School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-01

surname:	1572025
name:	YOGI KOSIM SINDUDIBROT
user:	1572025
start time:	2017-09-28 13:34:02
end time:	2017-09-28 14:12:36
time:	00:38:34
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**87.500 / 100.000 (88%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-01

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	0.000		281473913980676	13:34:02	13:39:30	05:28	328.507
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?							
-	1	RST flag scanning					
	2	SYN flag scanning					
	3	FIN flag scanning					
	4	ACK flag scanning					

2 S	6.250		281473913980676	13:39:34	13:41:32	01:58	46.292
Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point. Which of the following type of scans would be the most accurate and reliable option?							
	1	A half-scan					
	2	A FIN scan					
	3	A UDP scan					
+	4	A TCP Connect scan					

3 S	6.250		281473913980676	13:41:33	13:44:22	02:49	169.728
... is a query and response protocol used for querying databases that stores the registered users or assigness of an Internet resource, such as a domain name, an IP address block, or an autonomous system.							
	1	Traceroute					
	2	DNS query					
+	3	WHOIS					
	4	Ping					

4 S	6.250		281473913980676	13:44:23	13:54:34	10:11	14.057
... provide important information about location and type of servers.							
	1	Traceroute					
+	2	DNS records					
	3	Port lists					
	4	OS version					

5 S	6.250		281473913980676	13:46:28	13:50:03	03:35	215.119
Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?							
	1	External Scanning					
	2	Single Scanning					
+	3	Vulnerability Scanning					
	4	Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network?					

6 S	6.250		281473913980676	13:50:04	13:53:29	03:25	204.871
An ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and ...							
+	1	technical knowledge skills					
	2	books to gain knowledge					
	3	money to build infrastructure					
	4	massive field experience					

7 S	6.250		281473913980676	13:53:31	13:56:52	03:21	81.619
... is existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system.							
	1	Hack Value					
	2	Exploit					
	3	Target of Evaluation					
+	4	Vulnerability					

8 S	0.000	281473913980676	13:56:53	13:58:30	01:37	97.132

You are gathering competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators.

How can this help you in footprint the organization?

	1	An understanding of the number of employees in the company
	2	The IP range used by the target network
	3	The types of operating systems and applications being used.
-	4	How strong the corporate security policy is

9 S	6.250	281473913980676	13:58:31	13:59:52	01:21	81.053

According to the CEH methodology, what is the next step to be performed after footprinting/reconnaissance?

	1	System Hacking
+	2	Scanning
	3	Social Engineering
	4	Enumeration

10 S	6.250	281473913980676	13:59:54	14:03:39	03:45	224.84

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

	1	UDP Scanning
+	2	IP Fragment Scanning
	3	Inverse TCP flag scanning
	4	ACK flag scanning

11 S	6.250	281473913980676	14:03:39	14:05:42	02:03	120.181

Which of the following activities will NOT be considered as passive footprinting?

+	1	Scan the range of IP address found in the target DNS database.
	2	Search on financial site such as Yahoo Financial to identify assets.
	3	Perform multiples queries using a search engine.
	4	Go through the rubbish to find out any information that might have been discarded.

12 S	6.250	281473913980676	14:05:44	14:06:44	01:00	59.977

Hacking refers to ... and exploiting system vulnerabilities to gain unauthorized or inappropiate access to the system resources.

	1	Implementing new technologies
	2	Updating operating system
	3	Protecting system security
+	4	Compromising security controls

13 S	6.250	281473913980676	14:06:45	14:08:05	01:20	80.17

... is a defined way to breach the security of an IT system through vulnerability.

	1	Hack Value
+	2	Exploit
	3	Target of Evaluation
	4	Vulnerability

14 S	6.250	281473913980676	14:08:06	14:09:23	01:17	76.978

... is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

	1	Scanning
+	2	Footprinting
	3	Maintaining Access
	4	Gaining Access

15 S	6.250	281473913980676	14:09:23	14:12:02	02:39	158.34

Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic.
What type of scan is Hayden attempting here?

	1	Hayden is attempting to find live hosts on her company's network by using an XMAS scan
+	2	Hayden is using a half-open scan (stealth scan) to find live hosts on her network
	3	She is utilizing a FIN scan to find live hosts that are listening on her network
	4	The type of scan, she is using is called a NULL scan

16 S	6.250	281473913980676	14:12:02	14:12:36	00:34	33.752

... or cracker is one who accesses a computer system by evading its security system.

	1	Administrator
	2	Trader
+	3	Hacker
	4	User

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-01

surname:	1572030
name:	ANDIKA MULYAWAN DWI PR
user:	1572030
start time:	2017-09-28 13:32:15
end time:	2017-09-28 14:14:34
time:	00:42:19
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**87.500 / 100.000 (88%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-01

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	6.250	281473913980685	13:32:15	14:14:34	42:19	110.736

According to the CEH methodology, what is the next step to be performed after footprinting/reconnaissance?

	1	Enumeration
	2	Social Engineering
	3	System Hacking
+	4	Scanning

2 S	6.250	281473913980685	13:35:52	13:52:10	16:18	152.074

You are gathering competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators.

How can this help you in footprint the organization?

+	1	The types of operating systems and applications being used.
	2	How strong the corporate security policy is
	3	The IP range used by the target network
	4	An understanding of the number of employees in the company

3 S	6.250	281473913980685	13:36:58	13:58:47	21:49	397.399

Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic.
What type of scan is Hayden attempting here?

+	1	Hayden is using a half-open scan (stealth scan) to find live hosts on her network
	2	She is utilizing a FIN scan to find live hosts that are listening on her network
	3	Hayden is attempting to find live hosts on her company's network by using an XMAS scan
	4	The type of scan, she is using is called a NULL scan

4 S	6.250	281473913980685	13:38:04	13:38:22	00:18	18.184

... is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

+	1	Footprinting
	2	Maintaining Access
	3	Scanning
	4	Gaining Access

5 S	6.250	281473913980685	13:38:22	13:39:38	01:16	76.01

Attackers gather sensitive information through ... on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

+	1	Social Engineering
	2	Traceroute
	3	DNS records request
	4	Port scanning

6 S	0.000	281473913980685	13:39:38	14:02:03	22:25	104.583

... is a query and response protocol used for querying databases that stores the registered users or assigness of an Internet resource, such as a domain name, an IP address block, or an autonomous system.

	1	Ping
-	2	Traceroute
	3	WHOIS
	4	DNS query

7 S	6.250	281473913980685	13:41:37	13:42:08	00:31	30.222

... is a defined way to breach the security of an IT system through vulnerability.

+	1	Exploit
	2	Target of Evaluation

	3	Vulnerability
	4	Hack Value

8 S	6.250	281473913980685	13:42:08	14:04:43	22:35	78.502

Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.

Which of the following type of scans would be the most accurate and reliable option?

	1	A FIN scan
	2	A half-scan
	3	A UDP scan
+	4	A TCP Connect scan

9 S	0.000	281473913980685	13:43:26	14:07:27	24:01	163.542

Which of the following activities will NOT be considered as passive footprinting?

-	1	Search on financial site such as Yahoo Financial to identify assets.
	2	Perform multiples queries using a search engine.
	3	Scan the range of IP address found in the target DNS database.
	4	Go through the rubbish to find out any information that might have been discarded.

10 S	6.250	281473913980685	13:44:38	13:44:57	00:19	12.274

An ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and ...

	1	books to gain knowledge
+	2	technical knowledge skills
	3	massive field experience
	4	money to build infrastructure

11 S	6.250	281473913980685	13:44:57	13:46:44	01:47	106.464

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in TCP Port 139 and 445.
What protocol is most likely to be listening on those ports?

+	1	SMB
	2	FTP
	3	DNS
	4	Finger

12 S	6.250	281473913980685	13:46:44	13:47:17	00:33	32.686

This method is used to determine the Operating system and version running on a remote target system.
What is it called?

	1	Manual Target System
	2	Identification Scanning
	3	Service Degradation
+	4	OS Fingerprinting

13 S	6.250	281473913980685	13:47:17	14:11:55	24:38	132.267

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

	1	ACK flag scanning
	2	UDP Scanning
+	3	IP Fragment Scanning
	4	Inverse TCP flag scanning

14 S	6.250	281473913980685	13:47:38	13:47:58	00:20	20.331

Ethical hacking involves the use of tricks, techniques, and ... to identify vulnerabilities so as to ensure system security.

+	1	Use of hacking tools
	2	Computer
	3	Rules
	4	Document

15 S	6.250	281473913980685	13:47:58	13:48:39	00:41	40.593

These are the Elements of Information Security, except ...

	1	Availability
	2	Authenticity
	3	Integrity
+	4	Vulnerability

16 S	6.250	281473913980685	13:48:39	13:49:28	00:49	48.538

Hacking refers to ... and exploiting system vulnerabilities to gain unauthorized or inappropiate access to the system resources.

+	1	Compromising security controls
	2	Implementing new technologies
	3	Updating operating system
	4	Protecting system security

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-02

surname:	1572025
name:	YOGI KOSIM SINDUDIBROT
user:	1572025
start time:	2017-10-05 14:16:29
end time:	2017-10-05 14:51:29
time:	00:35:00
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**90.000 / 100.000 (90%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-02

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	5.000	281473913980692	14:16:29	14:51:29	35:00	115.569

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

2 S	5.000	281473913980692	14:16:44	14:22:35	05:51	350.619

... is a TCP/IP protocol used for remote-monitoring and managing hosts, routers, and other devices on a network.

	1	LDAP
	2	NTP
+	3	SNMP
	4	MIB

3 S	0.000	281473913980692	14:22:35	14:25:04	02:29	149.081

Active online attack majority succeeds on system that has bad passwords and ...

-	1	User stupidity
	2	Strong passwords
	3	Complex password
	4	Open authentication points

4 S	0.000	281473913980692	14:25:06	14:28:09	03:03	183.468

What is the following command used for?
net use \targetipc$ "" /u:""

-	1	Connecting to a Linux computer through Samba
	2	Grabbing the etc/passwd file
	3	This command is used to connect as a null session
	4	Grabbing the SAM

5 S	5.000	281473913980692	14:28:10	14:30:18	02:08	127.498

... is passive online attack activity.

+	1	Access and record the raw network traffic
	2	Generate all possible hashes and compare with the databases values

	3	Try all possible passwords
	4	Try different passwords from a list

6 S	5.000		281473913980692	14:30:19	14:31:26	01:07	66.901

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

	1	445, 447
	2	193, 195
	3	161, 163
+	4	137, 139

7 S	5.000		281473913980692	14:31:27	14:34:40	03:13	193.484

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

	1	Allow full DNS zone transfers.
+	2	Remove A records for internal hosts.
	3	Reject all invalid email received via SMTP.
	4	Enable null session pipes.

8 S	5.000		281473913980692	14:34:41	14:35:01	00:20	19.828

... is designed to synchronize clocks of networked computers.

	1	MIB
	2	LDAP
	3	SNMP
+	4	NTP

9 S	5.000		281473913980692	14:35:03	14:35:32	00:29	28.566

Which one is the hardest password to crack?

	1	758904
+	2	Ukm12345*
	3	password1
	4	HIJKLMNO

10 S	5.000		281473913980692	14:35:33	14:37:52	02:19	138.244

... is hybrid attack activity.

	1	Try all possible passwords
	2	Try different passwords from a list
+	3	Start with the dictionary and insert entropy
	4	Generate all possible hashes and compare with the databases values

11 S	5.000		281473913980692	14:37:52	14:39:01	01:09	68.439

Attackers use the specific port with telnet to enumerates the ... running on the remote host.

	1	OS version
	2	IDS
+	3	server version
	4	firewall

12 S	5.000		281473913980692	14:39:02	14:39:39	00:37	37.05

... is a technique to recover password protected files, it use machines across the network to decrypt passwords.

+	1	Distributed Network Attack
	2	Distributed Denial of Service
	3	Online Attack
	4	Offline Attack

13 S	5.000		281473913980692	14:39:41	14:41:43	02:02	122.175

... is pre-computed hashes attack activity.

	1	Try all possible passwords
	2	Try different passwords from a list
	3	Start with the dictionary and insert entropy
+	4	Generate all possible hashes and compare with the databases values

14 S	5.000		281473913980692	14:41:44	14:42:24	00:40	39.862

... is defined as the process of extracting user names, machine names, network resources, shares, and services from a system.

