



PRIFYSGOL CYMRU
Y Drindod Dewi Sant
UNIVERSITY OF WALES
Trinity Saint David
SWANSEA - ABERTAWE

Applied Computing

Wales Institute of Science and Art (WISA)

Advanced Cybersecurity (ACCB6000)



Lab 5: Post F(Ph)ishing



Reconnaissance



Scanning



Gaining Access

Nitheesh Murugan Kaliyamurthy – n.kaliyamurthy@uwtsd.ac.uk

Cisco | **Networking Academy**[®]
Mind Wide Open[™]

What we do?

1. Set up your Lab
2. Use tools to gain access
 - *Metagoofil*
 - *Metasploit*
 - *HackKey*
3. Record your reflections

Disclaimer

Do not try these in unsupervised environments/ real time environments. Attempting to use certain tools in real time environments or without proper written consents from the owners of the network is punishable offense. All our labs are only for educational purposes and to be practiced under supervised environments.

Takeaway

Document maintenance now adds value and credit for the owners for your life time!!! See how.... Yes, there is a shared folder created which could be assessable for all the Cybersecurity students. You could post your maintenance/ manual/ troubleshooting steps with your name and it will remain there for years. Each poster will be awarded with for their work 

Description

Metagoofil: Used to gather data/ available documents which are public. It uses search engines to search, download and then generate a report. Lets look what we can get!!!

Recommendations

You could use any of the following as per your convenience. Highlighted is used here.

- ✓ **VirtualBox**
- ✓ VMware Workstation Pro
- ✓ VMware Fusion Pro (for Mac),
- ✓ VMware ESXi
- ✓ Microsoft Hyper-V

- Virtual Machines running Kali Linux (*Attacker*), Windows 7/ XP
- Internet access

The configurations/ ip addressing below listed is based on this topology. Make necessary changes as you work on.



<u>Win 7</u>	<u>Win XP</u>	<u>Kali</u>
<u>10.0.2.6</u>	<u>10.0.2.4</u>	<u>10.0.2.15</u>
<u>10.0.2.1</u>	<u>10.0.2.1</u>	<u>10.0.2.1</u>



Task 1: Use Metagoofil

In Kali Linux:

```
kali@kali:~$ metagoofil
```

```
bash: metagoofil: command not found
```

```
kali@kali:~$ apt -get install metagoofil
```

```
E: Command line option 'g' [from -get] is not understood in combination with the other options.
```

```
kali@kali:~$ sudo metagoofil [sudo] password for kali:
```

```
sudo: metagoofil: command not found
```

```
kali@kali:~$ sudo apt-get install metagoofil
```

```
Reading package lists... Done
```

```
Building dependency tree
```

```
Reading state information... Done
```

```
E: Unable to locate package metagoofil
```

```
kali@kali:~$ sudo apt-get update
```

```
Get:1 http://kali.download/kali kali-rolling InRelease [30.5 kB]
```

```
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [16.7 MB]
```

```
Get:3 http://kali.download/kali kali-rolling/contrib amd64 Packages [101 kB]
```

```
Get:4 http://kali.download/kali kali-rolling/non-free amd64 Packages [200 kB]
```

Fetches 17.1 MB in 4s (4,590 kB/s)

Reading package lists... Done

kali@kali:~\$ sudo apt-get install checkinstall

Reading package lists... Done

Building dependency tree

Reading state information... Done

Suggested packages:

gettext

The following NEW packages will be installed:

checkinstall

0 upgraded, 1 newly installed, 0 to remove and 860 not upgraded.

Need to get 114 kB of archives.

After this operation, 455 kB of additional disk space will be used. Get:1

http://kali.download/kali kali-rolling/main amd64 checkinstall amd64

1.6.2+git20170426.d24a630-2 [114 kB]

Fetches 114 kB in 0s (264 kB/s)

Selecting previously unselected package checkinstall.

(Reading database ... 276117 files and directories currently installed.)

Preparing to unpack .../checkinstall_1.6.2+git20170426.d24a630-2_amd64.deb ...

