Illinois Tech Student

Hong Zhang

Exams Review Test Submission: Final Exam

# Review Test Submission: Final Exam

| | |
|---|---|
| User | Hong Zhang |
| Course | ITMS-448_IT-S-448-Parent.16S |
| Test | Final Exam |
| Started | 5/2/16 5:01 PM |
| Submitted | 5/2/16 6:35 PM |
| Due Date | 5/2/16 7:00 PM |
| Status | Completed |
| Attempt Score | 194.5 out of 198 points |
| Time Elapsed | 1 hour, 34 minutes |
| Results Displayed | Submitted Answers, Feedback, Incorrectly Answered Questions |

## Question 1

2 out of 2 points

A firewall you come across is set up with a default policy choice of implicit deny. Your boss wants to allow ssh traffic to enter the firewall. Which of the following rule types should be used to create that ssh rule?

Selected Answer: Explicit Allow Rule for SSH

## Question 2

2 out of 2 points

Which of the following standards offer all four goals of cryptographic ciphers?

Selected Answers: PGP/GPG<br>S/MIME<br>HTTPS

## Question 3

2 out of 2 points

Which of the following choices is the correct ctstate for:

When a packet is associated with a connection which has seen packets in both directions on a single port.

Selected Answer: ESTABLISHED

## Question 4

2 out of 2 points

The following is the options portion of a Snort rule:

(msg: "Exploit Kit - CrimeBoss"; reference:url,http://malwaredomainlist.org; content: "cb.php"; flow:to_server; nocase; sid: 1000005; ref:4)

Which of the following options in the above rule pertains to the actual signature that the alert is firing on?

Selected Answer: content: "cb.php"

## Question 5

5 out of 5 points

Please select "True" in order to acknowledge that you understand and agree to the following two items:

1. I will not use any of the knowledge or tools taught to me in this course in order to attack a third party without that third party's explicit written permission.

2. I understand that the reason I have been taught about various types of attacks and attack tools in this course is to help me to understand attacker techniques in order to help me better defend any computers and networks under my control against attack.

(If this question is not answered or "True" was not selected, I will need to speak with you prior to grading this exam.)

Selected Answer: True

## Question 6

5 out of 5 points

What is one difference between a typical wireless router and a typical wireless access point?

Selected Answer: The difference is a typical wireless router can connect with a mordem, DHCP server assign the internal IP addresses which works as a NAT box, or form as a VPN. The access point connects with DHCP sever, and could not assign internal IP address, or work as NAT, VPN.

Response Feedback: [None Given]

## Question 7

5 out of 5 points

Match the definition with the correct password cracking method.

Question Selected Match

| | |
|---|---|
| Can only crack a password if it is contained in the cracking program's dictionary wordlist. | B.<br>Dictionary Attack |
| Can eventually crack any password. | C.<br>Brute Force Attack |
| Takes a wordlist and pre-calculates all of the hashes and stores them in a table. | E. Lookup Table |
| Uses a lookup table but also keeps track of which usernames are mapped to which hashes. | D.<br>Reverse Lookup Table |
| Doesn't include all pre-calculated hashes and uses reduction function to reduce table size | A. Rainbow Table |

## Question 8

5 out of 5 points

How would you describe AccessData's Registry Viewer versus RegRipper?

| | |
|---|---|
| Selected Answer: | AccessData's Registry Viewer shows the log files, only some summary and RegRipper shows more details about the users' activities. You can abstract the files using RegRipper and get many information. |
| Response Feedback: | [None Given] |

## Question 9

4 out of 4 points

This question is in regards to public key cryptography.

| Question | Selected Match |
|---|---|
| Allows recipient to ensure a message has not been changed (integrity) and somewhat provides who the message came from (authentication). | B.<br>Digital Signature |
| Enforces non-repudiation and provides further strength to authentication for the message. | A.<br>Digital Certificates |
| Issues Digital Certificates to organizations. | D.<br>Root Certificate Authority |
| Mechanism to deal with invalid digital certificates. | C.<br>Certificate Revocation List (CRL) |

