

Target of Evaluation

Vulnerability

3



test: (Reg Ganjil 2017-2018) EH1-A: Kuis-01 (Reg Ganjil 2017-2018) EH1-A: Kuis-01 surname: 1572025 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 (0%) correct: wrong: (0%) (0%) unanswered: undisplayed: (0%) points: 87.500 / 100.000 (88%) - PASSED start [hh:mm:ss] end [hh:mm:ss] time [mm:ss] points 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 SYN flag scanning 2 FIN flag scanning 3 ACK flag scanning 2 S 6.250 281473913980676 01:58 46.292 13:39:34 13:41:32 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? A half-scan A FIN scan 2 3 A UDP scan 4 A TCP Connect scan 3 S 281473913980676 13:41:33 13:44:22 02:49 169.728 6.250 ... 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. Traceroute DNS query 2 WHOIS 3 4 Ping 6.250 281473913980676 4 S 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 OS version 4 281473913980676 5 S 6.250 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 Which of the following type of scanning utilizes automated process of proactively identifying vulnerabilities of the computing systems present on a network? 13:50:04 281473913980676 6 S 6.250 13:53:29 03:25 204.871 An ethical hacker should posses platform knowledge, network knowledge, computer expert, security knowledge, and ... technical knowledge skills books to gain knowledge 2 money to build infrastructure 3 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 Hack Value Exploit 2





8 S		0.000	281473913980676	13:56:53	13:58:30	01:37	97.132
	You ar	e gathei	ing competitive intelligence on	XYZ.com. You notice that they	have jobs listed on a few Inte	rnet job-hunting sites. Th	ere are two job postings
	for net	work an	d system administrators.	ŕ	,	,	,
			,				
	How c	an thic h	elp you in footprint the organiza	ation?			
-	1 IOW C	1 4					
-		1		per of employees in the company	у		
		2	The IP range used by the targ				
		3	The types of operating system	ns and applications being used.			
l	-	4	How strong the corporate sect	urity policy is			
l				and pency is			
			2011=20122222	10.50.04	10.50.50	24.04	
9 S		6.250	281473913980676	13:58:31	13:59:52	01:21	81.053
	Accord	ding to th	e CEH methodology, what is the	ne next step to be performed after	er footprinting/reconnaissand	e?	
		1	System Hacking				
i	+	2	Scanning				
ŀ	-	3	Social Engineering				
-							
		4	Enumeration				
10 S		6.250	281473913980676	13:59:54	14:03:39	03:45	224.84
	This tv	ne of Po	rt Scanning technique solits TO	CP header into several packets	so that the packet filters are r	not able to detect what the	packets intends to do
-		i .	UDP Scanning	or modes into coveral passess	so mar mo paonor mioro aro .	ior abio to actoor milat in	pacitote interide to de-
-		1					
	+	2	IP Fragment Scanning				
		3	Inverse TCP flag scanning				
İ		4	ACK flag scanning				
l		· · · ·					
44.0		6.050	204 47004 20222	44:00:00	44.05.40	00:00	400.404
11 S		6.250	281473913980676	14:03:39	14:05:42	02:03	120.181
	Which	of the fo		onsidered as passive footprintin	<u> </u>		
İ	+	1	Scan the range of IP address	found in the target DNS database	se.		
İ		2		as Yahoo Financial to identify as			
-		3	Perform multiples queries usir				
Į		4	Go through the rubbish to find	out any information that might h	nave been discarded.		
12 S		6.250	281473913980676	14:05:44	14:06:44	01:00	59.977
	Hackin			nerabilities to gain unauthorized			
-	Hackii	ī —			or mapproplate access to th	e system resources.	
		1	Implementing new technologie	25			
		2	Updating operating system				
		3	Protecting system security				
ı	+	4	Compromising security contro	ls			
Į.	-			· ·			
40.0		0.050	004470040000070	44:00:45	44.00.05	04.00	00.47
13 S		6.250	281473913980676	14:06:45	14:08:05	01:20	80.17
	is a	defined	way to breach the security of a	n IT system through vulnerability	/.		
		1	Hack Value				
l	+	2	Exploit				
ŀ		3	Target of Evaluation				
-							
Į		4	Vulnerability				
14 S		6.250	281473913980676	14:08:06	14:09:23	01:17	76.978
	is th	e proces		ation as possible about a target	network for identifying variou	is ways to intrude into an	organization's network
		-	so or concerning as macin informa	ation as possible about a target	network, for identifying various	33 ways to intrude into an	organization s network
}	system		Coonning				
ļ		1	Scanning				
	+	2	Footprinting				
Ī		3	Maintaining Access				
İ		4	Gaining Access				
Į	L	' '	, .30000				
					1		
15 S		6.250	281473913980676	14:09:23	14:12:02	02:39	158.34
	Hayde	n is the	network security administrator f	for her company, a large finance	e firm based in Miami. Hayde	n just returned from a sec	urity conference in Las
	Vegas	where t	ney talked about all kinds of old	and new security threats; many	of which she did not know of	of. Hayden is worried about	ut the current security
	state o	f her co	mpany's network so she decide	es to start scanning the network	from an external IP address.	To see how some of the	hosts on her network
	ı			nge. A number of IPs responds			
			•	on. She does this to see how her	· ·		
			•		intrasion detection system v	in log the tidillo.	
ļ	vvnat t	1	can is Hayden attempting here				
		1		ve hosts on her company's netw			
	+	2	Hayden is using a half-open s	can (stealth scan) to find live ho	sts on her network		
İ		3		ind live hosts that are listening of			
ŀ		4	The type of scan, she is using	<u> </u>			
Į		L 4	The type of Scart, site is using	is called a NULL SCAII			
				1			
16 S		6.250	281473913980676	14:12:02	14:12:36	00:34	33.752
	or c	racker is	one who accesses a computer	r system by evading its security	system.		
ł		1	Administrator	, , ,	-		
-	-						
		2	Trader				
	+	3	Hacker				
		4	User				
L		•					



Target of Evaluation



test: (Reg Ganjil 2017-2018) EH1-A: Kuis-01 (Reg Ganjil 2017-2018) EH1-A: Kuis-01 surname: 1572030 ANDIKA MULYAWAN DWI PR name: 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 (0%) correct: wrong: (0%) unanswered: (0%) (0%) undisplayed: points: 87.500 / 100.000 (88%) - PASSED start [hh:mm:ss] end [hh:mm:ss] time [mm:ss] points 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? Enumeration 1 2 Social Engineering System Hacking 3 4 Scanning 2 S 281473913980685 6 250 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? 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 An understanding of the number of employees in the company 4 3 S 281473913980685 13:36:58 13:58:47 21:49 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? 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 Hayden is attempting to find live hosts on her company's network by using an XMAS scan The type of scan, she is using is called a NULL scan 4 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 Footprinting 2 Maintaining Access Scanning 3 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. Social Engineering 2 Traceroute 3 DNS records request 4 Port scanning 281473913980685 6 S 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. Ping 2 Traceroute 3 WHOIS DNS query 281473913980685 13:42:08 00:31 30.222 7 S 6.250 13:41:37 is a defined way to breach the security of an IT system through vulnerability. Exploit





	_//						
		3	Vulnerability				
		4	Hack Value				
		1					
8 S		6.250	281473913980685	I	14:04:43	22:35	78.502
	Ann w	ould like	to perform a reliable scan aga	ainst a remote target. She is not	concerned about being stealth	at this point.	
	Mhigh	of the fe	llowing type of econe would b	e the most accurate and reliable	a antion?		
	VVIIICII	1	A FIN scan	e the most accurate and reliable	e option?		
		2	A half-scan				
		3	A UDP scan				
	+	4	A TCP Connect scan				
9 S		0.000	281473913980685		14:07:27	24:01	163.542
	Which			considered as passive footprint			
	-	2	Perform multiples queries us	as Yahoo Financial to identify a	assets.		
		3		s found in the target DNS datab	ase		
		4		nd out any information that might			
		1	<u> </u>	, ,			
10 S		6.250	281473913980685	13:44:38	13:44:57	00:19	12.274
	An eth	ical hac	·	owledge, network knowledge, c	omputer expert, security knowle	edge, and	
		1	books to gain knowledge				
	+	2	technical knowledge skills massive field experience				
		3	massive field experience money to build infrastructure				
		4	money to build infrastructure	•			
11 S		6.250	281473913980685	13:44:57	13:46:44	01:47	106.464
	Sandra			t network on which she is doing			
			ort 139 and 445.	C	•		·
	What p		is most likely to be listening or	n those ports?			
	+	1	SMB				
		3	FTP DNS				
		4	Finger				
		-	i iligei				
12 S		6.250	281473913980685	13:46:44	13:47:17	00:33	32.686
	This m	ethod is	used to determine the Opera	ting system and version running	on a remote target system.		
	What i	s it calle					
		1	Manual Target System				
		3	Identification Scanning Service Degradation				
	+	4	OS Fingerprinting				
	'	7	OO I Ingerprinting				
13 S		6.250	281473913980685	13:47:17	14:11:55	24:38	132.267
	This ty	pe of Po	ort Scanning technique splits 1	TCP header into several packets	s so that the packet filters are no	ot 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
140	Ethica			chniques, and to identify vulne			20.001
	+	1	Use of hacking tools			- >	
		2	Computer				
		3	Rules				
		4	Document				
				T			1
15 S	T	6.250	281473913980685		13:48:39	00:41	40.593
	inese		Elements of Information Secu	iniy, except			
		2	Availability Authenticity				
	<u> </u>	3	Integrity				
	+	4	Vulnerability				
16 S		6.250	281473913980685	13:48:39	13:49:28	00:49	48.538
	Hackir	ng refers	to and exploiting system vi	ulnerabilities to gain unauthorize	ed or inappropiate access to the	system resources.	·
	+	1	Compromising security contr		·	<u> </u>	
		2	Implementing new technolog	jies			
		3	Updating operating system				
		4	Protecting system security				





surname: 1572025

name: YOGI KOSIM SINDUDIBROT

user: 1572025

time: 00:35:00

start time: 2017-10-05 14:16:29 end time: 2017-10-05 14:51:29

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 192.168.1.102

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-monitor	oring and managing hosts, route	ers, and other devices on a netw	ork.	
		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 st	upidity	·	·		

0.0		0.000	2014/001000002	17.22.00	17.20.07	02.20	140.001			
	Active	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	\targeti	pc\$ "" /u:""						
	-	1	Connecting to a Linux computer	er through Samba					
		2	Grabbing the etc/passwd file						
		3	This command is used to conn	ect as a null session					
		4	Grabbing the SAM						

5 S	02:08	127.498						
	is pa	assive o	nline attack activity.					
	+ 1 Access and record the raw network traffic							
	2 Generate all possible hashes and compare with the databases values							





	_//	,							DAMAD
		3	Try all nos	ssible passwords					
		4		ent passwords from a l	ist				
	ı	-	i amore	passiroids iroili a i					
6 S		5.000		281473913980692	14:30:19	14:31:26	0	1:07	66.901
	What p				prevent NetBIOS traffic from				
		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	0	3:13	193.484
					s and an internal Intranet prot	ected by a firewall.			
	Which	techniq		protect against DNS	enumeration?				
		1		DNS zone transfers.					
	+	2		A records for internal h					
		3		invalid email received	via SMTP.				
		4	Enable nu	Ill session pipes.					
	1	=				1,050			T 40.000
8 S		5.000		281473913980692	14:34:41	14:35:01	0	0:20	19.828
	is de		to synchror MIB	nize clocks of network	eu computers.				
		2	LDAP						
		3	SNMP						
	+	4	NTP						
	+	4	INIF						
9 S		5.000		281473913980692	14:35:03	14:35:32	0	0:29	28.566
93	\/\hich			password to crack?	14.55.05	14.55.52	0	0.29	20.300
	VVIIICII	1	758904	password to crack:					
	+	2	Ukm1234	5*					
	т	3	password						
		4	HIJKLMN						
		-	THORLIVIA	0					
10 S	l	5.000		281473913980692	14:35:33	14:37:52	0	2:19	138.244
10.5	is hv		ack activity.		14.55.55	14.37.32	0	2.13	130.244
	10 119	1		ssible passwords					
		2		ent passwords from a l	iet				
	+	3		the dictionary and inse					
	-	4			nd compare with the database	s values			
					,				
11 S		5.000	2	281473913980692	14:37:52	14:39:01	0	1:09	68.439
	Attacke	ers use	the specific	port with telnet to enu	merates the running on the				,-L
		1	OS versio	n					
		2	IDS						
	+	3	server ver	sion					
		4	firewall						
		•	•						
12 S		5.000	2	281473913980692	14:39:02	14:39:39	0	0:37	37.05
	is a t	techniqu	ue to recove	er password protected	files, it use machines across	the network to decrypt passy	words.		
	+	1	Distribute	d Network Attack					
		2	Distributed	d Denial of Service					
		3	Online Att						
		4	Offline Att	ack					
13 S		5.000		281473913980692	14:39:41	14:41:43	0	2:02	122.175
	is pr			s attack activity.					
		1		ssible passwords					
		2		ent passwords from a l					
		3		the dictionary and inse					
	+	4	Generate	all possible hashes ar	nd compare with the database	s values			
						1			
14 S		5.000		281473913980692	14:41:44	14:42:24		0:40	39.862
	is de				ames, machine names, netwo	ork resources, snares, and se	ervices from a	system.	
		1	Covering						
		2	Escalating						
		3	Reconnais						
	+	4	Enumerat	ion					
45.0	1	F 000		204 4700 4000 200	44.40.07	11.10.10	-	0.40	47.00-
15 S		5.000		281473913980692	14:42:24	14:43:12	0	0:48	47.067
	requ			of network bandwidth					
		1	Offline att						
	+	2	Active onl	ine attacks					





	_							
		3	Non-electronic attac	cks				
		4	Passive online attac	cks				
		•						
16 S		5.000	281473913	3980692	14:43:12	14:44:34	01:22	81.625
	is a	term de	scribing a non-admin	user account the	at can gain administrat	or privilege.		
		1	Password cracking					
	+	2	Privilege escalation					
		3	Password sniffing					
		4	Hash dumping					
17 S		5.000	281473913		14:44:35	14:47:30	02:55	174.615
	is a	comma		to crack both Ur	ix/Linux and NT/Windo	ows passwords.		
	+	1	John the Ripper					
		2	SET					
		3	Cain & Abel					
		4	L0phtcrack					
							-	•
18 S		5.000	281473913		14:47:31	14:48:00	00:29	29.828
	are	, ''	of password attacks.					
		1	Active online attack					
		2	Non-electronic attac	-				
		3	Passive online attac	cks				
	+	4	Automatic attacks					
								T
19 S		5.000	281473913		14:48:01	14:48:45	00:44	43.508
			es service to gathe	r information suc	n as valid user names	, addresses, departmental details	, etc, that can be further	used to perform
	attack	s. 1	NTP					
		2	MIB					
		3	SNMP					
	+	4	LDAP					
		Т Т	LD/II					
20 S	1	5.000	28147391;	3980692	14:48:46	14:49:09	00:23	23.219
	is a					ects that can be managed using S		20.210
	+	1	MIB					
		2	SNMP					
		3	LDAP					
		4	NTP					
		<u> </u>	1					





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

MIB

LDAP NTP

2

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

#	poi	nts	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec
1 S	5.0		281473913980685		15:00:58	44:37	43.244
	is a TCP	/IP pr	otocol used for remote-mor	nitoring and managing hosts, ro	uters, and other devices on a net	work.	
	1		_DAP				
	2	_	MIB				
	3	_	NTP				
	+ 4	1 5	SNMP				
			T	T	T		T
2 S			281473913980685	14:17:53	14:19:04	01:11	70.924
			ine attack activity.				
			Try all possible passwords	- t d. t #:-			
	+ 2		Access and record the raw r				
	3		Try different passwords from				
		1 1	senerate all possible nasne	s and compare with the databa	ses values		
3 S	5.0	00	281473913980685	14:19:04	14:21:39	02:35	154.605
			ed hashes attack activity.	. 1.10.01		02.00	.01.000
	io più de		Try all possible passwords				
		_	Start with the dictionary and	insert entropy			
	+ 3			s and compare with the databa	ses values		
	4	_	Try different passwords from				
			•				
4 S	5.0	00	281473913980685	14:21:39	14:22:03	00:24	23.522
	is a virtu	al dat	abase containing formal de	scription of all the network obje	cts that can be managed using S	NMP.	•
	1	L	_DAP				
	2	2 5	SNMP				
	+ 3	3 [MIB				
	4	1	NTP				
							•
5 S			281473913980685		14:24:59	02:56	176.348
	is a com		-	both Unix/Linux and NT/Windo	ws passwords.		
	+ 1		John the Ripper				
	2		Cain & Abel				
	3		SET				
		ļ L	_Ophtcrack				
				1	1,000	24.25	
6 S	5.0		281473913980685		14:26:24	01:25	85.035
			Online Attack	cted files, it use machines acros	ss the network to decrypt passwo	ius.	
		_					
	+ 2		Distributed Network Attack				
	3		Offline Attack Distributed Denial of Service	<u> </u>			
		+ L	Distributed Definal Of Service	7			
7 S	5.0	00	281473913980685	14:26:24	14:26:48	00:24	24.223
				enumerates the running on t		UU.27	27.220
	/ titacitors t		OS version	Oracoo and an running off t			
	+ 2		server version				
	3		DS				
			irewall				
			*				
8 S	5.0	00	281473913980685	14:26:48	14:27:08	00:20	19.828
							used to perform





		4	SNMP							
9 S		5.000	281473913980685	14:27:08	14:28:07	00:59	58.296			
	are	1	of password attacks.							
		1	Non-electronic attacks							
	+	2	Automatic attacks							
-		3	Passive online attacks Active online attacks							
L		1 -	Notive offine attacks							
) S		0.000	281473913980685	14:28:07	14:57:13	29:06	89.231			
_	A com	pany ha	s publicly hosted web application				1			
Ľ	Which	techniq	ue will help protect against DNS	enumeration?						
	-	1	Enable null session pipes.							
-		2	Allow full DNS zone transfers.	1						
-		3	Remove A records for internal							
L		4	Reject all invalid email receive	u via Sivi i F.						
s		5.000	281473913980685	14:30:04	14:55:43	25:39	89.82			
_	What p				not coming through the firewall i					
Ŀ	2000,	and XP?				· .				
		1	445, 447							
		2	161, 163							
-	+	3	137, 139							
L		4	193, 195							
2 S		5.000	281473913980685	14:32:15	14:54:14	21:59	217.805			
_	Look a		owing output. What did the hac		14.54.14	21.00	217.000			
			P1 <<>> axfr domain.com @1							
	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. 3600 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)									
L		1	The hacker listed DNS records							
L		2	ŭ	ner publicly available records fo						
	+	3		ool to brute force the list of avai						
L		4	The nacker successfully transf	ered the zone and enumerated	trie nosts.					
s		5.000	281473913980685	14:33:03	14:50:36	17:33	86.311			
	and		LM Hashes are offline attack m		1 1.50.50	11.00	1 30.011			
T		1	Use poor passwords	~						
	+	2	Use good passwords							
		3	Use secure connection							
		4	Use firewall							
I S		5.000	281473913980685	14:33:46	14:34:48	01:02	62.602			
Ľ	Try dif		asswords until one works are ac	tivities of						
-		1	Offline attacks							
H	+	2	Active online attacks Passive online attacks							
+		3	Non-electronic attacks							
L		1 4	11011 GIGGLIGHIG ALLACES							
s		0.000	281473913980685	14:34:48	14:48:39	13:51	164.317			
	is a				ation time of password cracking					
Γ		1	Moore's law		. · ·					
		2	Einstein's law							





	_						EIP CONS. CO			
		3	Calculation law							
	-	4	Progressive law							
16 S		5.000	281473913980685	14:36:33	14:37:10	00:37	37.013			
,	is de	signed	to synchronize clocks of netwo	rked 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 de	fined as		names, machine names, netw	ork resources, shares, and ser	vices from a system.				
		1	Covering Track							
		2	Escalating Privilege							
		3	Reconnaissance							
	+	4	Enumeration							
			1		1					
18 S		0.000								
			Illowing command used for?							
	net use	target	tipe\$ "" /u:""							
		2	Grabbing the SAM Grabbing the etc/passwd file							
	-	3	Connecting to a Linux compu	tor through Samba						
		4	This command is used to con							
		4	This command is used to con	nect as a riuii session						
19 S		5.000	281473913980685	14:39:52	14:41:16	01:24	84.556			
100	Active			tem that has bad passwords ar	I .	01.21	01.000			
	7101170	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 br	ute-forc	e attack activity.	•	•	·				
		1	Try different passwords from	a list						
	+	2	Try all possible passwords							
		3	Start with the dictionary and in	nsert entropy						

4 Generate all possible hashes and compare with the databases values



SNMP



test: (Reg Ganjil 2017-2018) EH1: UTS (Reg Ganjil 2017-2018) EH1: UTS surname: 1572025 YOGI KOSIM SINDUDIBROT name: 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%) (0%) undisplayed: points: 76.250 / 100.000 (76%) # points 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? Scan the range of IP address found in the target DNS database. Perform multiples queries using a search engine. 3 Search on financial site such as Yahoo Financial to identify assets. Go through the rubbish to find out any information that might have been discarded. 281473913981968 16:09:09 2 S 0.000 16:10:01 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? Footprinting Escalating privileges Network mapping 3 4 Gaining access 281473913981968 0.000 17:43:52 33:51 20.94 3 S 16:10:01 What is the following command used for? net use \targetipc\$ "" /u:"" This command is used to connect as a null session Grabbing the etc/passwd file Grabbing the SAM 4 Connecting to a Linux computer through Samba 281473913981968 4 S 16:10:46 16:13:23 02:37 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? ACK flag scanning SYN flag scanning 2 RST flag scanning 3 FIN flag scanning 5 S 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 Exploit 2 Hack Value 3 Vulnerability Target of Evaluation 4 6 S 1.250 281473913981968 16:15:23 16:18:26 03:03 183.055 These are non-technical password cracking attacks, except .. Keyboard sniffing 2 Phishing attack Shoulder surfing 3 Social engineering 4 281473913981968 16:20:03 7 S 16:18:27 01:36 96.019 ... is a command-line tool designed to crack both Unix/Linux and NT/Windows passwords. Cain & Abel L0phtcrack 3 SET John the Ripper 4 281473913981968 8 S 1.250 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.