Unpacking checkinstall (1.6.2+git20170426.d24a630-2) ...

Setting up checkinstall (1.6.2+git20170426.d24a630-2) ...

Processing triggers for man-db (2.9.3-2) ...

Processing triggers for kali-menu (2020.3.2) ...

```
kali@kali:~$ sudo apt-get install metagoofil
```

```
Reading package lists... Done
```

```
Building dependency tree
```

```
Reading state information... Done
```

```
The following additional packages will be installed:
```

```
python3-googlesearch
```

```
The following NEW packages will be installed: metagoofil
```

```
python3-googlesearch
```

```
0 upgraded, 2 newly installed, 0 to remove and 860 not upgraded.
```

```
Need to get 61.6 kB of archives.
```

```
After this operation, 223 kB of additional disk space will be used.
```

```
Do you want to continue? [Y/n] Y
```

```
Get:1 http://kali.download/kali kali-rolling/main amd64 python3-googlesearch all 2.0.2-0kali1 [45.3 kB]
```

```
Get:2 http://kali.download/kali kali-rolling/main amd64 metagoofil all 2.2.+git201903070kali1 [16.3 kB]
```

```
Fetchd 61.6 kB in 1s (114 kB/s)
```

```
Selecting previously unselected package python3-googlesearch. (Reading database ... 276150 files and directories currently installed.) Preparing to unpack .../python3-googlesearch_2.0.2-0kali1_all.deb ...
```

```
Unpacking python3-googlesearch (2.0.2-0kali1) ...
```

```
Selecting previously unselected package metagoofil.
```

```
Preparing to unpack .../metagoofil_2.2.+git20190307-0kali1_all.deb ...
```

```
Unpacking metagoofil (2.2.+git20190307-0kali1) ...
```

```
Setting up python3-googlesearch (2.0.2-0kali1) ...
```

```
Setting up metagoofil (2.2.+git20190307-0kali1) ...
```

```
kali@kali:~$ sudo metagoofil usage: metagoofil.py [-h] -d DOMAIN [-e DELAY] [-f] [-i URL_TIMEOUT] [-l SEARCH_MAX] [-n DOWNLOAD_FILE_LIMIT] [-o SAVE_DIRECTORY] [-r NUMBER_OF_THREADS] [-t FILE_TYPES] [-u [USER_AGENT]] [-w] metagoofil.py: error: the following arguments are required: -d, -t
```

```
kali@kali:~$ sudo metagoofil -d apple.com -t doc,pdf -l 200 -n 5 -o applefiles -f [+]
```

Adding -w for you

[*] Downloaded files will be saved here: applefiles

[+] Creating folder: applefiles

[*] Searching for 200 .doc files and waiting 30.0 seconds between searches

[+] Downloading file - [41472 bytes]

<http://store.apple.com/Catalog/US/Images/ProofofAcademicIdentificationForm.doc>

[+] Downloading file - [76288 bytes]

http://store.apple.com/Catalog/China/Images/rejection_letter.doc

[+] Downloading file - [86528 bytes]

https://opensource.apple.com/source/Security/Security-29770/doc/AppleTP_Spec.doc

[+] Downloading file - [95744 bytes]

https://opensource.apple.com/source/Security/Security31122/doc/Apple_OID_Assignments.doc

[+] Downloading file - [492544 bytes]

<https://opensource.apple.com/source/bootp/bootp254/Documentation/BDSP.doc>

[*] Searching for 200 .pdf files and waiting 30.0 seconds between searches

[+] Downloading file - [523915 bytes]

https://www.apple.com/jp/support/cip/pdfs/optidrive_pmg4mdd.j.pdf

[+] Downloading file - [147348 bytes]

<https://www.apple.com/privacy/parentaldisclosureconsent.pdf>

[+] Downloading file - [650435 bytes]

https://www.apple.com/jp/support/cip/pdfs/powersupply_pmg4mdd.j.pdf

[+] Downloading file - [394620 bytes]

https://www.apple.com/jp/support/cip/pdfs/battery_pmg4mdd.j.pdf

[+] Downloading file - [337 bytes]

http://www.apple.com/certificateauthority/Application_Integration_CPS/

[+] Total download: 2509231 bytes / 2450.42 KB / 2.39 MB [+] Done!

Now, you could go to the folder and check the files downloaded...

-d DOMAIN

-t FILE_TYPES

-l SEARCH_MAX]

-n DOWNLOAD_FILE_LIMIT

-o SAVE_DIRECTORY

-f Output File

kali@kali:~\$ sudo metagoofil -d apple.com -t doc,pdf -l 200 -n 5 -o applefiles -f

Record your reflections about the tool you used.

Because I am not familiar with Linux, the commands seemed hard to understand. Once run (following the explanation) I was amazed at the information that can be gathered by using this tool (even though on this example most of the docs downloaded appear to be in Chinese!). I can certainly see how this could be used for digital reconnaissance work.

Task 2: Use Metasploit

In Kali Linux:

The Backend Database support... PostgreSQL

When attempting to do a pen-test, always remember based on the scenario it may take a long time to complete. In that case, we can use the backend database support for db. Using this support, you could store your results now and then.

Commands used here!!! – A summary

```
root@kali:~# systemctl start postgresql root@kali:~#
```

```
msfdb init
```

```
root@kali:~# msfdb
```

```
root@kali:~# sudo msfconsole
```

```
msf > services
```

The services command allows us to display the services running on the hosts

Hints

To modify the database configuration file, we can edit the database.yml file located in /usr/share/metasploit-framework/config/database.yml:

```
kali@kali: ~  
File Actions Edit View Help  
64 bytes from 10.0.2.6: icmp_seq=743 ttl=128 time=0.391 ms  
64 bytes from 10.0.2.6: icmp_seq=744 ttl=128 time=0.441 ms  
64 bytes from 10.0.2.6: icmp_seq=745 ttl=128 time=0.412 ms  
64 bytes from 10.0.2.6: icmp_seq=746 ttl=128 time=0.387 ms  
64 bytes from 10.0.2.6: icmp_seq=747 ttl=128 time=0.411 ms  
^C  
--- 10.0.2.6 ping statistics ---  
747 packets transmitted, 711 received, 4.81928% packet loss, time 761044ms  
rtt min/avg/max/mdev = 0.385/1.466/20.163/3.189 ms  
kali@kali:~$ systemctl start postgresql  
kali@kali:~$ msfdb init  
[i] Error: /usr/bin/msfdb must be run as root  
kali@kali:~$ sudo msfdb init  
[sudo] password for kali:  
[i] Database already started  
[i] The database appears to be already configured, skipping initialization  
kali@kali:~$ sudo msfdb  
Manage the metasploit framework database  
  
msfdb init      # start and initialize the database  
msfdb reinit    # delete and reinitialize the database  
msfdb delete    # delete database and stop using it  
msfdb start     # start the database  
msfdb stop      # stop the database  
msfdb status    # check service status  
msfdb run       # start the database and run msfconsole  
  
kali@kali:~$ sudo metasp  
sudo: metasp: command not found  
kali@kali:~$ sudo msfconsole
```

```

kali@kali: ~
01:38 AM

kali@kali: ~
File Actions Edit View Help

[... Metasploit Framework Output ...]

Metasploit tip: You can upgrade a shell to a Meterpreter session on many platforms using sessio
ns -u <session_id>

msf5 > db status
[*] Connected to msf. Connection type: postgresql.
msf5 >

```

In Kali Linux:

Auxiliary Modules... in Metasploit

We shall use Auxiliary modules like Enumerator (The way to collect information passively) to get the DNS details like zone transfers, reverse lookups, SRV record brute forcing etc.

```

kali@kali: ~
File Actions Edit View Help
msf5 > services -S Apache 10.0.2.15
Services
=====
host port proto name state info
-----
msf5 > use auxiliary/gather/enum_dns
msf5 auxiliary(gather/enum_dns) > info

Name: DNS Record Scanner and Enumerator
Module: auxiliary/gather/enum_dns
License: Metasploit Framework License (BSD)
Rank: Normal

Provided by:
Carlos Perez <carlos_perez@darkoperator.com>
Nixawk

Check supported: No

Basic options:
  Name          Current Setting  Required  Descripti
  --          -
  DOMAIN        true              yes       The targe
  t domain
  ENUM_A        true              yes       Enumerate
  DNS A record

```

Commands used here!!! – A summary

```

root@kali:~# Systemctl start postgresql
Sudo msfdb init
Sudo msfdb
Sudo msfconsole
Msf5> db_status
Msf5> use auxiliary/gather/enum_dns
> info

```

```

kali@kali: ~
File Actions Edit View Help

Description:
  This module can be used to gather information about a domain from a
  given DNS server by performing various DNS queries such as zone
  transfers, reverse lookups, SRV record brute forcing, and other
  techniques.

References:
  https://cvedetails.com/cve/CVE-1999-0532/
  OSVDB (492)

msf5 auxiliary(gather/enum_dns) > use auxiliary/gather/enum_dns
msf5 auxiliary(gather/enum_dns) > set domain nitheesh.com
domain => nitheesh.com
msf5 auxiliary(gather/enum_dns) > set THREADS 5
THREADS => 5
msf5 auxiliary(gather/enum_dns) > run

[*] Querying DNS NS records for nitheesh.com
[+] nitheesh.com NS: ns1.fastsecureservers.com
[+] nitheesh.com NS: ns2.fastsecureservers.com
[*] Attempting DNS AXFR for nitheesh.com from ns1.fastsecureservers.com
[*] Attempting DNS AXFR for nitheesh.com from ns2.fastsecureservers.com
[*] Querying DNS CNAME records for nitheesh.com
[*] Querying DNS NS records for nitheesh.com
[*] Querying DNS MX records for nitheesh.com
[*] Querying DNS SOA records for nitheesh.com
[*] Querying DNS TXT records for nitheesh.com
[*] Querying DNS SRV records for nitheesh.com
[*] Auxiliary module execution completed
msf5 auxiliary(gather/enum_dns) >

kali@kali: ~
File Actions Edit View Help

msf5 auxiliary(gather/enum_dns) > use auxiliary/gather/enum_dns
msf5 auxiliary(gather/enum_dns) > set domain nitheesh.com
domain => nitheesh.com
msf5 auxiliary(gather/enum_dns) > set THREADS 5
THREADS => 5
msf5 auxiliary(gather/enum_dns) > run

[*] Querying DNS NS records for nitheesh.com
[+] nitheesh.com NS: ns1.fastsecureservers.com
[+] nitheesh.com NS: ns2.fastsecureservers.com
[*] Attempting DNS AXFR for nitheesh.com from ns1.fastsecureservers.com
[*] Attempting DNS AXFR for nitheesh.com from ns2.fastsecureservers.com
[*] Querying DNS CNAME records for nitheesh.com
[*] Querying DNS NS records for nitheesh.com
[*] Querying DNS MX records for nitheesh.com
[*] Querying DNS SOA records for nitheesh.com
[*] Querying DNS TXT records for nitheesh.com
[*] Querying DNS SRV records for nitheesh.com
[*] Auxiliary module execution completed
msf5 auxiliary(gather/enum_dns) >
msf5 auxiliary(gather/enum_dns) > back
msf5 > use auxiliary/gather/corpwatch_lookup_name
msf5 auxiliary(gather/corpwatch_lookup_name) > set COMPANY_NAME VSIKMA
COMPANY_NAME => VSIKMA
msf5 auxiliary(gather/corpwatch_lookup_name) > set LIMIT 10
LIMIT => 10
msf5 auxiliary(gather/corpwatch_lookup_name) > run

[-] No companies returned
[*] Auxiliary module execution completed
msf5 auxiliary(gather/corpwatch_lookup_name) >

