response from a host using TCP?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access?

A. Bootrom Exploit
B. iBoot Exploit
C. Sandbox Exploit
D. Userland Exploit

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10

What is not a PCI compliance recommendation?

A. Use a firewall between the public network and the payment card data.
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. Limit access to card holder data to as few individuals as possible.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

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

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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

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

A. SQL injection attack
B. Cross-Site Scripting (XSS)
C. LDAP Injection attack

D. Cross-Site Request Forgery (CSRF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

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

Which of the following tools is being described?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

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

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

What type of activity has been logged?

A. Teardrop attack targeting 192.168.0.110
B. Denial of service attack targeting 192.168.0.105
C. Port scan targeting 192.168.0.110
D. Port scan targeting 192.168.0.105

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?

A. nmap –A - Pn
B. nmap –sP –p-65535-T5
C. nmap –sT –O –T0
D. nmap –A --host-timeout 99-T1

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16
Bob, your senior colleague, has sent you a mail regarding aa deal with one of the clients. You are requested to accept the offer and you oblige.
After 2 days, Bob denies that he had ever sent a mail.
What do you want to “know” to prove yourself that it was Bob who had send a mail?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
What is attempting an injection attack on a web server based on responses to True/False questions called?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18
Which method of password cracking takes the most time and effort?

A. Shoulder surfing
B. Brute force
C. Dictionary attack

D. Rainbow tables

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
Which of the following program infects the system boot sector and the executable files at the same time?

A. Stealth virus
B. Polymorphic virus
C. Macro virus
D. Multipartite Virus

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20
You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for. Which of the below scanning technique will you use?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
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. The employees cannot provide any information; but, anyway, he/she will provide the name of the person in charge.
B. Since the company's policy is all about Customer Service, he/she will provide information.
C. Disregarding the call, the employee should hang up.
D. The employee should not provide any information without previous management authorization.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
You perform a scan of your company’s network and discover that TCP port 123 is open. What services by default run on TCP port 123?

A. Telnet
B. POP3
C. Network Time Protocol
D. DNS

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Based on the below log, which of the following sentences are true?

Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
You have successfully comprised a server having an IP address of 10.10.0.5. You would like to enumerate all machines in the same network quickly.

What is the best nmap command you will use?

A. nmap -T4 -q 10.10.0.0/24
B. nmap -T4 -F 10.10.0.0/24
C. nmap -T4 -r 10.10.1.0/24
D. nmap -T4 -O 10.10.0.0/24

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25
.....is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 26
DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?

A. nslookup -fullrecursive update.antivirus.com
B. dnsnooping –rt update.antivirus.com
C. nslookup -norecursive update.antivirus.com
D. dns --snoop update.antivirus.com

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8.

While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP.

After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.

What kind of attack does the above scenario depict?

A. Botnet Attack
B. Spear Phishing Attack
C. Advanced Persistent Threats
D. Rootkit Attack

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 28
Which of the following is an adaptive SQL Injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?

A. Function Testing
B. Dynamic Testing
C. Static Testing
D. Fuzzing Testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30
In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes?
A. Keyed Hashing
B. Key Stretching
C. Salting
D. Double Hashing

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31
Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan?

A. –T0
B. –T5
C. -O
D. -A

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Which of the following provides a security professional with most information about the system's security posture?

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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 33
What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
What term describes the amount of risk that remains after the vulnerabilities are classified and the countermeasures have been deployed?

A. Deferred risk
B. Impact risk
C. Inherent risk

D. Residual risk

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
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 file reveals the passwords to the root user only.
B. The password file does not contain the passwords themselves.
C. He cannot read it because it is encrypted.
D. He can open it and read the user ids and corresponding passwords.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
A technician is resolving an issue where a computer is unable to connect to the Internet using a wireless access point. The computer is able to transfer files locally to other machines, but cannot successfully reach the Internet. When the technician examines the IP address and default gateway they are both on the 192.168.1.0/24. Which of the following has occurred?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
An attacker scans a host with the below command. Which three flags are set? (Choose three.)

#nmap –sX host.domain.com

A. This is ACK scan. ACK flag is set
B. This is Xmas scan. SYN and ACK flags are set

C. This is Xmas scan. URG, PUSH and FIN are set
D. This is SYN scan. SYN flag is set

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
If you want only to scan fewer ports than the default scan using Nmap tool, which option would you use?

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

Correct Answer: B
Section: (none)
Explanation
Explanation/Reference:

QUESTION 40
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41
What is the least important information when you analyze a public IP address in a security alert?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
You are the Network Admin, and you get a compliant that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then you try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 43
Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.

A. Work at the Data Link Layer
B. Protect the payload and the headers

C. Encrypt
D. Authenticate

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developers decided to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the customer's activity on the site. These tools are located on the servers of the marketing company. What is the main security risk associated with this scenario?