			53 7 WHS
	2	LDAP	
	3	MIB	
	4	NTP	
	1 -	TWO	
9 S	1.250	281473913981968 16:24:23 16:25:07 00:44 44	1.002
		ring competitive intelligence on XYZ.com. You notice that they have jobs listed on a few Internet job-hunting sites. There are two	
I	0	and system administrators.	Job bostii
loi ne	iwork an	u system auministrators.	
How	can thic h	help you in footprint the organization?	
11000	1	How strong the corporate security policy is	
	2	The types of operating systems and applications being used.	
+		71 1 0 7 11	
	3	An understanding of the number of employees in the company	
	4	The IP range used by the target network	
1			
0 S	1.250		5.924
is a		way to breach the security of an IT system through vulnerability.	
	1	Target of Evaluation	
	2	Hack Value	
	3	Vulnerability	
+	4	Exploit	
1 S	2.500	281473913981968 16:27:26 16:31:18 03:52 23:	1.593
	VOII STA	getting information about a web server, it is very important to know the HTTP Methods (GET, POST, HEAD, PUT, DELETE, TRA	
are av	vailable t	pecause there are two critical methods (PUT and DELETE). PUT can upload a file to the server and DELETE can delete a file from	n the
serve	r. You ca	an detect all these methods (GET, POST, HEAD, PUT, DELETE, TRACE) using NMAP script engine.	
What	NMAP s	cript will help you with this task?	
	1	http enum	
	2	http-headers	
-	_	1	
	3	http-git	
+	4	http-methods	
S	1.250	281473913981968 16:31:18 16:31:55 00:37 36	6.619
An et	hical hac	ker 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	
S	1.250	281473913981968 16:31:56 16:32:46 00:50 49	9.661
You a	re footpr	rinting an organization and gathering competitive intelligence. You visit the company's website for contact information and telepho	ne numl
		I 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	
S	1.250	281473913981968 16:32:46 16:33:29 00:43 43	3.252
is a	virtual c	database containing formal description of all the network objects that can be managed using SNMP.	
	1	SNMP	
	2	NTP	
		MIB	
+	3		
	4	LDAP	
S	2.500	281473913981968 16:33:30 16:33:47 00:17 16	6.787
Craig	received	a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software ge	nerated
report			
	1	A port scanner	
	2	A virus scanner	
-	3	A malware scanner	
+	4	A vulnerability scanner	
O I	2.500	281473913981968 16:33:48 16:35:27 01:39 99	9.731
5	canning	can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify lister	ning por
	•	d system. If a scanned port is open, what happens?	
Port s		The port will send an RST	
Port s	1 1	The port will ignore the packets	
Port s		I THE POIL WIII IGHOLE (HE PROVEIS	
Port s	2		
Port s	3	The port will send a SYN	
on the	2		
Port s on the	3	The port will send a SYN	
Port s	3	The port will send a SYN The port will send an ACK	3.418
Port s on the	2 3 4 1.250	The port will send a SYN The port will send an ACK	3.418





+							回数线制度
	2	Privilege escalation					
	3	Password cracking					
	4	Password sniffing					
3 S	1.250	28147391398196		6:37:12	16:39:08	01:56	115.815
This ty	-	ort Scanning technique splits UDP Scanning	ICP header into	o several packets :	so that the packet filters are r	ot able to detect what th	e packets intends to d
-	1 2	ACK flag scanning					
+	3	IP Fragment Scanning					
т	4	Inverse TCP flag scanning					
	·	interes is may seaming					
9 S	2.500	28147391398196	8 10	6:39:08	16:42:19	03:11	190.676
How c	an rainb	ow tables be defeated?					•
+	1	Password salting					
	2	Use of non-dictionary word					
	3	Lockout accounts under br		ord cracking attem	pts		
	4	All uppercase character pa	sswords				
) S	1.250	28147391398196	Q 10	6:42:20	16:43:09	00:49	49.332
		to synchronize clocks of net			10.45.05	00.49	49.002
	1	MIB	puto				
+	2	NTP					
	3	SNMP					
	4	LDAP					
S	0.000	28147391398196		6:43:10	16:45:04	01:54	113.475
You w		an ICMP scan on a remote		hping2. What is th	ne proper syntax?		
	1	hping2 -1 host.domain.com					
-	3	hping2set-ICMP host.do hping2 -i host.domain.com					
_	4	hping2 -i nost.domain.com					
-	4	ripingz nost.domain.com					
: S	2.500	28147391398196	8 1	6:45:04	16:46:55	01:51	110.5
	3	Enumeration Escalation					
	7	Localation					
3 S	2.500	28147391398196	8 10	6:46:55	16:49:59	03:04	184.054
Which	tool allo		to examine links	s between data usi	ing graphs and link analysis?		
	1	Metasploit					
	2						
+	_	Maltego					
+	3	Wireshark					
+	_						
	3 4	Wireshark Cain & Abel	8 16	6:50:00	16:52:50	02:50	169 908
IS	3 4 1.250	Wireshark Cain & Abel 28147391398196		6:50:00 any, a large finance	16:52:50 e firm based in Miami. Haydei	02:50	169.908 curity conference in La
I S Hayde	3 4 1.250 en is the	Wireshark Cain & Abel 28147391398196 network security administrat	tor for her compa	any, a large finance		n just returned from a sec	curity conference in La
Hayde Vegas state o	3 4 1.250 en is the s where to find the co	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec	tor for her compa fold and new sec cides to start scar	any, a large finance curity threats; many nning the network	e firm based in Miami. Haydel y of which she did not know o from an external IP address.	n just returned from a sec of. Hayden is worried abo To see how some of the	curity conference in La out the current security hosts on her network
Hayde Vegas state of react,	1.250 en is the swhere to of her coshe sen	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP	tor for her compa fold and new sec cides to start scar range. A numbe	any, a large finance curity threats; man nning the network er of IPs responds	e firm based in Miami. Hayde y of which she did not know o from an external IP address. with a SYN/ACK response. B	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
Hayde Vegas state of react, RST p	1.250 en is the s where to she sen backets t	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP o those hosts to stop the ses	for her compa fold and new sec cides to start scar for range. A numbe ssion. She does t	any, a large finance curity threats; man nning the network er of IPs responds	e firm based in Miami. Haydel y of which she did not know o from an external IP address.	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
S Hayde Vegas state of react, RST p	1.250 en is the s where to she sen backets t	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does t ere?	any, a large finance curity threats; many nning the network er of IPs responds this to see how he	e firm based in Miami. Hayder y of which she did not know o from an external IP address. with a SYN/ACK response. B r intrusion detection system v	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
S Hayde Vegas state of react, RST p	1.250 en is the swhere to the sen backets to type of sen	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP to those hosts to stop the sec can is Hayden attempting he	tor for her compa f old and new sec cides to start scar range. A numbe ssion. She does t ere? to find live hosts	any, a large finance curity threats; many nning the network er of IPs responds this to see how he that are listening of	e firm based in Miami. Hayder y of which she did not know o from an external IP address. with a SYN/ACK response. B r intrusion detection system v	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
Hayde Vegas state of react, RST p	1.250 en is the s where to she sen backets to type of s	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she de ds out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope	tor for her compaint of the compaint of the control	any, a large finance curity threats; many nning the network er of IPs responds this to see how he that are listening of ULL scan scan) to find live ho	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system von her network	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
Hayde Vegas state of react, RST p What the	1.250 en is the s where to f her co she sen packets to type of s	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she de ds out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope	tor for her compaint of the compaint of the control	any, a large finance curity threats; many nning the network er of IPs responds this to see how he that are listening of ULL scan scan) to find live ho	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system von her network	n just returned from a sec of. Hayden is worried abo To see how some of the efore the connection is e	curity conference in La out the current security hosts on her network
Hayde Vegas state of react, RST p What if	1.250 en is the swhere to the consumer of her consumer of the	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP of those hosts to stop the ses can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin	tor for her compain fold and new sectides to start scare range. A number ssion. She does there? It of find live hosts sing is called a Number scan (stealth start son here.)	any, a large finance curity threats; many nning the network er of IPs responds: this to see how he that are listening of ULL scan scan) to find live ho ter company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network losts on her network work by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is e vill log the traffic.	curity conference in La but the current security hosts on her network established she sends
S Hayde Vegas state of react, RST p What if	1.250 en is the s where to finer co she sen oackets to type of s 1.250 1.250	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she de ds out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin	tor for her compa f old and new sec cides to start scar P range. A numbe sssion. She does t ere? to find live hosts sing is called a Number scan (stealth sind live hosts on her	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La out the current security hosts on her network
Hayde Vegas state of react, RST p What if	1.250 en is the s where to finer co she sen oackets to type of s 1.250 1.250 1.250 1.250 1.250 1.250 1.250	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system	tor for her compa fold and new sec cides to start scar Prange. A numbe ssion. She does t ere? to find live hosts sing is called a NU en scan (stealth sind live hosts on her vulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network losts on her network work by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
Hayde Vegas state of react, RST p What if	1.250 en is the s where to fher co she sen packets t type of s 1 2 3 4 1.250 ng refers 1	Wireshark Cain & Abel 28147391398196 network security administrathey talked about all kinds of mpany's network so she ded so ut SYN packets to an IP or those hosts to stop the secan is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security	tor for her compa fold and new sec cides to start scar Prange. A numbe ssion. She does tere? to find live hosts sing is called a Nt en scan (stealth sind live hosts on her wulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
Hayde Vegas state of react, RST p What is the state of th	1.250 en is the s where to fine co she sen packets t type of s 1 2 3 4 1.250 en grefers 1 2	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP to those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system	tor for her compa fold and new sec cides to start scar Prange. A numbe ssion. She does tere? to find live hosts sing is called a Nt en scan (stealth sind live hosts on ho	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
Hayde Vegas state of react, RST p What if	3 4 1.250 en is the s where to for her co she sen backets to type of s 1 2 3 4 1.250 ng refers 1 2 3 4	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP to those hosts to stop the secan is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does tere? to find live hosts sing is called a Nt en scan (stealth sind live hosts on ho wulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
S Hayde Vegas state of react, RST p What is +	1.250 en is the s where to fine co she sen packets t type of s 1 2 3 4 1.250 en grefers 1 2	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP to those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does tere? to find live hosts sing is called a Nt en scan (stealth sind live hosts on ho wulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
Hayde Vegas state c react, RST p What t	3 4 1.250 en is the s where to for her co she sen backets to type of s 1 2 3 4 1.250 ng refers 1 2 3 4	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded ds out SYN packets to an IP to those hosts to stop the secan is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does t ere? to find live hosts sing is called a Nt en scan (stealth s d live hosts on he vulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live ho her company's network	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network vork by using an XMAS scan	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic.	curity conference in La but the current security hosts on her network established she sends
Hayde Vegas state correact, RST p What the Hacking Hac	3 4 1.250 en is the s where to for her coshe sen vackets to type of s 1 2 3 4 1.250 ng refers 1 2 3 4 0.000	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP to those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor Implementing new technole	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does tere? to find live hosts sing is called a Nt en scan (stealth so d live hosts on he vulnerabilities to	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live hower company's network of 52:51 or gain unauthorized 6:53:33	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network work by using an XMAS scan 16:53:32 d or inappropiate access to th	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic. 00:41 e system resources.	curity conference in La but the current security hosts on her network established she sends 41.484
Hayde Vegas state of react, RST p What the state of the s	3 4 1.250 en is the s where to for her cosen she sen sackets to type of s 1 2 3 4 1.250 ng refers 1 2 3 4 0.000 ch phase	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she dec ds out SYN packets to an IP to those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor Implementing new technole	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does t ere? to find live hosts sing is called a NU en scan (stealth si d live hosts on he vulnerabilities to n hitrols ogies 10 ess can Google P	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live hower company's network of 52:51 or gain unauthorized 6:53:33	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network work by using an XMAS scan 16:53:32 d or inappropiate access to th	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic. 00:41 e system resources.	curity conference in La but the current security hosts on her network established she sends 41.484
Hayde Vegas state of react, RST p What is the control of the contr	3 4 1.250 en is the s where to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she r	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded do out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor Implementing new technole 28147391398196 of the ethical hacking proces	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does t ere? to find live hosts sing is called a NU en scan (stealth si d live hosts on he vulnerabilities to n hitrols ogies 10 ess can Google P	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live hower company's network of 52:51 or gain unauthorized 6:53:33	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network work by using an XMAS scan 16:53:32 d or inappropiate access to th	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic. 00:41 e system resources.	curity conference in La but the current security hosts on her network established she sends 41.484
Hayde Vegas state coreact, RST p What the Hacking Hack	3 4 1.250 en is the s where to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she sen observed to the room she r	Wireshark Cain & Abel 28147391398196 network security administrat hey talked about all kinds of mpany's network so she ded do out SYN packets to an IP of those hosts to stop the sec can is Hayden attempting he She is utilizing a FIN scan The type of scan, she is us Hayden is using a half-ope Hayden is attempting to fin 28147391398196 to and exploiting system Protecting system security Updating operating system Compromising security cor Implementing new technole 28147391398196 of the ethical hacking proces	tor for her compa f old and new sec cides to start scar P range. A numbe ssion. She does t ere? to find live hosts sing is called a NU en scan (stealth si d live hosts on he vulnerabilities to n hitrols ogies 10 ess can Google P	any, a large finance curity threats; many nning the network er of IPs responds this to see how her that are listening of ULL scan scan) to find live hower company's network of 52:51 or gain unauthorized 6:53:33	e firm based in Miami. Hayder y of which she did not know of from an external IP address. with a SYN/ACK response. B r intrusion detection system v on her network work by using an XMAS scan 16:53:32 d or inappropiate access to th	n just returned from a set of. Hayden is worried about To see how some of the efore the connection is exill log the traffic. 00:41 e system resources.	curity conference in La but the current security hosts on her network established she sends 41.484





		1	Gaining A	loness				
		2	Reconnai					
		3	Maintaini	ng Access				
	-	4	Scanning	and Enumeration				
27 S		nent des	Ethical Had		16:55:37 ted by a private firm to conduct, the associated violations, and			
	1001011	1	Non-Disc	losure Agreement				
		2	-	evel Agreement				
		3	Project S					
	+	4	Terms of	Engagement				
28 S		0.000		281473913981968	16:58:49	16:59:52	01:03	62.619
200	What i			wing command?	10.00.40	10.00.02	01.00	02.013
				192.168.100.3				
		1			ating system, and scanning por	rts 123 to 153		
	-	2		scan, checking open p				
		3			n ports excluding ports 123 to	153		
		4	A stealth	scan, opening port 12	3 and 153			
29 S		1.250		281473913981968	16:59:53	17:00:23	00:30	29.945
230	Attack				n such as valid user names, ac			
	attack	•						
		1	MIB					
	+	2	LDAP					
		3	NTP					
		4	SNMP					
30 S		2.500		281473913981968	17:00:23	17:04:41	04:18	257.695
30 3	Whati				e layers of security controls to	-		
					alicious attacks or potential vul			
	+	1	Defense					
		2		Based Intrusion Detec	•			
		3		ed Intrusion Detection	System			
		4	Security t	hrough obscurity				
31 S		0.000		281473913981968	17:04:42	17:05:09	00:27	27.458
310	After to							
		1	nultiple exploits, you've gained root access to a Centos 6 server. To ensure you maintain access, what would you do first? Download and Install Netcat					
		2		(ey Services				
	-	3		ser Account				
		4	Disable II	PTables				
22.6		1.250		281473913981968	17:05:10	17:06:59	01:40	100 204
32 S	What r				prevent NetBIOS traffic from r		01:49	109.384
		and XP		ched on the mewan to	prevent recibioo traine nom	iot coming unough the mewa	ii ii your network is comprie	ca or windows ivi,
		1	445, 447					
		2	193, 195					
	+	3	137, 139					
		4	161, 163					
22.0		1.050		201 172012001060	47,07,00	47,07,20	00:27	26.906
33 S	is th	1.250 ne proce		281473913981968 eting as much informat	17:07:03 ion as possible about a target	17:07:30	00:27	
	systen		00 01 001100	ang ao maon imormat	ion do poddibio about a targot	notwork, for lacitalying variou	o wayo to mirado mio am o	gamzation o notwon
		1	Gaining A	Access				
		2	Scanning					
	+	3	Footprinti	-				
		4	Maintaini	ng Access				
24.0		2.500		201 172012001060	47,07,20	47,00,EE	02:25	11110
34 S	What i	2.500		281473913981968	17:07:30 resolving events that take place	17:09:55	02:25	144.49
	vviiati	1	Security I		Coording Cyclina that take place	o an organization!		
		2	Internal P					
	+	3		Management Process				
		4	Metrics					
					<u> </u>			
35 S	D:	2.500		281473913981968	17:09:55	17:11:27	01:32	91.373
					empetitor company. To secure curity through obscurity'.	tnese messages, he uses a t	ecnnique of hiding a secret	message within an
	Joidina	19 111633	uge. Hie li	John Inque provides Sec	any iniough obscurity.			
	What t	techniqu	e is Ricard	o using?				





//									
		1	Encryption						
		2	RSA algorithm	n					
	+	3	Steganograph	•					
		4	Public-key cry	yptography					
36 S		1.250	201	473913981968	17:11:28	17:12:29		01:01	61.172
30 3	These			formation Securit		17.12.29		01.01	01.172
	111000	1	Integrity	Torridation Coount	у, олоорт				
		2	Authenticity						
	+	3	Vulnerability						
		4	Availability						
			1 224	·=	47.40.00	17.10.01			
37 S	Attack	1.250		473913981968	17:12:29 numerates the running on the	17:13:01		00:32	31.28
	Allack	1	IDS	it with temet to en	idilierates the running on the	e remote nost.			
		2	firewall						
	+	3	server version	า					
		4	OS version						
			1						
38 S		1.250		473913981968	17:13:02	17:14:17		01:15	74.852
		is it calle		imie uie Operatin	ng system and version running	on a remote target system.			
		1	Identification	Scanning					
	+	2	OS Fingerprir	nting					
		3	Manual Targe					-	<u> </u>
		4	Service Degra	adation					
39 S		1.250	004	473913981968	17:14:18	17:17:14		02:56	176.844
39 5	Attack				on social networking websit		nace Link		
	rttack	1	Traceroute	ormation through	on social networking websit	es such as i accident, mye	pace, Eirii	team, rwitter, r int	creat, Google 1, etc.
	+	2	Social Engine	ering					
		3	Port scanning						
		4	DNS records	request					
			1						
40 S	Tho "w	2.500		473913981968	17:17:15	17:19:11		01:56	116.174
	THE V	1	ex testing" methodology enforces what kind of restriction? 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			a system is accessible to the te				
		4	Only the inter	nal operation of a	a system is known to the tester				
			1 224	·=	171010	17.10.00			10.000
41 S	Accord	1.250		473913981968	17:19:12 e next step to be performed aft	17:19:29	nco?	00:17	16.699
	+	1	Scanning	dology, what is the	e next step to be penormed an	er rootprinting/reconnaissa	nce :		
		2	System Hack	ina					
		3	Enumeration						
		4	Social Engine	ering					
			1						
42 S		1.250		473913981968	17:19:29	17:19:52		00:23	22.186
	is ai	n attack	Exploit Exploits	omputer application	on vulnerabilities before the sof	ware developer releases a	paich for	uie vuinerability.	
	+	2	Zero-Day Atta	ack					
		3	Target of Eva						
		4	Vulnerability						
			-						
43 S		1.250		473913981968	17:19:52	17:21:19	- 141 1 11 1	01:27	86.854
	Ann w	ouid like	to periorm a re	eliable scan agair	nst a remote target. She is not	concerned about being stea	aith at this	point.	
	Which	of the fo	ollowing type of	f scans would be	the most accurate and reliable	option?			
		1	A half-scan						
	+	2	A TCP Conne	ect scan					
		3	A UDP scan						
		4	A FIN scan						
44 S		1.250	201	473913981968	17:21:20	17:22:41		01:21	81.519
++ 3	Ethica				niques, and to identify vulne		stem seci		01.519
		1	Computer						
		2	Rules						
	+	3	Use of hackin	ig tools			_		
		4	Document						
45.0		0.000	001	470040004000	47:00 10	47.00.04	1	00.50	50.040
45 S	-	0.000	2814	473913981968	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?

V V	Hat is	Some try	ing 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 255.255.192. 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	.168.1.64/2	8						
	Why he ca	annot see th	ne 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								

	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 xxxxxxxx.

QUITTING!

What seems to be wrong?

	vviid	oomo to	bo mong.			
	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		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 a	These are offline attacks methods, except									
		1	Brute-force Attack								
		2	Dictionary Attack	Dictionary Attack							
		3	Hybrid Attack								
	+	4	Moore Attack								

49 S		0.000	281473913981968	17:29:04	17:30:01	00:57	57.113	
	Active o	nline a	tack majority succeeds on syst	em that has bad passwords and	d			
	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								

		1	Ping					
	+	2	WHOIS					
[3	DNS qu	iery				
[4	Tracero	oute				
•							•	
-40		0.000		004470040004000	47.00.00	47.04.40	04.00	00 777

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'						
		1	Traceroute to control the path	of the packets sent during the s	can		
	-	2	Fingerprinting to identify which	operating systems are running	on the network		
		3	Timing options to slow the spe	ed that the port scan is conduct	ed		
		4	ICMP ping sweep to determine	which hosts on the network are	e not available		
	•						

52 S	1.250	281473913981968	17:31:49	17:32:08	00:19	19.191
	or cracker is one wh	o accesses a computer	system by evading its security	system.		





	+	1	Hacker				
	•	2	Administrator				
		3	User				
		4	Trader				
		4	Trauer				
F2 C	ı	1.050	204 47204 2004 060	47.22.00	17:22:40	00:24	20.026
53 S		1.250	281473913981968	17:32:09	17:32:40	00:31	30.036
	prov		ortant information about locatio	on and type of servers.			
		1	Port lists				
	+	2	DNS records				
		3	OS version				
		4	Traceroute				
			1	1			
54 S		0.000	281473913981968	17:32:40	17:34:10	01:30	89.475
					unauthorized access, destruction	, disclosure, denial of	service or
	modific			erms 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 di	ctionary	attack activity.				
	+	1	Try different passwords from a	a list			
		2	Try all possible passwords				
		3	Generate all possible hashes	and compare with the database	s values		
		4	Start with the dictionary and in	•			
'			,				
56 S		1.250	281473913981968	17:36:31	17:38:58	02:27	147.617
	A com			ons and an internal Intranet prot		OL.L1	111.011
			ue will help protect against DNS		octod by a morrain.		
	· · · · · · · · · · · · · · · · · · ·	1	Allow full DNS zone transfers.				
		2	Enable null session pipes.	·			
	+	3	Remove A records for interna	I hooto			
	т .	4	Reject all invalid email receive				
		4	Reject all invalid email receive	eu via Sivi i F.			
F7.0	1	4.050	004 47004 0004 000	47:20:00	47:00:40	00:40	40.040
57 S	144 : 1	1.250	281473913981968	17:39:00	17:39:13	00:13	13.249
	vvnicn		ne 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	techniqu	ie to recover password protecti	ed 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 secu				are any deviations from the securi		
					curity policy must the security analy		
	allowe				, , , , , , , , , , , , , , , , , , ,	,	
	+	1	Acceptable-use policy				
		2	Remote-access policy				
		3	Firewall-management policy				
		4	Permissive policy				
	L	_ +	i citilissive policy				
60.0	l	1.050	201472042004000	47.44.45	17:40:04	00.36	25 427
60 S	Atta al-	1.250	281473913981968	17:41:45	17:42:21	00:36	35.437
	Апаск			out: network topology, trusted ro	outers, and irrewall locations.		
		1	Port scanning				
	+	2	Traceroute				
		3	Social Engineering				
		4	DNS records request				





test: (Reg Ganjil 2017-2018) EH1: UTS (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%) (0%) undisplayed: points: 67.500 / 100.000 (68%) # ΙP points start [hh:mm:ss] end [hh:mm:ss] time [mm:ss] reaction [sec] 1 S 0.000 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. IP Fragment Scanning Inverse TCP flag scanning 2 3 ACK flag scanning **UDP Scanning** 4 281473913981971 16:10:27 16:10:38 2 S 1.250 00:11 ... 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 Footprinting Maintaining Access Gaining Access 3 4 Scanning 3 S 281473913981971 36.856 1.250 16:10:38 16:11:15 00:37 .. is defined as the process of extracting user names, machine names, network resources, shares, and services from a system. Escalating Privilege 2 Reconnaissance 3 Covering Track Enumeration 4 4 S 281473913981971 17:58:13 16:11:15 46:58 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? FTP DNS 2 SMB 3 Finger 281473913981971 5 S 0.000 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? Wireshark 2 Metasploit Cain & Abel 3 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 A stealth scan, checking open ports 123 to 153 A stealth scan, checking all open ports excluding ports 123 to 153 3 A stealth scan, opening port 123 and 153 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 Hack Value 2 Target of Evaluation 3 Exploit Vulnerability 0.000 281473913981971 8 S 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? hping2 -i host.domain.com





		2	hning2 -1	1 host.domain.com				
		3		ost.domain.com				
	_	4		-set-ICMP host.domain	com			
	_		ripirigz	30t TOWN TIOSt.domain				
9 S		1.250		281473913981971	16:17:20	16:17:45	00:25	25.12
93						10.17.45	00.23	25.12
	IS U	1	MIB	onize clocks of network	ea computers.			
			LDAP					
		2						
		3	SNMP					
	+	4	NTP					
10.0	1					1 .===.		
10 S	 	1.250		281473913981971	16:17:45	17:55:24	37:39	5.806
				each the security of an	IT system through vulnerabil	iity.		
	+	1	Exploit					
		2	Hack Val					
		3		f Evaluation				
		4	Vulnerab	ility				
								1
11 S		1.250		281473913981971	16:18:43	17:55:18	36:35	90.69
			0	mmand used for?				
			ipc\$ "" /u:"					
	+	1		nmand is used to conne				
		2		ing to a Linux compute	r through Samba			
		3		g the etc/passwd file				
		4	Grabbing	g the SAM				
12 S		1.250		281473913981971	16:18:51	16:21:00	02:09	
					om sequence number, no res	sponse means port is filtere	d (Stateful firewall is	present) and RST response
	1		t is not filte					
	What	-		ning is this?				
		1		scanning				
	+	2		scanning				
		3	FIN flag					
		4	SYN flag	scanning				
						_		
13 S		1.250		281473913981971	16:21:00	16:22:57	01:57	
	is a	n attack			n vulnerabilities before the so	ofware developer releases a	a patch for the vulner	ability.
		1		f Evaluation				
	+	2	Zero-Day	y Attack				
		3	Exploit					
		4	Vulnerab	oility				
14 S		1.250			10.00.57	16:23:38		40.000
		re footor		281473913981971	16:22:57		00:41	
			inting an o	organization and gather	ring competitive intelligence.	You visit the company's we	bsite for contact infor	mation and telephone numbers
	but do		inting an o them liste	organization and gather ed there. You know they	ring competitive intelligence. y had the entire staff director	You visit the company's we y listed on their website 12	bsite for contact infor	mation and telephone numbers
		not find	inting an o them liste Visit the	organization and gather ad there. You know they company's partners an	ring competitive intelligence. y had the entire staff director id customers website for this	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers
	but do	not find 1 2	them liste Visit the	organization and gather ed there. You know they company's partners an hive.org web site to reti	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers
		not find	inting an o them liste Visit the Visit Arch Crawl the	organization and gather of there. You know they company's partners an hive.org web site to retile e entire website and store.	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers
		not find 1 2	inting an o them liste Visit the Visit Arch Crawl the	organization and gather of there. You know they company's partners an hive.org web site to retile e entire website and store.	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers
_		not find 1 2 3	inting an o them liste Visit the Visit Arch Crawl the	organization and gather of there. You know they company's partners an hive.org web site to retile e entire website and store.	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers
15 S	+	not find 1 2 3	them liste Visit the Visit Arch Crawl the Visit Goo	organization and gather of there. You know they company's partners an hive.org web site to retile e entire website and store.	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer	You visit the company's we y listed on their website 12 information	bsite for contact infor	mation and telephone numbers it is not there.
15 S	+	not find 1 2 3 4	inting an o them liste Visit the Visit Arch Crawl the Visit Goo	organization and gather of there. You know they company's partners an hive.org web site to retie e entire website and stoggle's search engine ar 281473913981971	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer and view the cached copy	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+	not find 1 2 3 4	inting an o them liste Visit the Visit Arch Crawl the Visit Goo	organization and gather of there. You know they company's partners an hive.org web site to retie e entire website and stoggle's search engine ar 281473913981971	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+	not find 1 2 3 4	inting an o them liste Visit the Visit Arch Crawl the Visit Goo	organization and gather and there. You know they company's partners an hive.org web site to retie entire website and stougle's search engine ar 281473913981971 extract information about ords request	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+ Attack	not find 1 2 3 4 1.250 eers conc	inting an o them liste Visit the Visit Arch Crawl the Visit Goo	organization and gather and there. You know they company's partners an hive.org web site to retie entire website and stopgle's search engine ar 281473913981971 extract information about the	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+ Attack	not find 1 2 3 4 1.250 ers cond 1 2	visit Archiviste Visit Archivist Good	organization and gather and there. You know they company's partners an hive.org web site to retie entire website and stopgle's search engine ar 281473913981971 extract information about the	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+ Attack	1.250 ers concers 2 3 3 4 3 3 4 3 3 4 3 3 4 3 3 3 3 3 3 3	visit Archiviste Visit Archivist Good	organization and gather and there. You know they company's partners an hive.org web site to retie entire website and stopgle's search engine ar 281473913981971 extract information about ords request ute	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
15 S	+ Attack	1.250 ers concers 2 3 3 4 3 3 4 3 3 4 3 3 4 3 3 3 3 3 3 3	inting an o them liste Visit the Visit Arct Crawl the Visit Goo Juct to e DNS rect Tracerou Port scar Social Er	organization and gather and there. You know they company's partners an hive.org web site to retie entire website and stopgle's search engine ar 281473913981971 extract information about ords request ute	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38	You visit the company's we y listed on their website 12 information the company's website	bsite for contact informonths ago but now	mation and telephone numbers it is not there.
	+ Attack	1.250 ers conce 1 2 3 4 4 2.500	inting an o them liste Visit the Visit Arct Crawl the Visit Goo Just to e DNS reco Tracerou Port scar Social Er	organization and gather and there. You know they company's partners and hive.org web site to retie entire website and strongle's search engine and 281473913981971 281473913981971 291979 281473913981971 281473913981971	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer ind view the cached copy 16:23:38 ut: network topology, trusted	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio	bsite for contact informonths ago but now 29:25 ns. 00:32	mation and telephone numbers it is not there. 49.4
	+ Attack + A com	1.250 ers conce 1 2 3 4 4 2.500 eputer sc	inting an o them liste Visit the Visit Arch Crawl the Visit Good Visit Good DNS reco Tracerou Port scar Social Er	organization and gather and the set there. You know they company's partners and hive.org web site to retire entire website and stopgle's search engine and 281473913981971 extract information about ords request utenning engineering 281473913981971 dent needs to fill some integration and the search and the	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application the	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer.
	+ Attack + A com	1.250 ers conc 1 2 2 3 4 4 2.500 puter sc d of requ	inting an o them liste Visit the Visit Arch Crawl the Visit Good U	organization and gather and the set there. You know they company's partners and hive.org web site to retie entire website and stopgle's search engine and 281473913981971 extract information abortords request ute nning engineering 281473913981971 dent needs to fill some inew document that allowed the set of	ring competitive intelligence. y had the entire staff director, id customers website for this rieve the Internet archive of t ore them into your computer and view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea	1.250 ers conc 1 2 3 4 2.500 eputer sc d of requonly usent attempt	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are 281473913981971 extract information about ords request attemning engineering 281473913981971 dent needs to fill some inew document that alloweds to try against the search and the sear	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea	1.250 ers conc 1 2 3 4 2.500 puter scd of requonly use	inting an o them liste Visit the Visit Arch Crawl the Visit Good United the Visit Good U	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are 281473913981971 extract information about ords request attemning engineering 281473913981971 dent needs to fill some inew document that alloweds to try against the search and the sear	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea	1.250 ers conc 1 2 3 4 2.500 eputer sc d of requonly usent attempt	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retrest entire website and strongle's search engine are 281473913981971 extract information about ords request attemning engineering 281473913981971 entire the document that allowed so try against the set hijacking	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea comm studer	not find 1 2 3 4 1.250 ers conc 1 2 3 4 2.500 puter sc dd of requonly useent attempt 1	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retrest entire website and strongle's search engine are 281473913981971 extract information about ords request attemning engineering 281473913981971 entire the document that allowed so try against the set hijacking	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea comm studer	not find 1 2 3 4 1.250 ers conc 1 2 3 4 2.500 puter sc dd of requonly uses at attempt 1 2	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are 281473913981971 extract information about ords request attemning engineering 281473913981971 dent needs to fill some inew document that allords to try against the sethijacking ry attack	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea comm studer	not find 1 2 3 4 1.250 ers conc 1 2 3 4 2.500 puter sc d of requ only use tt attemp 1 2 3 3	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retree entire website and strongle's search engine are 281473913981971 extract information about ords request attempting and the search engine are 281473913981971 extract information about ords request attempting and the search engine engineering en	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	mation and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of
	+ Attack + A com Instea comm studer	not find 1 2 3 4 1.250 ers conc 1 2 3 4 2.500 puter sc d of requ only use tt attemp 1 2 3 3	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retree entire website and strongle's search engine are 281473913981971 extract information about ords request attempting and the search engine are 281473913981971 extract information about ords request attempting and the search engine engineering en	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of t ore them into your computer id view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Ac wed the forms to be complet	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall locatio 16:26:54 dobe PDF job application theed, the student decides to v	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rite a script that pulls	and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of a cryptography attack is the
16 S	+ Attack + A com Instea comm studer	1.250 2.500 puter sc d of requonly use nt attempt 1 2 3 4 1.250	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle entire entire the entire that allowed the entire that	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of to ore them into your computer ind view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Act wed the forms to be complete ecured PDF until the correct	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall location 16:26:54 dobe PDF job application the d, the student decides to y password is found or the lisuance in the company's website	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rrite a script that pulls t is exhausted. Which	and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of a cryptography attack is the
16 S	+ Attack + A com Instea comm studer	1.250 2.500 puter sc d of requonly use nt attempt 1 2 3 4 1.250	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle entire entire the entire that allowed the entire that	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of to ore them into your computer ind view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Act wed the forms to be complete ecured PDF until the correct page 16:26:54	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall location 16:26:54 dobe PDF job application the d, the student decides to y password is found or the lisuance in the company's website	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rrite a script that pulls t is exhausted. Which	and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of a cryptography attack is the
16 S	+ Attack + A community and a community attack + or c	1.250 ers conc 1 2.500 ers conc 1 2.500 eputer sc d of requonly use nt attemp 1 2.3 4 1.250 ers concern attemp 1 1 2 3 4	inting an o them liste Visit the Visit Arch Crawl the Visit Good V	organization and gather and there. You know they company's partners and hive.org web site to retreat the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle's search engine are astract information about ords request attempting the entire website and strongle entire entire the entire that allowed the entire that	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of to ore them into your computer ind view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Act wed the forms to be complete ecured PDF until the correct page 16:26:54	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall location 16:26:54 dobe PDF job application the d, the student decides to y password is found or the lisuance in the company's website	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rrite a script that pulls t is exhausted. Which	and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of a cryptography attack is the
16 S	+ Attack + A community and a community attack + or c	2.500 puter sc d of requonly use nt attempt 1 2 3 4 1.250 cracker is 1	inting an o them liste Visit he Visit Arct Crawl the Visit Goo duct to e DNS reco Tracerou Port scar Social Er series and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and passworb tience stud testing and the passworb tience stud testing and the passworb tience stud testing and the passworb tience stud testing and the passworb the pass	organization and gather and there. You know they company's partners and hive.org web site to retire entire website and strongle's search engine and strongle's search engine and strongle's search engine and strongle's search engine and strongle's search engine and strongle's search engine and strongle's search engine and strongle's search engine and strongle search engine entire to information about ords request and strongle entire document that allowed and strongle entire search entire s	ring competitive intelligence. y had the entire staff director id customers website for this rieve the Internet archive of to ore them into your computer ind view the cached copy 16:23:38 ut: network topology, trusted 16:26:22 information into a secured Act wed the forms to be complete ecured PDF until the correct page 16:26:54	You visit the company's we y listed on their website 12 information the company's website 17:53:03 routers, and firewall location 16:26:54 dobe PDF job application the d, the student decides to y password is found or the lisuance in the company's website	bsite for contact informonths ago but now 29:25 ns. 00:32 at was received from rrite a script that pulls t is exhausted. Which	and telephone numbers it is not there. 49.4 32.286 a prospective employer. s passwords from a list of a cryptography attack is the





	4	User					
	1	•					
18 S	1.25		281473913981971	16:27:03	16:27:27	00:24	24.354
Α	An ethical ha			rledge, network knowledge, con	nputer expert, security know	rledge, and	
	1		ve field experience				
	+ 2		ical knowledge skills				
-	3		y to build infrastructure				
	4	DOOKS	to gain knowledge				
19 S	0.00	0	281473913981971	16:27:27	17:50:27	23:00	35.435
				nsidered as passive footprinting		20.00	00.100
	- 1			S Yahoo Financial to identify ass			
	2	Scan	the range of IP address for	ound in the target DNS databas	e.		
	3	Go thi	rough the rubbish to find o	out any information that might h	ave been discarded.		
L	4	Perfor	rm multiples queries using	g a search engine.			
			T T				1
20 S	2.50		281473913981971	16:28:58	17:47:24	18:26	51.208
				ersely impact a system through ms best matches the definition?		action, disclosure, denial	of service or
<u> </u>	1		rability	ns best matches the deminion:			
	+ 2	Threa					
	3	Attack					
	4	Risk					
	-						
21 S	0.00		281473913981971	16:30:52	17:45:02	14:10	82.363
				lient's internal network and succ			
	You want to network?	know whi	ich Microsoft Windows wo	orkstations have file sharing ena	abled. Which port would you	see listening on these W	indows machines in th
-	- 1	1433					
	2	161					
-	3	445					
	4	3389					
_	•						
22 S	2.50		281473913981971	16:31:51	17:43:12	11:21	91.05
				e layers of security controls to b		infrastructure, which impi	oves the security
P				alicious attacks or potential vuln	nerabilities?		
	+ 2	_	ork-Based Intrusion Detections in depth	tion System			
	+ 2		ity through obscurity				
-	4		Based Intrusion Detection	System			
L		1.1001					
23 S	1.25	0	281473913981971	16:32:04	16:32:26	00:22	21.484
Y	You are gath	ering cor	mpetitive intelligence on >	YZ.com. You notice that they h	ave jobs listed on a few Inte	ernet job-hunting sites. Th	ere are two job posting
fo	or network a	and syste	m administrators.				
١.	laur aan thia	بمبر جامط	in factoriat the argenizat	ian2			
-	1 1		u in footprint the organizate	er of employees in the company	i e		
	2		range used by the targe	1 7			
	+ 3			and applications being used.			
	4		strong the corporate secu				
L_		,	5				
24 S	1.25	0	281473913981971	16:32:26	16:32:33	00:07	7.807
Α	According to		• • • • • • • • • • • • • • • • • • • •	e next step to be performed afte	r footprinting/reconnaissand	ce?	
	1		m Hacking				
	2		eration				
	+ 3	Scann					
L	4	Social	I Engineering				
25 S	1.25	0	281473913981971	16:32:33	16:32:57	00:24	23.069
				niques, and to identify vulnera			23.008
<u> </u>	1	Comp				000u.ny.	
	2	Docur					
	3	Rules					
	+ 4	Use o	f hacking tools				
26 S	1.25		281473913981971	16:32:57	16:33:04	00:07	7.639
٧			lest password to crack?				
	1	HIJKL					
	2	75890					
	+ 3	Ukm1					
L	4	passw	void I				





