

WiFi Hacking 101

Task 1: The Basics - An Intro to WPA

Objectives:

- Understand the fundamental concepts of WPA (Wi-Fi Protected Access) and WPA2.
- Learn about the differences between WEP, WPA, and WPA2 encryption standards.

Key Takeaways:

- **WPA and WPA2:** Both provide strong security for wireless networks, with WPA2 being an improved version of WPA, using AES for encryption.
- **WEP vs. WPA/WPA2:** WEP is outdated and less secure compared to WPA/WPA2. WPA2 is currently the most secure standard.

Task 2: You're Being Watched - Capturing Packets to Attack

Objectives:

- Learn how to capture wireless data packets.
- Understand the importance of packet capturing in the context of wireless security.
- Use tools to capture packets for further analysis.

Key Takeaways:

- **Packet Capturing:** This process involves intercepting and logging traffic that passes over a wireless network.
- **Tools Used:** Tools like airodump-ng are essential for capturing data packets. These tools can capture the handshake packets required for WPA/WPA2 attacks.

Steps:

1. **Setting Up:** Prepare the environment by configuring the wireless network interface card (NIC) to monitor mode.

2. **Capturing Packets:** Use airodump-ng to capture packets from the target network. Look for handshake packets which are critical for cracking WPA/WPA2 encryption.

Task 3: Aircrack-ng - Let's Get Cracking

Objectives:

- Use captured packets to attempt decryption.
- Understand how to use aircrack-ng to crack WPA/WPA2 passwords.

Key Takeaways:

- **Aircrack-ng:** A powerful suite of tools used for auditing wireless networks. It is particularly useful for cracking WEP and WPA/WPA2-PSK keys.
- **Decryption Process:** Once the handshake packets are captured, aircrack-ng can be used to perform a dictionary attack on the captured data to find the network key.

Steps:

1. **Using Aircrack-ng:** Run aircrack-ng with the captured handshake file and a wordlist to attempt to crack the WPA/WPA2 password.
2. **Successful Decryption:** If the correct password is in the wordlist, aircrack-ng will find it and display the WPA/WPA2 key.

cs-sa07-24019

John_Mbithi_Mutave

The image is a composite of two screenshots. The left screenshot shows a web browser at the URL 'tryhackme.com/r/room/wifihacking101'. The page title is 'Wifi Hacking 101'. It features a 'Learn' section with a Wi-Fi icon and a brief description: 'Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.' Below this, it says 'Easy 0 min'. There are buttons for 'Help', 'Save Room', '1248' (likes), and 'Options'. A green bar at the bottom of the page indicates 'Room completed (100%)'. Below the main content, there are two task cards. 'Task 1' is titled 'The basics - An Intro to WPA' and 'Task 2' is titled 'You're being watched - Capturing packets to attack'. The right screenshot shows a terminal window with a root shell on IP 10.10.38.147. The terminal output shows the execution of 'aircrack-ng start wlan0', which results in 'ls: cannot access '/sys/class/ieee80211/': No such file or directory'. It then lists 4 processes that could cause trouble: 'PID Name', '989 wpa_supplicant', '1034 avahi-daemon', '1037 NetworkManager', and '1056 avahi-daemon'. The terminal also shows the output of 'airmon-ng check kill', which lists the PHY, Interface, Driver, and Chipset for each process. The terminal window has a title bar that says 'THM AttackBox' and a system tray showing '42min 25s'.

cs-sa07-24019
John_Mbithi_Mutave

The screenshot displays a web browser window with the URL `tryhackme.com/r/room/wifihacking101`. The page features a dark theme and a header with a search bar, a 'Go Premium' button, and a user profile icon. The main content area is titled 'Wifi Hacking 101' and includes a sub-header 'Learn to attack WPA(2) networks! Ideally you'll want a smartphone with you for this, preferably one that supports hosting wifi hotspots so you can follow along.' Below this, there are buttons for 'Help', 'Save Room', and 'Options'. A progress bar indicates 'Room completed (100%)'. Two tasks are listed: 'Task 1: The basics - An Intro to WPA' and 'Task 2: You're being watched - Capturing packets to attack'. The task description for Task 2 states: 'Using the Aircrack-ng suite, we can start attacking a wifi network. This will walk you through attacking a network yourself, assuming you have a monitor mode enabled NIC. The aircrack-ng suite consists of: aircrack-ng, airdecap-ng'.

