Sample exam with highlighted answers.

Q1

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

Q2

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

Q3

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

Q4

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

Q5

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

Q6

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 of the 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

Q7

this is a simillar question
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

Q8

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

Q9

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

Q10

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

Q11

this is a simillar question
A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed.

What type of alert is the IDS giving?

A. True Positive
B. False Negative
C. False Positive
D.False Positive

Answer: B

Q12

this is a simillar question

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

Q13

this is a simillar question

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

Q14

this is a simillar question

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

Q15

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.
or
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan.

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

Q16

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

Q17

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

Q18

Some clients of Corp A SA were redirected to a malicious site when they tried to access the Corp A main site. Bob a system administrator at Corp A SA found out that they were victims to DNS Cache poisoning.

How Should Bob recommend they deal with such a threat?

A. They use of security agents in clients computers
B. The use of DNSSEC
C. The use 2 factor authentication
D. Client awareness taining programs

Answer: B

Q19

this is a simillar question
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 is this 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

Q20

this is a simillar question
_____ 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

Q21

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

A. HIDS
B. WISS

C. WIPS
D. NIDS

Answer: C

Explanation:
Wireless Intrusion Prevention System (WIPS) | WatchGuard ...
https://www.watchguard.com/wgrd-products/access-points/wips
WatchGuard APs can even be installed as dedicated WIPS sensors in an environment with competing access points, delivering the best WIPS security on the network

Q22

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

Answer:A

Q23

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:
"HEAD / HTTP/1.0"

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

Q24

this is a simillar question
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).
PORT STATE SERVICE VERSION
80/tcp open http 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

Q24

Which one of the following Google Advanced search operateors allows an attacker to restrict the results to those websites in the given domain?

A. [inurl:]
B. [cache:]
C. [link:]
D. [Site:]

Answer: D

Q25

Assume a Business-crucial web-site of some company that is used to sell handsets to customers world wide. All the developed components are reviewed
by the internal security team on a monthly baisis.

In order to drive business further, the web-site developer decded to add some 3rd party marketing tools on it. The tools are written in JavaScript and can track the costomers activity on the site. These tools are located on the servers of the marketing company

What is the main security risk associated with this scenario?

A. Extenal scripts have direct access to t company servers and can steal the data
B. Extenal scripts increase the outbound company data traffic which leards to greater financial loss.
C. Extenal scripts contentets could be maliciouly modified without the security teams knowledge
D. There is no rinsk at all since the marketing company services are trustworthy

Answer: C

Q26

You are an Ethical Hacker who is auditing the ABC company.
When you verify the NOC Server, 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 secondstatic 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

Q27

Why should a security analyst dissable/remove unneccessary ISAPI filters?

A. To defend against wireless attacks
B. To defend against jailbreaking cel phones
C. To defend against webserver attacks
D. To defend against social engineering attacks

Answer: C

Q28

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

Q29

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

Q30

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

Q31
_____ 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

Q32

this is a simillar question
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

Q33

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: A

Q34

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

What's the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?

A. Display passwd content to prompt
B. Removes the passwd file
C. Changes all passwords in passwd
D. Add new user to the passwd file

Answer: A

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/

Q35

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

Q36

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

Q37

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

Q38
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

Q39

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

Q40

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

Q40

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

Q41
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

Q42

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

Q43

SOAP services use which technology to format information?

A. SATA
B. PCI
C. XML
D. ISDN

Answer: C

Q44

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

Q45

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 & OS scan on hosts 192.168.99.1 & 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

Q46

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

Q47

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

Q48

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

Q49

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

Q50

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

Q51

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

Q52

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

Q53

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

Q54

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: A

Q55

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)

Q56

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

Q57

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

Q58

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

Q59

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

Q60

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

Q61

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

Q62

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

Q63

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

Q64

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

Q65

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

Q66
While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan.

What would be the response of all open ports?

A. The port will send an ACK
B. The port will send a SYN
C. The port will ignore the packets
D. The port will send an RST

Answer: C

Q67

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

Q68
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

Q69

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

Q70

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

Q71

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

Q72

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
Q73

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

Q74

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

Q75
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

Q76

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

Q77

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

Q78

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

Q79

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

Q80

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

Q81

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

Q82
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

Q83

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

Fill in the blank with appropriate choice.

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

Answer: B

Q84

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

Q85

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

Q86

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: C

Q87

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

A. tcpdump
B. nmap
C. ping
D. tracer

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

Q88

TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications.

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

A. nmap
B. ping
C. tracert
D. tcpdump

Answer: C
Explanation:
The passive operating system fingerprinting is a feature built into both the pf and tcpdump tools, But using traceroute you can collect the configuration attribute of ("TTL") of the system which is a layer 4 network communications.

Q89

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

invictus@victim_server:~$ nmap -T4 -0 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!

Obviously, it is not going through.

What is the issue here?

A. OS Scan requires root privileges
B. The nmap syntax is wrong.
C. The outgoing TCP/IP fingerprinting is blocked by the host firewall
D. This is a common behavior for a corrupted nmap application

Answer: A

Q90

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:
All stages of hacking are either passive or active, depening on if you interact with the host or not

Q91

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

Q92

Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\IocaI directory and begins to beacon to a Command-and-control server to download additional malicious binaries.

What type of malware has Matthew encountered?

A. Key-logger
B. Trojan
C. Worm
D. Macro Virus

Answer: B

Q93

Jimmy is standing outside a secure entrance to a facility. He is pretending to have a tenseconversation 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

Q94

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

Q95

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.

Q96

A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails.

What type of Trojan did the hacker use?

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

Answer: C

Q97

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)

Q98

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

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

Answer: C

Q99

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

Answer: B

Q100

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

Q101

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

Q102

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 targethost.
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

Q103

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

Q104
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
Q 105

Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?

A. Use cryptographic storage to store all PII
B. Use full disk encryption on all hard drives to protect PII
C. Use encrypted communications protocols to transmit PII
D. Use a security token to log into all Web applications that use PII

Answer: C

Q106

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

Q107

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

Q108

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

Q109

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

Q110
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

Q111

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

Q112

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

Q113
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

Q114

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

Q115

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

Q116

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

Q117

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

Q118

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

Q119

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

Q120

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

Q121

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

Q122

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

Q123

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

Q124

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

Q125

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

Q126

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

Q127

You're doing an internal security audit and you want to find out what ports are open on all theservers.

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

Q128

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: D

Q129

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

Q130

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: C

Q131

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

Q132

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

Q133

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
d
Answer: D

Q134

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

Q135

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

Q136

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

Q137

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

Q138

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

Q139

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

Q140

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)

What did the hacker accomplish?

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

Answer: D

Q141

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 tool 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

Q142

```
#!/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

Q143

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

Q144

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 hashes result in the same value is?

A. Collision
B. Collusion
C. Polymorphism

D. Escrow
Answer: A

Q145

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

Q146

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

Q147

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

Q148

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

Q149

In both pharming and phishing attacks an attacker can create websites that look similar tolegitimate 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

Q150

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

Q151

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

Q152
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

Q153

Q154