7 S After						回物語为機
	0.000	281473913981971	16:33:04	16:33:27	00:23	22.947
			ot access to a Centos 6 server.			
	1	Disable Key Services		,	. , , , , , , , , , , , , , , , , , , ,	
	2	Disable IPTables				
	3	Download and Install Netcat				
-	4	Create User Account				
		Croate Coor Account				
8 S	2.500	281473913981971	16:33:27	17:39:51	06:24	60.238
			can Google hacking be employed			
Exan allinti	nple: itle: root p 1 2 3 4	Scanning and Enumeration Reconnaissance Maintaining Access Gaining Access 281473913981971	16:34:27 numerates the running on the	16:35:33 remote host.	01:06	65.766
	4	firewall				
os	2.500	281473913981971	16:35:33	17:38:48	03:15	91.786
		ollowing Nmap commands will p			130	2700
1017 1021 1023	cp open g /tcp open /tcp open	unknown exp1				
1750 111/u 123/u 137/u 2049 5353 1750 5185 5435 5622 5759 5948	l/tcp open I1/tcp open udp open udp open l/udp open l/udp oper l/udp oper I/udp oper	n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown				
1750 111/0 123/0 137/0 2049 5353 1750 5185 5435 5622 5759 5948	l/tcp open 1/tcp open udp open udp open udp open l/udp oper 1/udp oper 1/udp oper 1/udp oper 1/udp oper 18/udp oper	nfs n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown				
1750 111/0 123/0 137/0 2049 5353 1750 5185 5435 5622 5759 5948	/tcp open 11/tcp open udp open udp open udp open //udp oper //udp oper 11/udp oper 18/udp oper 8/udp oper 8/udp oper 8/udp oper 17/udp oper 18/udp oper 18/udp oper 18/udp oper 18/udp oper 18/udp oper 18/udp oper	nfs n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown	192 168 1 1			
1750 111/0 123/0 137/0 2049 5353 1750 5185 5435 5622 5759 5948	/tcp open 11/tcp ope udp open udp open udp open //udp oper 11/udp oper 11/udp oper 14/udp oper 18/udp oper 17/udp oper 17/udp oper 11/udp oper 17/udp oper 11/udp oper 11/udp oper 11/udp oper 11/udp oper	nfs n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered u				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tdp o	nfs n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1	1			
1750 111/0 123/0 137/0 2049 5353 1750 5185 5435 5622 5759 5948	/tcp open 11/tcp ope udp open udp open udp open //udp oper 11/udp oper 11/udp oper 14/udp oper 18/udp oper 17/udp oper 17/udp oper 11/udp oper 17/udp oper 11/udp oper 11/udp oper 11/udp oper 11/udp oper	nfs n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered u	1			
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tcp open 11/tcp open 12/tcp open 12/tcp open 13/tcp open 13/tcp open 14/tcp open 15/tcp o	nfs n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1 nmap -sS -sU -Pn -p 1-65535	192.168.1.1	16:38:48	nn-5a	50 446
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 11/tcp open 11/tdp o	nfs n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered	192.168.1.1	16:38:48 You would like to enumerat	00:59	59.446
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1 nmap -sS -sU -Pn -p 1-65535 281473913981971 essfully comprised a server ha AP command you will use?	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 1/tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.′ nmap -sS -sU -Pn -p 1-65535 281473913981971 essfully comprised a server ha AP command you will use? nmap -T4 -O 10.10.0.0/24	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.′ nmap -sS -sU -Pn -p 1-65535 281473913981971 essfully comprised a server ha AP command you will use? nmap -T4 -O 10.10.0.0/24 nmap -T4 -q 10.10.0.0/24	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 1/tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1 nmap -sS -sU -Pn -p 1-65535	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.′ nmap -sS -sU -Pn -p 1-65535 281473913981971 essfully comprised a server ha AP command you will use? nmap -T4 -O 10.10.0.0/24 nmap -T4 -q 10.10.0.0/24	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 1/tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1 nmap -sS -sU -Pn -p 1-65535	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002	/tcp open 1/tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.1 nmap -sS -sU -Pn -p 1-65535	192.168.1.1				
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002 +	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.7 nmap -sS -sU -Pn -p 1-65535 281473913981971 essfully comprised a server ha AP command you will use? nmap -T4 -O 10.10.0.0/24 nmap -T4 -q 10.10.0.0/24 nmap -T4 -r 10.10.1.0/24 nmap -T4 -r 10.10.1.0/24	192.168.1.1 16:37:49 ving an IP address of 10.10.0.5.	You would like to enumerat	e all machines in the same ne	etwork quickly. W	
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002 +	/tcp open //tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.7 nmap -sS -sU -Pn -p 1-65535	1 192.168.1.1 16:37:49 ving an IP address of 10.10.0.5.	You would like to enumerat	e all machines in the same ne	etwork quickly. W	
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002 +	//tcp open //tcp open	nfs n unknown rpcbind ntp netbios-ns n fs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.7 nmap -sS -sU -Pn -p 1-65535	192.168.1.1 16:37:49 ving an IP address of 10.10.0.5. 16:38:48 and compare with the databases	You would like to enumerat	e all machines in the same ne	etwork quickly. W
1750 111/k 123/k 137/k 2049 5353 1750 5185 5435 5622 5759 5948 6002 +	/tcp open 1/tcp s n unknown rpcbind ntp netbios-ns n nfs n zeroconf en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown en filtered unknown nmap -sS -Pn 192.168.1.1 nmap -sT -sX -Pn -p 1-65535 nmap -sN -Ps -T4 192.168.1.7 nmap -sS -sU -Pn -p 1-65535	192.168.1.1 16:37:49 ving an IP address of 10.10.0.5. 16:38:48 and compare with the databases a list	You would like to enumerat	e all machines in the same ne	etwork quickly. W	





	_							121 WAY 1600F
33 S		2.500		281473913981971	16:39:58	16:40:56	00:58	57.928
[Due to	a slow	down of	normal network operation	ons, IT department decided	to monitor internet traffic for	all of the employees. From a	a legal stand point, wh
٧	would l	be troub		to take this kind of meas				
	+	1	Not info	orming the employees th	nat they are going to be mor	nitored could be an invasion	of privacy.	
		2	All of th	ne employees would stop	p normal work activities			
		3	IT depa	artment would be telling	employees who the boss is			
		4	The ne	twork could still experier	nce 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-monito	ring and managing hosts, ro	outers, 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
Α	A netw	ork adm	ninistrato		nown files in the root director	rv of his Linux FTP server.	One of the files is a tarball, to	vo are shell script files
							er account logged in to the s	
							server's software. The ps cor	
							port. What kind of vulnerabi	
			•	k possible?	5aa 56.16 16 1.6 p. 66	ood to motoriming out a motiment	r porti Triiat ittia or Tairiorabi	
T T		1		orce login				
	-	2		ry traversal				
		3		stem permissions				
—		4		e escalation				
L		7	ııvııey	,				
6 S		1.250		281473913981971	16:44:38	16:45:21	00:43	42.822
	ie o v		atabass			ects that can be managed us		42.022
⊢:	is a	virtuai d	LDAP	containing formal descr	iphon of all the network obje	ous mai can be managed u	DING SINIVIF.	
		2	MIB					
	+							
-		3	SNMP					
		4	NTP					
37 S		1.250		281473913981971	16:45:21	17:31:15 ot concerned about being st	45:54	167.038
	+	2	A FIN s	scan Connect scan				
		4	A half-s					
L								
38 S		0.000		281473913981971	16:46:50	16:51:27	04:37	277.44
	As a C		Ethical F			duct an external security as:	sessment through penetratio	n testing. What
d		ent desc			, ,	,	n the organization's interest	•
	-	1	Non-Di	sclosure Agreement				
				Level Agreement				
		3	Project					
\vdash		4		of Engagement				
			1					
9 S		1.250		281473913981971	16:51:27	16:52:28	01:01	61.049
	is a		nd respo				signess of an Internet resou	
			-	lock, or an autonomous				,
T.	,	1	DNS qu		, -			
	+	2	WHOIS					
		3	Tracero					
—		4	Ping					
_		· ·	9					
0 S		1.250		281473913981971	16:52:28	17:28:23	35:55	87.673
	Active		ttack ma		em that has bad passwords		00.00	07.070
		1		authentication points	om machao bad passwords	unu		
	+	2		passwords				
-				•				
L		3		ex password				
		4	User st	upiaity				
								1
						17:25:55	31:13	00.044
		0.000		281473913981971	16:54:42	17.23.33	31.13	63.611
	prov			formation about location		17.25.55	31.13	63.611
	prov -	ide impo	Tracero	formation about location oute		17.20.33	31.13	63.611
	prov	ide impo	Tracero Port list	formation about location oute ts		17.23.33	31.13	63.611
	prov	ide impo	Tracero	formation about location oute ts		17.23.33	31.13	63.611
41 S	prov	ide impo	Tracero Port list	formation about location bute ts seconds		17.23.33	31.13	63.611





43 \$	1						
43 \$.250	281473913981971	16:55:43	16:57:00	01:17	76.434
43 \$				d files, it use machines across			
			Offline Attack				
	+	2 [Distributed Network Attack				
			Distributed Denial of Service				
			Online Attack				
			o /ao.				
	2	.500	281473913981971	16:57:00	16:57:45	00:45	45.273
				resolving events that take place		00.10	10.270
	+		ncident Management Process	. seeming everne unat take place	5 d.: 0.gaa		
	•		Metrics				
-			Security Policy				
			nternal Procedure				
	ļ	- I.	itomai i roccauro				
44 S	2	.500	281473913981971	16:57:45	17:24:38	26:53	25.456
			esting" methodology enforces		17.21.00	20.00	20.100
- '	TIC WITE			a system is accessible to the te	ster		
				em is only partly accessible to			
	+			em is completely known to the			
	т			system is known to the tester	tester		
		4	Thy 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
				ganization. The company want			
				ganization. The company want hat should be the first step in s		zansuc as possible, uletel	ore, they ald flot provide
Į ai	,		numeration	a. Ground be the mot step in s	security toothing the offerit!		
-			scalation				
	+		Reconnaissance				
			canning				
		- C	carring				
46 S	1	.250	281473913981971	16:58:22	17:00:58	02:36	156.546
			chnical password cracking att		17.00.50	02.30	130.340
	+		hishing attack	шоко, <u>слосрі</u>			
	т		Shoulder surfing				
			Ceyboard sniffing				
			Social engineering				
	ļ	4	ocial eligilieelilig				
47 S	1	.250	281473913981971	17:00:58	17:01:48	00:50	49.887
				prevent NetBIOS traffic from r			
	2000, and		a so sicolog on the meman to	provent notation trains from t	iot commig unicagn and mon	a y o a o t o	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	1		61, 163				
	+		37, 139				
			93, 195				
			45, 447				
			,				
48 S	2	.500	281473913981971	17:01:48	17:03:38	01:50	109.586
				later phases of the penetration			
				st important phase of ethical ha			
<u> </u>			scalating privileges		, , , , , , , , , , , , , , , , , , , ,		
			letwork mapping				
	+		ootprinting				
			Gaining access				
_	-						
49 S	1.	.250	281473913981971	17:03:38	17:04:41	01:03	62.62
			amounts of network bandwidtl				
	+		ctive online attacks				
<u> </u>			lon-electronic attacks				
			assive online attacks				
		_					
		4 (Offline attacks				
		4 (Offline attacks				
50 S	2	.500	Offline attacks 281473913981971	17:04:41	17:05:11	00:30	30.662
50 S		.500	281473913981971				
50 S	Ricardo w	.500 /ants to	281473913981971	ompetitor company. To secure			
50 S	Ricardo w	.500 /ants to	281473913981971 send secret messages to a co	ompetitor company. To secure			
50 S R	Ricardo w ordinary r	.500 vants to nessag	281473913981971 send secret messages to a co	ompetitor company. To secure			
50 S R	Ricardo w ordinary r	.500 vants to messag nnique i	281473913981971 send secret messages to a coe. The technique provides 'sec s Ricardo using?	ompetitor company. To secure			
50 S R	Ricardo w ordinary r	.500 vants to messag nnique i	281473913981971 send secret messages to a cue. The technique provides 'sec s Ricardo using?	ompetitor company. To secure			
50 S R	Ricardo w ordinary r	.500 vants to messag nnique i	281473913981971 send secret messages to a coe. The technique provides 'sec s Ricardo using?	ompetitor company. To secure			
50 S R	Ricardo w ordinary r	.500 vants to messag	281473913981971 send secret messages to a cree. The technique provides 'secons Ricardo using? SA algorithm Public-key cryptography	ompetitor company. To secure			
50 S R	Ricardo wordinary r	.500 vants to messag	281473913981971 send secret messages to a cree. The technique provides 'sec s Ricardo using? SA algorithm Public-key cryptography Incryption	ompetitor company. To secure			
50 S R	Ricardo wordinary r	.500 vants to messag	281473913981971 send secret messages to a cree. The technique provides 'sec s Ricardo using? SA algorithm Public-key cryptography Incryption	ompetitor company. To secure			
50 S R OI	Ricardo wordinary r What tech	zants to messag nnique in F 2 F 3 E 4 S	281473913981971 send secret messages to a core. The technique provides 'secoret second	ompetitor company. To secure curity through obscurity'.	these messages, he uses a	technique of hiding a sec	ret message within an





+	2	Compromising security contro	ıls			
	3	Protecting system security				
	4	Updating operating system				
3	0.000	281473913981971	17:05:39	17:23:01	17:22	113.688
Which	_		or adjust while scanning for op of the packets sent during the	en ports to avoid detection by the	he network's IDS?	
-	2		h operating systems are runnir			
-	3		e which hosts on the network a			
	4		eed that the port scan is condu			
	•					
3	1.250	281473913981971	17:05:52	17:06:43	00:51	51.034
These		Elements of Information Securi Availability	ity, except			
-	2	Authenticity				
+	3	Vulnerability				
	4	Integrity				
	•		_			
3	1.250	281473913981971	17:06:43	17:07:46	01:03	63.029
is a		nd-line tool designed to crack be	oth Unix/Linux and NT/Windov	vs passwords.		
-	2	SET Cain & Abel				
	3	L0phtcrack				
+	4	John the Ripper				
3	1.250	281473913981971	17:07:46	17:10:01	02:15	134.641
Attac			n on social networking webs	ites such as Facebook, MySpac	ce, LinkedIn, Twitter, Pint	erest, Google+, etc
	1	Traceroute				
+	3	Social Engineering DNS records request				
	4	Port scanning				
		<u> </u>				
3	0.000	281473913981971	17:10:01	17:10:58	00:57	56.423
is a			opment that will affect the calcu	ulation time of password cracking	ıg.	
-	1	Progressive law				
-	3	Calculation law Einstein's law				
	4	Moore's law				
3						54.411
I Emil	2.500	281473913981971	17:10:58	17:17:57	06:59	54.411
15,000		281473913981971 p to scan two hosts using this of		17:17:57	06:59	54.411
	uses nma	p to scan two hosts using this of		17:17:57	06:59	54.411
	uses nma			17:17:57	06:59	54.411
nmap	uses nma	p to scan two hosts using this of O 192.168.99.1 192.168.99.7		17:17:57	06:59	34.411
nmap He re	uses nma	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output:		17:17:57	06:59	54.411
nmap He re	uses nma p -sS -T4 eceives th p scan rep	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output:		17:17:57	06:59	54.411
nmap He re Nmap Host Not s	uses nma p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports		17:17:57	06:59	54.411
nmap He re Nmap Host Not s POR	p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: oort for 192.168.99.1 0082s latency). 4 filtered ports SERVICE		17:17:57	06:59	54.411
nmap He re Nmap Host Not s POR 21/tcp	p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp	p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp	p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE net		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tc	uses nma p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open de p open de p open htt top closed	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: cort for 192.168.99.1 0082s latency). 4 filtered ports SERVICE net imain ip snmp		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tc MAC	uses nma p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open do p open do p open do chosed: Address:	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE Intermediate the same properties of the same p		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Device	uses nma p -sS -T4 eccives the p scan rep is up (0.0 shown: 99 T STATE ip open tel ip open de ip open de ip closed Address: ce type: gr	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE Interpret to main to the post of the		17:17:57	06:59	54.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Devic Runn	uses nma p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open de p open de p open ht tcp closes: ce type: g ning: Linux	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE Interpret to main to the post of the		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Device Runn OS C OS de	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open de p open de p open ht top closed Address: ce type: g ning: Linux DPE: cpe:/details: Lin	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE net main p snmp B0:75:D5:33:57:74 (ZTE) eneral purpose c 2.6.X o:linux:linux_kernel:2.6 ux 2.6.9 - 2.6.33		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Device Runn OS C OS de	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open de p open de p open ht top closed Address: ce type: g ning: Linux DPE: cpe:/details: Lin	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet main possible properties of the port of the ports of the possible properties of the possible pr		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Devic Runn OS C OS d Netwo	p -sS -T4 - eceives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open dc cp open ht tcp closed Address: ce type: gn ining: Linux CPE: cpe:/ letails: Linux CPE: cpe:/	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet imain in position of the positio		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Device Runn OS C OS de Netwe	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open dc p open dc ch dddress: ce type: g ining: Linu CPE: cpe:/ details: Lin vork Distar p scan rep	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE net umain rip snmp B0:75:D5:33:57:74 (ZTE) eneral purpose of 2.6.X oo:linux:linux_kernel:2.6 ux 2.6.9 - 2.6.33 noce: 1 hop		17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tc; 23/tc; 53/tc; 80/tc; 161/tt MAC Devic Runn OS C OS di Netwo	p -sS -T4 eccives the p scan register of the population of the pop	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet imain in position of the positio	command:	17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tc MAC Devic Runn OS C OS d Netw Nmap Host All 10	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open tel p open dc p open ht top closed Address: ce type: g hing: Linu CPE: cpe:/ details: Lin /ork Distar p scan rep is up (0.0 000 scann many fingi	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 192.168.99.1 190.82 latency). 4 filtered ports SERVICE net main p snmp B0:75:D5:33:57:74 (ZTE) eneral purpose c 2.6.X o:linux:linux_kernel:2.6 ux 2.6.9 - 2.6.33 nce: 1 hop port for 192.168.99.7 190.0047s latency). ed ports on 192.168.99.7 are cerprints match this host to give	command:	17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tc MAC Devic Runn OS C OS d Netw Nmap Host All 10	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open tel p open dc p open ht top closed Address: ce type: g hing: Linu CPE: cpe:/ details: Lin /ork Distar p scan rep is up (0.0 000 scann many fingi	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet of the ports of the	command:	17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 53/tcp 161/tt MAC Devic Runn OS C OS d Netw Nmap Host All 10 Too n Netw	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open fte p open te p open ht top closed Address: ce type: g ning: Linux CPE: cpe:/ rork Distar p scan rep is up (0.0 000 scann many fing rork Distar	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet main in possible properties of the port of 192.168.99.7 (ZTE) eneral purpose (2.6.X) onet inux_linux_kernel:2.6 ux 2.6.9 - 2.6.33 ince: 1 hop port for 192.168.99.7 one of ports on 192.168.99.7 are comprists match this host to give noe: 0 hops	command:	17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 53/tcp 161/tt MAC Devic Runn OS C OS d Netw Nmap Host All 10 Too n Netw	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open tel p open dc p open ht top closed Address: ce type: g hing: Linu CPE: cpe:/ details: Lin /ork Distar p scan rep is up (0.0 000 scann many fingi	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 0082s latency). 4 filtered ports SERVICE onet main in possible properties of the port of 192.168.99.7 (ZTE) eneral purpose (2.6.X) onet inux_linux_kernel:2.6 ux 2.6.9 - 2.6.33 ince: 1 hop port for 192.168.99.7 one of ports on 192.168.99.7 are comprists match this host to give noe: 0 hops	command:	17:17:57	06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Devic Runn OS C OS d Netw Nmap Host All 10 Too n Netw	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open dc p open ht tcp closed Address: ce type: gn increase p scan rep is up (0.0 000 scann many fing ork Distar t is his con	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 10082s latency). 4 filtered ports SERVICE net main pp snmp B0:75:D5:33:57:74 (ZTE) eneral purpose 4 2.6. X o:linux:linux_kernel:2.6 ux 2.6.9 - 2.6.33 nce: 1 hop port for 192.168.99.7 00047s latency). ed ports on 192.168.99.7 are cerprints match this host to give nce: 0 hops nclusion? Host 192.168.99.7 is down	command:		06:59	34.411
nmap He re Nmap Host Not s POR 21/tcp 23/tcp 53/tcp 80/tcp 161/tt MAC Devic Runn OS C OS d Netw Nmap Host All 10 Too n Netw	uses nma p -sS -T4 eccives th p scan rep is up (0.0 shown: 99 T STATE p open ftp p open ftc tcp closed Address: ce type: ge ing: Linu CPE: cpe://details: Lin vork Distar p scan rep is up (0.0 000 scann many fing vork Distar t is his cor 1	p to scan two hosts using this of O 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 192.168.99.7 is output: port for 192.168.99.1 10082s latency). 4 filtered ports SERVICE net main pp snmp B0:75:D5:33:57:74 (ZTE) eneral purpose 4 2.6. X o:linux:linux_kernel:2.6 ux 2.6.9 - 2.6.33 nce: 1 hop port for 192.168.99.7 00047s latency). ed ports on 192.168.99.7 are cerprints match this host to give nce: 0 hops nclusion? Host 192.168.99.7 is down	closed specific OS details that he launched the scan fror d.	n	06:59	34.411





58 S		1.250	281473913981971	17:11:56	17:13:07	01:11	70.719
	If you send a SYN to		SYN to an open port, what is the	e 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
59 S			281473913981971 ollowing security operations is u			03:18	126.34
59 8				used for determining the attack	surface of an organization?	03:18	126.34
59 S	Which		ollowing security operations is u	used for determining the attack urity clearance for each emplo	surface of an organization?	03:18	126.34
59 S	Which	of the fo	ollowing security operations is understood Reviewing the need for a secure Running a network scan to de	used for determining the attack urity clearance for each emplo	surface of an organization? yee orporate DMZ	03:18	126.34
<u>59 S</u>	Which	of the fo	Reviewing the need for a seci Running a network scan to de Training employees on the se	used for determining the attack urity clearance for each emplo etect network services in the co curity policy regarding social of	surface of an organization? yee orporate DMZ	03:18	126.34
<u> 59 S</u>	Which	of the fo	Reviewing the need for a seci Running a network scan to de Training employees on the se	used for determining the attack urity clearance for each emplo etect network services in the co curity policy regarding social of	s surface of an organization? yee proporate DMZ engineering	03:18	126.34

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.





surname: 1572025

YOGI KOSIM SINDUDIBROT name:

1572025 user:

start time: 2017-11-16 13:29:25 end time: 2017-11-16 14:15:40 00:46:15

points to pass the exam: 70.000 correct: (0%) wrong: (0%) unanswered: (0%) (0%) undisplayed:

time:

points: 72.000 / 100.000 (72%) - PASSED

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

#	points	IP	start [hh:mm:ss] end [hh:mm		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?

VVIIGUR	ind of attack is being indistrated 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		Directory traversal				

65.705 3 S 4 000 281473913980691 13:35:10 13:36:15 01:05

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	TCP session					
		3	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 SQLI		SQL Injection				
		2	Sniffing Login				
	+ 3 Web defacement		Web defacement				
	4 Web server DDoS		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





						PH 3/15/07/19/25
	3	Trojan server attack				
	4	Spear phishing attack				
70	4.000	204.47204.2000004	42,47,52	42:40:45	00.52	F2.00
7 S Thesi	4.000	281473913980691 sons of session hijacking succe	13:47:52	13:48:45	00:53	52.09
+	1	Chyper Text Transmission	osidi idolor, except			
	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
		ollowing attacks takes best adva			00.00	30.400
+	1	Session Hijacking	<u> </u>			
	2	Password Guessing				
	3	Spoofing				
	4	Password Sniffing				
9 S	4.000	281473913980691	13:48:57	13:49:26	00:29	29.17
Thes	e are the	impact of webserver attacks, ex	ccept	-1		1
	1	Compromise of user accounts	i .			
+	2	OS patch updated				
	3	Data theft Website defacement				
	7	Website delacement				
10 S	4.000	281473913980691	13:49:27	13:54:37	05:10	111.218
	•	9 ,	•	crets, or put you out of business,	they just have to find a	job opening, prepare
some	eone to pa	ss the interview, have that pers	son hired, and they will be in the	ne organization.		
How	would vou	prevent such type of attacks?				
11011	1	Hire the people through third-p		them for you		
	2	Investigate their social network				
	3	It is impossible to block these				
+	4	Conduct thorough background	d checks before you engage th	em		
1 S	0.000	281473913980691	13:54:37	13:55:14	00:37	36.553
	in the cont			describes Social Engineering bes		
-	1	Social Engineering is the mea	ns put in place by human reso	ource to perform time accounting		
	2	Social Engineering is a training	g program within sociology stu	ıdies		
	3	Social Engineering is a training Social Engineering is the act of	g program within sociology stu of publicly disclosing information	idies on		
	_	Social Engineering is a training Social Engineering is the act of	g program within sociology stu of publicly disclosing information	ıdies		
	0.000	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of 281473913980691	g program within sociology stu of publicly disclosing information of getting needed information f 13:55:15	rdies on rom a person rather than breakin 13:57:31	ng into a system 02:16	136.34
After	0.000 a client se	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of 281473913980691 ands a connection request (SYI	g program within sociology studies of publicly disclosing information of getting needed information for the server, the server, the server, the server.	idies on rom a person rather than breakir	ng into a system 02:16	
After then	0.000 a client se	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is a training social Engineering is a training social Engineering is a training social Engineering is a training social Engineering is the act of Social Engineering is the act of	g program within sociology studies of publicly disclosing information of getting needed information of 13:55:15 N) packet to the server, the sent.	rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with	ng into a system 02:16 h a sequence number of	its choosing, which
After then This	0.000 a client se must be a sequence	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is a training social Engineering is a training social Engineering is a training social Engineering is a training social Engineering is the act of Social Engineering is the act of	g program within sociology study of publicly disclosing information of getting needed information of 13:55:15 N) packet to the server, the sent. ck connects to a service first were publicly stated in the service of	rdies on rom a person rather than breakin 13:57:31	ng into a system 02:16 h a sequence number of	its choosing, which
After then this sa second The a	0.000 a client se must be a sequence cond connattack doe	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering 1281473913980691 ends a connection request (SYI toknowledged (ACK) by the clied number is predictable; the attalection from a forged IP address isn't see the SYN-ACK (or any of Social Engineering IP).	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first was connected to the service for the service first was connected to a service for the server, of the packet) from the server,	dies on rather than breaking a person rather than breaking a person rather than breaking a person rather than breaking a person (357:31 rver will respond (SYN-ACK) with its own IP address, records the tour can guess the correct responding to the correct responding a person records the correct responding to the correct responding	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then this sa second The a	0.000 a client se must be a sequence cond connattack doe	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering 1281473913980691 ends a connection request (SYI toknowledged (ACK) by the clied number is predictable; the attalection from a forged IP address isn't see the SYN-ACK (or any of Social Engineering IP).	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first was connected to the service for the service first was connected to a service for the server, of the packet) from the server,	dies on rom a person rather than breakin 13:57:31 rver will respond (SYN-ACK) with its own IP address, records t	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then This s a sec The a	3 0.000 a client se must be a sequence cond connattack doe source IF	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI). The social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI). Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI).	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ock connects to a service first was other packet) from the server, then the attacker can use the server of the server.	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then This s a sec The a	3 0.000 a client se must be a sequence cond connattack doe source IF	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering 1281473913980691 ends a connection request (SYI toknowledged (ACK) by the clied number is predictable; the attalection from a forged IP address isn't see the SYN-ACK (or any of Social Engineering IP).	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first vis. other packet) from the server, tion, then the attacker can usualists a server using the above	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then then the same a second the all the	0.000 a client se must be a sequence cond conn attack doe source IF t attacks c	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYIcknowledged (ACK) by the clien number is predictable; the attalection from a forged IP address is the SYN-ACK (or any of Social Engineering is used for authentication and you successfully launch again which page defacement attacks IP spoofing attacks	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first vis. other packet) from the server, tion, then the attacker can usualists a server using the above	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then This s a sec The a	0.000 a client se must be a sequence cond conn attack doe source IF t attacks c	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYIcknowledged (ACK) by the clien umber is predictable; the attaction from a forged IP address is result of Social Engineering is act of Social Engineering in Social Engineering in Social Engineering is act of Social Engineering in Social Engineering is the act of Social Engineering in Social Engineering is the act of Social Engineering is t	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first vis. other packet) from the server, tion, then the attacker can usualists a server using the above	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then This sa sec The a	0.000 a client se must be a sequence cond conn attack doe source IF t attacks c	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYIcknowledged (ACK) by the clien number is predictable; the attalection from a forged IP address is the SYN-ACK (or any of Social Engineering is used for authentication and you successfully launch again which page defacement attacks IP spoofing attacks	g program within sociology studies of publicly disclosing information of getting needed information for 13:55:15 N) packet to the server, the sent. ck connects to a service first vis. other packet) from the server, tion, then the attacker can usualists a server using the above	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number charses.	its choosing, which
After then This s a sec The a If the What	0.000 a client se must be a sequence cond connattack doe source IF t attacks c	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) should be action request (SYI) cknowledged (ACK) by the clienumber is predictable; the attaction from a forged IP address is received in the social should be social social should be social social should be soci	g program within sociology studies of publicly disclosing information of getting needed information of 13:55:15 N) packet to the server, the sent. ck connects to a service first visconther packet) from the server, tion, then the attacker can use thins a server using the above is	dies on rather than breaking to a person rather than breaking to a person rather than breaking to a person rather than breaking to a person of the care than the correct response the one-sided communication to technique?	02:16 h a sequence number of the sequence number chanses. o break into the server.	its choosing, which osen, and then open
After then This: a sec The a If the What	3 4 0.000 a client semust be a sequence cond connattack doe a source IF t attacks c 1 2 3 4.000	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) acknowledged (ACK) by the clied number is predictable; the attacetion from a forged IP address is received in the social socia	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ck connects to a service first was other packet) from the server, tion, then the attacker can use sinst a server using the above of 13:57:32	tidies on rom a person rather than breaking 13:57:31 rver will respond (SYN-ACK) with with its own IP address, records to but can guess the correct respond to the one-sided communication to	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server.	its choosing, which osen, and then oper
After then This: a sec The a If the What	3 4 0.000 a client so must be a sequence cond conn attack doe a source IP t attacks c 1 2 3 4 4.000 nsultant is pany's buil	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social En	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ock connects to a service first with the server, the sent. och connects to a service first with the server, the sent. och connects to a service first with the server, attion, then the attacker can use the server using the above of the server using the server using the above of the server using the server using the server using the above of the server using the s	dides on rom a person rather than breaking to a person rather than breaking to a person rather than breaking to a person rather than breaking the state of the st	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then This: a sec The a If the What	3 4 0.000 a client so must be a sequence cond conn attack doe a source IP t attacks c 1 2 3 4 4.000 nsultant is pany's buil	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) acknowledged (ACK) by the clie number is predictable; the attalection from a forged IP address is the SYN-ACK (or any of Social Engineering is used for authentical and you successfully launch again which is social in the social IP spoofing attacks Denial of Service attacks Session Hijacking attacks 281473913980691 hired to do physical penetration	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ock connects to a service first with the server, the sent. och connects to a service first with the server, the sent. och connects to a service first with the server, attion, then the attacker can use the server using the above of the server using the server using the above of the server using the server using the server using the above of the server using the s	13:58:37 nom a person rather than breaking the person rather than breaking the person rather than breaking the person of the pe	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then the second of the s	3 4 0.000 a client semust be a sequence cond conn attack doe source IF t attacks c 1 2 3 4 0.000 nsultant is bany's bui	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engine	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in getting needed in getting needed in getting at a large financial or and waits in the lobby for an area.	13:58:37 nom a person rather than breaking the person rather than breaking the person rather than breaking the person of the pe	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then the same a second the a lift the what same a second the a s	3 4 0.000 a client semust be a sequence cond conn attack doe source IF t attacks c 1 2 3 4 0.000 nsultant is bany's bui	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social En	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in getting needed in getting needed in getting at a large financial or and waits in the lobby for an area.	13:58:37 norm a person rather than breaking the person rather than breaking the person rather than breaking the person of the care guess the correct response the one-sided communication to the person of the pers	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then the second of the s	3 4 0.000 a client symmetry be a sequence cond connutattack doe a source IF t attacks c 1 2 3 4 4.000 nsultant is bany's builtimployee be the type of a lieutenty and a li	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engineering is the act of Soci	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in getting needed in getting needed in getting at a large financial or and waits in the lobby for an area.	13:58:37 norm a person rather than breaking the person rather than breaking the person rather than breaking the person of the care guess the correct response the one-sided communication to the person of the pers	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then This s a sec The a If the What S A corrections the element of the second the	3 4 0.000 a client semust be a sequence cond connattack doe a source IF t attacks c 1 2 3 4 4.000 nsultant is bany's builtimployee beht type of a	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engineering (SYI) act of Social Engineering is the SYN-ACK (or any of Social Engineering at Social Engineering is the act of Social Engineering Shoulder Surfage (Social Engineering Shoulder Surfage).	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in getting needed in getting needed in getting at a large financial or and waits in the lobby for an area.	13:58:37 norm a person rather than breaking the person rather than breaking the person rather than breaking the person of the care guess the correct response the one-sided communication to the person of the pers	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then the second of the s	3 4 0.000 a client symmetry be a sequence cond connutattack doe a source IF t attacks c 1 2 3 4 4.000 nsultant is bany's builtimployee be the type of a lieutenty and a li	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engineering is the act of Soci	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in getting needed in getting needed in getting at a large financial or and waits in the lobby for an area.	13:58:37 norm a person rather than breaking the person rather than breaking the person rather than breaking the person of the care guess the correct response the one-sided communication to the person of the pers	og into a system 02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant	its choosing, which osen, and then oper
After then This s a sec The a If the What This s a sec The a If the What This s a sec The a If the What This s a sec The a If the What This s a sec The a If the a If the	3 4 0.000 a client se must be a sequence cond connattack doe source IF t attacks c 1 2 3 4 4.000 nsultant is coany's builtimployee beth type of a sequence cond connattack at a sequence condition and the control of th	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) acknowledged (ACK) by the clies of the act of Social Engineering (SYI) acknowledged (ACK) by the clies of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering Shoulder surfing Tailgating	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ck connects to a service first was other packet) from the server, tion, then the attacker can use the server using the above of 13:57:32 In testing at a large financial contains and waits in the lobby for an area.	13:58:37 may be responding to the meaning of the m	02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant ain access gate, then the	its choosing, which osen, and then open osen, and then open osen. 64.85 to goes to the econsultant follows
After then I This s a sec The a If the What I This s a sec If the What I This s a sec If the What I This s a sec If the a If the I This s a sec I The a If the I This s a sec I This s a s	3 4 0.000 a client so must be a sequence cond connattack doe a source IF t attacks c 1 2 3 4 4.000 nsultant is bany's builtimployee to the type of a 4.000 4.000	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (SYI) and Social Engineering (Social Engineering Shoulder Surfing Tailgating (SOCIAL Engineering Shoulder Surfing Social Engineering Shoulder Surfing Tailgating (SOCIAL Engineering Social Engineering Satiation (SOCIAL Engineering Social Engineering Shoulder Surfing Tailgating (SOCIAL Engineering Social Engineering Satiation (SOCIAL Engineering Shoulder Surfing Tailgating (SOCIAL Engineering Social Engineering Satiation (SOCIAL Engineering Social Engineering Satiation (SOCIAL Engineering Social Engineering Satiation (SOCIAL Engineering Social Engineering	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ock connects to a service first viscother packet) from the server, tion, then the attacker can usualist a server using the above of 13:57:32 In testing at a large financial contains and waits in the lobby for an area.	13:58:37 norm a person rather than breaking the person rather than breaking the person rather than breaking the person of the care guess the correct response the one-sided communication to the person of the pers	02:16 h a sequence number of the sequence number chases. o break into the server. 01:05 sessment, the consultant ain access gate, then the	its choosing, which osen, and then open osen, and then open osen. Galaxies of the econsultant follows 27.716
After then then the second the se	3 4 0.000 a client semust be a sequence cond conn cattack does source IP t attacks c 1 2 3 4 4.000 a client semust be a sequence cond conn cattack does source IP t attacks c 1 2 3 4 4.000 a client semust be a sequence cond conn cattack does source IP t attacks c 1 2 3 4 4.000 a client semust be a sequence cond cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does c	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering So	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ock connects to a service first viscother packet) from the server, ation, then the attacker can usualist a server using the above of 13:57:32 In testing at a large financial contains and waits in the lobby for an area. 13:58:38 Intract for Davidson Avionics.	13:57:31 rver will respond (SYN-ACK) with its own IP address, records the but can guess the correct respondent the one-sided communication to technique? 13:58:37 company. In the first day of his assemployee to pass through the member of the open sides of the open	02:16 h a sequence number of the sequence number chases. to break into the server. 01:05 sessment, the consultant ain access gate, then the consultant ain access gate are the consultant ain access gate.	64.85 It goes to the econsultant follows 27.716 Indices. He has been
then This: a sec The a If the What	3 4 0.000 a client semust be a sequence cond conn cattack does source IF t attacks c 1 2 3 4 0.000 a client semust be a sequence cond conn cattack does source IF t attacks c 1 2 3 4 0.000 a client semust be a sequence cond conn cattack does source IF t attacks c 1 2 3 4 0.000 a client semust be a sequence cond cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cond cattack does cattack does cond cattack does cond cattack does cond cattack does cattack does cond cattack does	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering So	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed information of getting needed in a service first visualization, then the attacker can usualize a server using the above of getting at a large financial contains and waits in the lobby for an area. 13:57:32 In testing at a large financial contains and waits in the lobby for an area. 13:58:38 Intract for Davidson Avionics. ary. Neil has created a fake contains a server and a server getting the server getting in the lobby for an area.	13:57:31 rver will respond (SYN-ACK) with its own IP address, records the one-sided communication the technique? 13:58:37 company. In the first day of his assemployee to pass through the members of the semployee to pass through the semployee to pass through the semployee to pass through the members of the semployee to pass through the semployee to pass through the semployee to pass through the semployee to pass through the semployee to pass through the semployee through the semploy	02:16 h a sequence number of the sequence number chases. to break into the server. 01:05 sessment, the consultant ain access gate, then the consultant ain access gate are the consultant ain access gate.	64.85 a goes to the e consultant follows 27.716 chics. He has been
After then then the same as second the same as seco	3 4 0.000 a client symust be a sequence cond connattack doe a source IF t attacks c 1 2 3 4 4.000 nsultant is bany's builtimployee beht type of a 4 4.000 is an IT see a permission and follows and fo	Social Engineering is a training Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering is the act of Social Engineering Social Engineeri	g program within sociology studies of publicly disclosing information of getting needed information of getting needed information of getting needed information of 13:55:15 N) packet to the server, the sent. ock connects to a service first viscother packet) from the server, ation, then the attacker can use the server using the above of 13:57:32 In testing at a large financial contains and waits in the lobby for an area. In 13:58:38 Intract for Davidson Avionics. ary. Neil has created a fake contains after they use their valid acceleration.	13:57:31 rver will respond (SYN-ACK) with its own IP address, records the one-sided communication the technique? 13:58:37 company. In the first day of his assemployee to pass through the members of the semployee to pass through the semployee to pass through the semployee to pass through the members of the semployee to pass through the semployee to pass through the semployee to pass through the semployee to pass through the semployee to pass through the semployee through the semploy	02:16 h a sequence number of the sequence number chases. to break into the server. 01:05 sessment, the consultant ain access gate, then the consultant ain access gate are the consultant ain access gate.	64.85 a goes to the e consultant follows 27.716 chics. He has been





$\overline{}$			
		3	Neil is using the technique of reverse social engineering to gain access to the offices of Davidson Avionics This type of social engineering attack is called man trapping
		4	He has used a piggybacking technique to gain unauthorized access
	I		
5 S		4.000	281473913980691 13:59:48 14:03:13 03:25 205.293
	Best cou		neasure of session hijacking is
		2	using static ARP using IDS
		3	using firewall
	+	4	using encryption
	,	•	1
6 S		0.000	281473913980691 14:03:14 14:04:15 01:01 60.886
	subcont security No emp	ractor f loyees	T security consultant, specializing in social engineering and external penetration tests. Shayla has been hired on by Treks Avionics, a for the Department of Defense. Shayla has been given authority to perform any and all tests necessary to audit the company's network of 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 employed any website contact pages. Then she befriends a female employee of the company through an online chat website. After meeting with the
			yee numerous times, Shayla is able to gain her trust and they become friends. One day, Shayla steals the employee's access badge and unauthorized access to the Treks Avionics offices.
	What typ		nsider 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 Because she does not have any legal access herself, Shayla would be considered an Outside Affiliate
		4	because sile does not have any legal access herself, Shayia would be considered an Outside Anniate
7 S		0.000	281473913980691 14:04:15 14:05:06 00:51 50.712
			technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in
			hether end-user security training would be beneficial?
		1	Application security testing
		2	Social engineering
		3	Network sniffing
	-	4	Vulnerability scanning
8 S		4.000	281473913980691 14:05:07 14:07:25 02:18 137.977
0.0			etwork-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 Physical Physic
9 S		4.000	281473913980691 14:07:26 14:08:14 00:48 48.607
	In session		cking, an attacker relies on to connect and authenticate, and will then take over the session.
		2	hijacker activity victim server
		3	correct time
	+	4	legitimate user
			1.00
0 S		4.000	281473913980691 14:08:15 14:09:50 01:35 95.001
	restricte	d area	or 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 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 open so that he can enter.
	What is	the be	est 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
		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 Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
l	1	-	1. 22. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2. 2
1 S		4.000	281473913980691 14:09:51 14:10:43 00:52 52.631
	These a	re com	nmon 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
		0.000	281473913980691 14:10:44 14:12:23 01:39 98.776
22 S			es social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legiti
2 S	This atta	ack use	es social engineering techniques to trick users into accessing a fake Web site and divulging personal information. Attackers send a legiti 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.
2 S	This atta	ack use e-mail 1	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. Switch and bait attack
2 S	This atta	ack use	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.





		4 Wiresharp attack						
23 S		4.000		281473913980691	14:12:24	14:13:01	00:37	36.698
	How w	ould you	ı preven	t session hijacking attac	cks?			
	+	1	Using u	unpredictable sequence	numbers secures sessions aga	ainst hijacking		
		2	Using b	piometrics access token	s secures sessions against hija	cking		
		3	Using h	nardware-based authen	tication secures sessions again	st hijacking		
		4	Using r	non-Internet protocols lik	ke http secures sessions agains	st hijacking		
		•						
24 S		4.000		281473913980691	14:13:01	14:14:59	01:58	118.048
	In sess	sion hija	cking att	ack, attacker steals a	which is used to get into the sy	stem and snoop the data.		
		1	compu	ter MAC Address				
		2	user va	alidation				
		3	networ	k connection				
	+	4	valid se	ession ID				
		•						<u> </u>
25 S		0.000		281473913980691	14:15:00	14:15:40	00:40	39.277
	The m	ost comi	monly us	sed webserver is				
		1	IIS					
		2	Apache	9				
		3	Tomca	t				
	-	4	Nginx					



4

4.000

7 S

sniffing session

281473913980685

13:40:27

14:14:49



test: (Reg Ganjil 2017-2018) EH1-A: Kuis-03 (Reg Ganjil 2017-2018) EH1-A: Kuis-03 surname: 1572030 ANDIKA MULYAWAN DWI PR name: 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 (0%) correct: wrong: (0%) unanswered: (0%) (0%) undisplayed: points: 72.000 / 100.000 (72%) - PASSED end [hh:mm:ss] time [mm:ss] reaction [sec] points start [hh:mm:ss] 1 S 4.000 281473913980685 13:30:10 13:32:37 02:27 146.698 What is the key advantage of Session Hijacking? It can be easily done and does not require sophisticated skills. You cannot be traced in case the hijack is detected. You can take advantage of an authenticated connection 3 4 You can successfully predict the sequence number generation. 2 S 281473913980685 13:32:37 0.000 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? Social engineering Network sniffing 2 Vulnerability scanning 3 Application security testing 4 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? Password Sniffing Spoofing 2 Password Guessing 3 4 Session Hijacking 281473913980685 13:34:17 13:37:01 02:44 4 S 0.000 163.74 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 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? She would be considered an Insider Affiliate Shayla is an Insider Associate since she has befriended an actual employee 2 3 Since Shayla obtained access with a legitimate company badge; she would be considered a Pure Insider 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? 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 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 TCP session computer session 2 3 spoofing session

page 1 / 4

73.252

34:22





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		

	1	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
				cret double fudge cookie recipe. Ja		
1.	U			has been a problem with some ac		, ,
	•		. , ,	amiss, and parts with her passwo	rd. Jack can now ac	cess Brown Co.'s
compu	uters with	n a valid user name and passwo	ord, to steal the cookie recipe.			
\A/b at (المامة م	ttook is being illustrated bars?				
vvnati	1	ttack is being illustrated here?				
-	1	Reverse Engineering				
	2	Reverse Psychology				
+	3	Social Engineering				
	4	Spoofing Identity				
			1	1		
16 S	4.000	281473913980685	13:55:35	13:57:12	01:37	97.571
000	urs whe	n an intruder maliciously alters v	visual appearance of a web pa	ige.		
	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 con	ext of Computer Security, which	h of the following statements of	describes Social Engineering best?	>	
+	1	Social Engineering is the act of	of getting needed information f	rom a person rather than breaking	into a system	
	2	Social Engineering is a trainin	g program within sociology stu	ıdies		
	3	Social Engineering is the act of	of publicly disclosing information	on		
	4	5 5		ource to perform time accounting		
18 S	4.000	281473913980685	13:57:46	13:58:39	00:53	53.286
				directories outside of the web serv		
	1	Port Scanning			,	
	2	Data Sniffing				
	3	SQL Injection				
+	4	Directory traversal				
т .	4	Directory traversar				
10.01	4.000	204 47204 2000005	12,50,20	12,50,20	00.50	40.000
19 S		281473913980685	13:58:39	13:59:29	00:50	49.926
ın a	-	acker pretends to be another us	ser or machine to gain access.	-		
-	1	MAC Address attack				
	2	factor attack				
	3	sniffing attack				
+	4	spoofing attack				
				1		
20 S	4.000	281473913980685	13:59:29	13:59:33	00:04	3.552
The m	ost com	monly 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
		easure of session hijacking is		•		•
-	1	using firewall				
	2	using encryption				
1		using static ARP				
-	3					
	4	-				
		using IDS				
22.8	4	using IDS	14.01.40	14.02.07	00.27	27 707
	4.000	using IDS 281473913980685	14:01:40	14:02:07	00:27	27.797
	4.000 sion hija	using IDS 281473913980685 cking, an attacker relies on to		14:02:07 and will then take over the session.	00:27	27.797
In sess	4.000 sion hija	using IDS 281473913980685 cking, an attacker relies on to victim server			00:27	27.797
	4.000 sion hija 1 2	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user			00:27	27.797
In sess	4.000 sion hija 1 2 3	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time			00:27	27.797
In sess	4.000 sion hija 1 2	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user			00:27	27.797
In sess	4.000 sion hija 1 2 3 4	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity	o connect and authenticate, an	nd will then take over the session.		
+ + 23 S	4.000 sion hija 1 2 3 4	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685	o connect and authenticate, and	nd will then take over the session. 14:04:57	02:50	70.984
In sess +	4.000 sion hija 1 2 3 4	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685	o connect and authenticate, and	nd will then take over the session.	02:50	
+ + 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong	o connect and authenticate, and authenticate and authenticate, and authenticate, and authenticate and authenticate, and authenticate and authe	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ + 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would	o connect and authenticate, and authenticate, and authenticate, and authenticate, and authenticate, and authenticate, and authenticate and authenticate, and	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ + 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t context 1	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would The connection can be taken of	14:02:07 g authentication. He is not confi	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would The connection can be taken of Token security is not widely us	14:02:07 g authentication. He is not confi	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t context 1	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would The connection can be taken of	14:02:07 g authentication. He is not confi	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ + 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would The connection can be taken of Token security is not widely us	14:02:07 g authentication. He is not confi	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	
+ + 23 S John is	4.000 sion hija 1 2 3 4 0.000 s using t context 1 2 3	using IDS 281473913980685 cking, an attacker relies on to victim server legitimate user correct time hijacker activity 281473913980685 okens for the purpose of strong of Session hijacking why would The connection can be taken of Token security is not widely us A token is not considered strong	14:02:07 g authentication. He is not confi	nd will then take over the session. 14:04:57 ident that his security is consideral	02:50	





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?

	ypt transmitted and transmitte					
+	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	
	The	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						





surname: 1572025

name: YOGI KOSIM SINDUDIBROT

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

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%)

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

	р	oints: 65.000 / 100.000 (659	%) - NOT PASSED					
#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec		
ısl	5.000	281473913980692	14:06:54	14:07:49	00:55	55.324		
			are injected by attacker via in		00.00	00.02		
	1	Directory Traversal						
+		SQL Injection						
	3	Cookie Poisoning						
	4	XSS						
S	0.000	281473913980692	14:07:50	14:08:41	00:51	50.972		
Ider	ntify SQL in	jection attack from the HTTP	requests shown below:		<u>'</u>	1		
	1			20src=%22http%3a%2f%2fwww.y	ourser			
		ver.c0m%2fbadscript.js%22%		2/000/000/ (#: # 0/00				
	3		in/bad.cgi?foo=%fc%80%80	%80%80%ar/bin/is%20-ai Bbupdate%20usertable%20set%2	20nace wd9/ 2d9/ 27h Av0r	9/ 279/ 2h 9/ 00		
_	4		ole?accountnumber=67891&c		:0pass wu /83u /827 11AXU1	/621 /63D /600		
		The part of the pa						
3 S	5.000	281473913980692	14:08:43	14:11:22	02:39	158.81		
The	se are web	application components, exc	ept					
+		Web Browser						
	2	User Permission						
	3 4	Web Server Data Store						
	4	Data Stole						
S	5.000	281473913980692	14:11:50	14:13:06	01:16	75.984		
'	at techniqu		nise a database? that executes an operating sy	stem command to compromise a				
	2	•		ccess with higher-than-expected				
+	3 4		n the system using XSS attacl	SQL injection technique to penetr	ate a target system			
		Simility can delace content of	Title system using 700 attack	<u> </u>				
S	5.000	281473913980692	14:13:07	14:14:35	01:28	87.737		
	-	ncern as attackers can exploi	t these flaws to perform or cre	ate a base for most of the web ar	oplication attacks, such a	s: XSS and buffer		
ove	rflow.	Defends and animation						
	2	Default authorization Session management						
	3	SQL injection						
+	-	Input validation flaws						
	•							
SS	0.000	281473913980692	14:14:36	14:15:30	00:54	54.451		
- 1	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	n displays server error. What is	s wrong with the web applicat	on?				
	1	User input is not sanitized	-					
	2	The ISP connection is not re		·	<u> </u>			
	3	The web server may be dow	n					
-	4	The email is not valid						
s	5.000	281473913980692	14:15:31	14:16:36	01:05	64.89		
		st description of SQL Injection		14.10.30	01.00	04.03		
+			nauthorized access to a datab	ase.				
	2	It is a Denial of Service Attac						
	3		ck between your SQL Server	and Web App Server.				
	1 4	It is an attack used to madify	and the factor and all and the second					





									TELEVICE STATE
8 S	5.000)	281473913980692	14:16	6:36	14:19:07	02	2:31	150.206
	attack can	be done	by providing the wrong in	put value to the	web services	by the attacker and gainir	na control over the	SQL. LDAF	P. XPATH, and shell
	commands.		.,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,			.,	3	,	, , , , , , , , , , , , , , , , , , , ,
i	+ 1	Param	eter manipulation						
	2		validation						
ŀ	3		oisoning						
-	4		misconfiguration						
Į	4	Server	misconinguration						
9 S	0.000	`	281473913980692	11.10	0.07	14.04.40	00	.44	464 202
93				14:19	9.07	14:21:48	02	2:41	161.303
-			lation is an example of	. аттаск.					
	1		misconfiguration						
-	2		validation						
	3		ervice routing issues						
Į	- 4	XML p	oisoning						
10 S	5.000		281473913980692	14:21		14:25:06		3:17	196.882
	see if SQL In	jection w	do a web application second be possible. Contact that Bob should use	•		e site is dynamic and must request?	make use of a ba	ack end data	base. Bob wants to
İ	1		e Quote	·		•			
	2		Column						
ŀ	3		nation Mark						
ł	+ 4	Single							
l	, ,	_ Cirigie	~~~~						
11 S	5.000)	281473913980692	14:25	5:07	14:25:49	00):42	41.394
113						14.25.49	00	,. + ∠	41.394
ļ			rabilities and inject malici	ous code into sy	ystern files.				
	1		rk Access						
ļ	2	_	n Fixation						
	3	_	Services						
	+ 4	File inj	ection						
12 S	5.000		281473913980692	14:25	5:49	14:26:34	00):45	44.337
	can be dor	ne by cha	nging the information ins	ide the cookie.			•		
	1		ory Traversal						
İ	2	XSS	,						
i	+ 3		Poisoning						
ł	4		dated Input						
Į	7	Onvan	dated input						
13 S	0.000	`	281473913980692	14:26	2.25	14:32:15	0.5	5:40	339.828
13.3						ries to break the validation			
	stored on the		reis exploits the vullierat	miles in the wer	servers and t	lies to break the validation	i illetilous to get a	iccess to the	comindential data
-			micoonfiguration						
-	1	_	misconfiguration						
-	2		validation						
	- 3		ervice routing issues						
Į	4	XML p	oisoning						
									ı
14 S	0.000		281473913980692	14:32		14:33:39	01	:24	83.386
7	SQL injection	ı, XSS, aı	nd Buffer Overflows can I	oe caused by	vulnerabilities				
Ī	1	Cookie	Poisoning			<u> </u>			
İ	2	Unvali	dated Input						
İ	- 3		ory Traversal						
f	4	XSS	<u>,</u>						
l		1							
15 S	0.000	<u> </u>	281473913980692	14:33	3.30	14:35:11	04	:32	91.4
100			cess to SOAP messages				1 0	.02	J 1.4
-				uiat ale commit	annoated betWe	en two enupolitis.			
-	1		misconfiguration						
	2		ervice routing issues						
ļ	- 3		oisoning						
Į	4	Client	validation						
16 S	5.000)	281473913980692	14:35	5:11	14:35:29	00):18	17.419
	With increasi	ng depen	dence, web applications	and web service	es are increas	ngly being targeted by va	rious that result	s in huge re	venue loss for the
	organizations	S							
İ	1	comm	ents						
İ	2	conter	nts						
ŀ	3	multim							
ł	+ 4	attacks							
l		Janack	<u> </u>						
17 S	F 000	1	201/72012000000	14:35	5:30	14.25.52	00	1.22	22.267
1/3	5.000		281473913980692			14:35:53	00):23	23.267
-			by using and they wi	ii be abie to acc	ess restricted	unectones.			
Į	1	Cookie	Poisoning						





+	2	Directory Traversal
	3	XSS
	4	Unvalidated Input

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

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								
	outcom	e.							
		1 Login							
	2 Attack vector								
	-	3	SQL command						
[4	Firewall						





test: (Reg Ganjil 2017-2018) EH1-A: Kuis-04 (Reg Ganjil 2017-2018) EH1-A: Kuis-04 surname: 1572030 ANDIKA MULYAWAN DWI PR name: 1572030 user: 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%) (0%) undisplayed: points: 60.000 / 100.000 (60%) - NOT PASSED end [hh:mm:ss] points start [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? Jimmy can submit user input that executes an operating system command to compromise a target system Jimmy can utilize this particular database threat that is an SQL injection technique to penetrate a target system Jimmy can deface content on the system using XSS attack Jimmy can utilize an incorrect configuration that leads to access with higher-than-expected privilege of the database 2 S 281473913980685 14:11:49 14:08:06 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? Single Quote Exclamation Mark 2 Double Quote 3 4 Semi Column 0.000 281473913980685 3 S 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 XML poisoning Client validation 2 3 Server misconfiguration Parameter manipulation 4 281473913980685 14.14.19

4 0	0.000		261473913960665	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 recent								
	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 o	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		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 S	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.	_									

overflo	W.	
	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				
	•					
5 S	0.000	281473913980685	14:29:51	14:31:07	01:16	76.044
What i	s the be	st description of SQL Injection?			-	•
	1	It is an attack used to gain una	authorized access to a databa	se.		
	2	It is a Denial of Service Attack				
-	3	It is an attack used to modify of	code in an application.			
	4	It is a Man-in-the-Middle attac		nd Web App Server.		
		•	•	• • • • • • • • • • • • • • • • • • • •		
SS	0.000	281473913980685	14:31:07	14:31:25	00:18	17.988
By 8	attack, th	ne attackers exploits the vulnera	abilites in the web servers and	tries to break the validation me	ethods to get access to the	e confidential data
	on the s				J	
	1	XML poisoning				
	2	Server misconfiguration				
-	3	Client validation				
	4	Web service routing issues				
7 S	5.000	281473913980685	14:31:25	14:31:46	00:21	20.864
With ir	ncreasing	g dependence, web application	s and web services are increa	singly being targeted by various	s that results in huge re	venue loss for the
	zations.				· ·	
	1	contents				
	2	multimedias				
+	3	attacks				
	4	comments				
	•					
8 S	5.000	281473913980685	14:31:46	14:32:13	00:27	27.082
	0.000	20147001000000		11.02.10	00. <u>-</u> 1	
		njection attack from the HTTP re		11.02.10	00.27	
			equests shown below:		00.27	
	y SQL in	njection attack from the HTTP rehttp://www.xsecurity.com/cgiir	equests shown below: n/bad.cgi?foo=%fc%80%80%			
	y SQL in	jection attack from the HTTP re http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22%	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e	.80%80%af/bin/ls%20-al 0src=%22http%3a%2f%2fwww.		
	y SQL in	pjection attack from the HTTP re http://www.xsecurity.com/cgiir http://www.myserver.com/scri	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e	.80%80%af/bin/ls%20-al 0src=%22http%3a%2f%2fwww.		
	y SQL in	pjection attack from the HTTP re http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl	equests shown below: 1/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre	.80%80%af/bin/ls%20-al 0src=%22http%3a%2f%2fwww.	yourser	
Identify	y SQL in	pjection attack from the HTTP re http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl	equests shown below: 1/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre	.80%80%af/bin/ls%20-al 0src=%22http%3a%2f%2fwww. editamount=999999999	yourser	
Identify +	y SQL in 1 2 3 4 5.000	http://www.myserver.com/sea http://www.victim.com/eximus/ http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea	equests shown below: 1/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?lname=smith%27%38	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .bupdate%20usertable%20set% 14:32:49	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
Identify +	y SQL in 1 2 3 4 5.000	http://www.myserver.com/sea http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea	equests shown below: 1/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?lname=smith%27%38	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .bupdate%20usertable%20set% 14:32:49	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
H H H H H H H H H H H H H H H H H H H	y SQL in 1 2 3 4 5.000 as forgot	http://www.myserver.com/sea http://www.victim.com/eximus/ http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea	equests shown below: 1/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?lname=smith%27%38	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .bupdate%20usertable%20set% 14:32:49	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother email	http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20;3e%3c%2fscript%3e le?accountnumber=67891&crerch.asp?lname=smith%27%3t	.80%80%af/bin/ls%20-al .8cc=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother email	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?lname=smith%27%3l 14:32:13 bookstore. The web applicatio wrong with the web applicatio	.80%80%af/bin/ls%20-al .8cc=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother emapplication 1	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?lname=smith%27%3l 14:32:13 bookstore. The web applicatio wrong with the web applicatio	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother emapplication 1 2	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3t 14:32:13 bookstore. The web application wrong with the web application able	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother emapplication 1	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. n displays server error. What is The ISP connection is not reliated the email is not valid.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3t 14:32:13 bookstore. The web application wrong with the web application able	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother emapplication 1 2	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3t 14:32:13 bookstore. The web application wrong with the web application able	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
+ OS Liza ha	y SQL in 1 2 3 4 5.000 as forgother email polication 1 2 3 3	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. n displays server error. What is The ISP connection is not reliated the email is not valid.	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3t 14:32:13 bookstore. The web application wrong with the web application able	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
Hentify Hentify Henters The apple Henters The app	y SQL in 1 2 3 4 5.000 her ema polication 1 2 3 4 0.000	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. In displays server error. What is The ISP connection is not reliant the email is not valid The web server may be down User input is not sanitized	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3I 14:32:13 bookstore. The web application wrong with the web application able 14:32:49	.80%80%af/bin/ls%20-al .80c=%22http%3a%2f%2fwww. .editamount=999999999 .pupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s	yourser 20pass wd%3d%27hAx0i	%27%3b%00 36.367
Hentify Hentify Henters The apple Henters The app	y SQL in 1 2 3 4 5.000 her ema polication 1 2 3 4 0.000	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. In displays server error. What is The ISP connection is not reliate the email is not valid The web server may be down User input is not sanitized	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3I 14:32:13 bookstore. The web application wrong with the web application able 14:32:49	.80%80%af/bin/ls%20-al .bsrc=%22http%3a%2f%2fwwweditamount=999999999 .oupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s .n?	yourser 20pass wd%3d%27hAx0i 00:36 to that they can send her t	%27%3b%00 36.367 he password. Liza
Hentify Hentify Henters The apple Henters The Section 1	y SQL in 1 2 3 4 5.000 as forgother emails optication 1 2 3 4 4 0.000 are som 1	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. In displays server error. What is The ISP connection is not reliant the email is not valid The web server may be down User input is not sanitized	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3I 14:32:13 bookstore. The web application wrong with the web application able 14:32:49	.80%80%af/bin/ls%20-al .bsrc=%22http%3a%2f%2fwwweditamount=999999999 .oupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s .n?	yourser 20pass wd%3d%27hAx0i 00:36 to that they can send her t	%27%3b%00 36.367 he password. Liza
Hentify Hentify Henters The apple Henters The Section 1	y SQL in 1 2 3 4 5.000 her ema pplication 1 2 3 4 0.000 are som	http://www.xsecurity.com/cgiir http://www.xsecurity.com/cgiir http://www.myserver.com/scri ver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. In displays server error. What is The ISP connection is not reliant is not valid The email is not valid The web server may be down User input is not sanitized 281473913980685 ne of the major web application	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3I 14:32:13 bookstore. The web application wrong with the web application able 14:32:49	.80%80%af/bin/ls%20-al .bsrc=%22http%3a%2f%2fwwweditamount=999999999 .oupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s .n?	yourser 20pass wd%3d%27hAx0i 00:36 to that they can send her t	%27%3b%00 36.367 he password. Liza
Hentify Hentify Henters The apple Henters The Section 1	y SQL in 1 2 3 4 5.000 as forgother emails optication 1 2 3 4 4 0.000 are som 1	pjection attack from the HTTP re http://www.xsecurity.com/cgiir http://www.myserver.com/scriiver.c0m%2fbadscript.js%22% http://www.victim.com/exampl http://www.myserver.com/sea 281473913980685 tten her password to an online lail liza@yahoo.com'. In displays server error. What is The ISP connection is not relia The email is not valid The web server may be down User input is not sanitized 281473913980685 1281473913980685 1281473913980685 13916 of the major web application Cross-site scripting	equests shown below: n/bad.cgi?foo=%fc%80%80% pt.php?mydata=%3cscript%20 .3e%3c%2fscript%3e le?accountnumber=67891&cre rch.asp?Iname=smith%27%3I 14:32:13 bookstore. The web application wrong with the web application able 14:32:49	.80%80%af/bin/ls%20-al .bsrc=%22http%3a%2f%2fwwweditamount=999999999 .oupdate%20usertable%20set% 14:32:49 .n asks her to key in her email s .n?	yourser 20pass wd%3d%27hAx0i 00:36 to that they can send her t	%27%3b%00 36.367 he password. Liza





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%)

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

#	poin	ts	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]			
1 S	4.00	0	281473913983769	13:46:03	13:52:46	06:43	7.885			
	These are th	e impact	of webserver attacks, exce	ept						
	1	Webs	ite defacement							
	2	Data	heft							
[3	Comp	romise of user accounts							
Į	+ 4	OS pa	atch updated							
1	4.00	•	00447004000700	10.50.10	40.50.57	00.44	10.044			
2 S	4.00		281473913983769	13:52:46	13:52:57	00:11	10.841			
1	can be done by changing the information inside the cookie. + 1 Cookie Poisoning									
ŀ	2	XSS	c i olsoriing							
ı	3		ory Traversal							
İ	4		idated Input							
3 S	4.00		281473913983769	13:52:57	13:53:07	00:10	9.647			
Ī			ndence, web applications a	and web services are increas	singly being targeted by various	that results in huge re-	venue loss for the			
-	organization									
-	1		nedias							
ŀ	2	conte								
ŀ	+ 3	attack								
L	4	COITIII	lents							
1 S	4.00	0	281473913983769	13:53:07	13:53:11	00:04	3.756			
			used webserver is		1					
Ī	1	Tomo	at							
Ī	2	Nginx								
Ī	+ 3	Apach	ne							
Į	4	IIS								
- 0	4.00	0	004470040000700	40-50-44	40.50.40	00.07	7 000			
5 S	4.00		281473913983769 arabilities and inject malicio	13:53:11	13:53:18	00:07	7.629			
ŀ	allack exp		ork Access	us code into system mes.						
ŀ	2		Services							
ŀ	+ 3		jection							
İ	4		on Fixation							
$\overline{}$	8.00		281473913983769	13:53:18	13:54:37	01:19	78.887			
0 0					f security vulnerability in their W					
0.5	,		•	,	nents to disallow users from ente	ering HTML as input into	their Web applicati			
0 0	1		olication vulnerability likely njection vulnerability	evioro III men 2011Mare;						
0 5	'									
0.5	+ 2	Cross-site scripting vulnerability								
0.5	+ 2		Cross-site Request Forgery vulnerability							
0.5	+ 2 3 4	Cross	 -site Request Forgery vulnon management vulnerabil 							
	3	Cross								
	3	Cross Sessi			13:54:49	00:12	11.622			
	4.00	Cross Sessi 0	on management vulnerabil 281473913983769 where SQL commands are	ity		00:12	11.622			
	4.00 is a type o	Cross Sessi Of attack v	on management vulnerabil 281473913983769 where SQL commands are ory Traversal	13:54:37		00:12	11.622			
	4.00 is a type of + 2	Cross Sessi O f attack v Direct SQL I	on management vulnerabil 281473913983769 where SQL commands are ory Traversal njection	13:54:37		00:12	11.622			
	4.00 is a type o 1 + 2	Cross Sessi O of attack v Direct SQL I Cooki	on management vulnerabil 281473913983769 where SQL commands are ory Traversal	13:54:37		00:12	11.622			
	4.00 is a type of + 2	Cross Sessi O f attack v Direct SQL I	on management vulnerabil 281473913983769 where SQL commands are ory Traversal njection	13:54:37		00:12	11.622			
7 S S S S S	4.00 is a type o 1 + 2	Cross Sessi O of attack v Direct SQL I Cooki XSS	on management vulnerabil 281473913983769 where SQL commands are ory Traversal njection	13:54:37		00:12	11.622			





