test: TryOut-1-CEH EH2-A (Reg Genap 2016-2017)

surname:	1472001	TryOut-1-CEH EH2-A (Reg Genap 2016-2017)
name:	FENITA SUPRAPTO	
user:	1472001	
start time:	2017-04-10 15:04:14	
end time:	2017-04-10 15:47:23	
time:	00:43:09	
points to pass the exam:	80.000	
correct:	(0%)	
wrong:	(0%)	
unanswered:	(0%)	
undisplayed:	(0%)	
points:	**42.400 / 100.000 (42%) - NOT PASSED**	

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913984533	15:04:14	15:05:02	00:48	48.337

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

	1	He will activate OSPF on the spoofed root bridge.
-	2	He will repeat this action so that it escalates to a DoS attack.
	3	He will repeat the same attack against all L2 switches of the network.
	4	He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.

2 S	0.000	281473913984533	15:05:02	15:05:40	00:38	37.479

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?

	1	Network mapping
	2	Gaining access
-	3	Escalating privileges
	4	Footprinting

3 S	0.800	281473913984533	15:05:40	15:06:02	00:22	22.636

A new wireless client is configured to join an 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?

+	1	The WAP does not recognize the client’s MAC address.
	2	The wireless client is not configured to use DHCP.
	3	Client is configured for the wrong channel
	4	The client cannot see the SSID of the wireless network

4 S	0.800	281473913984533	15:06:03	15:06:10	00:07	7.305

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

	1	Netstumbler
+	2	Kismet
	3	Nessus
	4	Abel

5 S	0.000	281473913984533	15:06:10	15:06:56	00:46	45.859

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?

	1	Require all employees to change their anti-virus program with a new one.
-	2	Issue new certificates to the web servers from the root certificate authority
	3	Place a front-end web server in a demilitarized zone that only handles external web traffic
	4	Move the financial data to another server on the same IP subnet

6 S	0.800	281473913984533	15:06:56	15:07:26	00:30	29.915

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 15917KC/s SHAGRN..SHENY9
```

What is she trying to achieve?

+	1	She is using John the Ripper to crack the passwords in the secret.txt file.
	2	She is using ftp to transfer the file to another hacker named John.
	3	She is encrypting the file.
	4	She is using John the Ripper to view the contents of the file.

7 S	0.000	281473913984533	15:07:26	15:07:59	00:33	32.913	
	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 program again. Which of the following terms best matches the definition?						
		1	Riskware				
		2	Ransomware				
		3	Spyware				
	-	4	Adware				

8 S	0.000	281473913984533	15:07:59	15:09:45	01:46	106.587	
	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?						
		1	Rootshock				
		2	Shellshock				
		3	Shellbash				
	-	4	Rootshell				

9 S	0.000	281473913984533	15:09:45	15:09:52	00:07	6.663	
	Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?						
		1	Presentation tier				
		2	Logic tier				
		3	Data tier				
	-	4	Application Layer				

10 S	0.800	281473913984533	15:09:52	15:09:58	00:06	5.662	
	Which of the following is not a Bluetooth attack?						
	+	1	Bluesmaking				
		2	Bluejacking				
		3	Bluesnarfing				
		4	Bluedriving				

11 S	0.800	281473913984533	15:09:58	15:10:09	00:11	11.037	
	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?						
		1	RST				
		2	SYN-ACK				
	+	3	SYN				
		4	ACK				

12 S	0.000	281473913984533	15:10:09	15:10:21	00:12	11.962	
	Which of the following is the least-likely physical characteristic to be used in biometric control that supports a large company?						
	-	1	Iris patterns				
		2	Fingerprints				
		3	Height and weight				
		4	Voice				

13 S	0.800	281473913984533	15:10:21	15:10:29	00:08	8.393	
	Which of the following will perform an Xmas scan using NMAP?						
		1	nmap -sV 192.168.1.254				
		2	nmap -sA 192.168.1.254				
	+	3	nmap -sX 192.168.1.254				
		4	nmap -sP 192.168.1.254				

14 S	0.800	281473913984533	15:10:29	15:11:45	01:16	75.293	
	A penetration test was done at a company. After the test, a reportwas 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?						
		1	There is access control policy between VLANs.				
	+	2	A stateful firewall can be used between intranet (LAN) and DMZ.				
		3	MAC Spoof attacks cannot be performed.				
		4	Possibility of SQL Injection attack is eliminated.				

15 S	0.800	281473913984533	15:11:45	15:11:59	00:14	13.858	
	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?

	1	Cross-Site Request Forgery
+	2	Cross-Site Scripting
	3	Browser Hacking
	4	SQL Injection

16 S	0.800	281473913984533	15:11:59	15:12:49	00:50	50.027

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?

	1	Turtle Trojans
	2	Ransomware Trojans
+	3	Botnet Trojan
	4	Banking Trojans

17 S	0.000	281473913984533	15:12:49	15:13:37	00:48	48.34

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?

	1	WEM
	2	Port forwarding
	3	Promiscuous mode
-	4	Multi-cast mode

18 S	0.800	281473913984533	15:13:37	15:13:43	00:06	6.054

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,""111111111111111111111111111111"");
}
```