A. External script contents could be maliciously modified without the security team knowledge
B. External scripts have direct access to the company servers and can steal the data from there
C. There is no risk at all as the marketing services are trustworthy
D. External scripts increase the outbound company data traffic which leads greater financial losses

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends “many” IP packets, based on the average number of packets sent by all origins and using some thresholds. In concept, the solution developed by Bob is actually:

A. Just a network monitoring tool
B. A signature-based IDS
C. A hybrid IDS
D. A behavior-based IDS

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 47
Which of the following is a low-tech way of gaining unauthorized access to systems?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?

A. Privilege Escalation
B. Shoulder-Surfing

C. Hacking Active Directory
D. Port Scanning

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
Which regulation defines security and privacy controls for Federal information systems and organizations?

A. HIPAA
B. EU Safe Harbor
C. PCI-DSS
D. NIST-800-53
Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 50
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. Confront the client in a respectful manner and ask her about the data.
B. Copy the data to removable media and keep it in case you need it.
C. Ignore the data and continue the assessment until completed as agreed.
D. Immediately stop work and contact the proper legal authorities.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 52
It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?

A. Discovery
B. Recovery
C. Containment
D. Eradication

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 53
In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case.
Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system whose credentials are known. It was written by sysinternals and has been integrated within the framework. The penetration testers successfully gain access to a system

through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbowtables to crack those hash values.

Which of the following is true hash type and sort order that is used in the psexec module's 'smbpass' option?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 54
You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers/ports, which can have direct internet access, and block the access to workstations.
Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say?

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

D. Bob is partially right. DMZ does not make sense when a stateless firewall is available

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Sam is working as s pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?

A. Denial-of-Service
B. False Positive Generation
C. Insertion Attack
D. Obfuscating

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drown based on these scan results?

TCP port 21 – no response
TCP port 22 – no response
TCP port 23 – Time-to-live exceeded

A. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error
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 firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering that NMAP result below, which of the following is likely to be installed on the target machine by the OS? Starting NMAP 5.21 at 20011-03-15 11:06 NMAP scan report for 172.16.40.65 Host ip up (1.00s latency). Not shown: 993 closed ports PORT STATE SERVICE 21/tcp open ftp 23/tcp open telnet 80/tcp open http 139/tcp open netbios-ssn 515/tcp open 631/tcp open ipp 9100/tcp open MAC Address: 00:00:48:0D:EE:8

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
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 scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
B. This is scam because Bob does not know Scott.
C. Bob should write to scottmelby@yahoo.com to verify the identity of Scott.
D. This is probably a legitimate message as it comes from a respectable organization.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.

<iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none""></iframe>

What is this type of attack (that can use either HTTP GET or HTTP POST) called?
A. Cross-Site Request Forgery
B. SQL Injection
C. Browser Hacking
D. Cross-Site Scripting

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61
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 this action so that is escalates to a DoS attack.
D. He will repeat the same attack against all L2 switches of the network.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
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. Stealth virus
B. Tunneling virus
C. Cavity virus
D. Polymorphic virus

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
If there is an Intrusion Detection System (IDS) in intranet, which port scanning technique cannot be used?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80. The engineer receives this output:

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

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?

A. Paros Proxy
B. BBProxy

C. Bloover
D. BBCrack

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
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. Linux
C. OS X
D. Unix

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 67
A network administrator discovers several unknown files in the root directory of his Linux FTP server. One of the files is a tarball, two are shell script files, and the third is a binary file is named "nc." The FTP server's access logs show that the anonymous user account logged in to the server, uploaded the files, and extracted the contents of the tarball and ran the script using a function provided by the FTP server's software. The ps command shows that the nc file is running as process, and the netstat command shows the nc process is listening on a network port.

What kind of vulnerability must be present to make this remote attack possible?

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

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 68
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 69
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 confidentially, 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.

Basic example to understand how cryptography works is given below:

SECURE (plain text)
+1 (+1 next letter.for example , the letter""T"" is used for "S" to encrypt.)
TFDVSF (encrypted text)
+=logic=>Algorithm
1=Factor=>Key

Which of the following choices true about cryptography?

A. Algorithm is not the secret; key is the secret.
B. Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.

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. 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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1

What is the main purpose of those static routes?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
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.

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 73
Look at the following output. What did the hacker accomplish?

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


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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
Which type of security feature stops vehicles from crashing through the doors of a building?

A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 76
Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications an unpatched security flaws in a computer system?

A. Nessus
B. Metasploit
C. Maltego

D. Wireshark

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
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. Masquerading
B. Tailgating
C. Phishing
D. Whaling

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 78
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79
What is the role of test automation in security testing?