										THE PLANT SHAPE AND ADDRESS OF THE PERSON OF
	+	2	Directo	ory traversal						
		3	Data S	•						
	<u> </u>	4		canning						
		4	FUIL S	anning						
9 S		4.000		281473913983769	13:55:01	13:55:09		80:00		7.036
	occı	urs wher	an intri	uder maliciously alters vis	sual appearance of a web pag	je.				
		1	Sniffing	g Login						
	+	2	Web d	efacement						
		3	SQL In	jection						
		4	Web se	erver DDoS						
		l	1							
10 S		4.000		281473913983769	13:55:09	13:55:23		00:14		14.804
100	By s		a attack		pilites in the web servers and t		methods to		the confi	
		on the		ers exploits the vullierab	miles in the web servers and t	nes to break the validation	memous to	ger access ic	THE COIN	identiai data
	310100	1		ervice routing issues						
	-	2		validation						
		3		oisoning						
	+	4	Server	misconfiguration						
						.				
11 S		4.000		281473913983769	13:55:23	13:55:30		00:07		6.948
	SQL ir	jection,	XSS, ar	nd Buffer Overflows can h	be caused by vulnerabilities	<u>. </u>				
	+	1	Unvalid	dated Input						
		2	Directo	ory Traversal						
		3	XSS							
		4	-	Poisoning						
			1							
12 S		0.000		281473913983769	13:55:30	13:55:57		00:27		26.454
.20	An atte		anges th		a particular user (victim) on the		er uses this		ate the vi	
				nit the data to the attacker		, was got woodate. The attack	tor doco ulic	, suring to upu	alo li lo VI	omino profile to a
	loxt iii	and th	on Subin	it the data to the attacker	i 3 database.					
	/ ifram	ne src-"	httn://w/	ww.vulnweb.com/undatei	if.php"" style=""display:none""	> < /iframe >				
	\ III aii	10 010-	тир.// •••	WW. Valimiob.com/apaato	m.pnp otyto= diopidy.none	> \/mamo>				
	 What i	e thie tw	ne of att	ack (that can use either l	HTTP GET or HTTP POST) ca	alled?				
	vviiati	1 1		er Hacking	1111 021 0111111 1 001) 0	anea:				
		2		Site Scripting						
		3		Site Request Forgery						
		3	C1055-	Sile Request Forgery						
		4	COL In	ination						
	-	4	SQL In	jection						
12.0	-		SQL In	,	42)55,57	12,50,20		00.22		24 500
13 S		0.000		281473913983769	13:55:57	13:56:29	an interaction	00:32	/han tha	31.599
13 S	While	0.000 perform	ng onlin	281473913983769 e banking using a Web b	prowser, a user receives an er	nail that contains a link to a		g Web site. W		user clicks on the
13 S	While link, ar	0.000 performinother W	ng onlin /eb brow	281473913983769 e banking using a Web b vser session starts and d	prowser, a user receives an er isplays a video of cats playing	nail that contains a link to a a piano. The next busines	s day, the ι	g Web site. W	what look	user clicks on the s like an email
13 S	While link, ar from h	0.000 performinother Wis bank,	ng onlin /eb brow indicatir	281473913983769 e banking using a Web byser session starts and d	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
13 S	While link, ar from h	0.000 perform nother W is bank, ization c	ng onlin /eb brow indicatir f a fund	281473913983769 e banking using a Web byser session starts and dong that his bank account is transfer that took place	prowser, a user receives an er isplays a video of cats playing	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
13 S	While link, ar from h	0.000 performinother Wis bank, ization o	ng onlin /eb brow indicatir of a fund Cross-	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
13 S	While link, ar from h	0.000 performing the rother Wiss bank, ization control 1	ng onlin /eb brow indicatir f a fund Cross- Cross-	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
13 S	While link, ar from h	0.000 performinother Wis bank, ization of 1 2 3	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
13 S	While link, ar from h	0.000 performing the rother Wiss bank, ization control 1	ng onlin /eb brow indicatir f a fund Cross- Cross-	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
	While link, ar from h	0.000 performinother Wiss bank, ization of 1 2 3 4	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F	281473913983769 e banking using a Web byser session starts and d ng that his bank account s transfer that took place Site Scripting Site Request Forgery orm Input Validation cking	orowser, a user receives an er isplays a video of cats playing has been accessed from a for b. What Web browser-based so	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
13 S	While link, ar from h	0.000 performinother Wis bank, ization of 1 2 3	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation	prowser, a user receives an er isplays a video of cats playing has been accessed from a for	nail that contains a link to a a piano. The next busines eign country. The email as	s day, the υ ks the user	g Web site. Waser receives to call his bar	what look nk and ve	user clicks on the s like an email
	While link, ar from h author	0.000 performinother Wiss bank, ization of 1 2 3 4	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking	orowser, a user receives an er isplays a video of cats playing has been accessed from a for b. What Web browser-based so	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author	0.000 performinother Wiss bank, ization of 1 2 3 4	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking	prowser, a user receives an er isplays a video of cats playing has been accessed from a for the What Web browser-based so 13:56:29	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author	0.000 performinother Wiss bank, ization of 2 3 4 4.000 are con	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web a	prowser, a user receives an er isplays a video of cats playing has been accessed from a for the What Web browser-based so 13:56:29	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author	0.000 performinother Wis bank, ization of 1 2 3 4 4.000 are con 1 2	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus	prowser, a user receives an er isplays a video of cats playing has been accessed from a for the What Web browser-based so 13:56:29	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author	0.000 performinother Wis bank, ization of 1 2 3 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ting System Anti Virus on Detection System	prowser, a user receives an er isplays a video of cats playing has been accessed from a for the What Web browser-based so 13:56:29	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author	0.000 performinother Wis bank, ization of 1 2 3 4 4.000 are con 1 2	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus	prowser, a user receives an er isplays a video of cats playing has been accessed from a for the What Web browser-based so 13:56:29	nail that contains a link to a a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. W iser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author	0.000 performinother Wiss bank, ization of the Wiss bank, ization of t	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a What Web browser-based so 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex	s day, the υ ks the user	g Web site. Waser receives to call his bar ompromise the	what look nk and ve	user clicks on the s like an email rify the
	While link, ar from h author These +	0.000 performinother Wiss bank, ization of the Wiss bank, ization of t	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall sing System Anti Virus on Detection System alidation.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a What Web browser-based so 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author These +	0.000 performing the Wissian Control of the W	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja	281473913983769 e banking using a Web baser session starts and drog that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effecti	prowser, a user receives an er isplays a video of cats playing has been accessed from a for . What Web browser-based so 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author These +	0.000 performing the r Wiss bank, ization of the r Wiss ba	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja Meb A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and d on the starts and d and the starts and the sta	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a What Web browser-based so a 13:56:29 application security, except 13:56:42 Ive ways to prevent Cross-site ing access to protected inform	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in seation and UI controls.	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author These +	0.000 performinather Wiss bank, ization of the following the second of the following t	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja mmon co Web A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and d ong that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation oking 281473913983769 untermeasures for web a pplication Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effective access right before allow gital certificates to auther	prowser, a user receives an er isplays a video of cats playing has been accessed from a for . What Web browser-based so . What Web browser-based so	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in selection and UI controls. g data.	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author These + Which	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the r Wiss bank, ization of the r Wiss bank, ization of the following the r Wiss bank, ization of the following the r Wiss bank, ization of the r Wiss ba	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja mmon co Web A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and d ong that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web a pplication Firewall sing System Anti Virus on Detection System allidation 281473913983769 is one of the most effective access right before allowigital certificates to auther ecurity policies and proce	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in selection and UI controls. g data.	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author These +	0.000 performinather Wiss bank, ization of the following the second of the following t	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja mmon co Web A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and d ong that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation oking 281473913983769 untermeasures for web a pplication Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effective access right before allow gital certificates to auther	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in selection and UI controls. g data.	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author - These + Which	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the room of the following the room of the roo	ng onlin /eb brow indicatir if a fund Cross- Cross- Web F Clickja mmon co Web A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effection access right before allowigital certificates to auther curity policies and proceste and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which +	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of	ng onlin /eb brow indicatir of a fund Cross- Cross- Web F Clickja nmon co Web A Operat Intrusic Input v	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effection access right before allow gital certificates to auther certificates and proceste and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except 13:56:42 application security, except ing access to protected informaticate a server prior to sending dures to define and implementation sent to a server. 13:57:09	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in selection and UI controls. g data.	ss day, the user ploited to co	g Web site. Waser receives to call his bar ompromise the operation of the control	what look nk and ve	user clicks on the s like an email rify the
14 S	While link, ar from h author - These + Which +	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effect access right before allow gital certificates to auther courity policies and procede and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except 13:56:42 application security, except ing access to protected informaticate a server prior to sending dures to define and implementation sent to a server. 13:57:09	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which +	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of the following the room of	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effection access right before allow gital certificates to auther certificates and proceste and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except 13:56:42 application security, except ing access to protected informaticate a server prior to sending dures to define and implementation sent to a server. 13:57:09	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which +	0.000 performing the results of the	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effect access right before allow gital certificates to auther courity policies and procede and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except 13:56:42 application security, except ing access to protected informaticate a server prior to sending dures to define and implementation sent to a server. 13:57:09	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which + These	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the r	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation. 281473913983769 is one of the most effect access right before allow gital certificates to auther accurity policies and proceive and escape all informatics.	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a 13:56:29 application security, except 13:56:42 application security, except ing access to protected informaticate a server prior to sending dures to define and implementation sent to a server. 13:57:09	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which + These	0.000 performing the Wissing Stank, ization of the Roman Stank Sta	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja mmon co Web A Operat Intrusic Input v bllowing Verify a Use dig Use se Validat ntermea anonyr enable incomi	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ing System Anti Virus on Detection System alidation. 281473913983769 is one of the most effect access right before allow gital certificates to auther peurity policies and proceive and escape all informatical surveys of the country of the count	and the state of t	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the control of	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which + These	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of t	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja mmon co Web A Operat Intrusic Input v bllowing Verify a Use dig Use se Validat ntermea anonyr enable incomi	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ting System Anti Virus on Detection System alidation. 281473913983769 is one of the most effect access right before allow gital certificates to auther ecurity policies and procede and escape all informations. Survey of hacking webser mous access restriction icmp requesting traffic filtering.	and the state of t	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the o	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These + Which + These	0.000 performing the r Wiss bank, ization of the r Wiss bank, ization of the room of the following the room of the following the room of t	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja mmon co Web A Operat Intrusic Input v bllowing Verify a Use dig Use se Validat ntermea anonyr enable incomi	281473913983769 e banking using a Web byser session starts and ding that his bank account is transfer that took place. Site Scripting Site Request Forgery orm Input Validation cking 281473913983769 untermeasures for web application Firewall ting System Anti Virus on Detection System alidation. 281473913983769 is one of the most effect access right before allow gital certificates to auther ecurity policies and procede and escape all informations. Survey of hacking webser mous access restriction icmp requesting traffic filtering.	and the state of t	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex 13:56:42 13:57:09 Scripting (XSS) flaws in so lation and UI controls. g data. t proper security settings.	ss day, the user ploited to co	g Web site. Wiser receives to call his bar pmpromise the output of the o	what look nk and ve	user clicks on the s like an email rify the 12.961
14 S	While link, ar from h author - These +	0.000 performinather Wiss bank, ization of 1 2 3 4 4.000 are con 1 2 3 4 8.000 of the fc 1 2 3 4 4.000 are cou 1 2 3 4 4.000 are cou 1 4.000 are cou 1 4.000	ng onlin/eb brow indicatir fa fund Cross-Cross-Cross-Web F Clickja mmon co Web A Operat Intrusic Input v bllowing Verify a Use dig Use se Validat ntermea anonyr enable incomi	281473913983769 e banking using a Web byser session starts and d og that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation oking 281473913983769 untermeasures for web a pplication Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effective access right before allow gital certificates to auther ecurity policies and proceive and escape all informations access restriction icmp request ing traffic filtering rulnerabilities immediatel	13:56:42 In a server prior to sendir dures to define and implemention sent to a server. 13:57:09 Vers, except	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex a security vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerab	ss day, the user ploited to co	g Web site. We ser receives to call his bar ompromise the operation of the control of the contro	what look nk and ve	user clicks on the s like an email rify the 12.961 26.694 10.061
14 S	While link, ar from h author - These +	0.000 performinather Wiss bank, ization of 1 2 3 4 4.000 are con 1 2 3 4 8.000 of the fc 1 2 3 4 4.000 are cou 1 2 3 4 4.000 are cou 1 4.000 are cou 1 4.000	ng onlin/eb brow indicatir of a fund Cross-Cross-Web F Clickja mmon co Web A Operat Intrusic Input v bllowing Verify a Use dig Use se Validat ntermea anonyr enable incomi patch v	281473913983769 e banking using a Web byser session starts and d og that his bank account is transfer that took place Site Scripting Site Request Forgery orm Input Validation oking 281473913983769 untermeasures for web a pplication Firewall ing System Anti Virus on Detection System alidation 281473913983769 is one of the most effective access right before allow gital certificates to auther incurity policies and proceive and escape all informative access restriction icmp requesting traffic filtering rulnerabilities immediatel	prowser, a user receives an er isplays a video of cats playing has been accessed from a for a what Web browser-based so a second process and a second process are a second process. What Web browser-based so a second process are a second process. It is a second process and a second process are process and a second process. It is a second process are process and a second process. It is a second process are process are process	nail that contains a link to a piano. The next busines eign country. The email as ecurity vulnerability was ex a security vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerability vulnerab	ss day, the user ploited to co	g Web site. We ser receives to call his bar ompromise the operation of the control of the contro	what look nk and ve	user clicks on the s like an email rify the 12.961 26.694 10.061



User Permission
Data Store
Web Browser

2



		2	Default accounts with their of	· · · · · · · · · · · · · · · · · · ·							
		3	Installing the server with def	ault setting							
		4	Security flaws in ther server	OS							
18 S		4.000 281473913983769 13:57:27 13:57:36 00:09 8.842									
	atta		e done by providing the wron	g input value to the web services	by the attacker and gaining co	ntrol over the SQL, LDAP,	XPATH, and she				
		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				
	and ar	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, exc	cept							
	-	1	Web Server								
		2	User Permission								





test: (Reg Ganjil 2018-2019) EH1-A: Kuis-05 (Reg Ganjil 2018-2019) EH1-A: Kuis-05 surname: 1672039 ANDRIANUS ALVIEN name: 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%) (0%) unanswered: (0%) undisplayed: points: 92.000 / 100.000 (92%) - PASSED start [hh:mm:ss] end [hh:mm:ss] time [mm:ss] reaction [sec] points 1 S 4.000 281473913983770 13:46:05 13:46:41 00:36 35.349 These are the impact of webserver attacks, except . Data theft 1 Website defacement Compromise of user accounts 3 4 OS patch updated 281473913983770 13:46:41 13:46:55 00:14 13.877 2 S 4 000 These are countermeasures of hacking webservers, except ... anonymous access restriction patch vulnerabilities immediately 2 3 enable icmp request 4 incoming traffic filtering 281473913983770 3 S 4.000 13:46:55 13:47:56 01:01 61.207 By ... attack, the attackers exploits the vulnerabilities in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers. XML poisoning Server misconfiguration Client validation 3 4 Web service routing issues 281473913983770 13:47:56 13:48:24 28.294 4 S 00:28 4.000 can be done by changing the information inside the cookie. Directory Traversal Cookie Poisoning 2 3 Unvalidated Input 4 XSS 5 S 281473913983770 13:48:24 13:48:39 00:15 14.467 attack can gives access to SOAP messages that are communicated between two endpoints. Web service routing issues Client validation 3 XML poisoning 4 Server misconfiguration 281473913983770 6 S 4.000 13:48:39 13:48:53 00:14 13.576 .. occurs when an intruder maliciously alters visual appearance of a web page. Sniffing Login Web server DDoS Web defacement 3 SQL Injection 4 7 S 281473913983770 13:48:53 13:50:38 01:45 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? Cross-Site Request Forgery Web Form Input Validation 2 3 Clickjacking

		4	Cross-	Site Scripting				
8 S		4.000		281473913983770	13:50:38	13:51:21	00:43	43.396
	In at	tack, att	ackers ı	use "/(dot-dot-slash)" s	equence to access restricted di	rectories outside of the web ser	ver 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
AJA		manipulation is an example of atta	ack.			
	1	Web service routing issues				
	2	Server misconfiguration				
	3	XML poisoning Client validation				
+	4	Client validation				
10 S	8.000	281473913983770	13:51:31	13:52:05	00:34	33.346
		testing a web application, it is very us				
		e response to find vulnerabilities. You				
	ners.					
Wha		ol will help you find web vulnerabilities	s?			
	1	Maskgen				
+	2	Burpsuite				
	3	Proxychains				
		Dimitry				
11 S	4.000	281473913983770	13:52:05	13:52:17	00:12	12.27
		XSS, and Buffer Overflows can be ca			00.12	12.21
1	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
Whic		llowing is one of the most effective w			are applications?	
	1	Verify access right before allowing a	· · · · · · · · · · · · · · · · · · ·			
	2	Use digital certificates to authentica				
	3 4	Use security policies and procedure		nt 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
		ncern as attackers can exploit these				
over	flow.	•		·	•	
	1	Default authorization				
	2	Session management				
+	3	Input validation flaws				
	4	SQL injection				
440	4.000	00447004000770	10.51.10	10.54.07	00.00	0.000
14 S	4.000	281473913983770 monly used webserver is	13:54:18	13:54:27	00:09	9.032
_		Apache				
- +	2	Nginx				
-	3	IIS				
	4	Tomcat				
	1					
15 S	0.000	281473913983770	13:54:27	13:54:51	00:24	23.142
		anges the profile information of a par		e target website. The attacker u	ses this string to update	the victim's profile to a
text	file and th	en submit the data to the attacker's d	atabase.			
		http://www.vaulousekkd-r	n	l lifeama		
< ifra	arne src="	http://www.vulnweb.com/updateif.php	p style=""display:none"	> < /iirame >		
\//ha	t is this tv	oe of attack (that can use either HTTI	P GET or HTTP POST)	alled?		
-	1	Cross-Site Request Forgery	<u> </u>	u		
	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
Thes	se are con	mon countermeasures for web appli	cation security, except			
	1	Web Application Firewall				
+	2	Operating System Anti Virus				
	3	Intrusion Detection System				
	4	Input validation				
47.01	1000	004470040000	40.55.05	10.55.00	00.45	146
17 S	4.000	281473913983770	13:55:05	13:55:20	00:15	14.6
Lines	e are con	mon web server vulnerabilities, exce	:μι			





	_//						回來是多姓民			
		1	Security flaws in ther server O	S						
İ	+	2	Proper file and directory permi	issions						
		3	Default accounts with their def	fault or no passwords						
Ī		4	Installing the server with defau	ult setting						
18 S		4.000	281473913983770	13:55:20	13:55:30	00:10	10.107			
	atta	attack exploit vulnerabilities and inject malicious code into system files.								
	+	1	File injection							
		2	Session Fixation							
		3	Web Services							
		4	Network Access							
	1			1		ı				
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?								
-	vviiai r	1	Cross-site Request Forgery vu	,						
-		2	Session management vulnera							
	+	3	Cross-site scripting vulnerabili							
ŀ	•	4	SQL injection vulnerability	9						
l			eq_mjeeden rumeraemty							
20 S		4.000	281473913983770	13:55:49	13:58:00	02:11	130.933			
	atta	ck can b	e done by providing the wrong	input value to the web services	by the attacker and gaining con	trol over the SQL, LDAP	, XPATH, and shell			
	comma	ands.								
[1	Server misconfiguration							
[2	XML poisoning							
	+	3	Parameter manipulation	·	·	·				
	1	4	Client validation							





test: (Reg Ganjil 2018-2019) EH1-A: Kuis-06 (Reg Ganjil 2018-2019) EH1-A: Kuis-06 surname: 1672051 LUKAS HANSEL GANDA name: 1672051 user: 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 (0%) correct: wrong: (0%) unanswered: (0%) (0%) undisplayed: points: 108.000 / 116.000 (93%) - PASSED end [hh:mm:ss] time [mm:ss] points start [hh: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 vulnerabilities in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers. XML poisoning Web service routing issues 2 3 Client validation Server misconfiguration 2 S 8.000 281473913983769 14:31:44 20.926 14:32:05 Attempting an injection attack on a web server based on responses to True/False questions is called which of the following? Compound SQLi Classic SQLi 2 DMS-specific SQLi 3 Blind SQLi 4 3 S 4.000 281473913983769 14:32:05 14:32:14 00:09 8.994 What is the best description of SQL Injection? It is an attack used to modify code in an application. It is an attack used to gain unauthorized access to a database It is a Man-in-the-Middle attack between your SQL Server and Web App Server. 3 It is a Denial of Service Attack. 4 281473913983769 4 S 4.000 14:32:14 14:32:22 00:08 8.307 These are some of the major web application vulnerabilities, except $\mbox{.}$ Security missconfiguration SQL injection 2 3 Cross-site scripting Login page 4 5 S 281473913983769 14:32:22 14:32:31 ... 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 Server misconfiguration XML poisoning Parameter manipulation 3 4 Client validation