Output:

```
Segmentation fault
```

	1	Java
+	2	C++
	3	Python
	4	C#

19 S	0.800	281473913984533	15:13:43	15:14:00	00:17	16.502

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

	1	Use full disk encryption on all hard drives to protect PII
	2	Use a security token to log into all Web applications that use PII
	3	Use cryptographic storage to store all PII
+	4	Use encrypted communications protocols to transmit PII

20 S	0.000	281473913984533	15:14:00	15:14:15	00:15	15.212

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?

	1	False negative
-	2	True positive
	3	True negative
	4	False positive

21 S	0.000	281473913984533	15:14:15	15:14:46	00:31	30.362

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

	1	The host is likely a Linux machine.
	2	The host is likely a router.
-	3	The host is likely a Windows machine.
	4	The host is likely a printer.

22 S	0.800	281473913984533	15:14:46	15:16:05	01:19	70.466

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?

	1	All of the employees would stop normal work activities

+	2	Not informing the employees that they are going to be monitored could be an invasion of privacy.
	3	IT department would be telling employees who the boss is
	4	The network could still experience traffic slow down.

23 S	0.000	281473913984533	15:16:05	15:16:15	00:10	10.421

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

	1	Defense in depth
	2	Security through obscurity
-	3	Network-Based Intrusion Detection System
	4	Host-Based Intrusion Detection System

24 S	0.000	281473913984533	15:16:15	15:16:25	00:10	9.904

How can rainbow tables be defeated?

	1	All uppercase character passwords
	2	Lockout accounts under brute force password cracking attempts
	3	Password salting
-	4	Use of non-dictionary words

25 S	0.800	281473913984533	15:16:25	15:17:14	00:49	49.118

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

+	1	Running a network scan to detect network services in the corporate DMZ
	2	Using configuration management to determine when and where to apply security patches
	3	Reviewing the need for a security clearance for each employee
	4	Training employees on the security policy regarding social engineering

26 S	0.000	281473913984533	15:17:14	15:17:29	00:15	14.627

You are performing information gathering for an important penetration test. You have found PDFs, DOCs, and images in your objective. You decide to extract metadata from these files and analyze it. What tool will help you with the task?

-	1	Armitage
	2	Metagoofil
	3	cdpsnarf
	4	Dimitry

27 S	0.000	281473913984533	15:17:29	15:18:05	00:36	36.116

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?

	1	Attack
	2	Risk
-	3	Vulnerability
	4	Threat

28 S	0.000	281473913984533	15:18:05	15:18:38	00:33	33.287

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?

	1	Insufficient database hardening
	2	Insufficient exception handling
-	3	Insufficient security management
	4	Insufficient input validation

29 S	0.800	281473913984533	15:18:38	15:19:08	00:30	29.254

Scenario:
1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content url.
4. 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?

+	1	ClickJacking Attack
	2	HTML Injection
	3	HTTP Parameter Pollution
	4	Session Fixation

30 S	0.000	281473913984533	15:19:08	15:20:39	01:31	91.722

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?