A. It is an option but it tends to be very expensive.
B. It should be used exclusively. Manual testing is outdated because of low spend and possible test setup inconsistencies.
C. Test automation is not usable in security due to the complexity of the tests.
D. It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80
A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.

Which sort of trojan infects this server?

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

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:

QUESTION 81
In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities.

Example:

allintitle: root passwd

A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 82
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.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.

An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is: nmap 192.168.1.64/28

Why he cannot see the servers?

A. He needs to change the address to 192.168.1.0 with the same mask
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. The network must be down and the nmap command and IP address are ok

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
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.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 85
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.

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?

A. msfencode
B. msfpayload
C. msfcli
D. msfd

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
Which of the following is a passive wireless packet analyzer that works on Linux-based systems?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 89
Seth is starting a penetration test from inside the network. He hasn't been given any information about the network. What type of test is he conducting?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 90
You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account. What should you do?
A. Do not report it and continue the penetration test.
B. Transfer money from the administrator's account to another account.
C. Do not transfer the money but steal the bitcoins.
D. Report immediately to the administrator.

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
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. Make sure that legitimate network routers are configured to run routing protocols with authentication. B. Disable all routing protocols and only use static routes
C. Only using OSPFv3 will mitigate this risk.
D. Redirection of the traffic cannot happen unless the admin allows it explicitly.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:

- Access List should be written between VLANs.
- Port security should be enabled for the intranet.
- A security solution which filters data packets should be set between intranet (LAN) and DMZ.
- A WAF should be used in front of the web applications.

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93
Trinity needs to scan all hosts on a /16 network for TCP port 445 only. What is the fastest way she can accomplish this with Nmap? Stealth is not a concern.

A. nmap –p 445 –n –T4 –open 10.1.0.0/16
B. nmap –p 445 –max –Pn 10.1.0.0/16
C. nmap –sn –sF 10.1.0.0/16 445
D. nmap –s 445 –sU –T5 10.1.0.0/16

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94
Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95
You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email (boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network. What testing method did you use?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name. What should be the first step in security testing the client?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
OpenSSL on Linux servers includes a command line tool for testing TLS. What is the name of the tool and the correct syntax to connect to a web server?

A. openssl s_client –site www.website.com:443
B. openssl_client –site www.website.com:443
C. openssl_client –connect www.website.com:443
D. openssl s_client –connect www.website.com:443

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
John is an incident handler at a financial institution. His steps in a recent incident are not up to the standards of the company. John frequently forgets some steps and procedures while handling responses as they are very stressful to perform. Which of the following actions should John take to overcome this problem with the least administrative effort?

A. Increase his technical skills
B. Read the incident manual every time it occurs
C. Select someone else to check the procedures
D. Create an incident checklist

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?
A. Voice

B. Fingerprints
C. Iris patterns
D. Height and Weight

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 100
It is an entity or event with the potential to adversely impact a system through unauthorized acces, destruction, disclosure, denial of service or modification of data. Which of the following terms best matches the definition?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
Gavin owns a white-hat firm and is performing a website security audit for one of his clients. He begins by running a scan which looks for common misconfigurations and outdated software versions. Which of the following tools is he most likely using?

A. Armitage
B. Nikto
C. Metasploit
D. Nmap

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
You have successfully logged on a Linux system. You want to now cover your track. Your login attempt may be logged on several files located in /var/log. Which file does NOT belong to the list:

A. wtmp
B. user.log
C. btmp
D. auth.log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
When you return to your desk after a lunch break, you notice a strange email in your inbox. The sender is someone you did business with recently, but the subject line has strange characters in it. What should you do?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Log monitoring tools performing behavioral analysis have alerted several suspicious logins on a Linux server occuring during non-business hours. After further examination of all login activities, it is notices that none of the logins have occurred during typical work hours. A Linux administrator who is investigating this problem realized the system time on the Linux server is wrong by more than twelve hours. What protocol used on Linux serves to synchronize the time has stopped working?

A. NTP
B. TimeKeeper
C. OSPF
D. PPP

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
Which of the following parameters describe LM Hash:

I – The maximum password length is 14 characters
II – There are no distinctions between uppercase and lowercase
III – The password is split into two 7-byte halves

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
A pen-tester is configuring a Windows laptop for a test. In setting up Wireshark, what river and library are required to allow the NIC to work in promiscous mode?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
During the security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?

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

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 109
While scanning with Nmap, Patin found several hosts which have the IP ID of incremental sequences. He then decided to conduct: nmap –Pn –p –sl kiosk.adobe.com www.riaa.com kiosk.adobe.com is the host with incremental IP ID sequence. What is the purpose of using "-sl" with Nmap?

A. Conduct stealth scan
B. Conduct ICMP scan
C. Conduct IDLE scan
D. Conduct silent scan

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110
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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference: