Exercise 05

Mar 09, 2023

# Overview

This exercise provides hands-on experience with launching of DDoS attack using network protocols ICMP, TCP, UDP and HTTP.

# Learning Objectives

* Understand basics of DDoS Attack
* Understand working of HTTP Protocol.
* Ability to launch Slowloris attack exploiting HTTP protocol.
* Ability to launch Reflection and Amplification attack.

# Reading Material

1. <https://www.kali.org/tools/slowhttptest/>
2. <https://www.kali.org/tools/hping3/>
3. <https://nmap.org/book/host-discovery-controls.html#host-discovery-list-scan>
4. <https://linux.die.net/man/8/tcpdump>
5. Principles of Computer Security, Stallings and Brown, Pearson 4th ed, Chap 07.
6. <https://ubuntu.com/server/docs/web-servers-apache>
7. Working of TCP protocol and connection setup using 3-way handshake. The details are available in any TCP/IP networking book.

# Prerequisites and environment familiarity

## Overview

Student should be familiar with Linux and command line terminal usage.

Student should be familiar with basics of networking protocols such as ICMP, TCP, UDP, and HTTP and their message structure for request and response messages.

As this homework involves launching an attack, we want to ensure that attack remains confined to within the cyber range sandboxes i.e., the machines on which these exercises are to be done should not be directly reachable from/to internet. This should ensure that these machines should not be able to generate any packets that go on the internet.

## Overview of VMs:

This homework exercise is to be done individually. In this exercise, you will be using three VMs. These VMs are a) Kali Linux, b) Ubuntu22, and c) Ubuntu-20. Also, verification of attack requires knowledge of capture filter for tcpdump. So, review your knowledge and skills for tcpdump so that you capture only application packets relevant to attack and not all kind of other packets. The access to Ubuntu-22 system remains as before i.e., using your assigned IP address and login id. On other two systems i.e., Kali Linux and Ubuntu-20, a user is created with username as “crsuser” and with the password as “crsuser”. Please do not change the password for this user “crsuser”. This user has sudo privileges on both these systems. Please use the sudo privilege with caution. Please do not login to root using sudo as any mistake in commands issues could be catastrophic.

1. Kali Linux: This will primarily be the attacker machine i.e. from where attack will be launched. You would be using packages such as ping, hping3, slowhttptest etc.
2. Ubuntu 20: This will be the target machine i.e., the system on which attacks will be launched. On this system, Apache 2 web server has been installed and should be up and running.
3. Ubuntu 22: This may also act as target machine for reflection and amplification attacks.

You have sudo privilege access on both the Kali Linux as well and Ubuntu20. For both these machines, shell prompt has been changed to reflect the machine type and IP address. Do not change the shell prompt as same shall be used for verifying your work origins.

## Accessing VMs

To access these machines, first you need to login to your assigned Ubuntu-22 VM. Consider that the IP address of your Ubuntu-22 VM is 130.85.a.x, where value of “a” and “x” will vary for individual Ubuntu-22 VM. The value of “a” is either 121 or 220. Value of “x” would be 34, 42, …

Open two terminal windows on your laptop (e.g. Macbook terminal or putty on Windows), one for accessing Kali Linux and other for accessing Ubuntu-20. On each of these terminal windows, first ssh into ubuntu-22 from your laptop.

$ ssh <username>@130.85.a.x

Note down the IP address of 2nd network interface i.e. ens192 of Ubuntu-22 VM by using the following command

$ ip addr show dev ens192

This will provide the IP address of 2nd network interface. That address would be something like 133.228.y.z e.g., 133.228.80.2 => 133.228.86.2/18

Now from the first terminal windows, login to Kali Linux as below by using appropriate value of y and z

$ ssh [crsuser@133.228.y.(z-1)](mailto:crsuser@133.228.y.(z-1))

So, for the above example IP address of 133.228.80.2, y is 80, and z is 2.

$ ssh [crsuser@133.228.80.1](mailto:crsuser@133.228.80.1)

From the second terminal window, log in to Ubuntu-20 system as follows.

$ ssh crsuser@133.228.y.(z+1)

For the above example, this would be

$ ssh [crsuser@133.228.80.3](mailto:crsuser@133.228.80.3)

## Activity recording.

Any attack activity that you launch should be recorded in a file. You do not need to submit screenshots. Make use of script command on Linux. When you run the script command on a terminal, any input entered and any output displayed on that terminal is recorded in the script file. To exit from script recording, just press Ctrl-D (or enter exit). Record your activity for each attack separately in each file. An example is given in the picture below.

Graphical user interface, text, application

Description automatically generated

This example creates a text file which captures the commands entered and their outputs. This script output file (e.g., exercise-a.txt) needs to be uploaded towards assignment submission for each of the exercise. Please do not upload any screenshots. To see the content of this script output file, you can use cat command to display the content on terminal..

You may need script output file for the attacker machine as well as the victim (target of attack) machine.

# Description

The assignment is to launch Denial of Service (DoS) attacks and verify the occurrence of attack at target machine. The attacks are to be launched from Kali Linux and target machine will be Ubuntu-20. Please ensure to take extreme caution when launching such attacks and ensure that such attacks do not last more than 200 seconds. The attacks for this homework are of following kind.

1. ICMP Flood attack
2. ICMP Smurf attack
3. UDP Flooding attack
4. TCP SYN Flooding attack
5. HTTP Slowloris attack.

## Note:

Please clean out files and directories related to previous work e.g. tcpdump, temporary files etc. Also, create a directory HA02 on each machine where you should carry the activity and save any output in this directory only.

Details for launching each kind of attack and recording your observation are as follows. In these exercises, IP address of Kali Linux is considered as 133.228.80.1, IP address of ubuntu-22 is considered as 133.228.80.2 and IP address of Ubuntu-20 machine is considered as 133.228.80.3. Please change these to the value as applicable to your exercise setup.

## Exercise A: ICMP Flood attack.

**Goal**: Launch ICMP flood attack

1. On Target machine, run tcpdump to save the ICMP packets from attacker. Please ensure to provide proper capture filter so that only those packets are captured those which are relevant to your attack. This command should be invoked first before launching the attack. An example of capturing ICMP packets is given below.

$ tcpdump -n -i ens192 -s0 -w icmpflood.pcap host 133.228.80.1 and icmp

1. From kali linux launch a flood of 100000 (100K) ICMP packets to target machine.

$ time sudo ping -f -c 100000 133.228.80.3

1. Note down the time it takes to send so many packets. iIn general 10000 ICMP request messages are sent per second to target flooding its network.
2. After the attack is completed, press Ctrl-C (^C) on target machine to abort tcpdump. Now analyze the tcpdump from the saved file e.g. icmpflood.pcap” on how many echo request packets were received and how many echo reply were sent. E.g. following will provide the count of ICMP requests received. Option “-r <pcap file>” is used to take data input from a file rather than network interface.

$ tcpdump -n -r icmpflood.pcap | grep "echo request" | wc -l

1. This count should be same as the number of ICMP packets sent by attacker e.g., 100K. IF the count mismatches, analyze the same identify the reasons.
2. You need to submit your script output for attacker and target machine for verification of this exercise.

## Exercise B: ICMP Smurf Attack.

**Goal**: Launch ICMP attack with spoofed IP address.

1. Identify 10 systems in the 133.228.64.0/18 network. Explore this network to catch the live systems in this network. You can either use nmap tool to scan for IP addresses, or alternatively explore with your classmates for their IP addresses in this network. Let us denote these addresses as A1, A2, …, A10. Following command may help you scan the network for live systems but it may take a while.

Nmap -sn -T4 133.228.64.0/18

1. On Target machine i.e., ubuntu20, run tcpdump to save the ICMP packets received from various systems used for smurf attack on the target system by attacker.
2. On Kali Linux machine, create a shell script as below, replacing the value of Ai with actual values of the IP Address. Use any text editor of your choice such as vi or nano. Let us call this script as smurfattack.sh (you can choose the name of your choice). For each smurfed IP, send N number ICMP Echo request packets.

#!/bin/bash

sudo hping3 -1 -q -c <N> -a <IP of target machine> A1 &

sudo hping3 -1 -q -c <N> -a <IP of target machine> A2 &

:

:

sudo hping3 -1 -q -c <N> -a <IP of target machine> A10 &

1. Make this script executable and invoke the script as

./smurfattack.sh

1. After the attack is over, stop/abort the tcpdump on target machine (press Ctrl-C to abort). Count the number of ICMP Echo Reply received from the tcpdump. There should be N\*10 replies. If any replies are missing, identify these.
2. You need to submit your script output for attacker and target machine for verification of this exercise.