6 S		4.000	281473913983769	14:32:31	14:32:40	00:09	8.936
	Attacke	rs explo	oit HTTP by using and they w	vill be able to access restricted of	lirectories.		
	+	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
	attac	k can g	ives access to SOAP messages	that are communicated between	en 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 Voles-Time Required Engrey				
1 2 Cross-Site Request Forgery	autho	rization o	of a funds transfer that took place. What Web browser-based security vulnerability was exploited to compromise the user?	
3 Clickjacking 4 200-281473913983789 14:33:00 14:33:14 00:06 8:394		1	Web Form Input Validation	
4 Cross-Site Scripting	+	2	Cross-Site Request Forgery	
9 S. 4.000		3		
SCLinjaction, XSS, and Buffer Overflows can be caused by vulnerabilities		4	Cross-Site Scripting	
SCLinjaction, XSS, and Buffer Overflows can be caused by vulnerabilities			100,000	
1 XSS 2 Coalele Poisoning + 3 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Unvalidated Input - 4 5 Coalele Poisoning				8.394
1 2 Cooke Placening	SQLI	injection,		
# 3 Unvalidated Input		2		
4 Directory Traversial	+		· · · · · · · · · · · · · · · · · · ·	
1. s a type of attack where SQL commands are injected by attacker via input data.			· · · · · · · · · · · · · · · · · · ·	
1. s a type of attack where SQL commands are injected by attacker via input data.				
1 SOL Injection 2 SSS 3 Cookies Poisoning 4 Directory Traversal 3 Cookies Poisoning 4 Directory Traversal 1 St. A000 281473913983769 14:33:23 14:33:30 00:07 7.1	10 S	4.000	281473913983769 14:33:14 14:33:23 00:09	8.647
2 XSS	is a	a type of	· · · · · · · · · · · · · · · · · · ·	
3 Cooke Poisoning	+	1		
1.5		_		
1.5 4.000			-	
With increasing dependence, web applications and web services are increasingly being targeted by various that results in huge revenue loss for the organizations, 1		4	Directory i raversai	
With increasing dependence, web applications and web services are increasingly being targeted by various that results in huge revenue loss for the organizations. 1	110	4.000	291472012092760 14/22/22 14/22/20 00:07	7.1
Contents				
1 contents 2 2 comments 3 multimedias 4 attacks 3 multimedias 4 4 attacks 3 multimedias 4 4 attacks 4 4 attacks 4 4 attacks 4 4 attacks 4 4 attacks 4 4 attacks 4 4 attacks 4 4 4 attacks 4 4 attacks 4 4 attacks 4 attacks exploit vulnerabilities and inject malicious code into system files. 1 Network Access 2 Session Fixation 4 3 File injection 4 4 Web Services 4 4 Web Services 4 4 Web Services 4 4 Web Services 4 4 Web Services 5 4 4 4 4 4 4 4 4 4	I		g asponence; not approximate not one not as including, zong angular z, nancas in man routine in negotion in a	1000 101 1110
3			contents	
# 4 attacks 4 0.00		2	comments	
2 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 4 3 File injection 4 4 Web Services 3 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 1 Web Injection 4 Web Server 5 User Permission 4 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 4 3 Single Quote 4 Double Quote 5 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 vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Massagen 4 3 Burpsuite 4 1 Proxychains 6 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 it ext file and then submit the data to the attacker's database. 4 If proxychains 6 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 it ext file and then submit the data to the attacker's database. 4 If cross-Site Scripting 5 S C Injection		3	multimedias	
attack exploit vulnerabilities and inject malicious code into system files. 1 Network Access 2 Session Fixation 4 Web Services 3 \$ 4.000	+	4	attacks	
attack exploit vulnerabilities and inject malicious code into system files. 1 Network Access 2 Session Fixation 4 Web Services 3 \$ 4.000	1			
1 Network Access 2 Session Fixation + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 3 File injection + 4 Web Servier - 2 User Permission + 4 Web Servier - 2 User Permission + 4 Web Browser + 4 Web Browser + 4 Web Browser + 4 File File File File File File File File				6.076
2 Session Fixation	atta			
# 3 File Injection 4 Web Services 3 S				
1 Web Services		_		
These are web application components, except 1			·	
These are web application components, except 1 Web Server 2 User Permission 3 Data Store + 4 Web Browser 4 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			- THE CONTROL	
1 Web Server	3 S	4.000	281473913983769 14:33:37 14:33:40 00:03	3.201
2 User Permission 3 Data Store + 4 Web Browser	These	e are wel	p application components, except	
3 Data Store		1	Web Server	
## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 Web Browser ## 4 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. ## 4 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 ## 4 Double Quote ## 5 8 8.000		2	User Permission	
4 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 4 3 Single Quote 4 Double Quote 5 S 8.000 281473913983769 14:33:48 14:34:20 0.032 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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 3 Burpsuite 4 Proxychains 6 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 text file and then submit the data to the attacker's database. < iframe src=""http://www.vulnweb.com/updateif.php" style=""display:none" > What is this type of attack (that can use either HTTP GET or HTTP POST) called? - 1 Cross-Site Request Forgery 2 Cross-Site Request Forgery 3 SQL Injection	+	4	Web Browser	
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 4 3 Single Quote 4 Double Quote 5 S 8.000 281473913983769 14:33:48 14:34:20 0.032 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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 3 Burpsuite 4 Proxychains 6 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 text file and then submit the data to the attacker's database. < iframe src=""http://www.vulnweb.com/updateif.php" style=""display:none" > What is this type of attack (that can use either HTTP GET or HTTP POST) called? - 1 Cross-Site Request Forgery 2 Cross-Site Request Forgery 3 SQL Injection		4.000	00447704000770	0.47
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				
What is the first character that Bob should use to attempt breaking valid SQL request? 1				bob wants to
1 Exclamation Mark 2 Semi Column	366 11	SQL IIIje	sction would be possible.	
2 Semi Column + 3 Single Quote 4 Double Quote 5 \$ 8.000	What	is the fire	st character that Bob should use to attempt breaking valid SQL request?	
+ 3 Single Quote 5 S 8.000		1	Exclamation Mark	
4 Double Quote 5 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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1		2	Semi Column	
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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 Proxychains 6 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 text file and then submit the data to the attacker's database. < iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none"" > What is this type of attack (that can use either HTTP GET or HTTP POST) called? - 1 Cross-Site Request Forgery 2 Cross-Site Request Forgery 3 SQL Injection	+	3	v .	
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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 Proxychains 6 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 text file and then submit the data to the attacker's database. < iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none"" > 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	Double Quote	
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 reque and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 Proxychains 6 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 text file and then submit the data to the attacker's database. < iframe src=""http://www.vulnweb.com/updateif.php"" style=""display:none"" > 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				
and analyze the response to find vulnerabilities. You can test parameter and headers manually to get more precise results than if using web vulnerabilities scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen 4 Proxychains 6 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 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				
scanners. What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen + 3 Burpsuite 4 Proxychains 6 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 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				
What proxy tool will help you find web vulnerabilities? 1 Dimitry 2 Maskgen + 3 Burpsuite 4 Proxychains 6 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 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		•	ie response to find vuinerabilities. You can test parameter and neaders manually to get more precise results than it using we	b vuinerability
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 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	I		ol will help you find web vulnerabilities?	
2 Maskgen + 3 Burpsuite 4 Proxychains 6 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 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	vviidt	<u> </u>		
+ 3 Burpsuite 4 Proxychains 6 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 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 Proxychains 6 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 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	+	_		
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 text file and then submit the data to the attacker's database. <irr display:none""="" style=""> 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</irr>		4	·	
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 text file and then submit the data to the attacker's database. <irr display:none""="" style=""> 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</irr>				
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	6 S	0.000	281473913983769 14:34:20 14:34:43 00:23	23.623
<pre>< 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? -</pre>				ctim's profile t
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	text fi	le and th	en submit the data to the attacker's database.	
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	.,			
- 1 Cross-Site Request Forgery 2 Cross-Site Scripting 3 SQL Injection	< ifrai	me src="	"nttp://www.vuinweb.com/updateif.php"" style=""display:none"" > < /iframe >	
- 1 Cross-Site Request Forgery 2 Cross-Site Scripting 3 SQL Injection	\//hat	is this tu	ne of attack (that can use either HTTP GET or HTTP POST) called?	
2 Cross-Site Scripting 3 SQL Injection	vviiat			
3 SQL Injection	_			
· · · · · · · · · · · · · · · · · · ·			, ,	
		_	'	





17 S	4.000	281473913983769	14:34:43	14:34:51	00:08	7.609
ar	e major co	oncern as attackers can exploit	these flaws to perform or create	a base for most of the web	application attacks, such a	s: XSS and buffer
overf	flow.		•			
	1	Session management				
	2	SQL injection				
+	3	Input validation flaws				
	4	Default authorization				
3 S	4.000	281473913983769	14:34:51	14:35:02	00:11	10.944
		jection attack from the HTTP re		14.55.02	00.11	10.344
ident	1	-	e?accountnumber=67891&cred	tamount=999999999		
+	2		ch.asp?lname=smith%27%3bu		%20nass wd%3d%27hAx0i	%27%3h%00
	3	-	/bad.cgi?foo=%fc%80%80%80		7020pado wa 700a 7027 117 (AO)	7021 7000 7000
	4	· · · · · · · · · · · · · · · · · · ·	ot.php?mydata=%3cscript%20si		w.vourser	
		ver.c0m%2fbadscript.js%22%		- /	,	
S	4.000	281473913983769	14:35:02	14:35:10	00:08	7.582
		neans by which an attacker car	n gain access to computer or ne	twork resources in order to	deliver an attack payload o	r cause a malicious
outco	1 1	Firewall				
-	2	SQL command				
+	3	Attack vector				
+	4					
	4	Login				
s	4.000	281473913983769	14:35:10	14:35:17	00:07	7.518
ca	n be done	by changing the information in	side the cookie.			II.
	1	xss				
	2	Unvalidated Input				
+	3	Cookie Poisoning				
	4	Directory Traversal				
S	4.000	281473913983769	14:35:17	14:35:24	00:07	6.883
AJA	X routines	manipulation is an example of .	attack.			
	1	Server misconfiguration				
	2	Web service routing issues				
	3	XML poisoning				
+	4	Client validation				
	4.000	00447004000700	140504	44.05.00	00.45	11.070
2 S	4.000	281473913983769	14:35:24 dvantage of poorly designed inp	14:35:39	00:15	14.873
priva	te data or t techniqu	execute commands in the dataled does Jimmy use to compromise Jimmy can submit user input the	base. se a database? hat executes an operating syste	m command to compromise	e a target system	
		I Jimmy can utilize this particula	er database threat that is an SQ	_ injection technique to pen	etrate a target system	
+	2					
+	3	Jimmy can deface content on t		101 1 1 1 2 2		
+		Jimmy can deface content on t	the system using XSS attack configuration that leads to acce	ss with higher-than-expecte	ed privilege of the database	
	3 4	Jimmy can deface content on Jimmy can utilize an incorrect	configuration that leads to acce			7 211
BS S	4.000	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769	configuration that leads to acce	14:35:47	00:08	7.211 the password. Liza
3 S Liza	3 4 4.000 has forgo	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769	configuration that leads to acce	14:35:47	00:08	
3 S Liza	3 4 4.000 has forgo	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 tten her password to an online be	configuration that leads to acce	14:35:47	00:08	
B S Liza enter	4.000 has forgors her ema	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 ten her password to an online bail liza@yahoo.com'. n displays server error. What is	configuration that leads to acce	14:35:47 asks her to key in her email	00:08	
B S Liza enter	4.000 has forgors her ema	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 ten her password to an online bail liza@yahoo.com'. n displays server error. What is User input is not sanitized	configuration that leads to acce 14:35:39 cookstore. The web application	14:35:47 asks her to key in her email	00:08	
Liza enter	4.000 has forgors her ema	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 ten her password to an online bail liza@yahoo.com'. n displays server error. What is	configuration that leads to acce 14:35:39 cookstore. The web application	14:35:47 asks her to key in her email	00:08	
Liza enter	4.000 has forgors her ema	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 ten her password to an online bail liza@yahoo.com'. displays server error. What is User input is not sanitized The email is not valid The web server may be down	configuration that leads to acce 14:35:39 cookstore. The web application access wrong with the web application?	14:35:47 asks her to key in her email	00:08	
Liza enter	4.000 has forgo rs her ema application 1 2	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 Iten her password to an online bail liza@yahoo.com'. In displays server error. What is User input is not sanitized The email is not valid	configuration that leads to acce 14:35:39 cookstore. The web application access wrong with the web application?	14:35:47 asks her to key in her email	00:08	
SS Liza enter	4.000 has forgo rs her ema application 1 2 3 4	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 Iten her password to an online ball liza@yahoo.com'. In displays server error. What is user input is not sanitized The email is not valid The web server may be down The ISP connection is not reliant.	configuration that leads to acce 14:35:39 cookstore. The web application and the web application and	14:35:47 asks her to key in her email	00:08 so that they can send her t	he password. Liza
3 S Liza enter	4.000 has forgors her ema application 1 2 3 4.000	Jimmy can deface content on Jimmy can utilize an incorrect 281473913983769 Iten her password to an online bail liza@yahoo.com'. In displays server error. What is User input is not sanitized The email is not valid The web server may be down The ISP connection is not relia 281473913983769	configuration that leads to acce 14:35:39 cookstore. The web application access wrong with the web application?	14:35:47 asks her to key in her email	00:08 so that they can send her t	he password. Liza

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



2

3

Cookie Poisoning

Unvalidated Input



test: (Reg Ganjil 2018-2019) EH1-A: Kuis-06 (Reg Ganjil 2018-2019) EH1-A: Kuis-06 surname: 1672039 ANDRIANUS ALVIEN name: 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 (0%) correct: wrong: (0%) unanswered: (0%) (0%) undisplayed: points: 116.000 / 116.000 (100%) - PASSED end [hh:mm:ss] points start [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? The web server may be down The ISP connection is not reliable 3 User input is not sanitized 4 The email is not valid 281473913983770 2 S 14:31:18 14:31:29 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? Cross-Site Request Forgery Clickjacking 2 3 Cross-Site Scripting 4 Web Form Input Validation 281473913983770 14:31:29 14:31:40 00:11 10.682 3 S 4.000 SQL injection, XSS, and Buffer Overflows can be caused by ... vulnerabilities. Directory Traversal XSS 2 3 Cookie Poisoning Unvalidated Input 4 4 S 281473913983770 14:31:40 14:31:51 00:11 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? Double Quote 2 **Exclamation Mark** Semi Column 3 Single Quote 281473913983770 5 S 4.000 14:31:51 14:32:01 00:10 9.61 These are common countermeasures for web application security, except . Input validation 2 Operating System Anti Virus Intrusion Detection System 3 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. Client validation Server misconfiguration 3 Web service routing issues 4 XML poisoning 281473913983770 7 S 4.000 14:32:10 14:32:22 00:12 11.421 Attackers exploit HTTP by using ... and they will be able to access restricted directories. **Directory Traversal**





	4	XSS						
8 S	4.000	281473913983770	14:32:22	14:32:30	00:08	8.363		
		application components, excep		14.32.30	00.08	0.303		
11.00	1							
+	2	Web Browser						
	3	Data Store						
	4	Web Server						
						_		
9 S	4.000	281473913983770	14:32:30	14:32:39	00:09	8.814		
		g dependence, web applications	s and web services are incre	asingly being targeted by various	that results in huge re	evenue loss for the		
orgar	nizations.	comments						
	2	multimedias						
	3	contents						
+	4	attacks						
0 S	4.000	281473913983770	14:32:39	14:32:49	00:10	9.333		
ca	n be done	by changing the information in	side the cookie.					
+	1	Cookie Poisoning						
	2	Directory Traversal						
	3	XSS						
	4	Unvalidated Input						
11 S	4.000	204 47204 2002 770	14:32:49	14:33:26	00:27	26.02		
	4.000	281473913983770 njection attack from the HTTP re		14.33.20	00:37	36.92		
+	1			Bbupdate%20usertable%20set%2	Onass wd%3d%27hΔy0	r%27%3h%00		
	2	http://www.victim.com/example			opa33 wa700a702711/1x0	170217000 7000		
	3	_ '						
	1 3	http://www.xsecurity.com/cgiin	/bad.cgi?foo=%fc%80%80	%80%80%af/bin/ls%20-al				
	4	<u> </u>		%80%80%af/bin/ls%20-al 20src=%22http%3a%2f%2fwww.y	ourser			
		<u> </u>	ot.php?mydata=%3cscript%2		ourser			
12.5	4	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e	20src=%22http%3a%2f%2fwww.y		11 200		
	8.000	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26	20src=%22http%3a%2f%2fwww.y	00:11	11.388		
Wher	8.000 n you are	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%; 281473913983770 testing a web application, it is v	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher	8.000 n you are analyze th	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%; 281473913983770 testing a web application, it is v	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy	20src=%22http%3a%2f%2fwww.y	00:11	ally test every reque		
When and a scan	8.000 n you are analyze the	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is vie response to find vulnerabilitie	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter an	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
When and a scan	8.000 n you are analyze the ners. t proxy too	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is v re response to find vulnerabilitie of will help you find web vulneral Proxychains	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter an	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher and a scan What	8.000 n you are analyze therers. t proxy to 1 2	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is v re response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter an	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher and a scan	8.000 n you are analyze the ners. t proxy to 1 2 3	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is v re response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry Burpsuite	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter an	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher and a scan What	8.000 n you are analyze therers. t proxy to 1 2	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is v re response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter an	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher and a scani What	8.000 n you are analyze theres. t proxy too 1 2 3 4	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is ver response to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
Wher and a scani What	8.000 n you are analyze the ners. t proxy too 1 2 3 4.000	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is veresponse to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and re	00:11	ally test every reque		
Wher and a scani What +	8.000 n you are analyze the proxy to 2 3 4.000 4.000 Croutines	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.com/script.js%	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
When and a scani What	8.000 n you are analyze the ners. t proxy too 1 2 3 4.000 (routines	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.com/script.js%	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
When and a scani What +	8.000 n you are analyze the proxy to 2 3 4.000 4.000 Croutines	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.com/script.js%	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
When and a scani What +	8.000 n you are analyze the ners. t proxy too 1 2 3 4.000 (routines	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.com/script.js%	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
When and a scani What +	8.000 n you are analyze the ners. t proxy too 1 2 3 4 4.000 (routines 1 2 3 3 3 4 4.000 (routines 1 2 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 3 4 4.000 (routines 1 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3 3	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.c0m%2fbadscript.js%22%iver.com/s2fbadscript.js%22%iver.co	ot.php?mydata=%3cscript%2 3e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter ar bilities?	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
Wher and a scani What +	8.000 n you are analyze the ners. t proxy ton 2 3 4 4.000 (routines 1 2 3 4 4.000	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is v ver response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more	00:11 esponse. You can manua precise results than if us	ally test every reque sing web vulnerabili		
Wher and a scani What +	8.000 n you are analyze the ners. t proxy ton 2 3 4 4.000 (routines 1 2 3 4 4.000	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is vote response to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		
Wher and a scani What +	8.000 n you are analyze the ners. t proxy to 1 2 3 4.000 (routines 1 2 3 4 4.000 e are son	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is vote response to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application of Cross-site scripting	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		
Wher and a scani What +	4	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is vie response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application Cross-site scripting Login page	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		
Wher and a scani What + 13 S AJAX + 14 S Thes	4 8.000 900	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is veresponse to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application of Cross-site scripting Login page SQL injection	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		
Wher and a scani What +	4	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is vie response to find vulnerabilitie of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application Cross-site scripting Login page	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		
and a scani What + 13 S AJAX + 14 S Thes	4 8.000 900	http://www.myserver.com/scrip ver.c0m%2fbadscript.js%22%: 281473913983770 testing a web application, it is veresponse to find vulnerabilities of will help you find web vulneral Proxychains Dimitry Burpsuite Maskgen 281473913983770 manipulation is an example of Client validation XML poisoning Server misconfiguration Web service routing issues 281473913983770 ne of the major web application of Cross-site scripting Login page SQL injection	ot.php?mydata=%3cscript%23e%3c%2fscript%3e 14:33:26 ery useful to employ a proxy s. You can test parameter arbilities? 14:33:37 attack.	20src=%22http%3a%2f%2fwww.y 14:33:37 tool to save every request and rend headers manually to get more 14:33:46	00:11 esponse. You can manua precise results than if us 00:09	ally test every reque sing web vulnerabili		

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? 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. The Hacker attempted Session hijacking, in which the Hacker opened an account with the bank, then logged in to receive a session ID, 3 guessed the next ID and took over Jason's session 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 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 Input validation flaws 2 Session management SQL injection 3 Default authorization 4 17 S 281473913983770 14:34:33 00:11 10.123 4.000 14:34:44 .. 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 Parameter manipulation XML poisoning 2 3 Server misconfiguration 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? It is an attack used to modify code in an application. It is a Man-in-the-Middle attack between your SQL Server and Web App Server. 2 3 It is an attack used to gain unauthorized access to a database. It is a Denial of Service Attack. 4 19 S 4.000 281473913983770 14:35:05 00:09 8.607 14:34:56 attack exploit vulnerabilities and inject malicious code into system files File injection Session Fixation 2 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 vulnerabilities in the web servers and tries to break the validation methods to get access to the confidential data stored on the servers. XML poisoning Web service routing issues 2 Server misconfiguration 3 4 Client validation 21 S 281473913983770 14:35:18 14:35:28 4.000 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 SQL command 2 Login 3 Firewall Attack vector 22 S 8.000 281473913983770 14:35:28 14:35:43 15.465 Attempting an injection attack on a web server based on responses to True/False questions is called which of the following? Blind SQLi DMS-specific SQLi Compound SQLi 3 4 Classic SQLi 8 000 281473913983770 14:35:43 15.305 23 S 14:35:59 00:16 Which of the following is one of the most effective ways to prevent Cross-site Scripting (XSS) flaws in software applications? Use security policies and procedures to define and implement proper security settings. Use digital certificates to authenticate a server prior to sending data. Verify access right before allowing access to protected information and UI controls. 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 In	jection					
	4 Directory Traversal								