	1	OS Scan requires root privileges
	2	This is a common behavior for a corrupted nmap application
	3	The nmap syntax is wrong.
-	4	The outgoing TCPXIP fingerprinting is blocked by the host firewall

31 S	0.000	281473913984533	15:20:40	15:20:54	00:14	14.422

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?

	1	The port will send an ACK
	2	The port will send an RST
-	3	The port will send a SYN
	4	The port will ignore the packets

32 S	0.800	281473913984533	15:20:54	15:21:30	00:36	35.689

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?

	1	Host 192.168.99.7 is down
	2	Host 192.168.99.1 is the host that he launched the scan from
	3	Host 192.168.99.7 is a an iPad.
+	4	He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7

33 S	0.800	281473913984533	15:21:30	15:21:34	00:04	4.001

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

+	1	Zero-Day
	2	No-Day
	3	Zero-Sum
	4	Zero-Hour

34 S	0.800	281473913984533	15:21:34	15:23:00	01:26	86.098

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?

	1	Man-in-the-middle attack
	2	Session hijacking
	3	Brute-force attack
+	4	Dictionary attack

35 S	0.000	281473913984533	15:23:00	15:23:22	00:22	21.793

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?

-	1	Install and use Telnet to encrypt all outgoing traffic from this server.
	2	Install Cryptcat and encrypt outgoing packets from this server.
	3	Use HTTP so that all traffic can be routed via a browser, thus evading the internal Intrusion Detection Systems.

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

36 S	0.800	281473913984533	15:23:22	15:25:36	02:14	133.62

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?

+	1	Report immediately to the administrator
	2	Do not report it and continue the penetration test
	3	Transfer money from the administrator’s account to another account
	4	Do not transfer the money but steal the bitcoins

37 S	0.000	281473913984533	15:25:36	15:26:45	01:09	69.435

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

```
; <<>> DiG 9.7.-P1 <<>> axfr domain.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 IN SOA 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)
```

	1	The hacker listed DNS records on his own domain
	2	The hacker used the ""fierce"" tool to brute force the list of available domains.
-	3	The hacker used whois to gather publicly available records for the domain.
	4	The hacker successfully transfered the zone and enumerated the hosts.

38 S	0.000	281473913984533	15:26:45	15:28:36	01:51	110.675

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 no body 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
```

	1	The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
	2	The ACL 104 needs to be first because is UDP
-	3	The ACL 110 needs to be changed to port 80
	4	The ACL for FTP must be before the ACL 110

39 S	0.000	281473913984533	15:28:36	15:29:02	00:26	26.202

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?

	1	c:\ncpa.cpl
	2	c:\gpedit
-	3	c:\services.msc
	4	c:\compmgmt.msc

40 S	0.800	281473913984533	15:29:02	15:29:11	00:09	9.368

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

	1	AH Tunnel mode
+	2	ESP transport mode
	3	AH promiscuous
	4	ESP confidential

41 S	0.000	281473913984533	15:29:11	15:29:23	00:12	11.43

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

	1	tcpdump
	2	tracert

	3	ping
-	4	nmap

42 S	0.800	281473913984533	15:29:23	15:29:32	00:09	8.976

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

	1	PEM
+	2	IPSEC
	3	PPP
	4	SET

43 S	0.800	281473913984533	15:29:32	15:31:57	02:25	144.518

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?

	1	The computer is not using a private IP address
	2	The gateway and the computer are not on the same network
+	3	The gateway is not routing to a public IP address
	4	The computer is using an invalid IP address

44 S	0.000	281473913984533	15:31:57	15:32:43	00:46	46.856

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?

	1	Full disk encryption
	2	Hidden folders
	3	Password protected files
-	4	BIOS password

45 S	0.000	281473913984533	15:32:44	15:33:02	00:18	18.159

Which results will be returned with the following Google search query? site:target.com -site:Marketing.target.com accounting

	1	Results for matches on target.com and Marketing.target.com that include the word
	2	Results matching all words in the query
-	3	Results from matches on the site marketing.target.com that are in the domain target.com but do not include the word accounting
	4	Results matching

46 S	0.800	281473913984533	15:33:02	15:33:22	00:20	20.075

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?

	1	True Negative
	2	False Positive
+	3	False Negative
	4	True Positive

47 S	0.000	281473913984533	15:33:22	15:33:27	00:05	5.055

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

-	1	Passive
	2	Distributive
	3	Reflective
	4	Active

48 S	0.000	281473913984533	15:33:27	15:33:38	00:11	10.758

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

	1	Maintaining Access
	2	Scanning and Enumeration
	3	Reconnaissance
-	4	Gaining Access

49 S	0.800	281473913984533	15:33:38	15:33:45	00:07	7.422

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?

	1	3389
	2	1433
	3	161
+	4	445

50 S	0.000	281473913984533	15:33:45	15:33:59	00:14	14.131

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
```

