MODULE 16 Hacking Wireless Networks
LAB SCREENSHOTS

Lara Alofi

VULNERABILITY ANALYSIS AND DEFENSE
Course Code: T44-17520

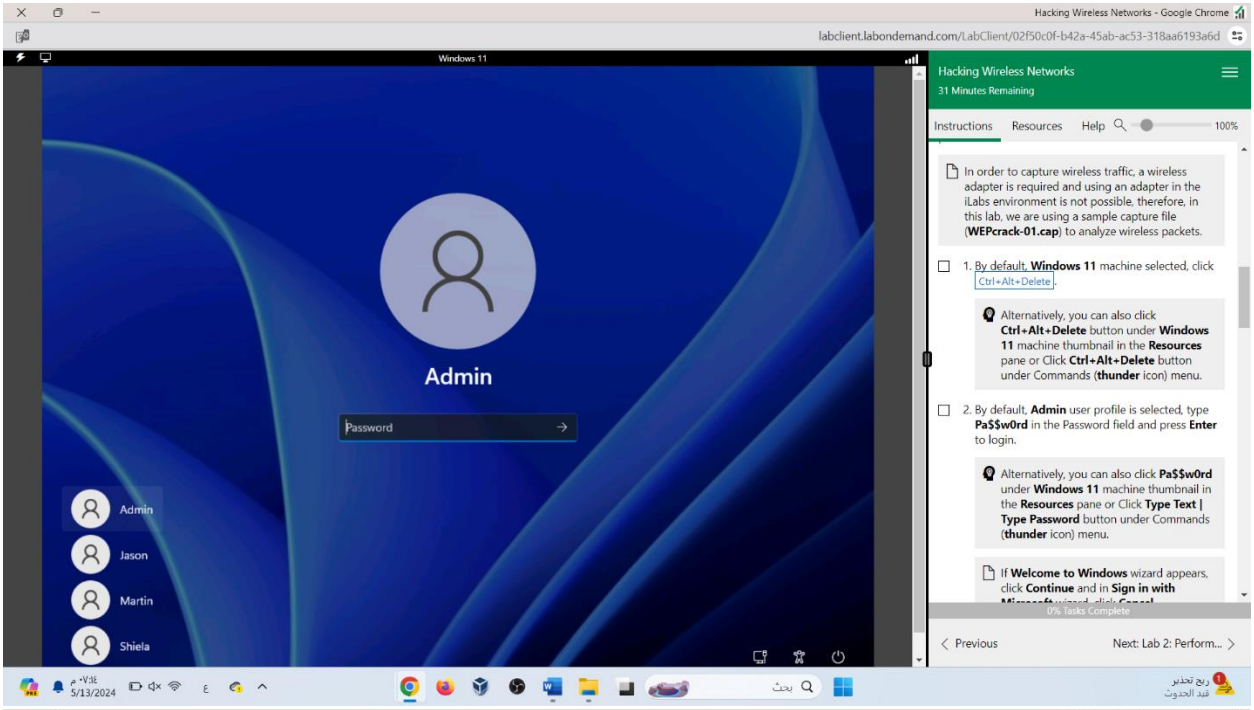