## Exercise C: UDP Flooding Attack.

Goal: Launch UDP Flooding attack.

1. Use the same set of steps as done in exercise B except that this time the attack should be done using UDP protocol instead of ICMP. When saving tcpdump file, in the capture filter use both the protocols ICMP and UDP with the specific attack port to capture the packets. UDP is required to receive UDP packets and ICMP is required the capture ICMP Error “Destination (Port) unreachable”.
2. On Target machine i.e., ubuntu20, run tcpdump to save the UDP packets (on to the specific port) received from various system used by attacker to launch smurf attack.
3. On Kali Linux machine, create a shell script like the one as created earlier but it should send UDP packets on a specific destination port e.g., P. The option -2 implies hping3 will send UDP packets and option -p is used to specify the destination port.
4. Make this script executable and invoke it.
5. After the attack is over, stop/abort the tcpdump on target machine (press Ctrl-C to abort). Count the number UDP packets received and ICMP errors generated. These should be 50 UDP packets and 50 ICMP Errors. If any is missing, identify which one is missing. Take a screenshot of the capture that counts the number of such packets. This screenshot needs to be uploaded towards homework submission.
6. You need to submit your script output for attacker and target machine for verification of this exercise.

## Exercise D: TCP SYN Flooding Attack.

Goal: Launch TCP SYN Flooding attack.

1. Use the same set of steps as done in exercise C except that this time the attack should be done using TCP protocol. When saving tcpdump file, use TCP as the protocol for capture filter to capture the packets
2. On Target machine i.e. ubuntu20, run tcpdump to save the TCP SYN packets received from various systems smurfed by attacker and TCP Reset send by the attacked machine. This command has to be invoked first before launching the attack.

$ sudo tcpdump -n -i ens192 -w tcpsyn.pcap tcp

1. On Kali Linux machine, create a shell script as before to send TCP SYN packet with destination port P to target machine which would receive this packet and generate an TCP Reset error sending it back to each of Ai machine.
2. Make this script executable and invoke it.
3. After the attack is over, stop/abort the tcpdump on target machine (press Ctrl-C to abort). Count the number of TCP SYN packets received and TCP Reset generated. These should be 10N TCP SYN packets received and TCP Reset packets sent. If any is missing, identify which one is missing.
4. You need to submit your script output for attacker and target machine for verification of this exercise.

## Exercise E: HTTP Slowloris Attack.

Goal: Launch Slowloris attack.

1. SlowHttpTest package has been installed on Kali Linux. In case it is not, please follow the steps in Appendix to install this package.
2. On Target machine i.e. ubuntu20, Apache web server has been installed. In case it is not, please follow the steps in Appendix to install this package
3. Read and understand how to launch HTTP slowloris attack using slowhttptest tool. Use this tool to launch an attack with 1000 connections and with 25 number of requests to be generated per second.
4. Launch the slowloris attack, observe the output of slowloris attack for your analysis.
5. Explain the parameters users to launch the slowloris attack and your analysis of Slowloris output shown on the screen.
6. You need to submit your script output for attacker machine for verification of this exercise.

# Assessment and Rubric

1. Please do submit the Readme.txt file which will contain the following information:
   1. Commands invoked on for each attack on all the VMs used in the attack.
   2. Script output taken during the attack and tcpdump capture analysis
   3. Challenges faced and how did you address these.
   4. Summary of your overall learning.
   5. References. Any website/resource that you used to took help.
2. Script capture file for each attack.
3. Rubric: Each exercise carries 2 marks.

# Note

Any plagiarism activity will result in penalties of being awarded 0 marks.

# Appendix

Various packages have been installed on Kali Linux using following command

Installing packages on Kali Linux

sudo apt install slowhttptest

sudo apt install dsniff

Installing packages on Ubuntu20

sudo apt install apache2

### Verification of installation

From terminal window of Kali Linux, run the following command, where a.b.c.d corresponds to IP Address of ubuntu20 system.

$ wget http://<a.b.c.d>

This should result in saving of index.html file.

<end of Exercise 05>