

# MODULE 16 Hacking Wireless Networks

## LAB SCREENSHOTS

---

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE  
Course Code: T44-17520

## Lab Session Identifiers

1. <https://labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d>

## Username on EC-Council System

1. 2110886@uj.edu.sa

## Lab 01: Perform Wireless Traffic Analysis

The screenshot displays a Windows 11 login screen with the 'Admin' user profile selected. The taskbar shows the date as 5/13/2024 and the time as 9:15 AM. A Chrome browser window is open, displaying a lab guide titled 'Hacking Wireless Networks' with a progress bar at 100%. The guide includes instructions for capturing wireless traffic and a list of tasks. The first task is to select the Windows 11 machine and the Admin user profile. The second task is to type the password 'Pa\$\$w0rd' and press Enter. The third task is to click 'Continue' and 'Sign in with Microsoft'.

Windows 11 login screen showing the 'Admin' user profile and a password field.

Chrome browser window displaying the 'Hacking Wireless Networks' lab guide. The guide includes instructions for capturing wireless traffic and a list of tasks.

Task 1: By default, Windows 11 machine selected, click **Ctrl+Alt+Delete**.

Alternatively, you can also click **Ctrl+Alt+Delete** button under Windows 11 machine thumbnail in the Resources pane or Click **Ctrl+Alt+Delete** button under Commands (thunder icon) menu.

Task 2: By default, Admin user profile is selected, type **Pa\$\$w0rd** in the Password field and press **Enter** to login.

Alternatively, you can also click **Pa\$\$w0rd** under Windows 11 machine thumbnail in the Resources pane or Click **Type Text | Type Password** button under Commands (thunder icon) menu.

If **Welcome to Windows** wizard appears, click **Continue** and in **Sign in with Microsoft** click **Continue**.

0% Tasks Complete

Previous Next: Lab 2: Perform...

The screenshot shows the Wireshark Network Analyzer interface. The 'File' menu is open, displaying options such as 'Open...', 'Open Recent...', 'Merge...', 'Import from Hex Dump...', 'Close', 'Save', 'Save As...', 'File Set', 'Export Specified Packets...', 'Export Packet Dissections', 'Export Packet Bytes...', 'Export PDU to File...', 'Export TLS Session Keys...', 'Export Objects', 'Print...', and 'Quit'. The 'Ready to load or capture' status bar is visible at the bottom.

Wireshark Network Analyzer interface showing the 'File' menu and various options.

Ready to load or capture

Windows 11

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Hacking Wireless Networks - Google Chrome

Hacking Wireless Networks  
29 Minutes Remaining

Instructions Resources Help 100%

6. Wireshark: Open Capture File window appears, navigate to E:\CEH-Tools\CEHv12 Module 16 Hacking Wireless Networks\Sample Captures, select WEPcrack-01.cap and click Open.

7. The WEPcrack-01.cap file opens in Wireshark window showing you the details of the packet for analysis. Here you can see the wireless packets captured which were otherwise masked to look like ethernet traffic.

Here 802.11 protocol indicates wireless packets.

0% Tasks Complete

< Previous Next: Lab 2: Perform... >

Windows 11

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Hacking Wireless Networks - Google Chrome

Hacking Wireless Networks  
29 Minutes Remaining

Instructions Resources Help 100%

containing passwords (only for websites implemented on HTTP channel), perform attacks such as session hijacking, and so on.

Similarly you can also analyze the WPA2crack-01.cap file for WPA packets.

8. This concludes the demonstration of how to analyze Wi-Fi packets using Wireshark.

9. Close all open windows and document all the acquired information.

10. You can also use other wireless traffic analyzers such as AirMagnet WiFi Analyzer PRO (<https://www.netally.com>), SteelCentral Packet Analyzer (<https://www.riverbed.com>), Omnicpeek

0% Tasks Complete

< Previous Next: Lab 2: Perform... >

## Lab 02: Perform Wireless Attacks

### Task 1: Crack a WEP network using Aircrack-ng

The image shows a Parrot Security virtual machine desktop environment. The desktop background is a dark blue geometric pattern. A login window titled "attacker" is open in the center, showing a password field with four dots and a right arrow button. The system tray at the bottom shows the date as 5/13/2024 and the time as 12:18.

On the right side, there is a tutorial sidebar titled "Hacking Wireless Networks" with a progress bar at 32% and "27 Minutes Remaining". It contains instructions for steps 2, 3, 4, and 5. Step 2 involves logging in with the username "attacker" and password "toor". Step 3 involves navigating to the "Places" section and clicking "Desktop". Step 4 involves navigating to the "CEHv12 Module 16 Hacking Wireless Networks" folder and copying "Sample Captures" and "Wordlist" folders. Step 5 involves pasting these folders to the Desktop using Ctrl+V.

The bottom window is a file manager showing the "CEHv12 Module 16 Hacking Wireless Networks" folder. The left sidebar shows the "Places" list with "attacker" and "Desktop" selected. The main pane shows the contents of the selected folder, and a context menu is open over a file, with the "Copy" option highlighted.

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Hacking Wireless Networks - Google Chrome

Parrot Security

Applications Places System

CEHv12 Module 16 Hacking Wireless Networks

File Edit View Go Bookmarks Help

Back Forward 100% Icon View

Places attacker Desktop CEHv12 Module 16 Hacking Wireless Networks

Computer

- attacker
- Desktop
- File System
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash

Devices

- Floppy Disk

Network

- Browse Net...

Open

- Open in 2 New Tabs
- Open in 2 New Windows
- Open With Git Cola
- Open With VSCodium
- Cut
- Copy**
- Make Links
- Rename...
- Copy to
- Move to
- Move to Trash
- Delete
- Send to...
- Compress...
- Properties

Prepare the selected files to be copied with a Paste command

5/13/2024 ENG 33°C

Hacking Wireless Networks

26 Minutes Remaining

Instructions Resources Help 100%

4. The **Desktop** window appears, navigate to the **CEHv12 Module 16 Hacking Wireless Networks** folder and copy **Sample Captures** and **Wordlist** folders.

To copy the folders, firstly select both the folders and then press **Ctrl+C**.

5. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.

32% Tasks Complete

Previous Next

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Hacking Wireless Networks - Google Chrome

Parrot Security

Applications Places System

Desktop

File Edit View Go Bookmarks Help

Back Forward 100% Icon View

Places attacker Desktop CEHv12 Module 16 Hacking Wireless Networks

Computer

- attacker
- Desktop**
- File System
- Documents
- Downloads
- Music
- Pictures
- Videos
- Trash

Devices

- Floppy Disk

Network

- Browse Net...

CEHv12 Module 13 Hacking Web Servers

CEHv12 Module 14 Hacking Web Applications

CEHv12 Module 16 Hacking Wireless Networks

Sample Captures

Wordlist

README.license

Security\_Script-.html

2 folders selected (containing a total of 9 items). Free space: 63.7 GB

5/13/2024 ENG 33°C

Hacking Wireless Networks

26 Minutes Remaining

Instructions Resources Help 100%

folders and then press **Ctrl+C**.

5. Now, navigate to the **Desktop** and press **Ctrl+V** to paste the copied folders (**Sample Captures** and **Wordlist**). Close the **Desktop** window.

32% Tasks Complete

Previous Next



Hacking Wireless Networks - Google Chrome

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Parrot Security

Applications Places System Mon May 13, 12:22

aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap' - Parrot Terminal

```
attacker@parrot]-[  
$sudo su  
[sudo] password for attacker:  
toSorry, try again.  
[sudo] password for attacker:  
[root@parrot]-[/home/attacker]  
#sudo su  
[root@parrot]-[/home/attacker]  
#aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'  
bash: aircrack-ng/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap: No such  
file or directory  
[x]-[root@parrot]-[/home/attacker]  
#aircrack-ng '/home/aGot 20509 out of 20000 IVsStarting PTW attack with 205  
09 ivs. packets, please wait...  
Opening /home/attacker/Desktop/Sample Captures/WEPcrack-01.cap  
Read 2464654 packets.  
  
# BSSID ESSID Encryption  
1 20:E5:2A:E4:38:00 CEHLabs WEP (20509 IVs)  
  
Choosing first network as target.  
Reading packets, please wait...
```

Hacking Wireless Networks

24 Minutes Remaining

Instructions Resources Help 100%

9. In the Parrot Terminal window, type **aircrack-ng** **'/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap'** and press Enter.

10. By issuing the above command **aircrack-ng** will crack the WEP key of the **CEHLabs** as shown in the screenshot.

In real-life attacks, attackers will use this key to connect to the access point and

32% Tasks Complete

< Previous Next >

33°C  
سما صافية

Hacking Wireless Networks - Google Chrome

labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

Parrot Security

Applications Places System Mon May 13, 12:22

aircrack-ng '/home/attacker/Desktop/Sample Captures/WEPcrack-01.cap' - Parrot Terminal

```
attacker's home  
[00:00:00] Tested 88 keys (got 13614 IVs)  
  
KB depth byte(vote)  
0 2/ 3 98(18432) 8B(17920) 3B(17408) 5D(17408) FC(17408)  
1 3/ 8 48(18176) 33(17920) 92(17408) C3(17408) 05(17408)  
2 0/ 2 31(20224) 15(18688) 7E(18688) 3B(18176) 8C(18176)  
3 0/ 1 97(22016) 03(19456) 48(18432) 7D(18432) AB(18176)  
4 0/ 2 49(20480) BF(19968) 14(18432) D7(18176) E8(18176)  
  
KEY FOUND! [ 98:48:35:97:49 ]  
Decrypted correctly: 100%  
  
[root@parrot]-[/home/attacker]  
#
```

Hacking Wireless Networks

24 Minutes Remaining

Instructions Resources Help 100%

10. By issuing the above command **aircrack-ng** will crack the WEP key of the **CEHLabs** as shown in the screenshot.

In real-life attacks, attackers will use this key to connect to the access point and join the target network. Once they enter the target network, they can use scanning tools to scan for open devices, perform a vulnerability analysis, and then start exploiting any vulnerabilities they find.

11. This concludes the demonstration of how to crack a WEP network using Aircrack-ng.

32% Tasks Complete

< Previous Next >

33°C  
سما صافية

## Task 2: Crack a WPA2 Network using Aircrack-ng

The screenshot shows a Parrot Security virtual machine environment. A terminal window is open, displaying the execution of the `aircrack-ng` command. The command is: `aircrack-ng -a2 -b 20:E5:2A:E4:38:00 -w /home/attacker/Desktop/Wordlist/password.txt /home/attacker/Desktop/Sample Captures/WEPcrack-01.cap`. The terminal output shows that 2464654 packets were read, but no potential targets were found, and a message states: "Packets contained no EAPOL data; unable to process this AP." The terminal also shows the user quitting `aircrack-ng`.

On the right side of the screen, there is a task instruction panel titled "Hacking Wireless Networks" with a progress bar at 70%. The panel contains the following instructions:

- Instructions:** In this task, we will use the Aircrack-ng suite to crack a WPA2 network.
- Before starting this task, you need to configure your access point router (CEHv12) to work in WPA2-PSK (Pre-Shared Key) encryption mode.** To do so, navigate to the router's default IP address and change the authentication mode from WPA to WPA2-PSK, with the password as **password1**.
- In order to capture wireless traffic, a wireless adapter is required and using an adapter in the ilabs environment is not possible, therefore, in this lab, we are using a sample capture file (WPA2crack-01.cap) to crack WPA key.**
- Ensure that Sample Captures and Wordlist folders are present at the location home/attacker/Desktop which we copied in the previous task.** If not, then navigate to the CEHv12 Module 16 Hacking Wireless Networks folder on the Desktop, copy the Sample Captures and Wordlist folders and paste them at the location home/attacker/Desktop.
- 1. Click the MATE Terminal icon at the top of the Desktop window to open a Terminal window.**

The bottom of the screen shows the system tray with the date 5/13/2024, time 12:29, and temperature 33°C.