Lab Session Identifiers

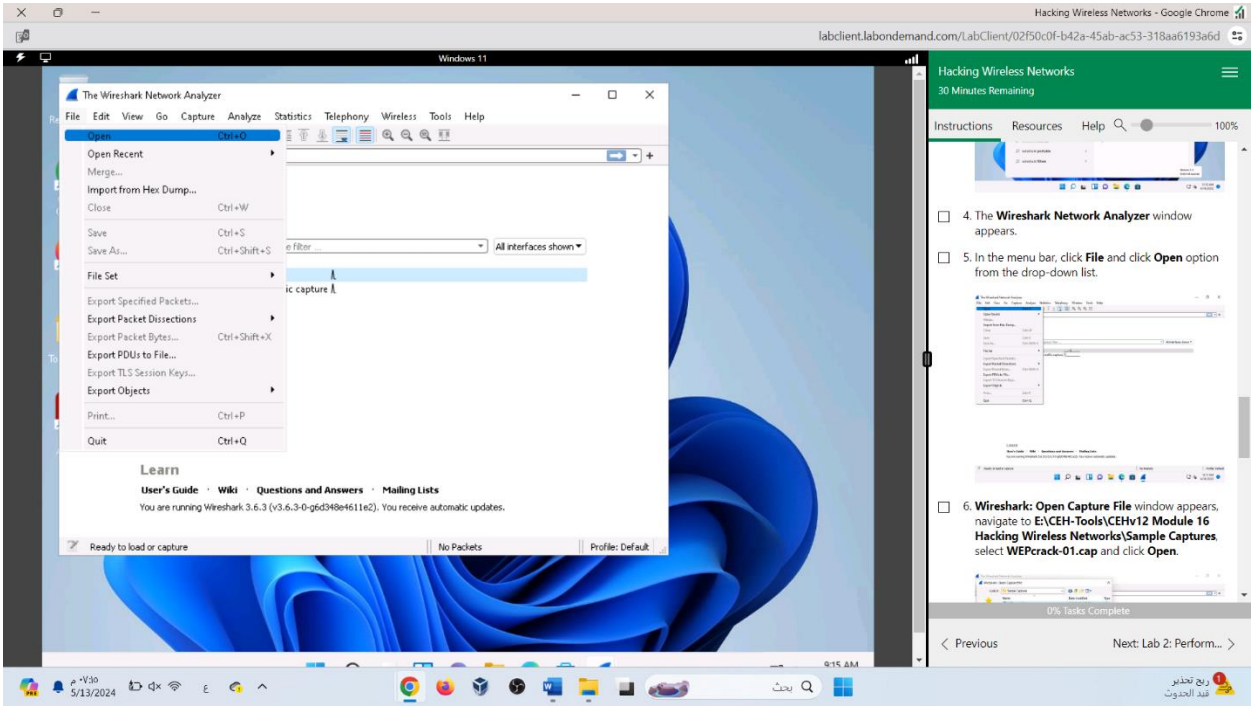
1. https://labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d

