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

## 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:

1. Primary Source: <https://www.hackingtutorials.org>
2. Primary Tutorials: <https://www.youtube.com/channel/UCAJ8Clc3188ek9T_5XTVzZQ>
3. VNC: <https://www.offensive-security.com/metasploit-unleashed/scanner-vnc-auxiliary-modules/>
4. RUBY: <https://www.hackingtutorials.org/metasploit-tutorials/hacking-druby-rmi-server-1-8/>
5. VSFTPD: <https://www.hackingtutorials.org/metasploit-tutorials/exploiting-vsftpd-metasploitable/>
6. UnrealIRCD: <https://computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson7/index.html>