In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 817: Advanced Network Security

Mehdi Kharrazi *Mehr 16^{th}, 1394*

Homework 1

Please email your answers/report in **PDF format** TO "kharrazi@sharif.edu" and CC "masalehi@ce.sharif.edu" and "masoudian@ce.sharif.edu". The HW file name should be **"Your Lastname-817- HW-1"**. Also the same title should be used as the subject of your email. Please follow the formatting. This homework is due by **Mehr 28th, 11:59 PM**. Also, you will have a face-to- face delivery, the time of which will be announced later.
Report what you write down should be your own words, analysis, reasons and results. There will be a zero tolerance policy for cheating/copying HWs.
Maximum Answer File Size = 1MB . (Try to include text result or reduce screenshot size included in your report.)

Part I: Theoretical

1. Explain differences of Web Application Firewall (WAF), IDS, and IPS?
2. Look for a real example of attacking a firewall. Explain how it works and name solutions to resist such attacks.
3. Discuss the best ways of protecting an internal network using firewalls from the following attacks:
   (a) SMTP Server Hijacking
   (b) Bugs in operating systems
   (c) ICMP redirect bombs
   (d) Denial of service
4. The *Address Resolution Protocol(ARP)* performs the address translation between the data link and network layer. This protocol works as follow:
   When host A looks for the Ethernet address of host B , it broadcast an ARP request including its IP address .As soon as B receives the request, it replies back an ARP packet containing its IP and Ethernet addresses. This protocol is vulnerable to ARP Spoofing.
   (a) Explain how an ARP spoof works and name the attacks that can be launched by this vulnerability.
   (b) Explain solutions for preventing these attacks.

Acknowledgment: Some of the questions may be taken from assignments handed out by similar courses in other universities.

Part II: Practical

Port Scanning

In this section of the homework you will use the NMAP and Hping2 utilities to scan a set of network addresses. The aim is to compare these tools and get familiar with port scanning tools. **Scanning a network or a specific computer could be taken as an offensive action by some network operators. BE CAREFUL as to what you scan, and AVOID scanning well known sites such as google, yahoo, and etc.**

(a) Get familiar with the "nmap" and "hping2" utility and Explain about their usages, important options and main differences.

(b) Explain how nmap and hping detect the following three port states: open, closed, and filtered. Compare the results.

(c) Take your SID (student id number), have k equal to the remainder of your SID divided by 30. Then you will be scanning the following IP range 213.233.(168 + k).0/24. For example if your SID is 89245654 then k = 4 and you should be scanning 213.233.172.0/24. Report the hosts you find. In case you find no hosts up in the IP range you are scanning, try another value for k (k++). (Hping and NMAP)

(d) Select two hosts from the list of hosts which you discovered in the previous step, and conduct a detailed scan on them. Report on the type of OS as well as the services they are running. (Hping and NMAP)

(e) Explain the following concepts and how to use them in practice by "nmap" and "hping" utility.

- TCP connect scanning
- Idle port scanning
- Dicoy port scanning
- Stealth port scanning
- FTP Bounce scanning

(f) Select two hosts from the list in question 3 and perform the port scan methods mentioned in the previous part. (Hping and NMAP)

Note: You report should include your student ID number, and the IP range you scanned.

Firewalls

In this section of the homework, you will be using iptables to conduct a number of tasks, based on a described scenario. It is assumed that you have root access to a Linux box for this experiment and have iptables installed. If you don't have such access, then you should install a Linux distribution either on your machine or in a virtual machine.

(a) The iptables uses tables and chains to organize rules. Explain the running order of tables and chains.

(b) What is Port Knocking"? Explain how it works

(c) Consider the Network topology depicted in 1 and write iptables rules to enforce following requirements:

- Allow all connections between DMZ and Internal Network if initiated from Internal Network.
- Drop all connections from Internet to Internal Network
- Allow HTTP, DNS , ICMP, SSH and SMTP connections from Internet to DMZ.

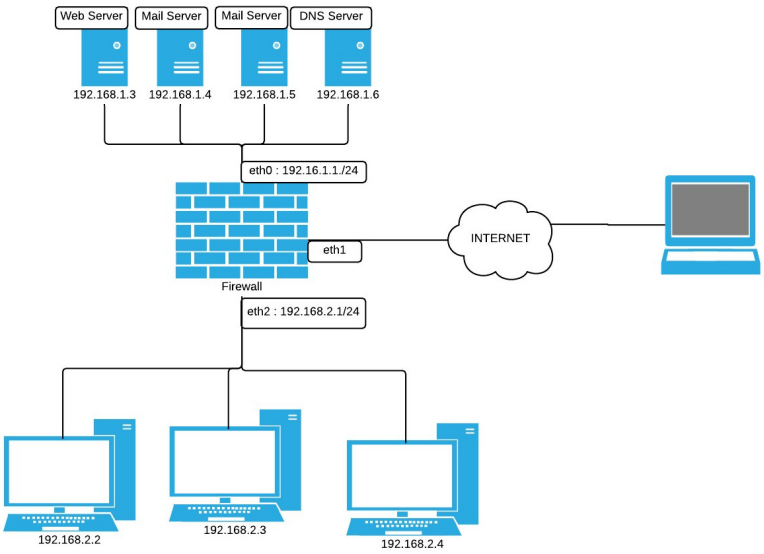

Figure 1: Network Topology

- Route all HTTP requests from Internet to HTTP server dedicated in DMZ on port 80
- Allow 100 connections per minute from Internet to HTTP server.
- Block all connections from Internal Network to www.example.com .
- Load balance SMTP requests to two Mail servers dedicated in DMZ.
- Log all rejected packets.

(d) What are TCP Split Handshake and Simultaneous-Open Connection concepts and explain can iptables logs TCP connections based on these two concepts? if yes, how? if no, write snort rules to log TCP connections based on these techniques.

(e) Explain how iptables can be used to detect ARP Spoofing.

(f) In the policies stated above, there was a requirement about blocking connection to a specific URL which is used to restrict access to some websites from Internal users. Is there any solution to bypass this mechanism in firewalls ? If yes, explain it with an example.

Vulnerability Analysis

There is an executable binary code named vuln in the course web page. The program gets a string as an argument and prints out that on screen. However, the author of the program inexplicably has forgotten to do bounds-checking on the array into a function call in program, and therefore the program is vulnerable to attack. You need to analyse the vulnerable binary code and answer the following questions:

(a) Explain what is that vulnerability and how it works and where the bug exists on the vulnerable binary code.

(b) Get a reverse shell by exploiting that vulnerability.

(c) Explain your solution for patching that vulnerability.

Important Note: Consider that this program was compiled in Unix 64-bit architecture.