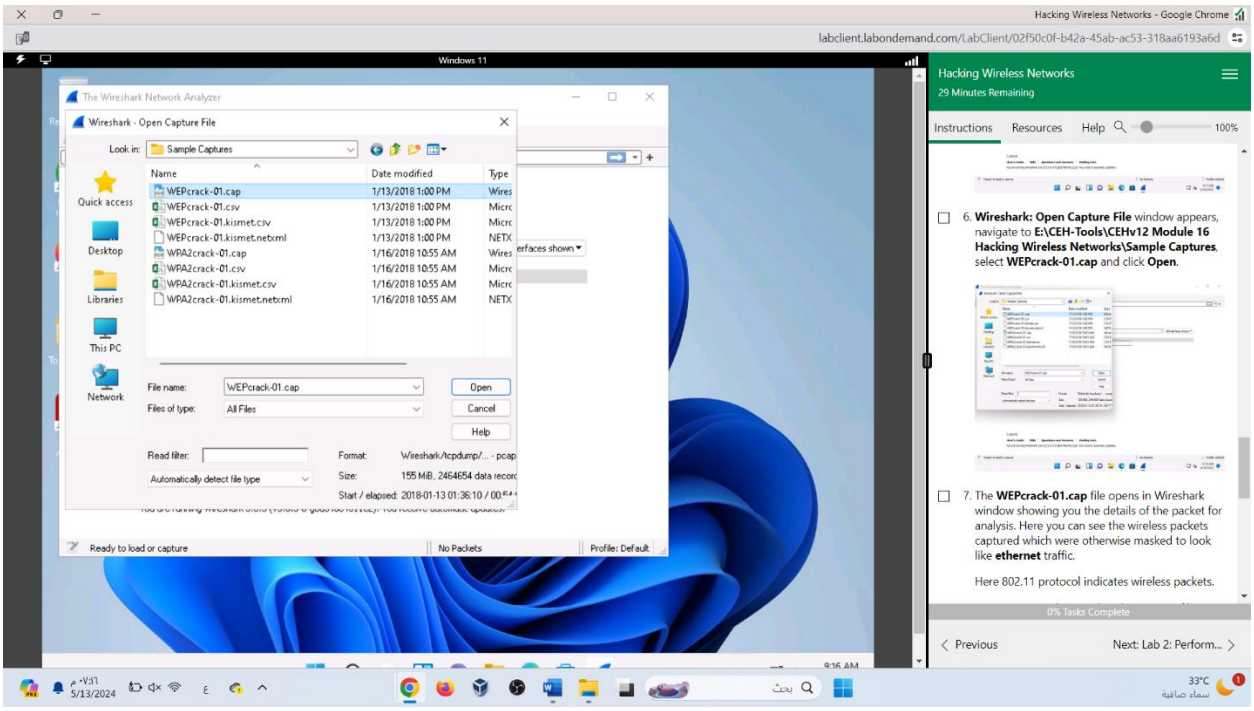
Username on EC-Council System

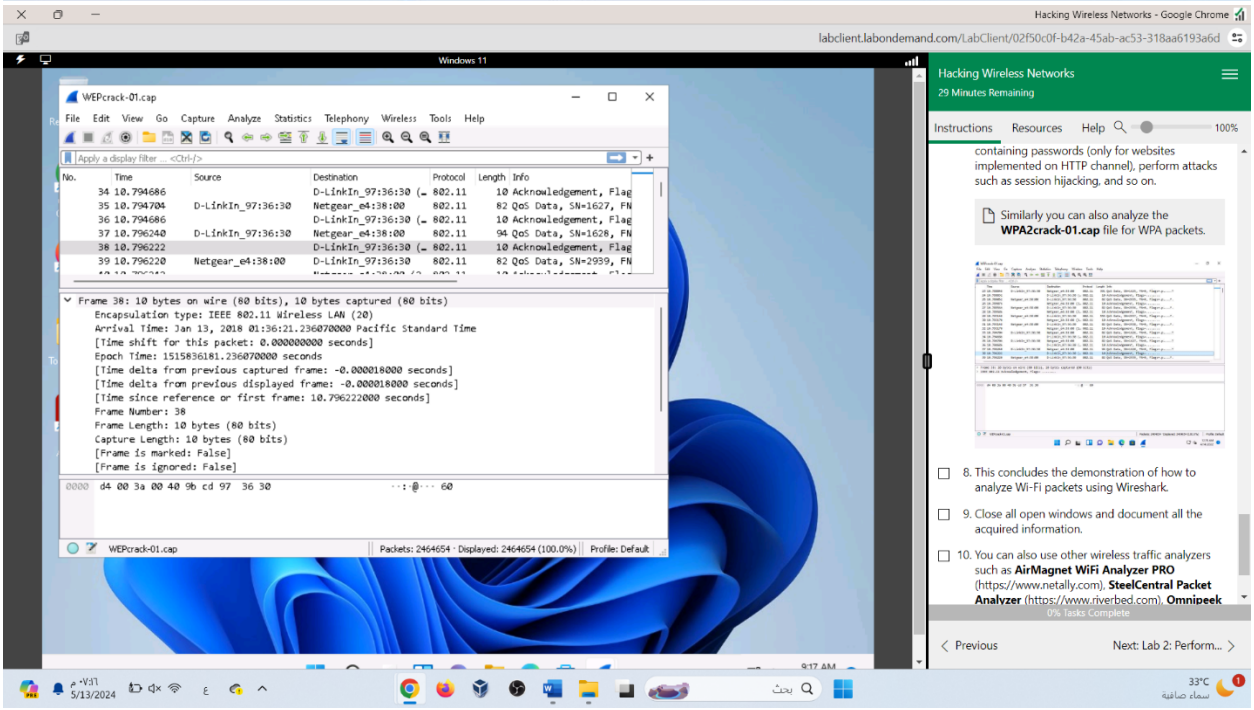
1. 2110886@uj.edu.sa

Lab 01: Perform Wireless Traffic Analysis



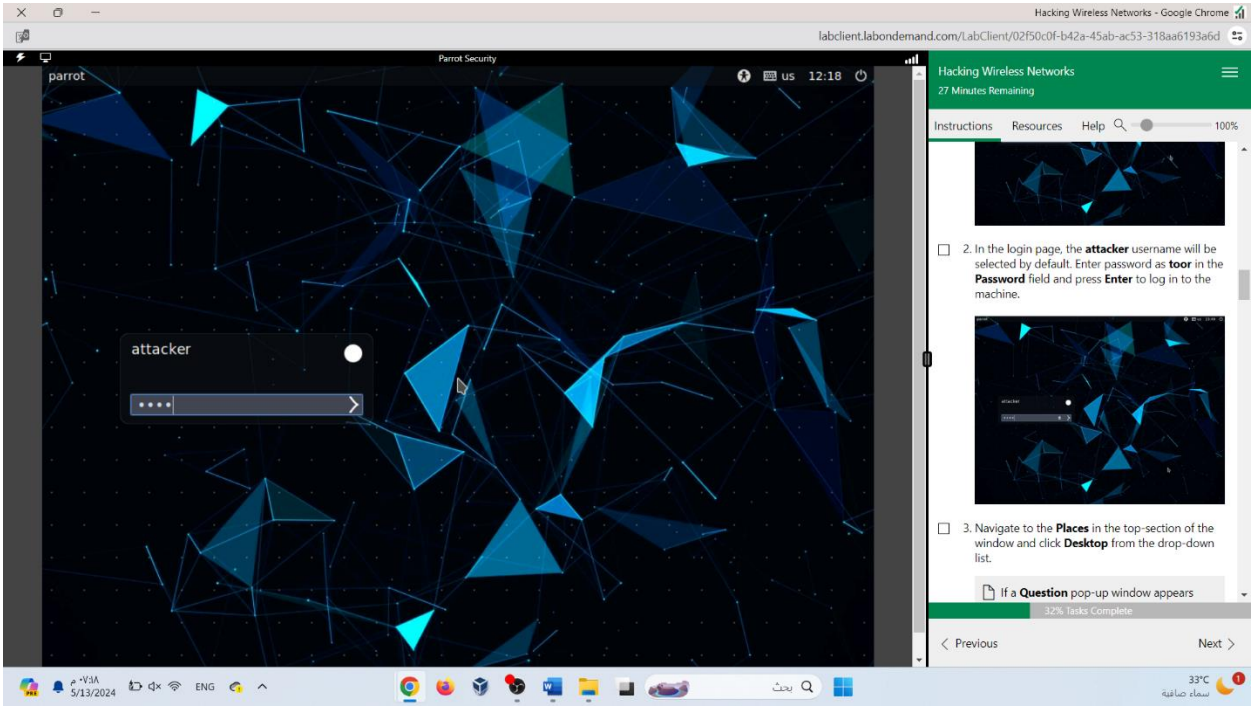


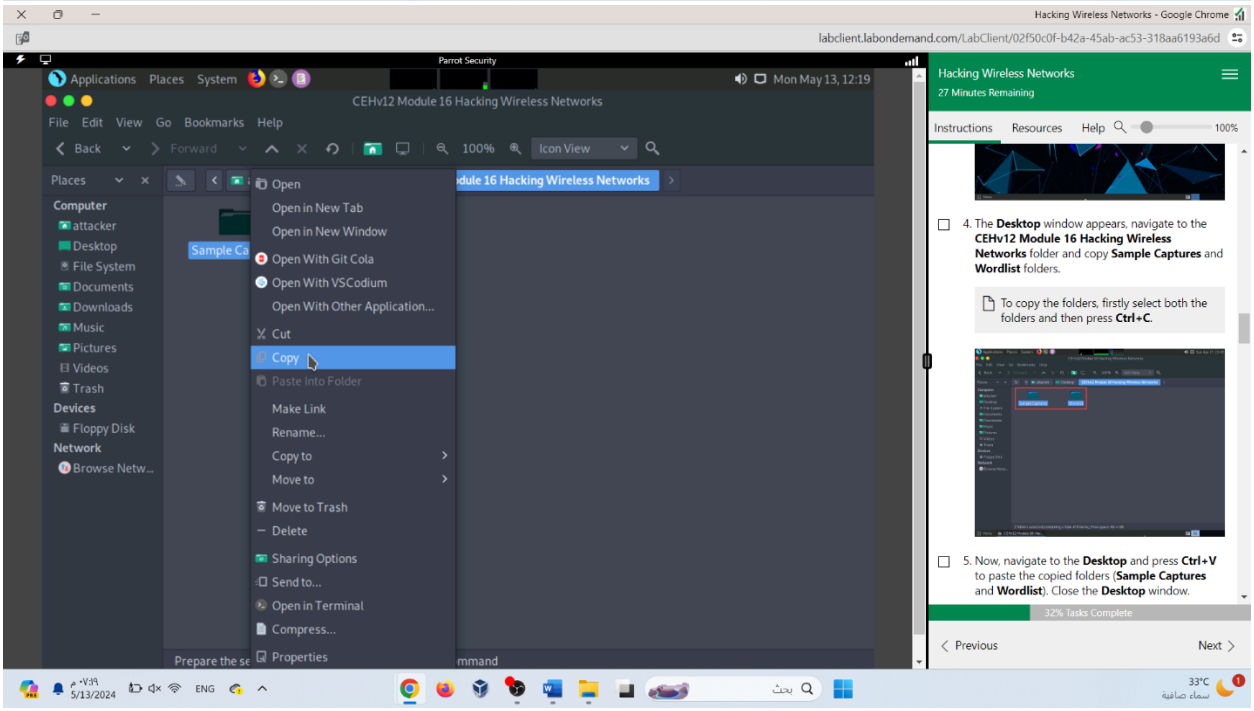

Hacking Wireless Networks - Google Chrome
labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d
Windows 11
The Wireshark Network Analyzer
Wireshark · Open Capture File
Look in: Sample Captures
Name
Date modified
Type
WEPcrack-01.cap
WEPcrack-01.csv
WEPcrack-01.kismet.csv
WEPcrack-01.kismet.netxml
WPA2crack-01.cap
WPA2crack-01.csv
WPA2crack-01.kismet.csv
WPA2crack-01.kismet.netxml
Quick access
Desktop
Libraries
This PC
Network
File name: WEPcrack-01.cap
Files of type: All Files
Open
Cancel
Help
Read filter:
Format:
Size:
Start / elapsed: 2018-01-13 01:36:10 / 00
Ready to load or capture
No Packets
Profile: Default
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...
5/13/2024
33°C