## Question 10

4 out of 4 points

Match the definition with the correct law/term.

| Question | Selected Match |
|---|---|
| Law against gaining unauthorized access to a "protected" computer. | B.<br>Computer Fraud and Abuse Act |
| Law against illegally storing or intercepting stored or transmitted communications without authorization. | A.<br>Electronic Communications Privacy Act |
| Law prohibiting circumvention of technological measures designed to protect a copyright. | D.<br>Digital Millennium Copyright Act |
| Computer involved in interstate of foreign commerce of communication. | C. "Protected Computer" |

## Question 11

2 out of 2 points

The four means of authenticating a user include:

1. Something you know
2. Something you have
3. Something you are

4 Something you do

Which of the following choices represent "something you have?"

Smartcard

Physical Key

## Question 12

5 out of 5 points

Describe what the Evil Twin wireless security threat entails. (Remember, an Evil Twin is not the same thing as a Rogue Access Point as there is a difference between the two.)

Selected Answer: Evil Twin is the attacker set up the wireless access point which like the legal one. When the user login, the attacker will get the user's crenditianl, such as username and password. Then, the attacker use it to access the internet.
A Rogue Access Point is an access point which is no password. when it is setted clost to the window and the attacker can access it without permission.

Response Feedback: [None Given]

## Question 13

5 out of 5 points

Match the following IDS definitions with the correct terms.

| Question | Selected Match |
|---|---|
| Monitors events between a single host and the network gateway. | C. HIDS |
| Responsible for collecting data such as packets, log files, etc. | F. Sensors |
| Monitors network traffic for a particular network segment. | A. NIDS |
| Ability to not only detect but also prevent an attack. | E. IPS |
| Receives input from one or more sensors or from other analyzers. Determines if an intrusion has occured. | B. Analyzer |
| Allows analyst to view output from IDS and /or control the beharior of the system. | D. User Interface |

## Question 14

2 out of 2 points

Which of the following are general authentication security issues?

Selected Answers: Eavesdropping
Host Attacks
Replay
Trojan Horse
DoS
Client Attacks

## Question 15

2 out of 2 points

This question relates to public key cryptography. In order the achieve Confidentiality, the **[x]** key encrypts data and the **[y]** key decrypts that data.

Specified Answer for: x public

Specified Answer for: y prviate

## Question 16

4 out of 4 points

Name at least four useful anomalies a HIDS might detect.

Selected Answer: 1. check the unusal login.
2. check the the time of logon
3. check the password.
4. check the exectuion of command.
5. check the usage of internert.

Response Feedback: [None Given]

## Question 17

2 out of 2 points

Un-partitioned space is identified by logical drive letters.

Selected Answer: False

## Question 18

5 out of 5 points

Explain what this iptables rule is basically doing overall. Then, briefly describe what each of the seven parts (argument option and value) of the rule do. (For example, "-A" is an argument and "INPUT" is the value for one of the seven parts.)

```
iptables - A INPUT -i eth0 -p tcp --sport 443 -m conntrack --ctstate ESTABLISHED -j
ACCEPT

            1         2      3     4           5              6                     7
```

Selected Answer: This rule is accept all the web page connection.
1. use the action which is input.
2. use the internet which is eth0.
3. use the protocle which is tcp.
4. the source port is 443.
5. will track the conntection.
6. the conntection state is established.
7. the action is accept.

Response Feedback: [None Given]

## Question 19

5 out of 5 points

You have been given the following information:

Ciphertext: HWDUYT

Cipher: Caesar

Shift: 5 places towards the front of the alphabet

Alphabet Scale: ABCDEFGHIJKLMNOPQRSTUVWXYZ

The decrypted plaintext is _________________

Selected Answer: crypto

## Question 20

5 out of 5 points

What is a honeypot and what is it designed to do?

