

Student Name:

ISA 656: Network Security

Midterm Examination

I, _____, hereby certify that I read the following:

University Policy Number 1301: Responsible Use of Computing

<http://www.gmu.edu/facstaff/policy/newpolicy/1301gen.html>

I understand that GMU takes its ethical obligations very seriously and violations will not be tolerated. I fully understand that GMU and its students must conduct the Program's activities in accordance with the highest possible ethical and legal standards. I know that I am responsible for ensuring that my personal conduct is above reproach. As a condition of studying in the ISA Program at GMU, I agree that violations of the standards described in the Code of Conduct shall be made known immediately to my appropriate faculty member(s) and that violations will result in dismissal from the Program and failure to receive the degree. I understand that this is a zero tolerance policy and that no second chances are given.

GENERAL INSTRUCTIONS

The midterm is worth 250 points (including 30 extra credit points): 110 points of theory and 140 points of Lab exercises. You have 40 minutes for the theory part; a short 10 minutes break and 60 minutes for the Lab part – plan accordingly. The questions are in no particular order of difficulty. Move on to easier ones if you find yourself stuck. You may answer questions in any order as long as they are clearly labeled.

THEORY/WRITTEN QUESTIONS (110 points)

1) [30 points]

- a) If passwords are exactly 8 characters long, each of which can be an upper- or lower-case English letter, or one of the ten digits (0–9), how many different passwords are possible?

Answer:

26 (upper-case letters) + 26 (lower-case letters) + 10 (digits) = 62 symbols for each position. For 8 independent positions we get:

$$\text{total password combinations} = 62^8$$

- b) Assume the function used to store the password was arithmetic addition: convert each letter to its ASCII numeric code (e.g., 'A' becomes 65, 'a' becomes 97, etc.) add the values and store the result in the /etc/passwords file.
- Is this a safe mechanism to store passwords?
 - Are there any attacks against this scheme?

Answer:

No, it is not a safe mechanism to store passwords because an attacker can read the file and attempt off-line attacks. In addition, plain addition of the password letters is a bad hash functions because it has many predicable collisions. An attacker can easily generate letter combinations that correspond to same arithmetic value stored in the passwords file without even knowing the correct password.

2) [50 points] **Firewalls**

- a) (20 points) If all traffic that comes through the gateway is encrypted how this can affect network level firewalls? How will it affect application level firewalls?

Answer:

Payload Encryption will not affect network-level firewalls since they don't perform deep-packet inspection but rather filter traffic using the IP header information. On the contrary, application-level firewalls will not be able to filter traffic since their operation depend on inspection of the content. Thus, and application-level firewall including web

proxies won't be able to filter traffic. However, host-based firewalls that inspect the traffic after it has been decrypted on the host would still be able to operate even if the network traffic that the host receives is encrypted.

b) (30 points)

Packet-filtering Firewalls (Hint: draw a picture of the networks involved).

a) Identify any redundant or conflicting parts of the stated firewall policy.

Answer:

In the Input chain, rule 4 conflicts with all the rules below it.

b) Show what would happen to the following packets under each of the three conflict-resolution strategies.

prot	src	dest
tcp	66.68.80.90:7800	23.45.68.10:80

First match: accept, rule 2

Last match: deny, rule 4

Best match: accept, rule 2

prot	src	dest
udp	66.68.80.90:9300	23.45.68.5:53

First match: accept, rule 1

Last match: deny, rule 4

Best match: accept, rule 1

```

      prot          src          dest
+-----+-----+-----+
| udp | 128.59.16.2:5589 | 23.45.68.3:4058 |
+-----+-----+-----+

```

First match: deny, rule 4
 Last match: deny, rule 4
 Best match: deny, rule 4

INPUT CHAIN (default DENY):

target	prot	source	destination	ports
ACCEPT	udp	0.0.0.0/0	23.45.68.5/32	* -> 53
ACCEPT	tcp	0.0.0.0/0	23.45.68.10/32	* -> 80
ACCEPT	tcp	0.0.0.0/0	23.45.68.11/32	* -> 80
DENY	all	0.0.0.0/0	23.45.68.0/24	* -> *
ACCEPT	tcp	23.45.67.0/24	23.45.68.0/24	* -> *
ACCEPT	udp	23.45.67.3/32	23.45.68.3/32	8000 -> 4058
REJECT	tcp	128.59.0.0/16	23.45.68.5/32	* -> *
ACCEPT	tcp	128.59.17.0/24	23.45.68.0/24	* -> 1099

OUTPUT CHAIN (default DENY):

target	prot	source	destination	ports
ACCEPT	tcp	23.45.68.10/32	0.0.0.0/0	80 -> *

3) [30 points] Crypto

You are encrypting with AES in ECB mode. You encrypt plaintext blocks A, B, C, D, E. However, the fourth block is garbled during transmission; in particular, the high-order bit is flipped.

Which blocks can the receiver successfully decrypt and why?

Answer:

Only block D will be affected since in ECB mode each block is encrypted independent from the rest of the blocks. So each block depends only on the key. Receiver will get blocks A, B, C, E intact.

LABORATORY QUESTIONS (140 points)

1) [40 points] NMAP

Use nmap to scan ite.gmu.edu and www.gmu.edu.

What are the services that they are running? What are the versions of the services that the servers are listening to (e.g. www, ssh, etc.)? Compare the two servers in terms of services they are running, which one is more secure and why?

Answer:

- `nmap -O -sS -A -v 129.174.1.52`
- `nmap -O -sS -A -v 129.174.93.130`

The list of open ports and the versions of the services show that ite.gmu.edu has both more services running and the services appear to be older versions. This makes ite.gmu.edu more vulnerable to attacks even though its operating system version is higher (Solaris 9/10) when compared to Solaris 8 of www.gmu.edu.

2) [50 points] Firewall Design

- a) (20) You are designing the security of a big organization with two branches, one in NY and one in DC. How many firewalls would you need to protect such organization? Assuming that each of the branches had multiple departments which of the departments would you protect?

Answer:

Two firewalls, one for each of the branches' gateways are required to protect the company's network. The department that needs to be protected is the one that will cause the more damage to the company if there is a breach. Usually, Human Resources and Accounting departments are the ones that companies try to protect first since they are directly related to the financial and customer information of the company. Of course, what we are going to protect depends on what the company deems as more important based on the company activities and profile.

- b) (30) Assume that you have one company branch with internal network 10.0.0.0/24, a Web server with IP Address 10.0.0.1, a File server (NFS) with address 10.0.0.2, and a DNS server with IP Address 10.0.0.3.
- What are the rules that you need to implement to allow outside access to the Web server but internal-only access to the File Server? The Web Server should be able to connect to the File server but only for NFS. Both servers should be reachable via SSH from the Internal network. Produce the iptable rules that you need to run on each of the machines assuming no central network firewall. What are the rules going to be if we have a central network firewall?

Answer:

Without Central Firewall:

Web Server Rules:

1. (Allow access to http/web):

ALLOW TCP FROM any host and all ports TO 10.0.0.1/32 port 80
iptables -A INPUT -s 0/0 -dport 80 -p TCP -j ACCEPT

2. (Allow internal access to ssh):

ALLOW TCP FROM 10.0.0.0/24 and all ports TO 10.0.0.1/32 port 22
iptables -A INPUT -s 10.0.0.0/24 -dport 22 -p TCP -j ACCEPT

3. (Deny the rest):

DENY ALL
iptables -A INPUT -s 0.0.0.0/0 -j DROP

File Server Rules:

4. (Allow access from Web Server to NFS):

ALLOW TCP FROM 10.0.0.1/32 and all ports TO 10.0.0.2/32 port 2049
iptables -A INPUT -s 10.0.0.1/32 -dport 2049 -p TCP -j ACCEPT

5. (Allow internal access to ssh):

ALLOW TCP FROM 10.0.0.0/24 and all ports TO 10.0.0.2/32 port 22
iptables -A INPUT -s 10.0.0.0/24 -dport 22 -p TCP -j ACCEPT

6. (Deny the rest):

DENY ALL

iptables -A INPUT -s 0/0 -j DROP

DNS Server Rules (optional):

7. (Allow access to DNS):

ALLOW UDP FROM 0/0 and all ports TO 10.0.0.3/32 port 53

iptables -A INPUT -s 0/0 -dport 53 -p UDP -j ACCEPT

8. (Deny the rest):

DENY ALL

iptables -A INPUT -s 0.0.0.0/0 -j DR

With a Central Firewall the following rules will be moved to the central Firewall:

1, 2, 5, 7 but not 4!

3) [50 points] **Wireshark & JAVA**

Use wireshark to capture the traffic of your chat client (if you don't have your own chat client, use the one provided in the lab). Record the packets that are part of the communication. What are the wireshark rules to capture this communication?

Answer:

Wireshark cannot listen on the loopback interface but it can listen to connections even within the localhost if we define the interface to be the public IP address of the machine (or one of the public IP addresses). The Wireshark filter that we could use to capture the traffic would filter on the machine's public IP address and port (in our case 19000). If we would like to make the filter more strict, we could also use the protocol (TCP).

Modify the chat **client** to send a password encrypted with DES to the **server**. Both client and the server read the DES key from the keyboard upon initialization. The server has to print the decrypted password on the screen. Assume the same DES Key and password for all users. No multi-threading is required! Modify existing code!