COMPUTER NETWORK SECURITY

Ganesh K. 01FB15ECS104

Mohammad

Salamuddin 01FB15ECS175

Malformed Packets and Anomaly Detecction

# REPORT

## Abstract:

Explore forming Malformed packets and analyze their impact on some target and writing a script to analyze the same. Programmatically analyze trace data to detect port scanning activity

## Objectives

## Our goal is to do the following:

## Forming Malformed Packets

* Craft a TCP packet or set of TCP packets (using a tool or a piece of code) to send to a target.
* Observe the target's response with a packet capturing tool or view the results of those packet attacks in the log files on the target.

## Anomaly Detection

* Programmatically analyze trace data to detect port scanning activity.
* Observe the target's response with a packet capturing tool or view the results of those packet attacks in the log files on the target.
* Develop a Python program that analyzes a PCAP file in order to detect possible port scans.

## Approach:

## Anomaly Detection:

The Python script is designed to read in pcap files and analyze for **port scans** and **DDOS attacks**.

*Usage:*

$ # python3 analyser.py <PATH\_TO\_FILE>

$ python3 analyser.py pcap/namp/nmap\_standard\_scan

*Working:*

The script aims at parsing pcap files and check for TCP packets. Then proceeds to check if it is a SYN packet.

syn\_flag = ( tcp.flags & dpkt.tcp.TH\_SYN ) != 0

ack\_flag = ( tcp.flags & dpkt.tcp.TH\_ACK ) != 0

We then keep track of SYN to ACK ratio per IP address.

We later check if it is a:

* DDos Attack by:

for ip, count in self.malicious\_ip.items():

if(count[0] > 3 \* count[1]):

# Add to attack list

* Port Scan by: **TYPE: TCP-HALF-OPEN**

for ip in s.get\_port\_lists().keys():

ports = self.port\_list[ip]

return len(ports) > 1000

## Forming Malformed Packets:

Packet Crafting:

Crafting, by definition, means to make or create something skillfully. As we know, all the vulnerability assessment tools used by network administrators to test the security of their networks are both a blessing and a curse. This is because the same set of tools can also be used by evil hackers to find vulnerabilities and then exploit those to their benefit. Packet crafting, too, is not an exception to this rule, and since it is a technically advanced yet complex type of vulnerability exploitation, it is difficult to detect and diagnose.

SOURCE: <http://opensourceforu.com/2012/05/cyber-attacks-explained-packet-crafting/>

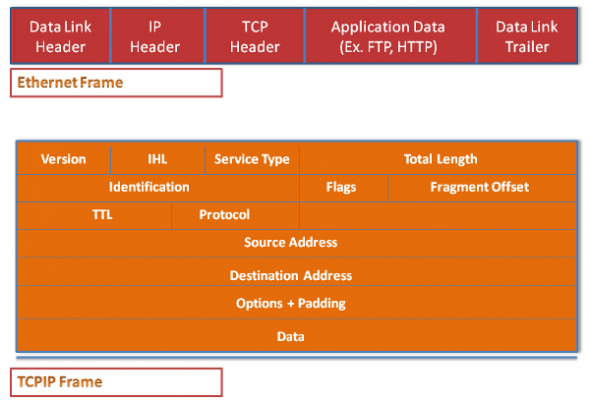


Figure 1. A basic Ethernet and TCP/IP packet

Packet crafting techniques:

* Ping fragmentation
* Packet flag manipulation
* Packet duplication
* Protocol manipulation
* Half open packets

We will be mainly focusing on packet flag manipulation and half open packets. The steps are:

Step 1: Lay of the land

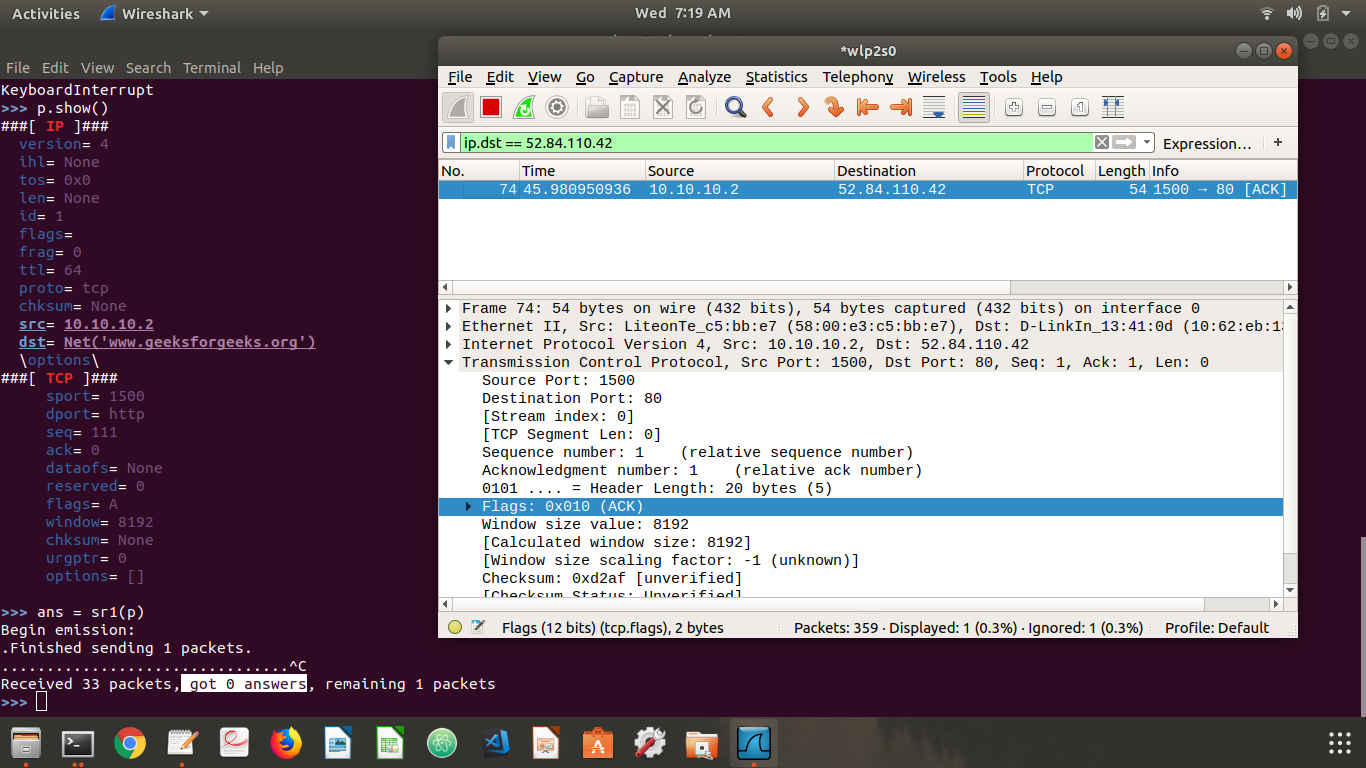
We test firewalls response to malformed packets:

Figure 1. A basic Ethernet and TCP/IP packet

-----------#code--------------

>>> ip = IP(src = "10.10.10.2",dst = "www.geeksforgeeks.org")

>>> tcp = TCP(dport=80,sport=1500,flags="A",seq=111)

>>> p = ip/tcp

>>> ans = sr1(p)

analysis: packet with a false source IP address and with ACK field bit set is dropped by the fire wall.

Step 2: setting the reset R

By setting the reset R flags we confuse the server. (firewall should drop it)

## 

Figure 1. A basic Ethernet and TCP/IP packet

-----------#code--------------

>>> p.payload.flags = "R"

>>> ans = sr1(p)

analysis: incoming packet with RESET flag set is dropped by the firewall.

Step 3: The DoS Attack

-----------#code--------------

>>> ip = IP(dst="www.slavehack.com")

>>> tcp = TCP(sport=1500,dport=25)

>>> p = ip/tcp

>>> # the attack!!!

>>> ans,unans=srloop(p,inter=0.1,retry=2,timeout=4)

## 

Figure 1. A basic Ethernet and TCP/IP packet

analysis: server stops accepting SYN connections as shown in the screenshot(DOS.png), thus resulting in denial of service.

more about DOS attack.

Client sends a TCP SYN (S flag) packet to begin a connection to the server. The target server replies with a TCP SYN-ACK (SA flag) packet, but the client does not respond to the SYN-ACK, leaving the TCP connection “half-open”. In normal operation, the client should send an ACK (a flag) packet followed by the data to be transferred, or an RST reply to reset the connection. On the target server, the connection is kept open, in a “SYN\_RECV” state, as the ACK packet may have been lost due to network problems.

## Acknowledgement:

* This project is developed as part of assignment for Computer Networks Security.
* We would like to thank our professors, Dr. Alka Agrawal and Prof. Amulya G

References: