Lab19 Physical Penetration Testing Tools

Scope

- To deploy a physical hacking tool in another lab room and use it to remotely exploit in the target network.

Tools

- Hak5 tools: I chose Shark Jack for this lab!
- Hak5 C2 server
- Payloads for the Shark Jack

Task 1. Choosing a device:

I chose Shark Jack.

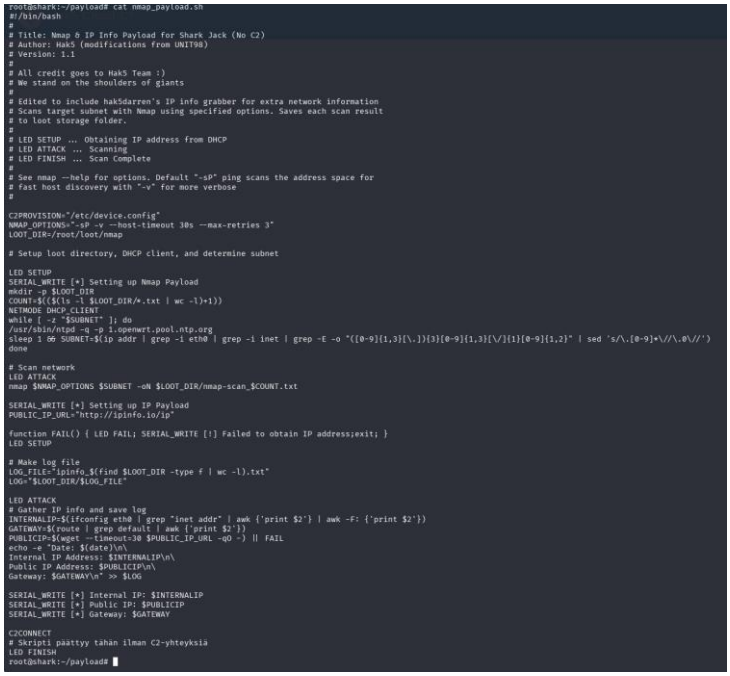
Step 2. Choosing a payload and setting up the device:

Configuration

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : lan
   Link-local IPv6 Address . . . . . : fe80::79a9:f392:1fab:6948%9
   IPv4 Address. . . . . . . . . . . : 172.16.24.202
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 172.16.24.1
```

```
BusyBox v1.28.4 () built-in shell (ash)

    \_____)\_____       Shark Jack       _____/(_____/
    /--v____ __°<        by Hak5         >°__ ____v--\
           )/                               \(

root@shark:~# ls
VERSION  loot     payload
root@shark:~# cd payload
root@shark:~/payload# ls
nmap_payload.sh  payload.sh
root@shark:~/payload#
```

Payload that i used:



```
root@shark:~/payload# cat nmap_payload.sh
#!/bin/bash
#
# Title: Nmap & IP Info Payload for Shark Jack (No C2)
# Author: Hak5 (modifications from UNIT98)
# Version: 1.1
#
# All credit goes to Hak5 Team :)
# We stand on the shoulders of giants
#
# Edited to include hak5darren's IP info grabber for extra network information
# Scans target subnet with Nmap using specified options. Saves each scan result
# to loot storage folder.
#
# LED SETUP ... Obtaining IP address from DHCP
# LED ATTACK ... Scanning
# LED FINISH ... Scan Complete
#
# See nmap --help for options. Default "-sP" ping scans the address space for
# fast host discovery with "-v" for more verbose
#

C2PROVISION="/etc/device.config"
NMAP_OPTIONS="-sP -v --host-timeout 30s --max-retries 3"
LOOT_DIR=/root/loot/nmap

# Setup loot directory, DHCP client, and determine subnet

LED SETUP
SERIAL_WRITE [+] Setting up Nmap Payload
mkdir -p $LOOT_DIR
COUNT=$((`ls -1 $LOOT_DIR/*.txt | wc -l`+1))
NETMODE DHCP_CLIENT
while [ -z "$SUBNET" ]; do
/usr/sbin/ntpd -q -p 1.openwrt.pool.ntp.org
sleep 1 && SUBNET=$(ip addr | grep -i eth0 | grep -i inet | grep -E -o "([0-9]{1,3}[\.]){3}[0-9]{1,3}[\/][1][0-9]{1,2}" | sed 's/\.[0-9]*\//\.0\//')
done