Overlaid on the right side of the browser window is a terminal window titled 'root@ip-10-10-38-147:~'. The terminal shows network statistics for two interfaces: `veth82f3224` and `vethbe53474`. The output for `veth82f3224` is: `flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500`, `inet6 fe80::7025:57ff:feeb:6a90 prefixlen 64 scopeid 0x20<link>`, `ether 72:25:57:eb:6a:90 txqueuelen 0 (Ethernet)`, `RX packets 0 bytes 0 (0.0 B)`, `RX errors 0 dropped 0 overruns 0 frame 0`, `TX packets 54 bytes 6960 (6.9 KB)`, `TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0`. The output for `vethbe53474` is: `flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500`, `inet6 fe80::88bf:cff:fe1d:556a prefixlen 64 scopeid 0x20<link>`, `ether 8a:bf:0c:1d:55:6a txqueuelen 0 (Ethernet)`, `RX packets 0 bytes 0 (0.0 B)`, `RX errors 0 dropped 0 overruns 0 frame 0`, `TX packets 55 bytes 7070 (7.0 KB)`, `TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0`. Below the network statistics, the terminal shows the command `ifconfig` being executed, resulting in the error `ifconfig: command not found`. The terminal window also shows the command `ifconfig` being executed, resulting in the error `ifconfig: command not found`.

The Windows taskbar at the bottom shows the system clock as 10:05 AM on 7/7/2024, and the battery level is at 52min 7s. The system is running Windows 10, and the language is set to English (UK).

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/wifihacking101

TryHackMe

DashboardLearnCompeteOther

Access MachinesGo Premium1

airmon-ng check kill

Correct AnswerHint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng

Correct Answer

What flag do you use to set the BSSID to monitor?

--bssid

Correct AnswerHint

And to set the channel?

--channel

Correct AnswerHint

And how do you tell it to capture packets to a file?

-w

Correct AnswerHint

Task 3Aircrack-ng - Let's Get Cracking

Created byNinjaJc01

Room TypeFree Room. Anyone can deploy virtual machines in the room (without being subscribed)!

Users in Room43,364

Created1634 days ago

USD/GBP+0.40%

Search

ENG UK9:22 AM7/7/2024

tryhackme.com/r/room/wifihacking101

TryHackMe

DashboardLearnCompeteOther

Access MachinesGo Premium1

use this command on Kali: head /usr/share/wordlists/rockyou.txt -n 10000 | shuf -n 5 -

You will need a monitor mode NIC in order to capture the 4 way handshake. Many wireless cards support this, but it's important to note that not all of them do.

Injection mode helps, as you can use it to deauth a client in order to force a reconnect which forces the handshake to occur again. Otherwise, you have to wait for a client to connect normally.

Answer the questions below

How do you put the interface "wlan0" into monitor mode with Aircrack tools? (Full command)

airmon-ng start wlan0

Correct Answer

What is the new interface name likely to be after you enable monitor mode?

wlan0mon

Correct Answer

What do you do if other processes are currently trying to use that network adapter?

airmon-ng check kill

Correct AnswerHint

What tool from the aircrack-ng suite is used to create a capture?

airodump-ng

Correct Answer

cs-sa07-24019

John_Mbithi_Mutave

tryhackme.com/r/room/wifihacking101

Answer the questions below

What flag do we use to specify a BSSID to attack?

-b ✓ Correct Answer Hint

What flag do we use to specify a wordlist?

-w ✓ Correct Answer Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

-j ✓ Correct Answer Hint

Using the rockyou wordlist, crack the password in the attached capture. What's the password?

greeneegsandham ✓ Correct Answer Hint

Where is password cracking likely to be fastest, CPU or GPU?

GPU ✓ Correct Answer Hint

Created by	Room Type	Users in Room	Created
NinjaJc01	Free Room. Anyone can deploy virtual machines	43,964	1634 days ago

Activate Windows
Settings to activate Windows

Heavy rain Tomorrow

Search

tryhackme.com/r/room/wifihacking101

Task 3 🟢 Aircrack-ng - Let's Get Cracking

I will attach a capture for you to practice cracking on. If you are spending more than 3 mins cracking, something is likely wrong. (A single core VM on my laptop took around 1min).

In order to crack the password, we can either use aircrack itself or create a hashcat file in order to use GPU acceleration. There are two different versions of hashcat output file, most likely you want 3.6+ as that will work with recent versions of hashcat.

Useful Information

BSSID: 02:1A:11:FF:D9:BD

ESSID: 'James Honor 8'

Answer the questions below

What flag do we use to specify a BSSID to attack?

-b ✓ Correct Answer Hint

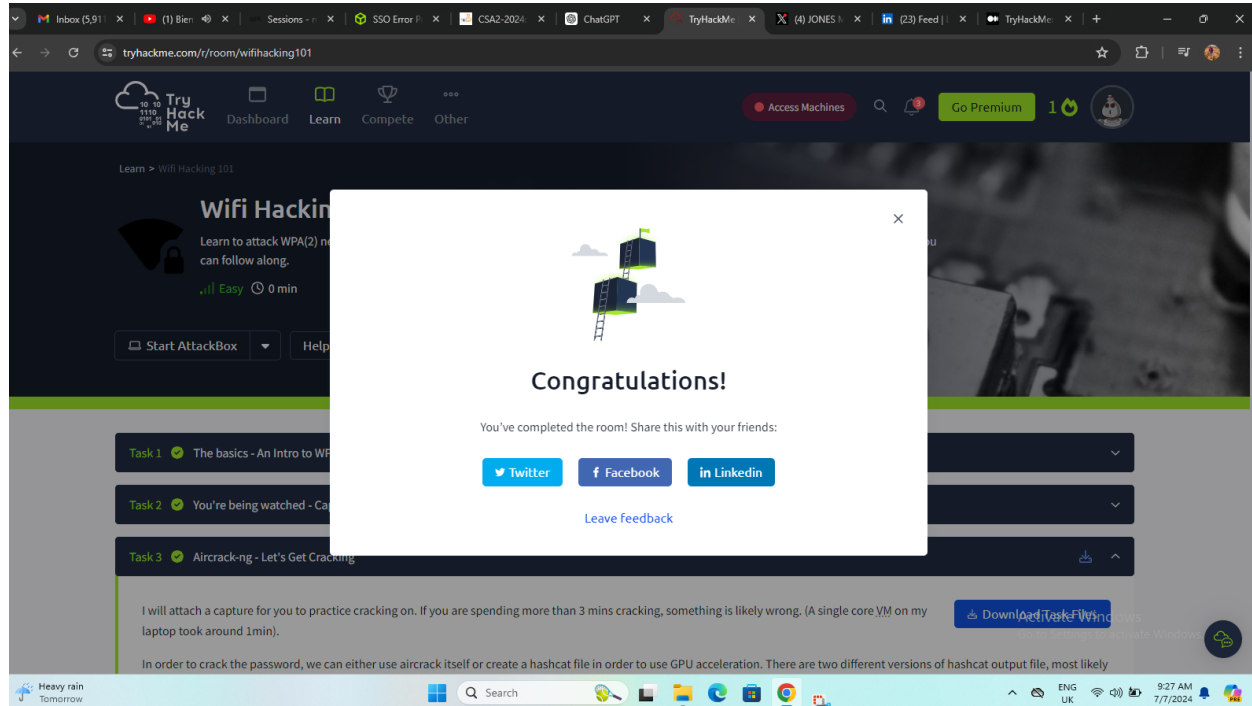
What flag do we use to specify a wordlist?

-w ✓ Correct Answer Hint

How do we create a HCCAPX in order to use hashcat to crack the password?

cs-sa07-24019

John_Mbithi_Mutave



Shareable Link - <https://tryhackme.com/r/room/wifihacking101>

Conclusion

The WiFi Hacking 101 module on TryHackMe provided a comprehensive introduction to attacking WPA(2) networks. The tasks covered the essential steps from understanding the basics of WPA, capturing data packets, and using aircrack-ng to crack the encryption. This hands-on experience is invaluable for understanding wireless security vulnerabilities and the importance of using strong, complex passwords and updated encryption standards to protect wireless networks.

Recommendations

1. **Use WPA3:** Upgrade to WPA3 where possible for enhanced security.
2. **Strong Passwords:** Use complex and lengthy passwords to make dictionary attacks less effective.
3. **Regular Monitoring:** Continuously monitor wireless network traffic for unusual activities that might indicate an attack.