-	1	nmap -sT -sX -Pn -p 1-65535 192.168.1.1
	2	nmap -sN -Ps -T4 192.168.1.1
	3	nmap -sS -sU -Pn -p 1-65535 192.168.1.1
	4	nmap -sS -Pn 192.168.1.1

51 S	0.000	281473913984533	15:34:00	15:34:19	00:19	19.186

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

	1	Encrypt the data on the hard drive
-	2	Use a strong logon password to the operating system
	3	Set a BIOS password
	4	Back up everything on the laptop and store the backup in a safe place

52 S	0.000	281473913984533	15:34:19	15:34:30	00:11	11.312

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

-	1	Availability
	2	Integrity
	3	Authentication
	4	Confidentiality

53 S	0.000	281473913984533	15:34:30	15:35:16	00:46	45.732

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?

	1	The security breach was a false positive.
	2	The attacker altered or erased events from the logs.
	3	The network devices are not all synchronized.
-	4	Proper chain of custody was not observed while collecting the logs.

54 S	0.800	281473913984533	15:35:16	15:35:32	00:16	15.665

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?

+	1	Vulnerability scanner
	2	Port scanner
	3	Intrusion Detection System
	4	Protocol analyzer

55 S	0.000	281473913984533	15:35:32	15:35:43	00:11	11.752

Which of the following parameters describe LM Hash:

I – The maximum password length is 14 characters.

II – There are no distinctions between uppercase and lowercase.

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

-	1	I, II, and III
	2	II

	3	I and II
	4	I

56 S	0.800	281473913984533	15:35:43	15:35:56	00:13	12.379

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 “no.” 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 no file is running as process, and the netstat command shows the no process is listening on a network port. What kind of vulnerability must be present to make this remote attack possible?

	1	Directory traversal
	2	Brute force login
	3	File system permissions
+	4	Privilege escalation

57 S	0.000	281473913984533	15:35:56	15:36:02	00:06	6.478

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?

	1	Bluetooth
	2	Radio-Frequency Identification
	3	InfraRed
-	4	WLAN

58 S	0.800	281473913984533	15:36:02	15:36:18	00:16	13.894

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

	1	A backup is the source of Malware or illicit information
	2	A backup is unavailable during disaster recovery
+	3	An un-encrypted backup can be misplaced or stolen
	4	A backup is incomplete because no verification was performed

59 S	0.800	281473913984533	15:36:18	15:36:38	00:20	19.624

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?

	1	Use an IDS in the entrance doors and install some of them near the corners
+	2	Install a CCTV with cameras pointing to the entrance doors and the street
	3	Use lights in all the entrance doors and along the company's perimeter
	4	Use fences in the entrance doors

60 S	0.800	281473913984533	15:36:38	15:36:52	00:14	13.717

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?

	1	Mutating
	2	Bounding
+	3	Fuzzing
	4	Randomizing

61 S	0.000	281473913984533	15:36:52	15:37:05	00:13	13.467

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?

-	1	Based on XML
	2	Only compatible with the application protocol HTTP
	3	Exchanges data between web services
	4	Provides a structured model for messaging

62 S	0.000	281473913984533	15:37:05	15:37:10	00:05	4.757

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

10110001
00111010

	1	10001011
-	2	10111100
	3	10011101
	4	11011000

63 S	0.000	281473913984533	15:37:10	15:37:29	00:19	3.423

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 gain access to the DNS server and redirect the direction www.google.com to his own IP address. Now when the employees of the office wants to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?

	1	MAC Flooding
-	2	ARP Poisoning
	3	DNS spoofing
	4	Smurf Attack

64 S	0.000	281473913984533	15:37:24	15:37:46	00:22	17.207
	How does the Address Resolution Protocol (ARP) work?					
		1	It sends a reply packet for a specific IP, asking for the MAC address			
	-	2	It sends a reply packet to all the network elements, asking for the MAC address from a specific IP			
		3	It sends a request packet to all the network elements, asking for the domain name from a specific IP			
		4	It sends a request packet to all the network elements, asking for the MAC address from a specific IP			

65 S	0.000	281473913984533	15:37:46	15:38:02	00:16	15.681
	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?					
		1	Unix			
	-	2	OS X			
		3	Linux			
		4	Windows			

66 S	0.800	281473913984533	15:38:02	15:38:14	00:12	12.473
	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?					
		1	He needs to change the address to 192.168.1.0 with the same mask			
		2	He needs to add the command ""ip address"" just before the IP address			
		3	The network must be down and the nmap command and IP address are ok			
	+	4	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			

67 S	0.000	281473913984533	15:38:14	15:38:28	00:14	13.391
	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?					
	-	1	Avoid			
		2	Accept			
		3	Mitigate			
		4	Delegate			

68 S	0.800	281473913984533	15:38:28	15:38:53	00:25	24.888
	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?					
		1	Cavity virus			
		2	Polymorphic virus			
		3	Tunneling virus			
	+	4	Stealth virus			

69 S	0.800	281473913984533	15:38:53	15:38:57	00:04	4.435
	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?					
		1	Third party running the code			
		2	Sandboxing the code			
		3	String validating the code			
	+	4	Fuzzy-testing the code			

70 S	0.000	281473913984533	15:38:57	15:39:01	00:04	3.89
	Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?					
		1	Blind SQLi			
		2	Compound SQLi			
		3	Classic SQLi			
	-	4	DMS-specific SQLi			

71 S	0.800	281473913984533	15:39:01	15:39:08	00:07	6.841
	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?					
		1	Delete the email and pretend nothing happened.			
	+	2	Forward the message to your company’s security response team and permanently delete the message from your computer.			
		3	Forward the message to your supervisor and ask for her opinion on how to handle the situation.			
		4	Reply to the sender and ask them for more information about the message contents.			

72 S	0.800	281473913984533	15:39:08	15:39:19	00:11	10.852
	env x=`(){ :; };echo exploit` bash -c ‘cat /etc/passwd’ What is the Shellshock bash vulnerability attempting to do on a vulnerable Linux host?					
		1	Removes the passwd file			
		2	Changes all passwords in passwd			
		3	Add new user to the passwd file			
	+	4	Display passwd content to prompt			

73 S	0.000	281473913984533	15:39:19	15:39:28	00:09	9.009

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?

	1	Preparation phase
-	2	Containment phase
	3	Recovery phase
	4	Identification phase

74 S	0.000	281473913984533	15:39:28	15:39:33	00:05	5.36

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?

	1	Social Engineering
	2	Eavesdropping
	3	Piggybacking
-	4	Tailgating

75 S	0.000	281473913984533	15:39:33	15:39:37	00:04	3.762

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?

	1	Maskgen
-	2	Proxychains
	3	Burpsuite
	4	Dimitry

76 S	0.000	281473913984533	15:39:37	15:39:43	00:06	5.824

.... 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.

	1	Sinkhole Attack
	2	Collision Attack
	3	Evil Twin Attack
-	4	Signal Jamming Attack

77 S	0.800	281473913984533	15:39:43	15:40:24	00:41	41.272

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 his 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?