# Scan network
LED ATTACK
nmap $NMAP_OPTIONS $SUBNET -oN $LOOT_DIR/nmap-scan_$COUNT.txt

SERIAL_WRITE [+] Setting up IP Payload
PUBLIC_IP_URL="http://ipinfo.io/ip"

function FAIL() { LED FAIL; SERIAL_WRITE [!] Failed to obtain IP address;exit; }
LED SETUP

# Make log file
LOG_FILE="ipinfo_$(find $LOOT_DIR -type f | wc -l).txt"
LOG="$LOOT_DIR/$LOG_FILE"

LED ATTACK
# Gather IP info and save log
INTERNALIP=$(ifconfig eth0 | grep "inet addr" | awk {'print $2'} | awk -F: {'print $2'})
GATEWAY=$(route | grep default | awk {'print $2'})
PUBLICIP=$(wget --timeout=30 $PUBLIC_IP_URL -qO -) || FAIL
echo -e "Date: $(date)\n\
Internal IP Address: $INTERNALIP\n\
Public IP Address: $PUBLICIP\n\
Gateway: $GATEWAY\n" >> $LOG

SERIAL_WRITE [+] Internal IP: $INTERNALIP
SERIAL_WRITE [+] Public IP: $PUBLICIP
SERIAL_WRITE [+] Gateway: $GATEWAY

C2CONNECT
# Skripti päättyy tähän ilman C2-yhteyksiä
LED FINISH
root@shark:~/payload#
```

Final step was the succesfull attack:

```
Host is up (-0.20s latency).
MAC Address: 00:13:3B:50:AE:30 (Speed Dragon Multimedia Limited)
Nmap scan report for 172.25.21.34
Host is up (-0.20s latency).
MAC Address: 00:D8:61:F3:43:29 (Unknown)
Nmap scan report for 172.25.21.35
Host is up (-0.20s latency).
MAC Address: D8:BB:C1:ED:DB:8B (Unknown)
Nmap scan report for 172.25.21.37
Host is up (-0.20s latency).
MAC Address: 2C:F0:5D:4F:97:F7 (Unknown)
Nmap scan report for 172.25.21.38
Host is up (-0.20s latency).
MAC Address: D8:BB:C1:ED:DA:A3 (Unknown)
Nmap scan report for 172.25.21.99
Host is up (0.00043s latency).
MAC Address: D8:BB:C1:ED:D9:00 (Unknown)
Nmap scan report for 172.25.21.106
Host is up (-0.20s latency).
MAC Address: 2C:F0:5D:BC:7E:74 (Unknown)
Nmap scan report for 172.25.21.111
Host is up (0.00098s latency).
MAC Address: D8:BB:C1:ED:DB:40 (Unknown)
Nmap scan report for 172.25.21.113
Host is up (0.00025s latency).
MAC Address: 00:D8:61:F4:98:A5 (Unknown)
Nmap scan report for 172.25.21.114
Host is up (0.00051s latency).
MAC Address: 00:D8:61:F3:43:2E (Unknown)
Nmap scan report for 172.25.21.116
Host is up (0.0012s latency).
MAC Address: D8:BB:C1:ED:DA:A7 (Unknown)
Nmap scan report for 172.25.21.251
Host is up (-0.20s latency).
MAC Address: CC:EF:48:8C:2E:CB (Cisco Systems)
Nmap scan report for 172.25.21.252
Host is up (0.0084s latency).
MAC Address: FC:5B:39:F4:73:E8 (Cisco Systems)
Nmap scan report for 172.25.21.130
Host is up.
# Nmap done at Thu Apr 10 05:31:38 2025 -- 256 IP addresses (29 hosts up) scanned in 9.39 seconds
```