	1	Covering Track
	2	Escalating Privilege
	3	Reconnaissance
+	4	Enumeration

15 S	5.000		281473913980692	14:42:24	14:43:12	00:48	47.067

... requires huge amounts of network bandwidth.

	1	Offline attacks
+	2	Active online attacks

	3	Non-electronic attacks
	4	Passive online attacks

16 S	5.000	281473913980692	14:43:12	14:44:34	01:22	81.625

... is a term describing a non-admin user account that can gain administrator privilege.

	1	Password cracking
+	2	Privilege escalation
	3	Password sniffing
	4	Hash dumping

17 S	5.000	281473913980692	14:44:35	14:47:30	02:55	174.615

... is a command-line tool designed to crack both Unix/Linux and NT/Windows passwords.

+	1	John the Ripper
	2	SET
	3	Cain & Abel
	4	L0phtcrack

18 S	5.000	281473913980692	14:47:31	14:48:00	00:29	29.828

... are <u>not</u> type of password attacks.

	1	Active online attacks
	2	Non-electronic attacks
	3	Passive online attacks
+	4	Automatic attacks

19 S	5.000	281473913980692	14:48:01	14:48:45	00:44	43.508

Attacker queries ... service to gather information such as valid user names, addresses, departmental details, etc, that can be further used to perform attacks.

	1	NTP
	2	MIB
	3	SNMP
+	4	LDAP

20 S	5.000	281473913980692	14:48:46	14:49:09	00:23	23.219

... is a virtual database containing formal description of all the network objects that can be managed using SNMP.

+	1	MIB
	2	SNMP
	3	LDAP
	4	NTP

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-02

surname:	1572030
name:	ANDIKA MULYAWAN DWI PR
user:	1572030
start time:	2017-10-05 14:16:21
end time:	2017-10-05 15:00:58
time:	00:44:37
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**85.000 / 100.000 (85%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-02

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913980685	14:16:21	15:00:58	44:37	43.244

... is a TCP/IP protocol used for remote-monitoring and managing hosts, routers, and other devices on a network.

	1	LDAP
	2	MIB
	3	NTP
+	4	SNMP

2 S	5.000	281473913980685	14:17:53	14:19:04	01:11	70.924

... is passive online attack activity.

	1	Try all possible passwords
+	2	Access and record the raw network traffic
	3	Try different passwords from a list
	4	Generate all possible hashes and compare with the databases values

3 S	5.000	281473913980685	14:19:04	14:21:39	02:35	154.605

... is pre-computed hashes attack activity.

	1	Try all possible passwords
	2	Start with the dictionary and insert entropy
+	3	Generate all possible hashes and compare with the databases values
	4	Try different passwords from a list

4 S	5.000	281473913980685	14:21:39	14:22:03	00:24	23.522

... is a virtual database containing formal description of all the network objects that can be managed using SNMP.

	1	LDAP
	2	SNMP
+	3	MIB
	4	NTP

5 S	5.000	281473913980685	14:22:03	14:24:59	02:56	176.348

... is a command-line tool designed to crack both Unix/Linux and NT/Windows passwords.

+	1	John the Ripper
	2	Cain & Abel
	3	SET
	4	L0phtcrack

6 S	5.000	281473913980685	14:24:59	14:26:24	01:25	85.035

... is a technique to recover password protected files, it use machines across the network to decrypt passwords.

	1	Online Attack
+	2	Distributed Network Attack
	3	Offline Attack
	4	Distributed Denial of Service

7 S	5.000	281473913980685	14:26:24	14:26:48	00:24	24.223

Attackers use the specific port with telnet to enumerates the ... running on the remote host.

	1	OS version
+	2	server version
	3	IDS
	4	firewall

8 S	5.000	281473913980685	14:26:48	14:27:08	00:20	19.828

Attacker queries ... service to gather information such as valid user names, addresses, departmental details, etc, that can be further used to perform attacks.

	1	MIB
+	2	LDAP
	3	NTP

	4	SNMP

9 S	5.000	281473913980685	14:27:08	14:28:07	00:59	58.296	
... are not type of password attacks.							
	1	Non-electronic attacks					
+	2	Automatic attacks					
	3	Passive online attacks					
	4	Active online attacks					

10 S	0.000	281473913980685	14:28:07	14:57:13	29:06	89.231	
A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against DNS enumeration?							
-	1	Enable null session pipes.					
	2	Allow full DNS zone transfers.					
	3	Remove A records for internal hosts.					
	4	Reject all invalid email received via SMTP.					

11 S	5.000	281473913980685	14:30:04	14:55:43	25:39	89.82	
What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?							
	1	445, 447					
	2	161, 163					
+	3	137, 139					
	4	193, 195					

12 S	5.000	281473913980685	14:32:15	14:54:14	21:59	217.805	
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 whois to gather publicly available records for the domain.					
+	3	The hacker used the "fierce" tool to brute force the list of available domains.					
	4	The hacker successfully transfered the zone and enumerated the hosts.					

13 S	5.000	281473913980685	14:33:03	14:50:36	17:33	86.311	
... and remove LM Hashes are offline attack mitigations.							
	1	Use poor passwords					
+	2	Use good passwords					
	3	Use secure connection					
	4	Use firewall					

14 S	5.000	281473913980685	14:33:46	14:34:48	01:02	62.602	
Try different passwords until one works are activities of ...							
	1	Offline attacks					
+	2	Active online attacks					
	3	Passive online attacks					
	4	Non-electronic attacks					

15 S	0.000	281473913980685	14:34:48	14:48:39	13:51	164.317	
... is a law about hardware progressive development that will affect the calculation time of password cracking.							
	1	Moore's law					
	2	Einstein's law					

	3	Calculation law
-	4	Progressive law

16 S	5.000	281473913980685	14:36:33	14:37:10	00:37	37.013

... is designed to synchronize clocks of networked computers.

	1	LDAP
+	2	NTP
	3	SNMP
	4	MIB

17 S	5.000	281473913980685	14:37:10	14:37:26	00:16	15.846

... is defined as the process of extracting user names, machine names, network resources, shares, and services from a system.

	1	Covering Track
	2	Escalating Privilege
	3	Reconnaissance
+	4	Enumeration

18 S	0.000	281473913980685	14:37:26	14:39:52	02:26	145.365

What is the following command used for?
net use \targetipc$ "" /u:""

	1	Grabbing the SAM
-	2	Grabbing the etc/passwd file
	3	Connecting to a Linux computer through Samba
	4	This command is used to connect as a null session

19 S	5.000	281473913980685	14:39:52	14:41:16	01:24	84.556

Active online attack majority succeeds on system that has bad passwords and ...

	1	Complex password
+	2	Open authentication points
	3	Strong passwords
	4	User stupidity

20 S	5.000	281473913980685	14:41:16	14:42:24	01:08	40.988

... is brute-force attack activity.

	1	Try different passwords from a list
+	2	Try all possible passwords
	3	Start with the dictionary and insert entropy
	4	Generate all possible hashes and compare with the databases values

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1: UTS

surname:	1572025
name:	YOGI KOSIM SINDUDIBROT
user:	1572025
start time:	2017-10-19 16:06:13
end time:	2017-10-19 17:47:20
time:	01:41:07
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**76.250 / 100.000 (76%)**

(Reg Ganjil 2017-2018) EH1: UTS

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	1.250	281473913981968	16:06:13	17:47:20	41:07	35.377
Which of the following activities will NOT be considered as passive footprinting?						
+	1	Scan the range of IP address found in the target DNS database.				
	2	Perform multiples queries using a search engine.				
	3	Search on financial site such as Yahoo Financial to identify assets.				
	4	Go through the rubbish to find out any information that might have been discarded.				

2 S	0.000	281473913981968	16:09:09	16:10:01	00:52	51.853
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	Footprinting				
	2	Escalating privileges				
	3	Network mapping				
-	4	Gaining access				

3 S	0.000	281473913981968	16:10:01	17:43:52	33:51	20.94
What is the following command used for? net use \targetipc$ "" /u:""						
	1	This command is used to connect as a null session				
	2	Grabbing the etc/passwd file				
-	3	Grabbing the SAM				
	4	Connecting to a Linux computer through Samba				

4 S	0.000	281473913981968	16:10:46	16:13:23	02:37	157.208
Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered. What type of Port Scanning is this?						
	1	ACK flag scanning				
	2	SYN flag scanning				
-	3	RST flag scanning				
	4	FIN flag scanning				

5 S	1.250	281473913981968	16:13:23	16:15:23	02:00	116.272
... is existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system.						
	1	Exploit				
	2	Hack Value				
+	3	Vulnerability				
	4	Target of Evaluation				

6 S	1.250	281473913981968	16:15:23	16:18:26	03:03	183.055
These are non-technical password cracking attacks, except ...						
	1	Keyboard sniffing				
+	2	Phishing attack				
	3	Shoulder surfing				
	4	Social engineering				

7 S	1.250	281473913981968	16:18:27	16:20:03	01:36	96.019
... is a command-line tool designed to crack both Unix/Linux and NT/Windows passwords.						
	1	Cain & Abel				
	2	L0phtcrack				
	3	SET				
+	4	John the Ripper				

8 S	1.250	281473913981968	16:20:03	16:24:23	04:20	259.517
... is a TCP/IP protocol used for remote-monitoring and managing hosts, routers, and other devices on a network.						
+	1	SNMP				

	2	LDAP
	3	MIB
	4	NTP

9 S	1.250	281473913981968	16:24:23	16:25:07	00:44	44.002

You are gathering competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators.

How can this help you in footprint the organization?

	1	How strong the corporate security policy is
+	2	The types of operating systems and applications being used.
	3	An understanding of the number of employees in the company
	4	The IP range used by the target network

10 S	1.250	281473913981968	16:25:10	16:27:25	02:15	135.924

... is a defined way to breach the security of an IT system through vulnerability.

	1	Target of Evaluation
	2	Hack Value
	3	Vulnerability
+	4	Exploit

11 S	2.500	281473913981968	16:27:26	16:31:18	03:52	231.593

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-headers
	3	http-git
+	4	http-methods

12 S	1.250	281473913981968	16:31:18	16:31:55	00:37	36.619

An ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and ...

	1	massive field experience
+	2	technical knowledge skills
	3	money to build infrastructure
	4	books to gain knowledge

13 S	1.250	281473913981968	16:31:56	16:32:46	00:50	49.661

You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there.

	1	Visit Google's search engine and view the cached copy
+	2	Visit Archive.org web site to retrieve the Internet archive of the company's website
	3	Visit the company's partners and customers website for this information
	4	Crawl the entire website and store them into your computer

14 S	1.250	281473913981968	16:32:46	16:33:29	00:43	43.252

... is a virtual database containing formal description of all the network objects that can be managed using SNMP.

	1	SNMP
	2	NTP
+	3	MIB
	4	LDAP

15 S	2.500	281473913981968	16:33:30	16:33:47	00:17	16.787

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

16 S	2.500	281473913981968	16:33:48	16:35:27	01:39	99.731

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

17 S	1.250	281473913981968	16:35:28	16:37:12	01:44	103.418

... is a term describing a non-admin user account that can gain administrator privilege.

	1	Hash dumping

+	2	Privilege escalation
	3	Password cracking
	4	Password sniffing

18 S	1.250	281473913981968	16:37:12	16:39:08	01:56	115.815

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

	1	UDP Scanning
	2	ACK flag scanning
+	3	IP Fragment Scanning
	4	Inverse TCP flag scanning

19 S	2.500	281473913981968	16:39:08	16:42:19	03:11	190.676

How can rainbow tables be defeated?

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

20 S	1.250	281473913981968	16:42:20	16:43:09	00:49	49.332

... is designed to synchronize clocks of networked computers.

	1	MIB
+	2	NTP
	3	SNMP
	4	LDAP

21 S	0.000	281473913981968	16:43:10	16:45:04	01:54	113.475

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

	1	hping2 -1 host.domain.com
	2	hping2 --set-ICMP host.domain.com
	3	hping2 -i host.domain.com
-	4	hping2 host.domain.com

22 S	2.500	281473913981968	16:45:04	16:46:55	01:51	110.5

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	Scanning
+	2	Reconnaissance
	3	Enumeration
	4	Escalation

23 S	2.500	281473913981968	16:46:55	16:49:59	03:04	184.054

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

	1	Metasploit
+	2	Maltego
	3	Wireshark
	4	Cain & Abel

24 S	1.250	281473913981968	16:50:00	16:52:50	02:50	169.908

Hayden is the network security administrator for her company, a large finance firm based in Miami. Hayden just returned from a security conference in Las Vegas where they talked about all kinds of old and new security threats; many of which she did not know of. Hayden is worried about the current security state of her company's network so she decides to start scanning the network from an external IP address. To see how some of the hosts on her network react, she sends out SYN packets to an IP range. A number of IPs responds with a SYN/ACK response. Before the connection is established she sends RST packets to those hosts to stop the session. She does this to see how her intrusion detection system will log the traffic.
What type of scan is Hayden attempting here?

	1	She is utilizing a FIN scan to find live hosts that are listening on her network
	2	The type of scan, she is using is called a NULL scan
+	3	Hayden is using a half-open scan (stealth scan) to find live hosts on her network
	4	Hayden is attempting to find live hosts on her company's network by using an XMAS scan

25 S	1.250	281473913981968	16:52:51	16:53:32	00:41	41.484

Hacking refers to ... and exploiting system vulnerabilities to gain unauthorized or inappropiate access to the system resources.

	1	Protecting system security
	2	Updating operating system
+	3	Compromising security controls
	4	Implementing new technologies

26 S	0.000	281473913981968	16:53:33	16:55:36	02:03	123.051

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

27 S	2.500	281473913981968	16:55:37	16:58:49	03:12	191.675

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

28 S	0.000	281473913981968	16:58:49	16:59:52	01:03	62.619

What results will the following command?
nmap -sS -O -p 123-153 192.168.100.3

	1	A stealth scan, determine operating system, and scanning ports 123 to 153
-	2	A stealth scan, checking open ports 123 to 153
	3	A stealth scan, checking all open ports excluding ports 123 to 153
	4	A stealth scan, opening port 123 and 153

29 S	1.250	281473913981968	16:59:53	17:00:23	00:30	29.945

Attacker queries ... service to gather information such as valid user names, addresses, departmental details, etc, that can be further used to perform attacks.

	1	MIB
+	2	LDAP
	3	NTP
	4	SNMP

30 S	2.500	281473913981968	17:00:23	17:04:41	04:18	257.695

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	Network-Based Intrusion Detection System
	3	Host-Based Intrusion Detection System
	4	Security through obscurity

31 S	0.000	281473913981968	17:04:42	17:05:09	00:27	27.458

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

32 S	1.250	281473913981968	17:05:10	17:06:59	01:49	109.384

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

	1	445, 447
	2	193, 195
+	3	137, 139
	4	161, 163

33 S	1.250	281473913981968	17:07:03	17:07:30	00:27	26.906

... is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

	1	Gaining Access
	2	Scanning
+	3	Footprinting
	4	Maintaining Access

34 S	2.500	281473913981968	17:07:30	17:09:55	02:25	144.49

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

	1	Security Policy
	2	Internal Procedure
+	3	Incident Management Process
	4	Metrics

35 S	2.500	281473913981968	17:09:55	17:11:27	01:32	91.373

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	RSA algorithm
+	3	Steganography
	4	Public-key cryptography

36 S	1.250	281473913981968	17:11:28	17:12:29	01:01	61.172

These are the Elements of Information Security, except ...

	1	Integrity
	2	Authenticity
+	3	Vulnerability
	4	Availability

37 S	1.250	281473913981968	17:12:29	17:13:01	00:32	31.28

Attackers use the specific port with telnet to enumerates the ... running on the remote host.

	1	IDS
	2	firewall
+	3	server version
	4	OS version

38 S	1.250	281473913981968	17:13:02	17:14:17	01:15	74.852

This method is used to determine the Operating system and version running on a remote target system.
What is it called?

	1	Identification Scanning
+	2	OS Fingerprinting
	3	Manual Target System
	4	Service Degradation

39 S	1.250	281473913981968	17:14:18	17:17:14	02:56	176.844

Attackers gather sensitive information through ... on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

	1	Traceroute
+	2	Social Engineering
	3	Port scanning
	4	DNS records request

40 S	2.500	281473913981968	17:17:15	17:19:11	01:56	116.174

The “white box testing” methodology enforces what kind of restriction?

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

41 S	1.250	281473913981968	17:19:12	17:19:29	00:17	16.699

According to the CEH methodology, what is the next step to be performed after footprinting/reconnaissance?

+	1	Scanning
	2	System Hacking
	3	Enumeration
	4	Social Engineering

42 S	1.250	281473913981968	17:19:29	17:19:52	00:23	22.186

... is an attack that exploits computer application vulnerabilities before the sofware developer releases a patch for the vulnerability.

	1	Exploit
+	2	Zero-Day Attack
	3	Target of Evaluation
	4	Vulnerability

43 S	1.250	281473913981968	17:19:52	17:21:19	01:27	86.854

Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.

Which of the following type of scans would be the most accurate and reliable option?

	1	A half-scan
+	2	A TCP Connect scan
	3	A UDP scan
	4	A FIN scan

44 S	1.250	281473913981968	17:21:20	17:22:41	01:21	81.519

Ethical hacking involves the use of tricks, techniques, and ... to identify vulnerabilities so as to ensure system security.

	1	Computer
	2	Rules
+	3	Use of hacking tools
	4	Document

45 S	0.000	281473913981968	17:22:42	17:23:34	00:52	52.016

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

46 S	2.500	281473913981968	17:23:42	17:25:02	01:20	80.86

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	The network must be down and the nmap command and IP address are ok
+	3	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
	4	He needs to add the command ""ip address"" just before the IP address

47 S	0.000	281473913981968	17:25:05	17:26:07	01:02	62.005

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

48 S	1.250	281473913981968	17:26:07	17:29:03	02:56	175.386

These are offline attacks methods, except ...

	1	Brute-force Attack
	2	Dictionary Attack
	3	Hybrid Attack
+	4	Moore Attack

49 S	0.000	281473913981968	17:29:04	17:30:01	00:57	57.113

Active online attack majority succeeds on system that has bad passwords and ...

	1	Strong passwords
	2	Open authentication points
	3	Complex password
-	4	User stupidity

50 S	1.250	281473913981968	17:30:01	17:30:25	00:24	23.922

... is a query and response protocol used for querying databases that stores the registered users or assigness of an Internet resource, such as a domain name, an IP address block, or an autonomous system.

	1	Ping
+	2	WHOIS
	3	DNS query
	4	Traceroute

51 S	0.000	281473913981968	17:30:26	17:31:49	01:23	82.777

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

	1	Traceroute to control the path of the packets sent during the scan
-	2	Fingerprinting to identify which operating systems are running on the network
	3	Timing options to slow the speed that the port scan is conducted
	4	ICMP ping sweep to determine which hosts on the network are not available

52 S	1.250	281473913981968	17:31:49	17:32:08	00:19	19.191

... or cracker is one who accesses a computer system by evading its security system.

+	1	Hacker
	2	Administrator
	3	User
	4	Trader

53 S	1.250	281473913981968	17:32:09	17:32:40	00:31	30.036

... provide important information about location and type of servers.

	1	Port lists
+	2	DNS records
	3	OS version
	4	Traceroute

54 S	0.000	281473913981968	17:32:40	17:34:10	01:30	89.475

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	Vulnerability
	3	Risk
	4	Threat

55 S	1.250	281473913981968	17:34:11	17:36:28	02:17	137.285

... is dictionary attack activity.

+	1	Try different passwords from a list
	2	Try all possible passwords
	3	Generate all possible hashes and compare with the databases values
	4	Start with the dictionary and insert entropy

56 S	1.250	281473913981968	17:36:31	17:38:58	02:27	147.617

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

	1	Allow full DNS zone transfers.
	2	Enable null session pipes.
+	3	Remove A records for internal hosts.
	4	Reject all invalid email received via SMTP.

57 S	1.250	281473913981968	17:39:00	17:39:13	00:13	13.249

Which one is the hardest password to crack?

	1	758904
	2	password1
+	3	Ukm12345*
	4	HIJKLMNO

58 S	1.250	281473913981968	17:39:14	17:40:20	01:06	66.019

... is a technique to recover password protected files, it use machines across the network to decrypt passwords.

	1	Offline Attack
	2	Online Attack
+	3	Distributed Network Attack
	4	Distributed Denial of Service

59 S	2.500	281473913981968	17:40:21	17:41:45	01:24	84.252

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	Acceptable-use policy
	2	Remote-access policy
	3	Firewall-management policy
	4	Permissive policy

60 S	1.250	281473913981968	17:41:45	17:42:21	00:36	35.437

Attackers conduct ... to extract information about: network topology, trusted routers, and firewall locations.

	1	Port scanning
+	2	Traceroute
	3	Social Engineering
	4	DNS records request

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1: UTS

surname:	1572030
name:	ANDIKA MULYAWAN DWI PR
user:	1572030
start time:	2017-10-19 16:08:18
end time:	2017-10-19 17:58:13
time:	01:49:55
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**67.500 / 100.000 (68%)**

(Reg Ganjil 2017-2018) EH1: UTS

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	0	16:08:18	--:--:--	--:--	0

This type of Port Scanning technique splits TCP header into several packets so that the packet filters are not able to detect what the packets intends to do.

	1	IP Fragment Scanning
	2	Inverse TCP flag scanning
	3	ACK flag scanning
	4	UDP Scanning

2 S	1.250	281473913981971	16:10:27	16:10:38	00:11	11.192

... is the process of collecting as much information as possible about a target network, for identifying various ways to intrude into an organization's network system.

+	1	Footprinting
	2	Maintaining Access
	3	Gaining Access
	4	Scanning

3 S	1.250	281473913981971	16:10:38	16:11:15	00:37	36.856

... is defined as the process of extracting user names, machine names, network resources, shares, and services from a system.

	1	Escalating Privilege
	2	Reconnaissance
	3	Covering Track
+	4	Enumeration

4 S	0.000	281473913981971	16:11:15	17:58:13	46:58	9.158

Sandra has been actively scanning the client network on which she is doing a vulnerability assessment test. While conducting a port scan she notices open ports in TCP Port 139 and 445.
What protocol is most likely to be listening on those ports?

	1	FTP
-	2	DNS
	3	SMB
	4	Finger

5 S	0.000	281473913981971	16:13:23	17:58:04	44:41	10.8

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

	1	Wireshark
	2	Metasploit
-	3	Cain & Abel
	4	Maltego

6 S	0.000	281473913981971	16:13:35	16:15:17	01:42	102.396

What results will the following command?
nmap -sS -O -p 123-153 192.168.100.3

-	1	A stealth scan, checking open ports 123 to 153
	2	A stealth scan, checking all open ports excluding ports 123 to 153
	3	A stealth scan, opening port 123 and 153
	4	A stealth scan, determine operating system, and scanning ports 123 to 153

7 S	1.250	281473913981971	16:15:17	16:16:04	00:47	46.685

... is existence of a weakness, design, or implementation error that can lead to an unexpected and undesirable event compromising the security of the system.

	1	Hack Value
	2	Target of Evaluation
	3	Exploit
+	4	Vulnerability

8 S	0.000	281473913981971	16:16:04	17:56:40	40:36	73.067

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

	1	hping2 -i host.domain.com

	2	hping2 -1 host.domain.com
	3	hping2 host.domain.com
-	4	hping2 --set-ICMP host.domain.com

9 S	1.250	281473913981971	16:17:20	16:17:45	00:25	25.12

... is designed to synchronize clocks of networked computers.

	1	MIB
	2	LDAP
	3	SNMP
+	4	NTP

10 S	1.250	281473913981971	16:17:45	17:55:24	37:39	5.806

... is a defined way to breach the security of an IT system through vulnerability.

+	1	Exploit
	2	Hack Value
	3	Target of Evaluation
	4	Vulnerability

11 S	1.250	281473913981971	16:18:43	17:55:18	36:35	90.69

What is the following command used for?
net use \targetipc$ "" /u:""

+	1	This command is used to connect as a null session
	2	Connecting to a Linux computer through Samba
	3	Grabbing the etc/passwd file
	4	Grabbing the SAM

12 S	1.250	281473913981971	16:18:51	16:21:00	02:09	128.173

Attackers send an ACK probe packet with random sequence number, no response means port is filtered (Stateful firewall is present) and RST response means the port is not filtered.
What type of Port Scanning is this?

	1	RST flag scanning
+	2	ACK flag scanning
	3	FIN flag scanning
	4	SYN flag scanning

13 S	1.250	281473913981971	16:21:00	16:22:57	01:57	117.683

... is an attack that exploits computer application vulnerabilities before the sofware developer releases a patch for the vulnerability.

	1	Target of Evaluation
+	2	Zero-Day Attack
	3	Exploit
	4	Vulnerability

14 S	1.250	281473913981971	16:22:57	16:23:38	00:41	40.826

You are footprinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telephone numbers but do not find them listed there. You know they had the entire staff directory listed on their website 12 months ago but now it is not there.

	1	Visit the company's partners and customers website for this information
+	2	Visit Archive.org web site to retrieve the Internet archive of the company's website
	3	Crawl the entire website and store them into your computer
	4	Visit Google's search engine and view the cached copy

15 S	1.250	281473913981971	16:23:38	17:53:03	29:25	49.4

Attackers conduct ... to extract information about: network topology, trusted routers, and firewall locations.

	1	DNS records request
+	2	Traceroute
	3	Port scanning
	4	Social Engineering

16 S	2.500	281473913981971	16:26:22	16:26:54	00:32	32.286

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

17 S	1.250	281473913981971	16:26:54	16:27:03	00:09	8.86

... or cracker is one who accesses a computer system by evading its security system.

+	1	Hacker
	2	Trader
	3	Administrator

	4	User

18 S	1.250	281473913981971	16:27:03	16:27:27	00:24	24.354	
An ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and ...							
	1	massive field experience					
+	2	technical knowledge skills					
	3	money to build infrastructure					
	4	books to gain knowledge					

19 S	0.000	281473913981971	16:27:27	17:50:27	23:00	35.435	
Which of the following activities will NOT be considered as passive footprinting?							
-	1	Search on financial site such as Yahoo Financial to identify assets.					
	2	Scan the range of IP address found in the target DNS database.					
	3	Go through the rubbish to find out any information that might have been discarded.					
	4	Perform multiples queries using a search engine.					

20 S	2.500	281473913981971	16:28:58	17:47:24	18:26	51.208	
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	Vulnerability					
+	2	Threat					
	3	Attack					
	4	Risk					

21 S	0.000	281473913981971	16:30:52	17:45:02	14:10	82.363	
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	1433					
	2	161					
	3	445					
	4	3389					

22 S	2.500	281473913981971	16:31:51	17:43:12	11:21	91.05	
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	Network-Based Intrusion Detection System					
+	2	Defense in depth					
	3	Security through obscurity					
	4	Host-Based Intrusion Detection System					

23 S	1.250	281473913981971	16:32:04	16:32:26	00:22	21.484	
You are gathering competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two job postings for network and system administrators. How can this help you in footprint the organization?							
	1	An understanding of the number of employees in the company					
	2	The IP range used by the target network					
+	3	The types of operating systems and applications being used.					
	4	How strong the corporate security policy is					

24 S	1.250	281473913981971	16:32:26	16:32:33	00:07	7.807	
According to the CEH methodology, what is the next step to be performed after footprinting/reconnaissance?							
	1	System Hacking					
	2	Enumeration					
+	3	Scanning					
	4	Social Engineering					

25 S	1.250	281473913981971	16:32:33	16:32:57	00:24	23.069	
Ethical hacking involves the use of tricks, techniques, and ... to identify vulnerabilities so as to ensure system security.							
	1	Computer					
	2	Document					
	3	Rules					
+	4	Use of hacking tools					

26 S	1.250	281473913981971	16:32:57	16:33:04	00:07	7.639	
Which one is the hardest password to crack?							
	1	HIJKLMNO					
	2	758904					
+	3	Ukm12345*					
	4	password1					

27 S	0.000	281473913981971	16:33:04	16:33:27	00:23	22.947

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

28 S	2.500	281473913981971	16:33:27	17:39:51	06:24	60.238

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	Scanning and Enumeration
+	2	Reconnaissance
	3	Maintaining Access
	4	Gaining Access

29 S	0.000	281473913981971	16:34:27	16:35:33	01:06	65.766

Attackers use the specific port with telnet to enumerates the ... running on the remote host.

	1	IDS
-	2	OS version
	3	server version
	4	firewall

30 S	2.500	281473913981971	16:35:33	17:38:48	03:15	91.786

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

31 S	0.000	281473913981971	16:37:49	16:38:48	00:59	59.446

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

32 S	1.250	281473913981971	16:38:48	16:39:58	01:10	70.251

... is passive online attack activity.

	1	Generate all possible hashes and compare with the databases values
	2	Try different passwords from a list
+	3	Access and record the raw network traffic
	4	Try all possible passwords

33 S	2.500		281473913981971	16:39:58	16:40:56	00:58	57.928

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

34 S	0.000		281473913981971	16:40:56	16:44:08	03:12	191.44

... is a TCP/IP protocol used for remote-monitoring and managing hosts, routers, and other devices on a network.

	1	NTP
-	2	LDAP
	3	MIB
	4	SNMP

35 S	0.000		281473913981971	16:44:08	17:34:52	50:44	214.082

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

36 S	1.250		281473913981971	16:44:38	16:45:21	00:43	42.822

... is a virtual database containing formal description of all the network objects that can be managed using SNMP.

	1	LDAP
+	2	MIB
	3	SNMP
	4	NTP

37 S	1.250		281473913981971	16:45:21	17:31:15	45:54	167.038

Ann would like to perform a reliable scan against a remote target. She is not concerned about being stealth at this point.

Which of the following type of scans would be the most accurate and reliable option?

	1	A UDP scan
	2	A FIN scan
+	3	A TCP Connect scan
	4	A half-scan

38 S	0.000		281473913981971	16:46:50	16:51:27	04:37	277.44

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

39 S	1.250		281473913981971	16:51:27	16:52:28	01:01	61.049

... is a query and response protocol used for querying databases that stores the registered users or assigness of an Internet resource, such as a domain name, an IP address block, or an autonomous system.

	1	DNS query
+	2	WHOIS
	3	Traceroute
	4	Ping

40 S	1.250		281473913981971	16:52:28	17:28:23	35:55	87.673

Active online attack majority succeeds on system that has bad passwords and ...

+	1	Open authentication points
	2	Strong passwords
	3	Complex password
	4	User stupidity

41 S	0.000		281473913981971	16:54:42	17:25:55	31:13	63.611

... provide important information about location and type of servers.

-	1	Traceroute
	2	Port lists
	3	DNS records
	4	OS version

42 S	1.250	281473913981971	16:55:43	16:57:00	01:17	76.434

... is a technique to recover password protected files, it use machines across the network to decrypt passwords.

	1	Offline Attack
+	2	Distributed Network Attack
	3	Distributed Denial of Service
	4	Online Attack

43 S	2.500	281473913981971	16:57:00	16:57:45	00:45	45.273

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

+	1	Incident Management Process
	2	Metrics
	3	Security Policy
	4	Internal Procedure

44 S	2.500	281473913981971	16:57:45	17:24:38	26:53	25.456

The “white box testing” methodology enforces what kind of restriction?

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

45 S	2.500	281473913981971	16:57:55	16:58:22	00:27	26.743

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	Enumeration
	2	Escalation
+	3	Reconnaissance
	4	Scanning

46 S	1.250	281473913981971	16:58:22	17:00:58	02:36	156.546

These are non-technical password cracking attacks, except ...

+	1	Phishing attack
	2	Shoulder surfing
	3	Keyboard sniffing
	4	Social engineering

47 S	1.250	281473913981971	17:00:58	17:01:48	00:50	49.887

What ports should be blocked on the firewall to prevent NetBIOS traffic from not coming through the firewall if your network is comprised of Windows NT, 2000, and XP?

	1	161, 163
+	2	137, 139
	3	193, 195
	4	445, 447

48 S	2.500	281473913981971	17:01:48	17:03:38	01:50	109.586

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	Escalating privileges
	2	Network mapping
+	3	Footprinting
	4	Gaining access

49 S	1.250	281473913981971	17:03:38	17:04:41	01:03	62.62

... requires huge amounts of network bandwidth.

+	1	Active online attacks
	2	Non-electronic attacks
	3	Passive online attacks
	4	Offline attacks

50 S	2.500	281473913981971	17:04:41	17:05:11	00:30	30.662

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	RSA algorithm
	2	Public-key cryptography
	3	Encryption
+	4	Steganography

51 S	1.250	281473913981971	17:05:11	17:05:39	00:28	27.666

Hacking refers to ... and exploiting system vulnerabilities to gain unauthorized or inappropiate access to the system resources.

	1	Implementing new technologies

+	2	Compromising security controls
	3	Protecting system security
	4	Updating operating system

52 S	0.000	281473913981971	17:05:39	17:23:01	17:22	113.688

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

	1	Traceroute to control the path of the packets sent during the scan
	2	Fingerprinting to identify which operating systems are running on the network
-	3	ICMP ping sweep to determine which hosts on the network are not available
	4	Timing options to slow the speed that the port scan is conducted

53 S	1.250	281473913981971	17:05:52	17:06:43	00:51	51.034

These are the Elements of Information Security, except ...

	1	Availability
	2	Authenticity
+	3	Vulnerability
	4	Integrity

54 S	1.250	281473913981971	17:06:43	17:07:46	01:03	63.029

... is a command-line tool designed to crack both Unix/Linux and NT/Windows passwords.

	1	SET
	2	Cain & Abel
	3	L0phtcrack
+	4	John the Ripper

55 S	1.250	281473913981971	17:07:46	17:10:01	02:15	134.641

Attackers gather sensitive information through ... on social networking websites such as Facebook, MySpace, LinkedIn, Twitter, Pinterest, Google+, etc.

	1	Traceroute
+	2	Social Engineering
	3	DNS records request
	4	Port scanning

56 S	0.000	281473913981971	17:10:01	17:10:58	00:57	56.423

... is a law about hardware progressive development that will affect the calculation time of password cracking.

-	1	Progressive law
	2	Calculation law
	3	Einstein's law
	4	Moore's law

57 S	2.500	281473913981971	17:10:58	17:17:57	06:59	54.411

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

58 S	1.250	281473913981971	17:11:56	17:13:07	01:11	70.719

If you send a SYN to an open port, what is the correct response?

	1	FIN
	2	SYN
	3	PSH
+	4	SYN+ACK

59 S	0.000	281473913981971	17:13:07	17:16:25	03:18	126.34

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

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

60 S	0.000	281473913981971	17:13:28	17:14:18	00:50	31.569

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

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-03

surname:	1572025
name:	YOGI KOSIM SINDUDIBROT
user:	1572025
start time:	2017-11-16 13:29:25
end time:	2017-11-16 14:15:40
time:	00:46:15
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**72.000 / 100.000 (72%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-03

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	4.000	281473913980691	13:29:25	13:31:44	02:19	139.37

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe.

What kind of attack is being illustrated here?

	1	Reverse Engineering
+	2	Social Engineering
	3	Reverse Psychology
	4	Spoofing Identity

2 S	4.000	281473913980691	13:31:45	13:35:08	03:23	203.04

In ... attack, attackers use "../(dot-dot-slash)" sequence to access restricted directories outside of the web server directory.

	1	SQL Injection
	2	Port Scanning
	3	Data Sniffing
+	4	Directory traversal

3 S	4.000	281473913980691	13:35:10	13:36:15	01:05	65.705

John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

	1	A token is not considered strong authentication.
	2	Token security is not widely used in the industry.
+	3	The connection can be taken over after authentication.
	4	The token based security cannot be easily defeated.

4 S	4.000	281473913980691	13:36:16	13:38:38	02:22	141.723

In TCP session hijacking, an attacker takes over a ... between two machines.

	1	spoofing session
+	2	TCP session
	3	computer session
	4	sniffing session

5 S	4.000	281473913980691	13:38:39	13:39:07	00:28	28.548

... occurs when an intruder maliciously alters visual appearance of a web page.

	1	SQL Injection
	2	Sniffing Login
+	3	Web defacement
	4	Web server DDoS

6 S	0.000	281473913980691	13:39:08	13:50:49	11:41	27.131

An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.

Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.

What is this deadly attack called?

	1	Javelin attack
-	2	Social networking attack

	3	Trojan server attack
	4	Spear phishing attack

7 S	4.000		281473913980691	13:47:52	13:48:45	00:53	52.09

These are reasons of session hijacking successful factor, except ...

+	1	Chyper Text Transmission
	2	Weak Session ID Generation Algorithm
	3	Insecure Handling
	4	Small Session IDs

8 S	4.000		281473913980691	13:48:45	13:52:40	03:55	33.406

Which of the following attacks takes best advantage of an existing authenticated connection?

+	1	Session Hijacking
	2	Password Guessing
	3	Spoofing
	4	Password Sniffing

9 S	4.000		281473913980691	13:48:57	13:49:26	00:29	29.17

These are the impact of webserver attacks, except ...

	1	Compromise of user accounts
+	2	OS patch updated
	3	Data theft
	4	Website defacement

10 S	4.000		281473913980691	13:49:27	13:54:37	05:10	111.218

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

How would you prevent such type of attacks?

	1	Hire the people through third-party job agencies who will vet them for you
	2	Investigate their social networking profiles
	3	It is impossible to block these attacks
+	4	Conduct thorough background checks before you engage them

11 S	0.000		281473913980691	13:54:37	13:55:14	00:37	36.553

Within the context of Computer Security, which of the following statements describes Social Engineering best?

-	1	Social Engineering is the means put in place by human resource to perform time accounting
	2	Social Engineering is a training program within sociology studies
	3	Social Engineering is the act of publicly disclosing information
	4	Social Engineering is the act of getting needed information from a person rather than breaking into a system

12 S	0.000		281473913980691	13:55:15	13:57:31	02:16	136.34

After a client sends a connection request (SYN) packet to the server, the server will respond (SYN-ACK) with a sequence number of its choosing, which then must be acknowledged (ACK) by the client.
This sequence number is predictable; the attack connects to a service first with its own IP address, records the sequence number chosen, and then opens a second connection from a forged IP address.
The attack doesn't see the SYN-ACK (or any other packet) from the server, but can guess the correct responses.
If the source IP address is used for authentication, then the attacker can use the one-sided communication to break into the server.

What attacks can you successfully launch against a server using the above technique?

	1	Web page defacement attacks
-	2	IP spoofing attacks
	3	Denial of Service attacks
	4	Session Hijacking attacks

13 S	4.000		281473913980691	13:57:32	13:58:37	01:05	64.85

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?

	1	Man trap
	2	Social engineering
	3	Shoulder surfing
+	4	Tailgating

14 S	4.000		281473913980691	13:58:38	13:59:05	00:27	27.716

Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance.

What type of social engineering attack has Neil employed here?

+	1	Neil has used a tailgating social engineering attack to gain access to the offices

	2	Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics
	3	This type of social engineering attack is called man trapping
	4	He has used a piggybacking technique to gain unauthorized access

15 S	4.000	281473913980691	13:59:48	14:03:13	03:25	205.293

Best countermeasure of session hijacking is ...

	1	using static ARP
	2	using IDS
	3	using firewall
+	4	using encryption

16 S	0.000	281473913980691	14:03:14	14:04:15	01:01	60.886

Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.

No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.

What type of insider threat would Shayla be considered?

	1	Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider
-	2	Shayla is an Insider Associate since she has befriended an actual employee
	3	She would be considered an Insider Affiliate
	4	Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate

17 S	0.000	281473913980691	14:04:15	14:05:06	00:51	50.712

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

	1	Application security testing
	2	Social engineering
	3	Network sniffing
-	4	Vulnerability scanning

18 S	4.000	281473913980691	14:05:07	14:07:25	02:18	137.977

By attacking network-level sessions, the attacker gathers some critical information that is used to attack ... session.

+	1	Application-level
	2	Datalink-level
	3	Transport-level
	4	Physical-level

19 S	4.000	281473913980691	14:07:26	14:08:14	00:48	48.607

In session hijacking, an attacker relies on ... to connect and authenticate, and will then take over the session.

	1	hijacker activity
	2	victim server
	3	correct time
+	4	legitimate user

20 S	4.000	281473913980691	14:08:15	14:09:50	01:35	95.001

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter.

What is the best way to undermine the social engineering activity of tailgating?

	1	Setup a mock video camera next to the special card reader adjacent to the secure door
	2	Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
+	3	Educate and enforce physical security policies of the company to all the employees on a regular basis
	4	Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door

21 S	4.000	281473913980691	14:09:51	14:10:43	00:52	52.631

These are common web server vulnerabilities, except ...

	1	Installing the server with default setting
	2	Default accounts with their default or no passwords
+	3	Proper file and directory permissions
	4	Security flaws in ther server OS

22 S	0.000	281473913980691	14:10:44	14:12:23	01:39	98.776

This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

	1	Switch and bait attack
	2	Phishing attack
-	3	Man-in-the-Middle attack

	4	Wiresharp attack

23 S	4.000	281473913980691	14:12:24	14:13:01	00:37	36.698

How would you prevent session hijacking attacks?

+	1	Using unpredictable sequence numbers secures sessions against hijacking
	2	Using biometrics access tokens secures sessions against hijacking
	3	Using hardware-based authentication secures sessions against hijacking
	4	Using non-Internet protocols like http secures sessions against hijacking

24 S	4.000	281473913980691	14:13:01	14:14:59	01:58	118.048

In session hijacking attack, attacker steals a ... which is used to get into the system and snoop the data.

	1	computer MAC Address
	2	user validation
	3	network connection
+	4	valid session ID

25 S	0.000	281473913980691	14:15:00	14:15:40	00:40	39.277

The most commonly used webserver is ...

	1	IIS
	2	Apache
	3	Tomcat
-	4	Nginx

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-03

surname:	1572030
name:	ANDIKA MULYAWAN DWI PR
user:	1572030
start time:	2017-11-16 13:30:10
end time:	2017-11-16 14:18:14
time:	00:48:04
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**72.000 / 100.000 (72%) - PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-03

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	4.000	281473913980685	13:30:10	13:32:37	02:27	146.698

What is the key advantage of Session Hijacking?

	1	It can be easily done and does not require sophisticated skills.
	2	You cannot be traced in case the hijack is detected.
+	3	You can take advantage of an authenticated connection.
	4	You can successfully predict the sequence number generation.

2 S	0.000	281473913980685	13:32:37	14:18:14	45:37	26.308

When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?

	1	Social engineering
	2	Network sniffing
-	3	Vulnerability scanning
	4	Application security testing

3 S	4.000	281473913980685	13:33:23	14:17:47	44:24	8.563

Which of the following attacks takes best advantage of an existing authenticated connection?

	1	Password Sniffing
	2	Spoofing
	3	Password Guessing
+	4	Session Hijacking

4 S	0.000	281473913980685	13:34:17	13:37:01	02:44	163.74

Shayla is an IT security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a subcontractor for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network security.

No employees for the company, other than the IT director, know about Shayla's work she will be doing. Shayla's first step is to obtain a list of employees through company website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the female employee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and uses it to gain unauthorized access to the Treks Avionics offices.

What type of insider threat would Shayla be considered?

	1	She would be considered an Insider Affiliate
	2	Shayla is an Insider Associate since she has befriended an actual employee
	3	Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider
-	4	Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate

5 S	0.000	281473913980685	13:37:01	14:17:26	40:25	34.431

If a competitor wants to cause damage to your organization, steal critical secrets, or put you out of business, they just have to find a job opening, prepare someone to pass the interview, have that person hired, and they will be in the organization.

How would you prevent such type of attacks?

	1	Investigate their social networking profiles
-	2	Hire the people through third-party job agencies who will vet them for you
	3	Conduct thorough background checks before you engage them
	4	It is impossible to block these attacks

6 S	0.000	281473913980685	13:38:00	13:40:27	02:27	146.711

In TCP session hijacking, an attacker takes over a ... between two machines.

	1	TCP session
-	2	computer session
	3	spoofing session
	4	sniffing session

7 S	4.000	281473913980685	13:40:27	14:14:49	34:22	73.252

Neil is an IT security consultant working on contract for Davidson Avionics. Neil has been hired to audit the network of Davidson Avionics. He has been given permission to perform any tests necessary. Neil has created a fake company ID badge and uniform. Neil waits by one of the company's entrance doors and follows an employee into the office after they use their valid access card to gain entrance.

What type of social engineering attack has Neil employed here?

	1	He has used a piggybacking technique to gain unauthorized access
	2	This type of social engineering attack is called man trapping
	3	Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics
+	4	Neil has used a tailgating social engineering attack to gain access to the offices

8 S	4.000	281473913980685	13:43:07	14:13:36	30:29	177.275

An attacker finds a web page for a target organization that supplies contact information for the company. Using available details to make the message seem authentic, the attacker drafts e-mail to an employee on the contact page that appears to come from an individual who might reasonably request confidential information, such as a network administrator.

The email asks the employee to log into a bogus page that requests the employee's user name and password or click on a link that will download spyware or other malicious programming.

Google's Gmail was hacked using this technique and attackers stole source code and sensitive data from Google servers. This is highly sophisticated attack using zero-day exploit vectors, social engineering and malware websites that focused on targeted individuals working for the company.

What is this deadly attack called?

	1	Social networking attack
	2	Trojan server attack
+	3	Spear phishing attack
	4	Javelin attack

9 S	4.000	281473913980685	13:43:31	13:43:47	00:16	15.525

This attack uses social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legitimate-looking e-mail asking users to update their information on the company's Web site, but the URLs in the e-mail actually point to a false Web site.

	1	Man-in-the-Middle attack
+	2	Phishing attack
	3	Wiresharp attack
	4	Switch and bait attack

10 S	4.000	281473913980685	13:43:47	13:45:45	01:58	118.451

These are reasons of session hijacking successful factor, except ...

	1	Insecure Handling
+	2	Chyper Text Transmission
	3	Weak Session ID Generation Algorithm
	4	Small Session IDs

11 S	4.000	281473913980685	13:45:45	13:48:44	02:59	178.512

These are countermeasures of hacking webservers, except ...

	1	patch vulnerabilities immediately
+	2	enable icmp request
	3	anonymous access restriction
	4	incoming traffic filtering

12 S	0.000	281473913980685	13:48:44	13:49:51	01:07	66.961

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter.

What is the best way to undermine the social engineering activity of tailgating?

	1	Setup a mock video camera next to the special card reader adjacent to the secure door
	2	Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
-	3	Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
	4	Educate and enforce physical security policies of the company to all the employees on a regular basis

13 S	4.000	281473913980685	13:49:51	13:50:24	00:33	33.201

By attacking network-level sessions, the attacker gathers some critical information that is used to attack ... session.

	1	Transport-level
	2	Physical-level
+	3	Application-level
	4	Datalink-level

14 S	4.000	281473913980685	13:50:24	13:54:04	03:40	220.241

In session hijacking attack, attacker steals a ... which is used to get into the system and snoop the data.

	1	user validation
	2	computer MAC Address
+	3	valid session ID
	4	network connection

15 S	4.000	281473913980685	13:54:04	13:55:35	01:31	90.226

Jack Hacker wants to break into Brown Co.'s computers and obtain their secret double fudge cookie recipe. Jack calls Jane, an accountant at Brown Co., pretending to be an administrator from Brown Co. Jack tells Jane that there has been a problem with some accounts and asks her to verify her password with him "just to double check our records." Jane does not suspect anything amiss, and parts with her password. Jack can now access Brown Co.'s computers with a valid user name and password, to steal the cookie recipe.

What kind of attack is being illustrated here?

	1	Reverse Engineering
	2	Reverse Psychology
+	3	Social Engineering
	4	Spoofing Identity

16 S	4.000	281473913980685	13:55:35	13:57:12	01:37	97.571

... occurs when an intruder maliciously alters visual appearance of a web page.

	1	Web server DDoS
+	2	Web defacement
	3	Sniffing Login
	4	SQL Injection

17 S	4.000	281473913980685	13:57:12	13:57:46	00:34	33.774

Within the context of Computer Security, which of the following statements describes Social Engineering best?

+	1	Social Engineering is the act of getting needed information from a person rather than breaking into a system
	2	Social Engineering is a training program within sociology studies
	3	Social Engineering is the act of publicly disclosing information
	4	Social Engineering is the means put in place by human resource to perform time accounting

18 S	4.000	281473913980685	13:57:46	13:58:39	00:53	53.286

In ... attack, attackers use "../(dot-dot-slash)" sequence to access restricted directories outside of the web server directory.

	1	Port Scanning
	2	Data Sniffing
	3	SQL Injection
+	4	Directory traversal

19 S	4.000	281473913980685	13:58:39	13:59:29	00:50	49.926

In a ... , the attacker pretends to be another user or machine to gain access.

	1	MAC Address attack
	2	factor attack
	3	sniffing attack
+	4	spoofing attack

20 S	4.000	281473913980685	13:59:29	13:59:33	00:04	3.552

The most commonly used webserver is ...

	1	Nginx
	2	IIS
+	3	Apache
	4	Tomcat

21 S	0.000	281473913980685	13:59:33	14:01:40	02:07	126.612

Best countermeasure of session hijacking is ...

-	1	using firewall
	2	using encryption
	3	using static ARP
	4	using IDS

22 S	4.000	281473913980685	14:01:40	14:02:07	00:27	27.797

In session hijacking, an attacker relies on ... to connect and authenticate, and will then take over the session.

	1	victim server
+	2	legitimate user
	3	correct time
	4	hijacker activity

23 S	0.000	281473913980685	14:02:07	14:04:57	02:50	70.984

John is using tokens for the purpose of strong authentication. He is not confident that his security is considerably strong.

In the context of Session hijacking why would you consider this as a false sense of security?

	1	The connection can be taken over after authentication.
	2	Token security is not widely used in the industry.
	3	A token is not considered strong authentication.
-	4	The token based security cannot be easily defeated.

24 S	4.000	281473913980685	14:02:30	14:02:52	00:22	21.616

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?

+	1	Tailgating
	2	Social engineering
	3	Man trap
	4	Shoulder surfing

25 S	4.000	281473913980685	14:02:52	14:03:44	00:52	52.265

These are common web server vulnerabilities, except ...

	1	Installing the server with default setting
+	2	Proper file and directory permissions
	3	Default accounts with their default or no passwords
	4	Security flaws in ther server OS

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-04

surname:	1572025
name:	YOGI KOSIM SINDUDIBROT
user:	1572025
start time:	2017-12-07 14:06:54
end time:	2017-12-07 14:40:28
time:	00:33:34
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**65.000 / 100.000 (65%) - NOT PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-04

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	5.000	281473913980692	14:06:54	14:07:49	00:55	55.324

... is a type of attack where SQL commands are injected by attacker via input data.

	1	Directory Traversal
+	2	SQL Injection
	3	Cookie Poisoning
	4	XSS

2 S	0.000	281473913980692	14:07:50	14:08:41	00:51	50.972

Identify SQL injection attack from the HTTP requests shown below:

	1	http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e
	2	http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
	3	http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20pass wd%3d%27hAx0r%27%3b--%00
-	4	http://www.victim.com/example?accountnumber=67891&creditamount=999999999

3 S	5.000	281473913980692	14:08:43	14:11:22	02:39	158.81

These are web application components, except ...

+	1	Web Browser
	2	User Permission
	3	Web Server
	4	Data Store

4 S	5.000	281473913980692	14:11:50	14:13:06	01:16	75.984

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database.

What technique does Jimmy use to compromise a database?

	1	Jimmy can submit user input that executes an operating system command to compromise a target system
	2	Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database
+	3	Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
	4	Jimmy can deface content on the system using XSS attack

5 S	5.000	281473913980692	14:13:07	14:14:35	01:28	87.737

... are major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, such as: XSS and buffer overflow.

	1	Default authorization
	2	Session management
	3	SQL injection
+	4	Input validation flaws

6 S	0.000	281473913980692	14:14:36	14:15:30	00:54	54.451

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'.

The application displays server error. What is wrong with the web application?

	1	User input is not sanitized
	2	The ISP connection is not reliable
	3	The web server may be down
-	4	The email is not valid

7 S	5.000	281473913980692	14:15:31	14:16:36	01:05	64.89

What is the best description of SQL Injection?

+	1	It is an attack used to gain unauthorized access to a database.
	2	It is a Denial of Service Attack.
	3	It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
	4	It is an attack used to modify code in an application.

8 S	5.000	281473913980692	14:16:36	14:19:07	02:31	150.206

... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.

+	1	Parameter manipulation
	2	Client validation
	3	XML poisoning
	4	Server misconfiguration

9 S	0.000	281473913980692	14:19:07	14:21:48	02:41	161.303

AJAX routines manipulation is an example of ... attack.

	1	Server misconfiguration
	2	Client validation
	3	Web service routing issues
-	4	XML poisoning

10 S	5.000	281473913980692	14:21:49	14:25:06	03:17	196.882

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible.

What is the first character that Bob should use to attempt breaking valid SQL request?

	1	Double Quote
	2	Semi Column
	3	Exclamation Mark
+	4	Single Quote

11 S	5.000	281473913980692	14:25:07	14:25:49	00:42	41.394

... attack exploit vulnerabilities and inject malicious code into system files.

	1	Network Access
	2	Session Fixation
	3	Web Services
+	4	File injection

12 S	5.000	281473913980692	14:25:49	14:26:34	00:45	44.337

... can be done by changing the information inside the cookie.

	1	Directory Traversal
	2	XSS
+	3	Cookie Poisoning
	4	Unvalidated Input

13 S	0.000	281473913980692	14:26:35	14:32:15	05:40	339.828

By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.

	1	Server misconfiguration
	2	Client validation
-	3	Web service routing issues
	4	XML poisoning

14 S	0.000	281473913980692	14:32:15	14:33:39	01:24	83.386

SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.

	1	Cookie Poisoning
	2	Unvalidated Input
-	3	Directory Traversal
	4	XSS

15 S	0.000	281473913980692	14:33:39	14:35:11	01:32	91.4

... attack can gives access to SOAP messages that are communicated between two endpoints.

	1	Server misconfiguration
	2	Web service routing issues
-	3	XML poisoning
	4	Client validation

16 S	5.000	281473913980692	14:35:11	14:35:29	00:18	17.419

With increasing dependence, web applications and web services are increasingly being targeted by various ... that results in huge revenue loss for the organizations.

	1	comments
	2	contents
	3	multimedias
+	4	attacks

17 S	5.000	281473913980692	14:35:30	14:35:53	00:23	23.267

Attackers exploit HTTP by using ... and they will be able to access restricted directories.

	1	Cookie Poisoning

+	2	Directory Traversal
	3	XSS
	4	Unvalidated Input

18 S	5.000	281473913980692	14:35:54	14:37:46	01:52	111.806

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
ActualTests.com
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank?

	1	The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
	2	Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
+	3	The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.
	4	The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.

19 S	5.000	281473913980692	14:37:49	14:38:48	00:59	59.009

These are common countermeasures for web application security, except ...

	1	Web Application Firewall
+	2	Operating System Anti Virus
	3	Input validation
	4	Intrusion Detection System

20 S	0.000	281473913980692	14:38:49	14:40:28	01:39	98.651

... is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

	1	Login
	2	Attack vector
-	3	SQL command
	4	Firewall

School name
first row
second row
third row

test: (Reg Ganjil 2017-2018) EH1-A: Kuis-04

surname:	1572030
name:	ANDIKA MULYAWAN DWI PR
user:	1572030
start time:	2017-12-07 14:06:59
end time:	2017-12-07 14:33:19
time:	00:26:20
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**60.000 / 100.000 (60%) - NOT PASSED**

(Reg Ganjil 2017-2018) EH1-A: Kuis-04

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913980685	14:06:59	14:08:06	01:07	67.462

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database.

What technique does Jimmy use to compromise a database?

-	1	Jimmy can submit user input that executes an operating system command to compromise a target system
	2	Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
	3	Jimmy can deface content on the system using XSS attack
	4	Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database

2 S	5.000	281473913980685	14:08:06	14:11:49	03:43	222.863

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible.

What is the first character that Bob should use to attempt breaking valid SQL request?

+	1	Single Quote
	2	Exclamation Mark
	3	Double Quote
	4	Semi Column

3 S	0.000	281473913980685	14:11:49	14:17:59	06:10	1.92

... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.

	1	XML poisoning
-	2	Client validation
	3	Server misconfiguration
	4	Parameter manipulation

4 S	0.000	281473913980685	14:14:19	14:17:57	03:38	20.697

... attack can gives access to SOAP messages that are communicated between two endpoints.

-	1	XML poisoning
	2	Web service routing issues
	3	Client validation
	4	Server misconfiguration

5 S	5.000	281473913980685	14:18:00	14:19:00	01:00	60.371

Attackers exploit HTTP by using ... and they will be able to access restricted directories.

	1	XSS
+	2	Directory Traversal
	3	Cookie Poisoning
	4	Unvalidated Input

6 S	5.000	281473913980685	14:19:00	14:19:17	00:17	16.71

... is a type of attack where SQL commands are injected by attacker via input data.

	1	XSS
	2	Directory Traversal
+	3	SQL Injection
	4	Cookie Poisoning

7 S	5.000	281473913980685	14:19:41	14:20:57	01:16	76.087

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs

and found the following entries:

Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
ActualTests.com
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank?

	1	The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
	2	Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
+	3	The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.
	4	The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.

8 S	5.000	281473913980685	14:20:57	14:22:03	01:06	66.002

... can be done by changing the information inside the cookie.

	1	Unvalidated Input
	2	Directory Traversal
+	3	Cookie Poisoning
	4	XSS

9 S	5.000	281473913980685	14:22:03	14:22:49	00:46	46.431

SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.

	1	Directory Traversal
+	2	Unvalidated Input
	3	XSS
	4	Cookie Poisoning

10 S	0.000	281473913980685	14:22:49	14:25:46	02:57	123.993

... is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

-	1	Login
	2	Firewall
	3	SQL command
	4	Attack vector

11 S	5.000	281473913980685	14:25:46	14:27:10	01:24	83.955

AJAX routines manipulation is an example of ... attack.

	1	Web service routing issues
	2	Server misconfiguration
+	3	Client validation
	4	XML poisoning

12 S	0.000	281473913980685	14:27:10	14:28:51	01:41	101.5

These are web application components, except ...

-	1	User Permission
	2	Web Browser
	3	Data Store
	4	Web Server

13 S	5.000	281473913980685	14:28:51	14:29:22	00:31	30.342

... are major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, such as: XSS and buffer overflow.

	1	Default authorization
+	2	Input validation flaws
	3	SQL injection
	4	Session management

14 S	5.000	281473913980685	14:29:22	14:29:51	00:29	29.056

... attack exploit vulnerabilities and inject malicious code into system files.

	1	Network Access
	2	Session Fixation
	3	Web Services

+	4	File injection

15 S	0.000	281473913980685	14:29:51	14:31:07	01:16	76.044

What is the best description of SQL Injection?

	1	It is an attack used to gain unauthorized access to a database.
	2	It is a Denial of Service Attack.
-	3	It is an attack used to modify code in an application.
	4	It is a Man-in-the-Middle attack between your SQL Server and Web App Server.

16 S	0.000	281473913980685	14:31:07	14:31:25	00:18	17.988

By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.

	1	XML poisoning
	2	Server misconfiguration
-	3	Client validation
	4	Web service routing issues

17 S	5.000	281473913980685	14:31:25	14:31:46	00:21	20.864

With increasing dependence, web applications and web services are increasingly being targeted by various ... that results in huge revenue loss for the organizations.

	1	contents
	2	multimedias
+	3	attacks
	4	comments

18 S	5.000	281473913980685	14:31:46	14:32:13	00:27	27.082

Identify SQL injection attack from the HTTP requests shown below:

	1	http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
	2	http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourserver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e
	3	http://www.victim.com/example?accountnumber=67891&creditamount=999999999
+	4	http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20pass wd%3d%27hAx0r%27%3b--%00

19 S	5.000	281473913980685	14:32:13	14:32:49	00:36	36.367

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'.

The application displays server error. What is wrong with the web application?

	1	The ISP connection is not reliable
	2	The email is not valid
	3	The web server may be down
+	4	User input is not sanitized

20 S	0.000	281473913980685	14:32:49	14:33:19	00:30	29.824

These are some of the major web application vulnerabilities, except ...

	1	Cross-site scripting
	2	Login page
-	3	SQL injection
	4	Security missconfiguration

School name
first row
second row
third row

test: (Reg Ganjil 2018-2019) EH1-A: Kuis-05

surname:	1672051
name:	LUKAS HANSEL GANDA
user:	1672051
start time:	2018-12-06 13:46:03
end time:	2018-12-06 13:57:57
time:	00:11:54
points to pass the exam:	60.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**80.000 / 100.000 (80%) - PASSED**

(Reg Ganjil 2018-2019) EH1-A: Kuis-05

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	4.000	281473913983769	13:46:03	13:52:46	06:43	7.885
These are the impact of webserver attacks, except ...						
	1	Website defacement				
	2	Data theft				
	3	Compromise of user accounts				
+	4	OS patch updated				

2 S	4.000	281473913983769	13:52:46	13:52:57	00:11	10.841
... can be done by changing the information inside the cookie.						
+	1	Cookie Poisoning				
	2	XSS				
	3	Directory Traversal				
	4	Unvalidated Input				

3 S	4.000	281473913983769	13:52:57	13:53:07	00:10	9.647
With increasing dependence, web applications and web services are increasingly being targeted by various ... that results in huge revenue loss for the organizations.						
	1	multimedias				
	2	contents				
+	3	attacks				
	4	comments				

4 S	4.000	281473913983769	13:53:07	13:53:11	00:04	3.756
The most commonly used webserver is ...						
	1	Tomcat				
	2	Nginx				
+	3	Apache				
	4	IIS				

5 S	4.000	281473913983769	13:53:11	13:53:18	00:07	7.629
... attack exploit vulnerabilities and inject malicious code into system files.						
	1	Network Access				
	2	Web Services				
+	3	File injection				
	4	Session Fixation				

6 S	8.000	281473913983769	13:53:18	13:54:37	01:19	78.887
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	SQL injection vulnerability				
+	2	Cross-site scripting vulnerability				
	3	Cross-site Request Forgery vulnerability				
	4	Session management vulnerability				

7 S	4.000	281473913983769	13:54:37	13:54:49	00:12	11.622
... is a type of attack where SQL commands are injected by attacker via input data.						
	1	Directory Traversal				
+	2	SQL Injection				
	3	Cookie Poisoning				
	4	XSS				

8 S	4.000	281473913983769	13:54:49	13:55:01	00:12	12.258
In ... attack, attackers use "../(dot-dot-slash)" sequence to access restricted directories outside of the web server directory.						
	1	SQL Injection				

+	2	Directory traversal
	3	Data Sniffing
	4	Port Scanning

9 S	4.000	281473913983769	13:55:01	13:55:09	00:08	7.036

... occurs when an intruder maliciously alters visual appearance of a web page.

	1	Sniffing Login
+	2	Web defacement
	3	SQL Injection
	4	Web server DDoS

10 S	4.000	281473913983769	13:55:09	13:55:23	00:14	14.804

By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.

	1	Web service routing issues
	2	Client validation
	3	XML poisoning
+	4	Server misconfiguration

11 S	4.000	281473913983769	13:55:23	13:55:30	00:07	6.948

SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.

+	1	Unvalidated Input
	2	Directory Traversal
	3	XSS
	4	Cookie Poisoning

12 S	0.000	281473913983769	13:55:30	13:55:57	00:27	26.454

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

13 S	0.000	281473913983769	13:55:57	13:56:29	00:32	31.599

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

14 S	4.000	281473913983769	13:56:29	13:56:42	00:13	12.961

These are common countermeasures for web application security, except ...

	1	Web Application Firewall
+	2	Operating System Anti Virus
	3	Intrusion Detection System
	4	Input validation

15 S	8.000	281473913983769	13:56:42	13:57:09	00:27	26.694

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

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

16 S	4.000	281473913983769	13:57:09	13:57:19	00:10	10.061

These are countermeasures of hacking webservers, except ...

	1	anonymous access restriction
+	2	enable icmp request
	3	incoming traffic filtering
	4	patch vulnerabilities immediately

17 S	4.000	281473913983769	13:57:19	13:57:27	00:08	7.867

These are common web server vulnerabilities, except ...

+	1	Proper file and directory permissions

	2	Default accounts with their default or no passwords
	3	Installing the server with default setting
	4	Security flaws in ther server OS

18 S	4.000	281473913983769	13:57:27	13:57:36	00:09	8.842

... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.

	1	XML poisoning
	2	Client validation
	3	Server misconfiguration
+	4	Parameter manipulation

19 S	8.000	281473913983769	13:57:36	13:57:48	00:12	12.437

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	Dimitry
+	2	Burpsuite
	3	Maskgen
	4	Proxychains

20 S	0.000	281473913983769	13:57:48	13:57:57	00:09	8.632

These are web application components, except ...

-	1	Web Server
	2	User Permission
	3	Data Store
	4	Web Browser

School name
first row
second row
third row

test: (Reg Ganjil 2018-2019) EH1-A: Kuis-05

surname:	1672039
name:	ANDRIANUS ALVIEN
user:	1672039
start time:	2018-12-06 13:46:05
end time:	2018-12-06 13:58:00
time:	00:11:55
points to pass the exam:	60.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**92.000 / 100.000 (92%) - PASSED**

(Reg Ganjil 2018-2019) EH1-A: Kuis-05

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	4.000	281473913983770	13:46:05	13:46:41	00:36	35.349
These are the impact of webserver attacks, except ...						
	1	Data theft				
	2	Website defacement				
	3	Compromise of user accounts				
+	4	OS patch updated				

2 S	4.000	281473913983770	13:46:41	13:46:55	00:14	13.877
These are countermeasures of hacking webservers, except ...						
	1	anonymous access restriction				
	2	patch vulnerabilities immediately				
+	3	enable icmp request				
	4	incoming traffic filtering				

3 S	4.000	281473913983770	13:46:55	13:47:56	01:01	61.207
By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.						
	1	XML poisoning				
+	2	Server misconfiguration				
	3	Client validation				
	4	Web service routing issues				

4 S	4.000	281473913983770	13:47:56	13:48:24	00:28	28.294
... can be done by changing the information inside the cookie.						
	1	Directory Traversal				
+	2	Cookie Poisoning				
	3	Unvalidated Input				
	4	XSS				

5 S	4.000	281473913983770	13:48:24	13:48:39	00:15	14.467
... attack can gives access to SOAP messages that are communicated between two endpoints.						
+	1	Web service routing issues				
	2	Client validation				
	3	XML poisoning				
	4	Server misconfiguration				

6 S	4.000	281473913983770	13:48:39	13:48:53	00:14	13.576
... occurs when an intruder maliciously alters visual appearance of a web page.						
	1	Sniffing Login				
	2	Web server DDoS				
+	3	Web defacement				
	4	SQL Injection				

7 S	8.000	281473913983770	13:48:53	13:50:38	01:45	105.225
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	Clickjacking				
	4	Cross-Site Scripting				

8 S	4.000	281473913983770	13:50:38	13:51:21	00:43	43.396
In ... attack, attackers use "../(dot-dot-slash)" sequence to access restricted directories outside of the web server directory.						

	1	SQL Injection
	2	Port Scanning
	3	Data Sniffing
+	4	Directory traversal

9 S	4.000	281473913983770	13:51:21	13:51:31	00:10	9.588

AJAX routines manipulation is an example of ... attack.

	1	Web service routing issues
	2	Server misconfiguration
	3	XML poisoning
+	4	Client validation

10 S	8.000	281473913983770	13:51:31	13:52:05	00:34	33.346

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	Burpsuite
	3	Proxychains
	4	Dimitry

11 S	4.000	281473913983770	13:52:05	13:52:17	00:12	12.27

SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.

	1	XSS
	2	Cookie Poisoning
	3	Directory Traversal
+	4	Unvalidated Input

12 S	8.000	281473913983770	13:52:17	13:54:03	01:46	105.535

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

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

13 S	4.000	281473913983770	13:54:03	13:54:18	00:15	15.657

... are major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, such as: XSS and buffer overflow.

	1	Default authorization
	2	Session management
+	3	Input validation flaws
	4	SQL injection

14 S	4.000	281473913983770	13:54:18	13:54:27	00:09	9.032

The most commonly used webserver is ...

+	1	Apache
	2	Nginx
	3	IIS
	4	Tomcat

15 S	0.000	281473913983770	13:54:27	13:54:51	00:24	23.142

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	SQL Injection
	4	Browser Hacking

16 S	4.000	281473913983770	13:54:51	13:55:05	00:14	14.056

These are common countermeasures for web application security, except ...

	1	Web Application Firewall
+	2	Operating System Anti Virus
	3	Intrusion Detection System
	4	Input validation

17 S	4.000	281473913983770	13:55:05	13:55:20	00:15	14.6

These are common web server vulnerabilities, except ...

	1	Security flaws in ther server OS
+	2	Proper file and directory permissions
	3	Default accounts with their default or no passwords
	4	Installing the server with default setting

18 S	4.000	281473913983770	13:55:20	13:55:30	00:10	10.107

... attack exploit vulnerabilities and inject malicious code into system files.

+	1	File injection
	2	Session Fixation
	3	Web Services
	4	Network Access

19 S	8.000	281473913983770	13:55:30	13:55:49	00:19	19.074

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

20 S	4.000	281473913983770	13:55:49	13:58:00	02:11	130.933

... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.

	1	Server misconfiguration
	2	XML poisoning
+	3	Parameter manipulation
	4	Client validation

School name
first row
second row
third row

test: (Reg Ganjil 2018-2019) EH1-A: Kuis-06

surname:	1672051
name:	LUKAS HANSEL GANDA
user:	1672051
start time:	2018-12-06 14:30:57
end time:	2018-12-06 14:36:23
time:	00:05:26
points to pass the exam:	60.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**108.000 / 116.000 (93%) - PASSED**

(Reg Ganjil 2018-2019) EH1-A: Kuis-06

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]

1 S	4.000	281473913983769	14:30:57	14:31:44	00:47	46.237
By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.						
	1	XML poisoning				
	2	Web service routing issues				
	3	Client validation				
+	4	Server misconfiguration				

2 S	8.000	281473913983769	14:31:44	14:32:05	00:21	20.926
Attempting an injection attack on a web server based on responses to True/False questions is called which of the following?						
	1	Compound SQLi				
	2	Classic SQLi				
	3	DMS-specific SQLi				
+	4	Blind SQLi				

3 S	4.000	281473913983769	14:32:05	14:32:14	00:09	8.994
What is the best description of SQL Injection?						
	1	It is an attack used to modify code in an application.				
+	2	It is an attack used to gain unauthorized access to a database.				
	3	It is a Man-in-the-Middle attack between your SQL Server and Web App Server.				
	4	It is a Denial of Service Attack.				

4 S	4.000	281473913983769	14:32:14	14:32:22	00:08	8.307
These are some of the major web application vulnerabilities, except ...						
	1	Security missconfiguration				
	2	SQL injection				
	3	Cross-site scripting				
+	4	Login page				

5 S	4.000	281473913983769	14:32:22	14:32:31	00:09	8.406
... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.						
	1	Server misconfiguration				
	2	XML poisoning				
+	3	Parameter manipulation				
	4	Client validation				

6 S	4.000	281473913983769	14:32:31	14:32:40	00:09	8.936
Attackers exploit HTTP by using ... and they will be able to access restricted directories.						
+	1	Directory Traversal				
	2	Cookie Poisoning				
	3	XSS				
	4	Unvalidated Input				

7 S	4.000	281473913983769	14:32:40	14:32:48	00:08	8.482
... attack can gives access to SOAP messages that are communicated between two endpoints.						
	1	Server misconfiguration				
+	2	Web service routing issues				
	3	XML poisoning				
	4	Client validation				

8 S	8.000	281473913983769	14:32:48	14:33:06	00:18	17.486
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	Web Form Input Validation
+	2	Cross-Site Request Forgery
	3	Clickjacking
	4	Cross-Site Scripting

9 S	4.000	281473913983769	14:33:06	14:33:14	00:08	8.394
	SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.						
	1	XSS					
	2	Cookie Poisoning					
+	3	Unvalidated Input					
	4	Directory Traversal					

10 S	4.000	281473913983769	14:33:14	14:33:23	00:09	8.647
	... is a type of attack where SQL commands are injected by attacker via input data.						
+	1	SQL Injection					
	2	XSS					
	3	Cookie Poisoning					
	4	Directory Traversal					

11 S	4.000	281473913983769	14:33:23	14:33:30	00:07	7.1
	With increasing dependence, web applications and web services are increasingly being targeted by various ... that results in huge revenue loss for the organizations.						
	1	contents					
	2	comments					
	3	multimedias					
+	4	attacks					

12 S	4.000	281473913983769	14:33:30	14:33:37	00:07	6.076
	... attack exploit vulnerabilities and inject malicious code into system files.						
	1	Network Access					
	2	Session Fixation					
+	3	File injection					
	4	Web Services					

13 S	4.000	281473913983769	14:33:37	14:33:40	00:03	3.201
	These are web application components, except ...						
	1	Web Server					
	2	User Permission					
	3	Data Store					
+	4	Web Browser					

14 S	4.000	281473913983769	14:33:40	14:33:48	00:08	8.47
	Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible. What is the first character that Bob should use to attempt breaking valid SQL request?						
	1	Exclamation Mark					
	2	Semi Column					
+	3	Single Quote					
	4	Double Quote					

15 S	8.000	281473913983769	14:33:48	14:34:20	00:32	31.004
	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	Dimitry					
	2	Maskgen					
+	3	Burpsuite					
	4	Proxychains					

16 S	0.000	281473913983769	14:34:20	14:34:43	00:23	23.623
	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	SQL Injection					
	4	Browser Hacking					

17 S	4.000	281473913983769	14:34:43	14:34:51	00:08	7.609

... are major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, such as: XSS and buffer overflow.

