In the name of God

Sharif University of Technology
Department of Computer Engineering

CE 817: Advanced Network Security

*Mehdi Kharrazi* *Aban $11^{th}$, 1394*

# Homework 1

Please email your answers/report in **PDF format** TO "kharrazi@sharif.edu" and CC "masalehi@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 **Aban 24th, 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. 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 eachother. The checklist should be complete and accurate.
      i. Zues or Zbot
      ii. Carna botnet
      iii. Storm Botnet
2. 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.

## Part II: Practical

### Botnet

In the first part of theoretical questions, you got familier with botnet topologies and some well-known examples of it. In this part, you should analyze a botnet traffic dump prepared in a pcap file and answer the following questions:

1. What is the C&C server of this botnet?
2. Based on communication streams, what type of commands and data were exchanged between clients and C&C server ?
3. What is the attack type of this botnet.
4. Find victims' IP addresses.
5. How many packets are sent out by this botnet to each victim?
6. Report the 5 top source port number who sent out most packets.
7. Assume that the C&C server IP address is variable. now block the communication between client and C&C server with DPI (Deep Packet Inspection) techniques.

## Worm

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.

1. 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.
2. Identify the related worm who generated the traffic. How did you find the worm?
3. Write an iptables rule to block this worm.
4. How many packets are sent out by the worm?
5. 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.
6. Extract worm packets which are sent out by 7 IP addresses of previous question. For these packets, draw following 2D diagram:
   (a) 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),
   (b) The origin of the 2D graph (i.e. the (0, 0) point) is placed at bottom/left corner,
   (c) 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),
   (d) Report scripts that you used to draw the graph and of course the graph itself,
   (e) 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.
7. Analyze the graph of previous question. What is the scanning pattern of the worm? How does it select vulnerable targets to exploit them?