Network Scanner – Simple IDS

Project Report

2024

## Overview

This project is a Python-based network traffic monitoring tool using Scapy. It is designed to detect and alert users about common network security threats such as ARP spoofing, DNS spoofing, DoS, DDoS, and port scanning. The tool monitors live network traffic and generates alerts for any suspicious activity.

## Global Variables

* **arp\_cache:** Stores ARP IP-MAC mappings to track spoofing.
* **traffic\_count:** Tracks packet counts per IP for detecting DoS and DDoS.
* **port\_scan\_attempts:** Logs accessed ports for each IP to identify port scans.
* **alerted\_ports:** Prevents duplicate alerts for vulnerable ports.
* **vulnerable\_ports:** List of ports commonly exploited (e.g., 21, 22, 80).

## Execution Flow

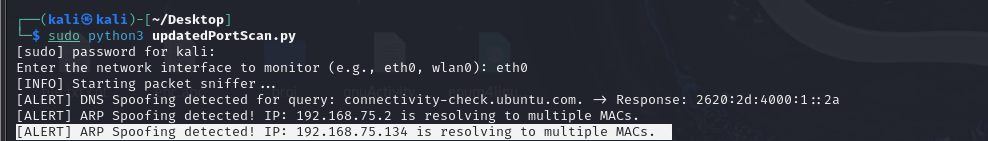
1. **User Input:**
   * Enter the network interface to monitor.
2. **Packet Capture:**
   * Captures live network traffic using Scapy's sniff() function.
3. **Packet Processing:**
   * Each packet is passed to detection functions:
     + detect\_arp\_spoof
     + detect\_dos
     + detect\_ddos
     + detect\_port\_scanning
     + detect\_dns\_spoof
4. **Alerting:**
   * Suspicious activities generate alerts printed to the console.

## ARP Spoofing Attack:



## Arp Spoofing Detection:

* **Input:** Captures ARP packets.
* **Logic:** Alerts if an IP resolves to multiple MAC addresses.



## DNS Spoofing Detection:

* **Input:** Monitors DNS queries and responses.
* **Logic:** Alerts if a DNS response originates from an untrusted IP.

A screen shot of a computer

Description automatically generated

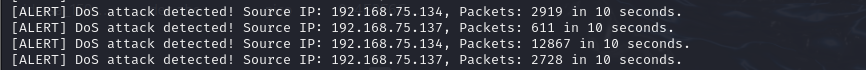
## DOS Attack:

A computer screen shot of a computer code

Description automatically generated

## DOS Attack Detection:

* **Input:** Counts packets per IP.
* **Logic:** Alerts if packets from an IP exceed DOS\_THRESHOLD within 10 seconds.

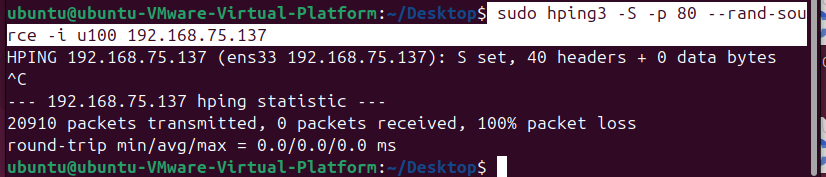


## Vulnerable Port Scanning:

* **Input:** Tracks destination ports accessed by each IP.
* **Logic:**
  + Alerts if an IP accesses more than PORT\_SCAN\_THRESHOLD ports.
  + Highlights attempts to access vulnerable ports.



## DDOS Attack:



## DDOS Detection:

* **Input:** Tracks SYN packets to identify SYN flood attacks.
* **Logic:** Alerts if an IP exceeds HALF\_OPEN\_THRESHOLD SYN packets.

A screen shot of a computer screen

Description automatically generated