Selected Answer: Honeypot is the fake host and hope the attacker to get its wrong information. It is designed to attract the hacker, collect the attacker's information and deny the attack.

Response Feedback: [None Given]

## Question 21

2 out of 2 points

Alternate Data Streams: You have an overt file named syllabus.txt. Choose the correct command to insert the message "My voice is my password." within a covert file named secret.txt which is then hidden as an ADS of the syllabus.txt file.

Selected Answer: echo "My voice is my password." > syllabus.txt:secret.txt

## Question 22

5 out of 5 points

Let's say you show up at a suspect's home and their desktop is on. Should you pull the power plug and remove the hard drive right away for imaging (yes or no)? Why or why not?

Selected Answer: No. Because we need to check if the disk is encrypted or not. If encrypted, this method will not lost all information in the disk. The best way is copying the RAM and get the part files which are not encrypted. If not encrypted, you can copy the whole physical disk, shut down the computer and remove the hard disk.

if n

Response Feedback: [None Given]

## Question 23

8 out of 8 points

Match the definitions with the correct terms.

| Question | Selected Match |
|---|---|
| Steganography | C.<br>Science of hiding messages so that the existence of the message is unknown to outsiders. |
| Cryptography | A. Science of hiding the meaning of messages that are known to exist. |
| Coding | B. |

| | |
|---|---|
| (Substituting) | Parts of a message are substituted with external letters, words, phrases, etc. |
| Transposing | F.<br>Parts of a message are moved around from one place to another within the message. |
| Hashing | H. Creation of a fixed size value using a message as a source. |
| Cryptanalyst | G. Person that tries to decipher encrypted messages. |
| Plaintext | E. Unencrypted message |
| Ciphertext | D. Encrypted message output |

## Question 24

5 out of 5 points

What are two ways a DoS could be performed on a wireless network?

Selected Answer: 1. MAC flooding
2. ARP flooding

Response Feedback: [None Given]

## Question 25

2 out of 2 points

In Steganography, an overt file is the file to hidden and the covert file is the carrier file.

Selected Answer: False

## Question 26

2 out of 2 points

In WPA, which of the two ciphers is more secure?

Selected Answer: AES

## Question 27

2 out of 2 points

In the SSH in-class lab, which tool was used to avoid having to enter the key passphrase each time a system is accessed?

Selected Answer: pageant

## Question 28

5 out of 5 points

How does NAT work and why can't hosts on the Internet directly connect to hosts sitting behind a NAT box that have been assigned addresses from the NAT box's DHCP server?

Selected Answer: NAT can assign internal IP addresses to the hosts behide it and they form a internal network. Actually, the hosts which behide the NAT box use different IP addresses comparing with the host which is outside the NAT box. Hence, there is no rout between them. That is the reason why can't hosts on the Internet directly connect to hosts sitting behind a NAT box that have been assigned addresses from the NAT box's DHCP server.

Response Feedback: [None Given]

## Question 29

2 out of 2 points

In a brute force attack against DES, knowing part of the key will not speed up the attack. True or False?

(We demoed a brute force attack in Cryptool)

Selected Answer: False

## Question 30

4 out of 4 points

You have a file called salesdoc1.

1. Via letters, what is the complete command to remove write permission from the file's group? **[a]**

2. Via letters, what is the complete command to add execute permission to all users of the file (user, group, and other) **[b]**

3. Via numbers, what is the complete command to provide the following permissions for the file (rw- --x rwx) **[c]**

4. Via numbers what is the complete command to provide the following permissions for the file (rwx -w- rw-) **[d]**

| | |
|---|---|
| Specified Answer for: a | chmod g-w salesdoc1 |
| Specified Answer for: b | chmod a+x salesdoc1 |
| Specified Answer for: c | chmod 617 salesdoc1 |
| Specified Answer for: d | chmod 726 salesdoc1 |

## Question 31

2 out of 2 points

A Kerberos Key Distribution Center (KDC) typically consists of which of the following components?

User Database

Authentication Server

Ticket Granting Server

## Question 32

5 out of 5 points

In Linux, provide a scenario where would you need to set an ACL on a file instead of just setting permissions for the file?

| | |
|---|---|
| Selected Answer: | when the user need to read, write or execute a file which is belong to another user and another group, it need to use ACL. |
| Response Feedback: | [None Given] |

## Question 33

5 out of 5 points

What is a password salt and how can it prevent an attacker using a lookup table?

| | |
|---|---|
| Selected Answer: | A password salt is some strings which is setting before the encryption. When saving the password, we will add the salt and encrypt them together. To prevent an attacker, should use different salt and the salt is greater than 8 bits in each encryption. |
| Response Feedback: | [None Given] |

## Question 34

4 out of 4 points

Steganography:  Match the following ways to hide covert data with the correct data hiding method.

| Question | Selected Match |
|---|---|
| Data is hidden by modifying part of the carrier file content such as the LSB. | C. Substitution |
| Covert data is hidden in the slack space or header of a file that the opening application ignores. | A. Insertion |
| Message is hidden in plain sight as part of the carrier file.  This is similar to the period and comma text example hiding the binary number. | B. Generation |

## Question 35

2 out of 2 points

In a passive sensor of an IDS, traffic is monitored through the use of a switch span port or network tap.

Selected Answer: True

## Question 36

2 out of 2 points

In Steganography, which of the following hiding methods will cause the file size of the original carrier file to increase when covert data is added?

Selected Answer: Insertion

## Question 37

2 out of 2 points

This question relates to Public Key Cryptography.  Bob needs to verify that a message actually came from Alice and wasn't intercepted and modified in transit.  Bob compares his hash of the message with the hash contained in the _________ that Alice sent along with the message.

Selected Answer: Digital Certificate

## Question 38

2 out of 2 points

Alternate Data Streams:  You have been provided a file named homework.txt.  Someone told you there might be an ADS named hidden.txt tied to the homework.txt.  What is the correct command to view the content of the hidden.txt file in the **Windows** command shell?

Selected Answer: more < homework.txt:hidden.txt

## Question 39

1.5 out of 2 points

Which of the following are capabilities most firewalls should have?

| | |
|---|---|
| Selected Answers: | Defines a single choke point (meaning all traffic entering the network must flow through the firewall.)<br>Creates logs of monitored security events<br>NAT, IPS/IDS |

## Question 40

2 out of 2 points

In a typical password authentication implementation, the user entered password in a form is compared directly against a plaintext representation of the password stored on the server.

Selected Answer: False

## Question 41

2 out of 2 points

Unallocated space contains deleted files.

Selected Answer: True

## Question 42

4 out of 4 points

Match the definition with the correct Iptables rule action.

| Question | Selected Match |
|---|---|
| Packet is rejected and no response is returned. | C. DROP |
| Packet is accepted through the firewall into the system. | A. ACCEPT |
| Packet is rejected and an ICMP or TCP response is returned to sender. | B. REJECT |

## Question 43

4 out of 5 points

Match the definition with the correct 802.11 wireless architecture term.

| Question | Selected Match |
|---|---|
| The wireless client (laptop, phone, etc.) | B. Station (STA) |
| Wireless network of one AP supporting one or many clients | D.<br>Basic Service Set (BSS) |
| Two or more BSSs that are connected via a wired network | A.<br>Extended Service Set (ESS) |
| This connects multiple BSSs within an ESS and allows a client to move or roam from one BSS to another BSS. | E.<br>Distribution System (DS) |
| Ad hoc wireless network where clients connect directly to each other without the use of access points. | A.<br>Extended Service Set (ESS) |

## Question 44

2 out of 2 points

The following is the header portion of a Snort rule:

```
alert  tcp  192.168.1.42  5256 -> 158.22.2.4 443
```

Answer this question by choosing which part of the above rule pertains to the Source Port.

Selected Answer: 5256

## Question 45

2 out of 2 points

Which imaging method records a bit by bit copy of an entire hard drive?

Selected Answer: Physical Drive Image

## Question 46

5 out of 5 points

What are at least four potential questions computer forensic analysis may answer?

Selected Answer:
1. find the downloads which the user try to download.
2. find the websites which the user access to.
3. find the USB's files which the user try to use.
4. find the login activies.
5. find the deleted files or unallocated disk.
6. recover the files.

Response Feedback: [None Given]

## Question 47

3.5 out of 5 points

What are the advantages and disadvantages of placing a NIDS in front of the firewall vs behind the firewall? Please answer this question in the following format by providing at least one advantage and disadvantage for each of the two scenarios:

1. Behind the firewall

Advantage:

Disadvantage:

2. In front of the firewall

Advantage:

Disadvantage:

Selected Answer:
1. Behind the firewall
Advantage: there is no noise.
Disadvantage: depends on the firewall's setting rules.
2. In front of the firewall
Advantage: can deny all attackers' traffices.
Disadvantage: there are many noise and will affect you to distugish the traffice which one is from the attacker.

Response Feedback: [None Given]

## Question 48

2 out of 2 points

In Steganography, most any covert file type can theoretically be hidden within a carrier file and the nature of the covert file is irrelevant.

Selected Answer: True

## Question 49

2 out of 4 points

Match the definition with the correct type of firewall.

| Question | Selected Match |
|---|---|
| Uses SOCK-ified client applications.  Example is torsocks. | A. Application-level proxy firewall. |
| Applies rules to each incoming and outgoing packet based on IP header, TCP/UDP headers, firewall interface. | C. Stateless packet filtering firewall |
| Evaluates contents of each packet and keeps track of connection state in order to make desicions.  Specifially looks at sequence and ack numbers from TCP headers. | D. Stateful inspection firewall |
| Isolates client and server from each other and can look into the packet payloads in order to permit or deny a connection. | B. Circuit-level proxy firewall |

## Question 50

2 out of 2 points

What are the four goals of cryptographic ciphers?

Selected Answers: Integrity
Confidentiality
Authentication
Non-Repudiation

## Question 51

2 out of 2 points

In Kerberos, the Ticket Granting Ticket (TGT) allows direct access to the application server without any other needed service granting ticket.

Selected Answer: False

## Question 52

5 out of 5 points

Why is it more secure to put password hashes in the /etc/shadow file rather than putting them in the /etc/passwd file?

Selected Answer: Because only root user can access the /etc/shadow file.

Response Feedback: [None Given]

## Question 53

2 out of 2 points

Match the descriptions with the correct Snort's IDS mode.

| Question | Selected Match |
|---|---|
| Acts as IDS and watches copy of traffic from switch SPAN port or network TAP.  Most popular deployment. | B. Passive Offline |
| Acts as IDS and allows all traffic to pass through.  Doesn't just look at copy of traffic, actually forwards it but takes no action. | D. Passive Inline |
| Monitors copy of traffic but acts as psudeo IPS by denying some traffic through sending RST or ICMP error messages to shut down remote connections. | A. Active Offline |
| Acts as IPS and forwards/denies all traffic based on ruleset. | C. Active Inline |

## Question 54

2 out of 2 points

In symmetric key cryptography, two different keys are used.

Selected Answer: False

## Question 55

5 out of 5 points

Name and describe at least four of the general steganalysis detection techniques.

Selected Answer:

Search the original file in the internet and compare in eyes.
Find the statices of the frequencey.
Use Winhen or notepad's compareing function to compares the original and stego file.
Check the histogram graph for the frequency.
Use hashing function to hash the original and stego file.

