Sharif University of Technology
Department of Computer Engineering

Advance Network Security
Instructor: Dr.AmirMehdi SadeghZadeh *24 Aban, 1402*

Homework 2*

1 Part One: Theorical

1.1 Botnets

Botnet is a collection of computers infected with a worm, trojan, etc. which allows someone (a bot master) to control them remotely.

(a) Explain different C&C topologies and enumerate their pros/cons.

(b) In this part, you are asked to get familiar with the following botnets . Therefore, explain each of them and design a checklist for comparing them with each other. The checklist should be complete and accurate.

i. Zues or Zbot
ii. Carna botnet
iii. Storm Botnet

1.2 DDoS

One of the many forms of Distributed Denial of Service (DDoS) attacks is a Reflection Attack. This attack works when an attacker sends forged requests to to a large number of servers. Spoofing the IP address of the sender can lead the replies go to the victim machine and making it down.

(a) Why are UDP-based protocols often used as the basis for DDoS reection attacks?

(b) What is the amplication concept in DDoS attacks, and why is it attractive to attackers?

(c) One of the recent Reflection Attack is NTP based one. Network Time Protocol(NTP) is a protocol for clock synchronization between computer systems .How does the attack works? Which NTP features can be used to launch a DDoS attack ? Enumerate the mechanisms to stop this attack . Also, write an iptable rule to prevent it.

2 Part Two: Practical

2.1 IPTables

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.

*Acknowledgement: This homework was orginally developed by Behman Momeni

(b) What is “Port Knocking”? Explain how it works.

(c) A similar concept is “URL Knocking” in which client must visit a sequence of URLs to unblock a secret URL. Using iptables commands, setup a “URL Knocking” scenario which unblocks the http://www.example.com/the/blocked/and/secure/url address for 5 seconds for the client who visits following 3 URLs respectively:

(i) http://www.example.com/initial/normal/url

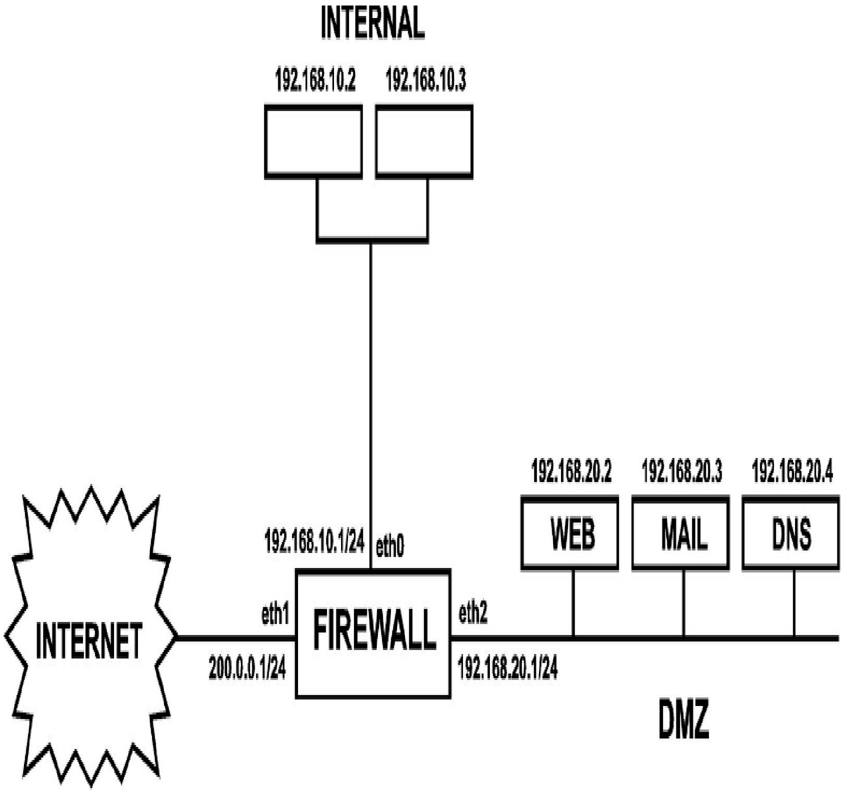
(ii) http://www.example.com/continues/by

(iii) http://www.example.com/the/third/one

Assume that your iptables commands are executed on the www.example.com server and packets are received on eth0 interface.

There are many different ways to design a network with a DMZ. The basic method is to use a single Linux firewall with three Ethernet cards. The following simple example shows a DMZ setup (see Fig):

Figure 1: Linux-based DMZ setup [modified from Wikipedia article]



- eth0 with 192.168.10.1/24 private IP address – Internal LAN / Desktop system
- eth1 with 200.0.0.1/24 public IP address – Internet.
- eth2 with 192.168.20.1/24 private IP address – DMZ connected to Mail / Web / DNS and other private servers

Provide iptables rules to enforce following requirements (if there is any inconsistency/redundancy in requirements, resolve them):

Case 1- Forward traffic between Internal network and DMZ only if initiated from Internal network.

Case 2- Forward ssh, www, and dns traffic between Internal network and INTERNET only if initiated from Internal network.

Case 3- DROP all traffic from Internal network to Internet except ssh, icmp, udp destination port 666, and TCP destination ports 10000, 20000, and 30000.

Case 4- Allow traffic from INTERNET to DMZ.

Case 5- Set a rule for routing all incoming SMTP requests to a dedicated Mail server at IP address 192.168.20.3 and port 25.

Case 6- LOG all "rejected" packets.

2.2 Worms

Worm is a Malware which can infect vulnerable computers through network and use the infected computer to further spread itself. One of the consequences of worms, even when they have no specific malicious intent, is the huge traffic generated while exploiting new hosts. In this part of the homework, you will analyze a pcap file which demonstrates network activities of a worm. Download the pcap file from http://mawi.nezu.wide.ad.jp/mawi/samplepoint-B/2003/200302161400.dump.gz address. Take care of the file size. The large size makes it impractical to use GUI based software like Wireshark. You need to work with tcpdump and write required scripts (e.g. Bash and Awk script) to process packets.

(a) There are some suspected UDP activities in the given pcap file. Report number of UDP packets and also 10 destination UDP port numbers who have been visited more than others.

(b) Identify the related worm who generated the traffic. How did you find the worm?

(c) Write an iptables rule to block this worm.

(d) How many packets are sent out by the worm?

(e) Find all (src-ip, dst-ip) pairs from packets which are sent by the worm. Report the 7 top IP addresses who sent out most packets.

(f) Extract worm packets which are sent out by 7 IP addresses of previous question. For these packets, draw following 2D diagram:

   i. For each IP address in the form a.b.c.d, draw one point at (x = horizontal axis = a*256+b, y = vertical axis = c*256 + d),

   ii. The origin of the 2D graph (i.e. the (0, 0) point) is placed at bottom/left corner,

   iii. Connect two points (x1,y1) and (x2,y2) if and only if their corresponding IP addresses were communicating (within the extracted network traffic of this question),

   iv. Report scripts that you used to draw the graph and of course the graph itself,

   v. If the graph is too compressed, you can eliminate some lines (e.g. draw 1 line out of every 10 lines). Find out the reasonable sampling rate which produces a comprehensible graph.

(g) Analyze the graph of previous question. What is the scanning pattern of the worm? How does it select vulnerable targets to exploit them?

3 HW Submission

You should submit .pdf file containing answers to theorical questions , a detailed report for practical questions, with screenshots for Terminals to describe what you have done and what you have observed, as well as the program source code. You also need to provide explanation to the observations that are interesting or surprising. Please also list the important code snippets followed by explanation. Simply attaching code without any explanation will not receive credits. Your report must be written in your own words to demonstrate your own analysis, reasoning, and obtained results. There will be a zero tolerance policy for cheating/copying HWs.

Finally, submit all of your answers in .zip file on the Quera course page with the following format:
HW[HWNo]-[FamilyName]-[stdNo] .zip (For example, HW3-Hoseini-401234567.zip)