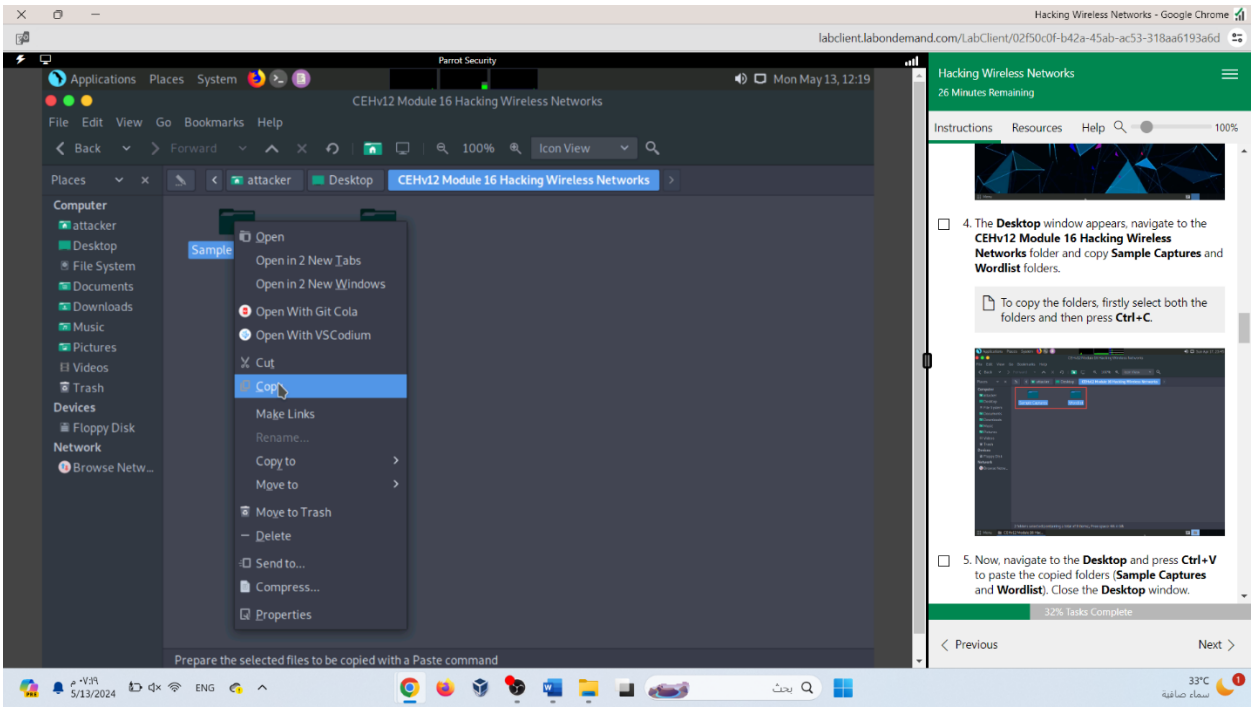

Hacking Wireless Networks - Google Chrome
labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d
Windows 11
WEPcrack-01.cap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
34 10.794686 D-LinkIn_97:36:30 (… 802.11 10 Acknowledgement, Flag
35 10.794704 D-LinkIn_97:36:30 Netgear_e4:38:00 802.11 82 QoS Data, SN=1627, FN
36 10.794686 D-LinkIn_97:36:30 (… 802.11 10 Acknowledgement, Flag
37 10.796240 D-LinkIn_97:36:30 Netgear_e4:38:00 802.11 94 QoS Data, SN=1628, FN
38 10.796222 D-LinkIn_97:36:30 (… 802.11 10 Acknowledgement, Flag
39 10.796220 Netgear_e4:38:00 D-LinkIn_97:36:30 802.11 82 QoS Data, SN=2939, FN
Frame 38: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
Encapsulation type: IEEE 802.11 Wireless LAN (20)
Arrival Time: Jan 13, 2018 01:36:21.236070000 Pacific Standard Time
[Time shift for this packet: 0.000000000 seconds]
Epoch Time: 1515836181.236070000 seconds
[Time delta from previous captured frame: -0.000018000 seconds]
[Time delta from previous displayed frame: -0.000018000 seconds]
[Time since reference or first frame: 10.796222000 seconds]
Frame Number: 38
Frame Length: 10 bytes (80 bits)
Capture Length: 10 bytes (80 bits)
[Frame is marked: False]
[Frame is ignored: False]
0000 d4 00 3a 00 40 9b cd 97 36 30
WEPcrack-01.cap
Packets: 2464654 · Displayed: 2464654 (100.0%)
Profile: Default
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), Omnipeek
0% Tasks Complete
Previous
Next: Lab 2: Perform...
5/13/2024
33°C

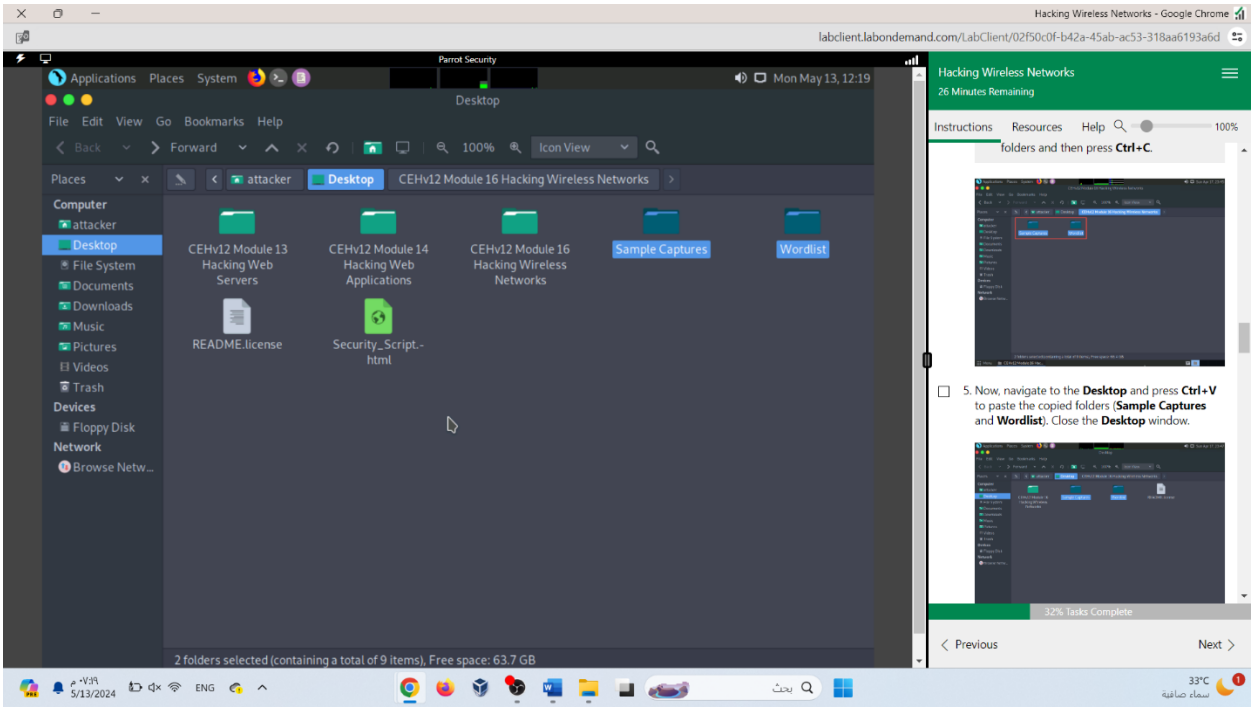
Lab 02: Perform Wireless Attacks

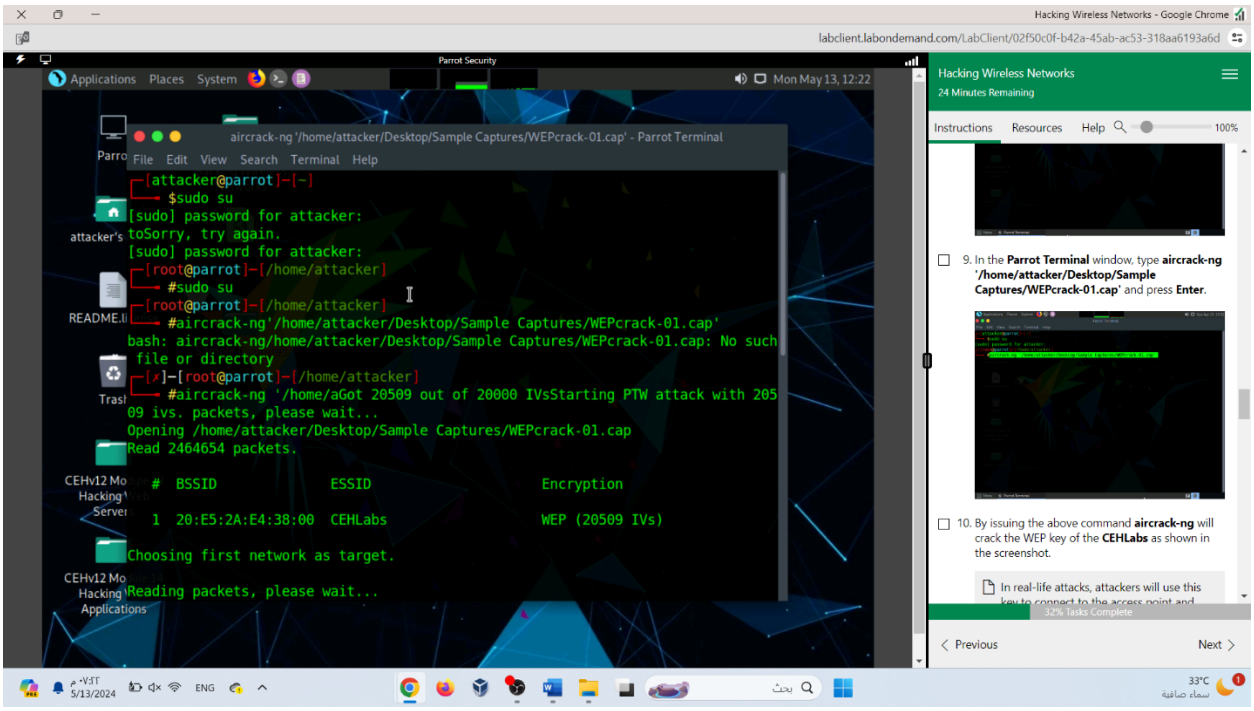
Task 1: Crack a WEP network using Aircrack-ng

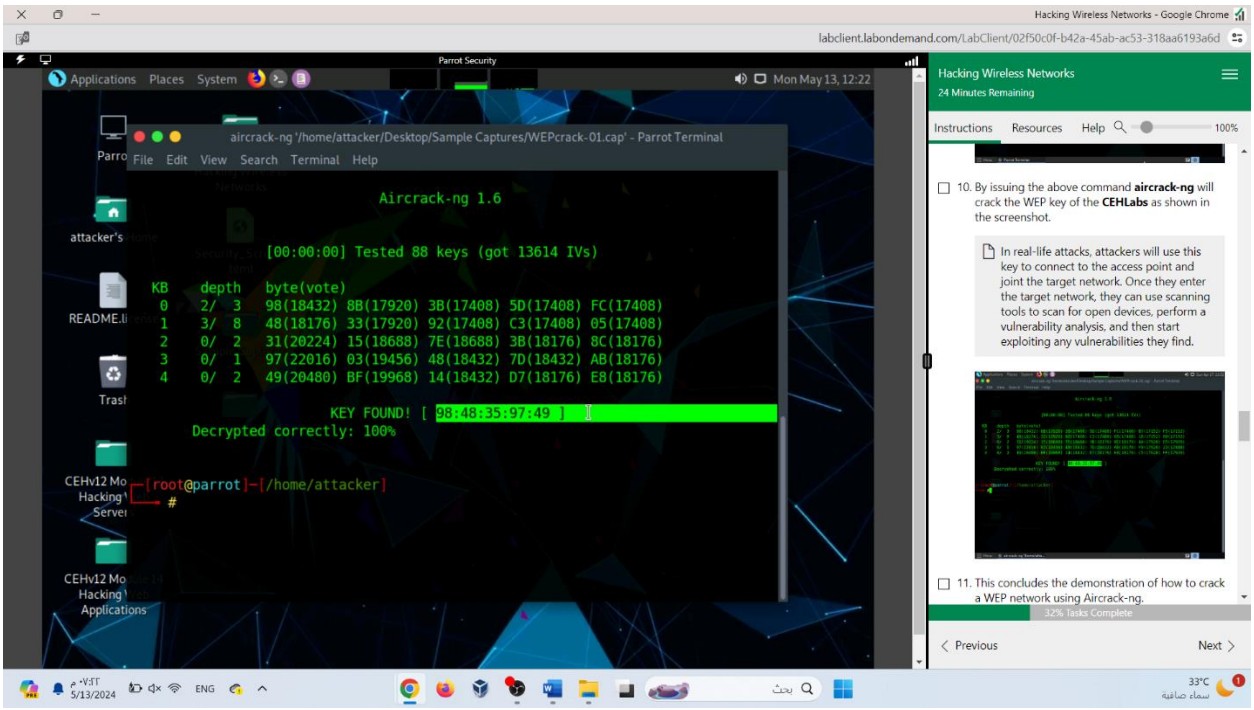





Hacking Wireless Networks - Google Chrome
labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d
Parrot Security
Applications Places System
Mon May 13, 12:19
CEHv12 Module 16 Hacking Wireless Networks
File Edit View Go Bookmarks Help
Back Forward 100% Icon View
Places attacker Desktop CEHv12 Module 16 Hacking Wireless Networks
Computer
attacker
Desktop
File System
Documents
Downloads
Music
Pictures
Videos
Trash
Devices
Floppy Disk
Network
Browse Netw...
Sample
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
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
5/13/2024
ENG
33°C


Hacking Wireless Networks - Google Chrome
labclient.labondemand.com/LabClient/02f50c0f-b42a-45ab-ac53-318aa6193a6d
Parrot Security
Applications Places System
Mon May 13, 12:19
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 Netw...
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
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
5/13/2024
ENG
33°C


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
File Edit View Search Terminal Help
[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 20509 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
32% Tasks Complete
Previous
Next
5/13/2024
ENG
33°C


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
File Edit View Search Terminal Help
Aircrack-ng 1.6
[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 joint 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
5/13/2024
ENG
33°C

Task 2: Crack a WPA2 Network using Aircrack-ng