	1	Both static routes indicate that the traffic is internal with different gateway
	2	Both static routes indicate that the traffic is external with different gateway
+	3	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 and external gateway
	4	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

78 S	0.800	281473913984533	15:40:24	15:40:34	00:10	9.608

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?

	1	Session management vulnerability
	2	SQL injection vulnerability
	3	Cross-site Request Forgery vulnerability
+	4	Cross-site scripting vulnerability

79 S	0.800	281473913984533	15:40:34	15:40:41	00:07	6.408

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?

	1	Both pharming and phishing attacks are identical
	2	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
	3	Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
+	4	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

80 S	0.000	281473913984533	15:40:41	15:40:56	00:15	15.793
	Which type of security feature stops vehicles from crashing through the doors of a building?					
		1	Turnstile			
		2	Receptionist			
		3	Bollards			
	-	4	Mantrap			

81 S	0.800	281473913984533	15:40:56	15:41:39	00:43	42.085
	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?					
		1	Ignore the data and continue the assessment until completed as agreed			
		2	Copy the data to removable media and keep it in case you need it			
		3	Confront the client in a respectful manner and ask her about the data			
	+	4	Immediately stop work and contact the proper legal authorities			

82 S	0.800	281473913984533	15:41:39	15:41:47	00:08	8.18
	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?					
		1	How long it takes to setup individual user accounts			
		2	The amount of time it takes to convert biometric data into a template on a smart card			
	+	3	The amount of time it takes to be either accepted or rejected from when an individual provides Identification and authentication information.			
		4	The amount of time and resources that are necessary to maintain a biometric system			

83 S	0.800	281473913984533	15:41:47	15:42:04	00:17	13.618
	A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?					
	+	1	Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.			
		2	Ignore it.			
		3	Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.			
		4	Try to sell the information to a well-paying party on the dark web.			

84 S	0.000	281473913984533	15:42:04	15:42:08	00:04	4.622
	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?					
	-	1	Intrusion Prevention System (IPS)			
		2	Vulnerability scanner			
		3	Protocol analyzer			
		4	Network sniffer			

85 S	0.000	281473913984533	15:42:08	15:42:26	00:18	17.917
	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?					
		1	$100			
	-	2	$1320			
		3	$440			
		4	$146			

86 S	0.000	281473913984533	15:42:26	15:43:17	00:51	50.237
	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?					
	-	1	Firewall-management policy			
		2	Remote-access policy			
		3	Acceptable-use policy			
		4	Permissive policy			

87 S	0.000	281473913984533	15:43:17	15:43:20	00:03	3.121
	PGP, SSL, and IKE are all examples of which type of cryptography?					
	-	1	Hash Algorithm			
		2	Secret Key			
		3	Digest			
		4	Public Key			

88 S	0.000	281473913984533	15:43:20	15:43:29	00:09	9.519
	You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?					
		1	hping2 --set-ICMP host.domain.com			
		2	hping2 host.domain.com			
	-	3	hping2 -i host.domain.com			
		4	hping2 -1 host.domain.com			

89 S	0.800	281473913984533	15:43:29	15:43:34	00:05	4.34
	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?					
	+	1	This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.			
		2	This is probably a legitimate message as it comes from a respectable organization.			
		3	This is a scam because Bob does not know Scott			
		4	Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.			

90 S	0.800	281473913984533	15:43:34	15:43:38	00:04	3.786
	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?					
		1	Only using OSPFv3 will mitigate this risk.			
		2	Disable all routing protocols and only use static routes			
	+	3	Make sure that legitimate network routers are configured to run routing protocols with authentication.			
		4	Redirection of the traffic cannot happen unless the admin allows it explicitly.			

91 S	0.000	281473913984533	15:43:38	15:43:40	00:02	2.161
	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?					
		1	Shared			
	-	2	Root			
		3	Private			
		4	Public			

92 S	0.800	281473913984533	15:43:40	15:43:43	00:03	2.749
	A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing - Reports https://ibt1.prometric.com/users/custom/report_queue/rq_str... corporate network. What tool should the analyst use to perform a Blackjacking attack?					
		1	BBCrack			
	+	2	BBProxy			
		3	Paros Proxy			
		4	Blooover			

93 S	0.800	281473913984533	15:43:43	15:43:45	00:02	2.251
	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'					
	+	1	LM:NTLM			
		2	LM:NT			
		3	NT:LM			
		4	NTLM:LM			

94 S	0.000	281473913984533	15:43:45	15:43:49	00:04	3.819
	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's APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries. What type of malware has Jesse encountered?					
		1	Worm			
		2	Key-logger			
	-	3	Macro Virus			
		4	Trojan			

95 S	0.000	281473913984533	15:43:49	15:43:51	00:02	1.978
	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?					
		1	Encryption			
		2	Steganography			
	-	3	Public-key cryptography			
		4	RSA algorithm			

96 S	0.000	281473913984533	15:43:51	15:43:53	00:02	2.158
	In order to have a anonymous Internet surf, which of the following is best choice?					
	-	1	Use SSL sites when entering personal information			
		2	Use public VPN			

	3	Use shared WiFi
	4	Use Tor network with multi-node

97 S	0.000	281473913984533	15:43:53	15:43:57	00:04	3.362

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?

-	1	Service Level Agreement
	2	Project Scope
	3	Terms of Engagement
	4	Non-Disclosure Agreement

98 S	0.000	281473913984533	15:43:57	15:44:04	00:07	7.223

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?

	1	TCP/IP doesn't support ICMP
-	2	You need to run the ping command with root privileges
	3	ARP is disabled on the target server
	4	ICMP could be disabled on the target server

99 S	0.800	281473913984533	15:44:04	15:44:07	00:03	3.084

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?

	1	Eradication
+	2	Containment
	3	Recovery
	4	Discovery

100 S	0.000	281473913984533	15:44:07	15:44:24	00:17	17.318

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

	1	Only the internal operation of a system is known to the tester
	2	Only the external operation of a system is accessible to the tester
-	3	The internal operation of a system is only partly accessible to the tester
	4	The internal operation of a system is completely known to the tester

101 S	0.000	281473913984533	15:44:24	15:44:31	00:07	6.375

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

-	1	Modifies directory table entries so that directory entries point to the virus code instead of the actual program.
	2	Overwrites the original MBR and only executes the new virus code.
	3	Moves the MBR to another location on the RAM and copies itself to the original location of the MBR.
	4	Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR.

102 S	0.800	281473913984533	15:44:31	15:44:33	00:02	2.231

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?

	1	A virus scanner
	2	A port scanner
	3	A malware scanner
+	4	A vulnerability scanner

103 S	0.000	281473913984533	15:44:33	15:44:37	00:04	4.163

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

-	1	ICMP
	2	SNMP
	3	SMS
	4	SYSLOG

104 S	0.000	281473913984533	15:44:41	15:44:45	00:04	4.005

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

	1	Network layer headers and the session layer port numbers
	2	Transport layer port numbers and application layer headers
	3	Presentation layer headers and the session layer port numbers
-	4	Application layer port numbers and the transport layer headers

105 S	0.800	281473913984533	15:44:45	15:44:56	00:11	11.156

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

	1	Firewalls
	2	Host-based intrusion detection system (HIDS)
+	3	Network-based intrusion detection system (NIDS)
	4	Honeypots

106 S	0.000	281473913984533	15:44:56	15:45:01	00:05	4.256

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?

	1	DIAMETER
	2	TACACS+
	3	RADIUS
-	4	Kerberos

107 S	0.000	281473913984533	15:45:01	15:45:04	00:03	3.022

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

	1	Use digital certificates to authenticate a server prior to sending data.
	2	Validate and escape all information sent to a server.
-	3	Use security policies and procedures to define and implement proper security settings.
	4	Verify access right before allowing access to protected information and UI controls.

108 S	0.000	281473913984533	15:45:04	15:45:23	00:19	18.752

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?

	1	Cross-Site Request Forgery
-	2	Web Form Input Validation
	3	Cross-Site Scripting
	4	Clickjacking

109 S	0.000	281473913984533	15:45:23	15:45:28	00:05	4.995

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?

	1	Circuit
-	2	Packet Filtering
	3	Stateful
	4	Application

110 S	0.800	281473913984533	15:45:28	15:45:31	00:03	3.268

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

	1	Create User Account
+	2	Download and Install Netcat
	3	Disable IPTables
	4	Disable Key Services

111 S	0.000	281473913984533	15:45:31	15:45:37	00:06	5.701

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?

	1	Discretionary Access Control (DAC)
	2	Single sign-on
-	3	Role Based Access Control (RBAC)
	4	Windows authentication

112 S	0.800	281473913984533	15:45:37	15:45:39	00:02	2.432

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

	1	HIPAA
	2	PCI-DSS
	3	EU Safe Harbor
+	4	NIST SP 800-53

113 S	0.800	281473913984533	15:45:39	15:45:47	00:08	1.267

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?

+	1	PKI
	2	Single-Sign On
	3	Biometrics
	4	SOA

114 S	0.000	281473913984533	15:45:44	15:45:54	00:10	6.577

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?

	1	Exclamation mark
	2	Semicolon
	3	Single quote
-	4	Double quote

115 S	0.000	281473913984533	15:45:54	15:46:15	00:21	20.732

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?

	1	Mail relaying, which is a technique of bouncing e-mail from internal to external mail servers continuously.
	2	Tools that will reconfigure a mail server’s relay component to send the e-mail back to the spammers occasionally.
-	3	A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
	4	A blacklist of companies that have their mail server relays configured to be wide open.

116 S	0.800	281473913984533	15:46:15	15:46:22	00:07	7.039

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?

	1	http enum
	2	http-git
+	3	http-methods
	4	http-headers

117 S	0.000	281473913984533	15:46:22	15:46:37	00:15	14.865

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

	1	Inherent risk
-	2	Impact risk
	3	Residual risk
	4	Deferred risk

118 S	0.800	281473913984533	15:46:37	15:46:40	00:03	3.174

What is the role of test automation in security testing?

	1	It should be used exclusively. Manual testing is outdated because of low speed and possible test setup inconsistencies
	2	It is an option but it tends to be very expensive
	3	Test automation is not usable in security due to the complexity of the tests
+	4	It can accelerate benchmark tests and repeat them with a consistent test setup. But it cannot replace manual testing completely.

119 S	0.000	281473913984533	15:46:40	15:46:49	00:09	9.12

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

-	1	Wireshark
	2	Cain & Abel
	3	Maltego
	4	Metasploit

120 S	0.000	281473913984533	15:46:49	15:46:55	00:06	5.489

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?

	1	nmap -T4 -r 10.10.1.0/24
	2	nmap -T4 -F 10.10.0.0/24
	3	nmap -T4 -q 10.10.0.0/24
-	4	nmap -T4 -O 10.10.0.0/24

121 S	0.000	281473913984533	15:46:55	15:46:58	00:03	3.39

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

	1	In a cool dry environment
	2	On a different floor in the same building
	3	In a climate controlled facility offsite
-	4	Inside the data center for faster retrieval in a fireproof safe

122 S	0.000	281473913984533	15:46:58	15:47:05	00:07	6.826

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?

	1	Escalation
	2	Reconnaissance
-	3	Enumeration
	4	Scanning

123 S	0.800	281473913984533	15:47:05	15:47:12	00:07	6.878

What is correct about digital signatures?

	1	Digital signatures may be used in different documents of the same type.
	2	A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
	3	Digital signatures are issued once for each user and can be used everywhere until they expire.
+	4	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.

124 S	0.800	281473913984533	15:47:12	15:47:17	00:05	4.757

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

	1	Security Policy

+	2	Incident Management Process
	3	Internal Procedure
	4	Metrics

125 S	0.000	281473913984533	15:47:17	15:47:23	00:06	6.301

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?

	1	The port scan alone is adequate. This way he saves time.
	2	First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
	3	The sequence does not matter. Both steps have to be performed against all hosts.
-	4	First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.