	1	Session management
	2	SQL injection
+	3	Input validation flaws
	4	Default authorization

18 S	4.000	281473913983769	14:34:51	14:35:02	00:11	10.944

Identify SQL injection attack from the HTTP requests shown below:

	1	http://www.victim.com/example?accountnumber=67891&creditamount=999999999
+	2	http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20pass wd%3d%27hAx0r%27%3b--%00
	3	http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al
	4	http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourser ver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e

19 S	4.000	281473913983769	14:35:02	14:35:10	00:08	7.582

... is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

	1	Firewall
	2	SQL command
+	3	Attack vector
	4	Login

20 S	4.000	281473913983769	14:35:10	14:35:17	00:07	7.518

... can be done by changing the information inside the cookie.

	1	XSS
	2	Unvalidated Input
+	3	Cookie Poisoning
	4	Directory Traversal

21 S	4.000	281473913983769	14:35:17	14:35:24	00:07	6.883

AJAX routines manipulation is an example of ... attack.

	1	Server misconfiguration
	2	Web service routing issues
	3	XML poisoning
+	4	Client validation

22 S	4.000	281473913983769	14:35:24	14:35:39	00:15	14.873

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database.

What technique does Jimmy use to compromise a database?

	1	Jimmy can submit user input that executes an operating system command to compromise a target system
+	2	Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
	3	Jimmy can deface content on the system using XSS attack
	4	Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database

23 S	4.000	281473913983769	14:35:39	14:35:47	00:08	7.211

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'.

The application displays server error. What is wrong with the web application?

+	1	User input is not sanitized
	2	The email is not valid
	3	The web server may be down
	4	The ISP connection is not reliable

24 S	4.000	281473913983769	14:35:47	14:36:12	00:25	25.48

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B

ActualTests.com
Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank?

+	1	The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.
	2	The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.
	3	The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
	4	Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.

25 S	4.000	281473913983769	14:36:12	14:36:23	00:11	10.291

These are common countermeasures for web application security, except ...

+	1	Operating System Anti Virus
	2	Input validation
	3	Intrusion Detection System
	4	Web Application Firewall

School name
first row
second row
third row

test: (Reg Ganjil 2018-2019) EH1-A: Kuis-06

surname:	1672039
name:	ANDRIANUS ALVIEN
user:	1672039
start time:	2018-12-06 14:31:05
end time:	2018-12-06 14:36:24
time:	00:05:19
points to pass the exam:	60.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**116.000 / 116.000 (100%) - PASSED**

(Reg Ganjil 2018-2019) EH1-A: Kuis-06

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	4.000	281473913983770	14:31:05	14:31:18	00:13	13.192

Liza has forgotten her password to an online bookstore. The web application asks her to key in her email so that they can send her the password. Liza enters her email liza@yahoo.com'.

The application displays server error. What is wrong with the web application?

	1	The web server may be down
	2	The ISP connection is not reliable
+	3	User input is not sanitized
	4	The email is not valid

2 S	8.000	281473913983770	14:31:18	14:31:29	00:11	10.609

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	Clickjacking
	3	Cross-Site Scripting
	4	Web Form Input Validation

3 S	4.000	281473913983770	14:31:29	14:31:40	00:11	10.682

SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities.

	1	Directory Traversal
	2	XSS
	3	Cookie Poisoning
+	4	Unvalidated Input

4 S	4.000	281473913983770	14:31:40	14:31:51	00:11	11.349

Bob has been hired to do a web application security test. Bob notices that the site is dynamic and must make use of a back end database. Bob wants to see if SQL Injection would be possible.

What is the first character that Bob should use to attempt breaking valid SQL request?

	1	Double Quote
	2	Exclamation Mark
	3	Semi Column
+	4	Single Quote

5 S	4.000	281473913983770	14:31:51	14:32:01	00:10	9.61

These are common countermeasures for web application security, except ...

	1	Input validation
+	2	Operating System Anti Virus
	3	Intrusion Detection System
	4	Web Application Firewall

6 S	4.000	281473913983770	14:32:01	14:32:10	00:09	9.541

... attack can gives access to SOAP messages that are communicated between two endpoints.

	1	Client validation
	2	Server misconfiguration
+	3	Web service routing issues
	4	XML poisoning

7 S	4.000	281473913983770	14:32:10	14:32:22	00:12	11.421

Attackers exploit HTTP by using ... and they will be able to access restricted directories.

+	1	Directory Traversal
	2	Cookie Poisoning
	3	Unvalidated Input

	4	XSS

8 S	4.000		281473913983770	14:32:22	14:32:30	00:08	8.363
These are web application components, except ...							
	1	User Permission					
+	2	Web Browser					
	3	Data Store					
	4	Web Server					

9 S	4.000		281473913983770	14:32:30	14:32:39	00:09	8.814
With increasing dependence, web applications and web services are increasingly being targeted by various ... that results in huge revenue loss for the organizations.							
	1	comments					
	2	multimedias					
	3	contents					
+	4	attacks					

10 S	4.000		281473913983770	14:32:39	14:32:49	00:10	9.333
... can be done by changing the information inside the cookie.							
+	1	Cookie Poisoning					
	2	Directory Traversal					
	3	XSS					
	4	Unvalidated Input					

11 S	4.000		281473913983770	14:32:49	14:33:26	00:37	36.92
Identify SQL injection attack from the HTTP requests shown below:							
+	1	http://www.myserver.com/search.asp?lname=smith%27%3bupdate%20usertable%20set%20pass wd%3d%27hAx0r%27%3b--%00					
	2	http://www.victim.com/example?accountnumber=67891&creditamount=999999999					
	3	http://www.xsecurity.com/cgiin/bad.cgi?foo=..%fc%80%80%80%80%af../bin/ls%20-al					
	4	http://www.myserver.com/script.php?mydata=%3cscript%20src=%22http%3a%2f%2fwww.yourser ver.c0m%2fbadscript.js%22%3e%3c%2fscript%3e					

12 S	8.000		281473913983770	14:33:26	14:33:37	00:11	11.388
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	Proxychains					
	2	Dimitry					
+	3	Burpsuite					
	4	Maskgen					

13 S	4.000		281473913983770	14:33:37	14:33:46	00:09	8.492
AJAX routines manipulation is an example of ... attack.							
+	1	Client validation					
	2	XML poisoning					
	3	Server misconfiguration					
	4	Web service routing issues					

14 S	4.000		281473913983770	14:33:46	14:33:54	00:08	8.246
These are some of the major web application vulnerabilities, except ...							
	1	Cross-site scripting					
+	2	Login page					
	3	SQL injection					
	4	Security missconfiguration					

15 S	4.000		281473913983770	14:33:54	14:34:20	00:26	25.576

Bank of Timbuktu is a medium-sized, regional financial institution in Timbuktu. The bank has deployed a new Internet-accessible Web application recently. Customers can access their account balances, transfer money between accounts, pay bills and conduct online financial business using a Web browser.

John Stevens is in charge of information security at Bank of Timbuktu. After one month in production, several customers have complained about the Internet enabled banking application. Strangely, the account balances of many of the bank's customers had been changed! However, money hasn't been removed from the bank; instead, money was transferred between accounts. Given this attack profile, John Stevens reviewed the Web application's logs and found the following entries:

Attempted login of unknown user: johnm
Attempted login of unknown user: susaR
Attempted login of unknown user: sencat
Attempted login of unknown user: pete'';
Attempted login of unknown user: ' or 1=1--
Attempted login of unknown user: '; drop table logins--
Login of user jason, sessionID= 0x75627578626F6F6B
ActualTests.com

Login of user daniel, sessionID= 0x98627579539E13BE
Login of user rebecca, sessionID= 0x9062757944CCB811
Login of user mike, sessionID= 0x9062757935FB5C64
Transfer Funds user jason
Pay Bill user mike
Logout of user mike

What kind of attack did the Hacker attempt to carry out at the bank?

+	1	The Hacker first attempted logins with suspected user names, then used SQL Injection to gain access to valid bank login IDs.
	2	Brute force attack in which the Hacker attempted guessing login ID and password from password cracking tools.
	3	The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, guessed the next ID and took over Jason's session.
	4	The Hacker used a generator module to pass results to the Web server and exploited Web application CGI vulnerability.

16 S	4.000	281473913983770	14:34:20	14:34:33	00:13	13.506

... are major concern as attackers can exploit these flaws to perform or create a base for most of the web application attacks, such as: XSS and buffer overflow.

+	1	Input validation flaws
	2	Session management
	3	SQL injection
	4	Default authorization

17 S	4.000	281473913983770	14:34:33	14:34:44	00:11	10.123

... attack can be done by providing the wrong input value to the web services by the attacker and gaining control over the SQL, LDAP, XPATH, and shell commands.

+	1	Parameter manipulation
	2	XML poisoning
	3	Server misconfiguration
	4	Client validation

18 S	4.000	281473913983770	14:34:44	14:34:56	00:12	12.485

What is the best description of SQL Injection?

	1	It is an attack used to modify code in an application.
	2	It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
+	3	It is an attack used to gain unauthorized access to a database.
	4	It is a Denial of Service Attack.

19 S	4.000	281473913983770	14:34:56	14:35:05	00:09	8.607

... attack exploit vulnerabilities and inject malicious code into system files.

+	1	File injection
	2	Session Fixation
	3	Web Services
	4	Network Access

20 S	4.000	281473913983770	14:35:05	14:35:18	00:13	13.089

By ... attack, the attackers exploits the vulnerabilites in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers.

	1	XML poisoning
	2	Web service routing issues
+	3	Server misconfiguration
	4	Client validation

21 S	4.000	281473913983770	14:35:18	14:35:28	00:10	9.515

... is a path or means by which an attacker can gain access to computer or network resources in order to deliver an attack payload or cause a malicious outcome.

	1	SQL command
	2	Login
	3	Firewall
+	4	Attack vector

22 S	8.000	281473913983770	14:35:28	14:35:43	00:15	15.465

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	DMS-specific SQLi
	3	Compound SQLi
	4	Classic SQLi

23 S	8.000	281473913983770	14:35:43	14:35:59	00:16	15.305

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

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

24 S	4.000	281473913983770	14:35:59	14:36:13	00:14	14.086

Jimmy, an attacker, knows that he can take advantage of poorly designed input validation routines to create or alter SQL commands to gain access to private data or execute commands in the database.

What technique does Jimmy use to compromise a database?

+	1	Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system
	2	Jimmy can deface content on the system using XSS attack
	3	Jimmy can submit user input that executes an operating system command to compromise a target system
	4	Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database

25 S	4.000	281473913983770	14:36:13	14:36:24	00:11	10.579

... is a type of attack where SQL commands are injected by attacker via input data.

	1	XSS
	2	Cookie Poisoning
+	3	SQL Injection
	4	Directory Traversal