Response Feedback: [None Given]

## Question 56

2 out of 2 points

✓ Which of the following are Block Ciphers?

AES
Diffie-Hellman
RSA

## Question 57

2 out of 2 points

✓ LM Windows passwords are more secure than NT Windows passwords.

Selected Answer: False

## Question 58

2 out of 2 points

✓ During the forensic lecture in-class lab, which EnCase feature did we use to search the hard drive to find any files that may have contained Ringo Johnson's SSN?

Selected Answer: String Searching

## Question 59

2 out of 2 points

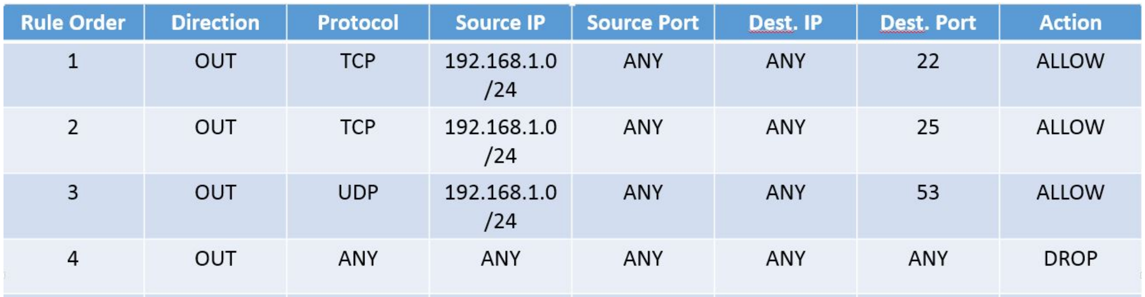
✓ You have taken an image of the RAM of a suspect's system and later use volatility to analyze it. The memory capture will most likely contain the suspect's recent logon credentials for gmail's website.

Selected Answer: True

## Question 60

0.5 out of 5 points

Below are a few generic rules for a stateless packet filter. Explain what they do. (You must also include in your answer the name of the service that runs on each port number as well as what the /24 means.)



| Rule Order | Direction | Protocol | Source IP | Source Port | Dest. IP | Dest. Port | Action |
|---|---|---|---|---|---|---|---|
| 1 | OUT | TCP | 192.168.1.0 /24 | ANY | ANY | 22 | ALLOW |
| 2 | OUT | TCP | 192.168.1.0 /24 | ANY | ANY | 25 | ALLOW |
| 3 | OUT | UDP | 192.168.1.0 /24 | ANY | ANY | 53 | ALLOW |
| 4 | OUT | ANY | ANY | ANY | ANY | ANY | DROP |

Selected Answer: It allows the host will respond the FTP, SSL connection, and the DNS query.

Response Feedback: [None Given]

## Question 61

0 out of 2 points

The TCP header flag fields that stateful packet filters often evaluate are the ACK, RST, SYN, and FIN flags.

Selected Answer: False

## Question 62

2 out of 2 points

What was Whitfield Diffie's answer to sending the key securely?

Selected Answer: It send public information and keep the private key. It shows the concept that we can only share some public keys or information but keep the private key not to be changed. However, Whitfield Diffie use sysmetrice key to encrypt the message.

Response Feedback: [None Given]

## Question 63

2 out of 2 points

This question relates to Public Key Cryptography. To achieve Authentication, the **[x]** key encrypts data and the **[y]** key decrypts that data.

Specified Answer for: x private

Specified Answer for: y public

## Question 64

0 out of 5 points

An attacker tries to send a dissociation message to wireless access point in order to disconnect all of the attached client devices but finds they are blocked by MAC filtering. What can the attacker do to be able to successfully deliver their attack?

Selected Answer: Use Dos attack.

Response Feedback: [None Given]

Friday, May 6, 2016 11:29:56 AM CDT

← OK