```

We shall use Auxiliary modules like Enumerator (The way to collect information actively) by setting ENUM_BRT (Brute forcing mode) to true.

```

File  Actions  Edit  View  Help
t domain
ENUM_A true yes Enumerate
DNS A record
ENUM_AXFR true yes Initiate
a zone transfer against each NS record
ENUM_BRT false yes Brute for
ce subdomains and hostnames via the supplied wordlist
ENUM_CNAME true yes Enumerate
DNS CNAME record
ENUM_MX true yes Enumerate
DNS MX record
ENUM_NS true yes Enumerate
DNS NS record
ENUM_RVL false yes Reverse l
ookup a range of IP addresses
ENUM_SOA true yes Enumerate
DNS SOA record
ENUM_SRV true yes Enumerate
the most common SRV records
ENUM_TLD false yes Perform a
TLD expansion by replacing the TLD with the IANA TLD list
ENUM_TXT true yes Enumerate
DNS TXT record
IPRANGE no The targe
t address range or CIDR identifier
NS no Specify t
he nameservers to use for queries, space separated
Proxies no A proxy c
hain of format type:host:port[,type:host:port][ ... ]
RPORT 53 yes The targe
t port (TCP)

```

We shall use Auxiliary modules like Enumerator to search for company names too...

```

kali@kali: ~
File Actions Edit View Help
[*] Querying DNS MX records for nitheesh.com
[*] Querying DNS SOA records for nitheesh.com
[*] Querying DNS TXT records for nitheesh.com
[*] Querying DNS SRV records for nitheesh.com
[*] Auxiliary module execution completed
msf5 auxiliary(gather/enum_dns) >
msf5 auxiliary(gather/enum_dns) > back
msf5 > use auxiliary/gather/corpwatch_lookup_name
msf5 auxiliary(gather/corpwatch_lookup_name) > set COMPANY_NAME VSIGMA
COMPANY_NAME => VSIGMA
msf5 auxiliary(gather/corpwatch_lookup_name) > set LIMIT 10
LIMIT => 10
msf5 auxiliary(gather/corpwatch_lookup_name) > run

[-] No companies returned
[*] Auxiliary module execution completed
msf5 auxiliary(gather/corpwatch_lookup_name) > set COMPANY_NAME INFOSYS
COMPANY_NAME => INFOSYS
msf5 auxiliary(gather/corpwatch_lookup_name) > set LIMIT 10
LIMIT => 10
msf5 auxiliary(gather/corpwatch_lookup_name) > run

[*] Company Information
-----
[*] CorpWatch (cw) ID: cw_16272
[*] Company Name: Infosys Ltd
[*] Address: ELECTRONICS CITY HOSUR RD, BANGALORE KARNATAKA INDIA, BANGALORE K7 560 100
[*] Sector: Business services
[*] Industry: Services-computer programming services
[*] Auxiliary module execution completed
msf5 auxiliary(gather/corpwatch_lookup_name) >

```

```

kali@kali: ~
File Actions Edit View Help
msf5 auxiliary(gather/corpwatch_lookup_name) > set COMPANY_NAME INFOSYS
COMPANY_NAME => INFOSYS
msf5 auxiliary(gather/corpwatch_lookup_name) > set LIMIT 10
LIMIT => 10
msf5 auxiliary(gather/corpwatch_lookup_name) > run

[*] Company Information
-----
[*] CorpWatch (cw) ID: cw_16272
[*] Company Name: Infosys Ltd
[*] Address: ELECTRONICS CITY HOSUR RD, BANGALORE KARNATAKA INDIA, BANGALORE K7 560 100
[*] Sector: Business services
[*] Industry: Services-computer programming services
[*] Auxiliary module execution completed
msf5 auxiliary(gather/corpwatch_lookup_name) > back
msf5 > use auxiliary/gather/searchengine_subdomains_collector
msf5 auxiliary(gather/searchengine_subdomains_collector) > set TARGET cisco.com
TARGET => cisco.com
msf5 auxiliary(gather/searchengine_subdomains_collector) > run

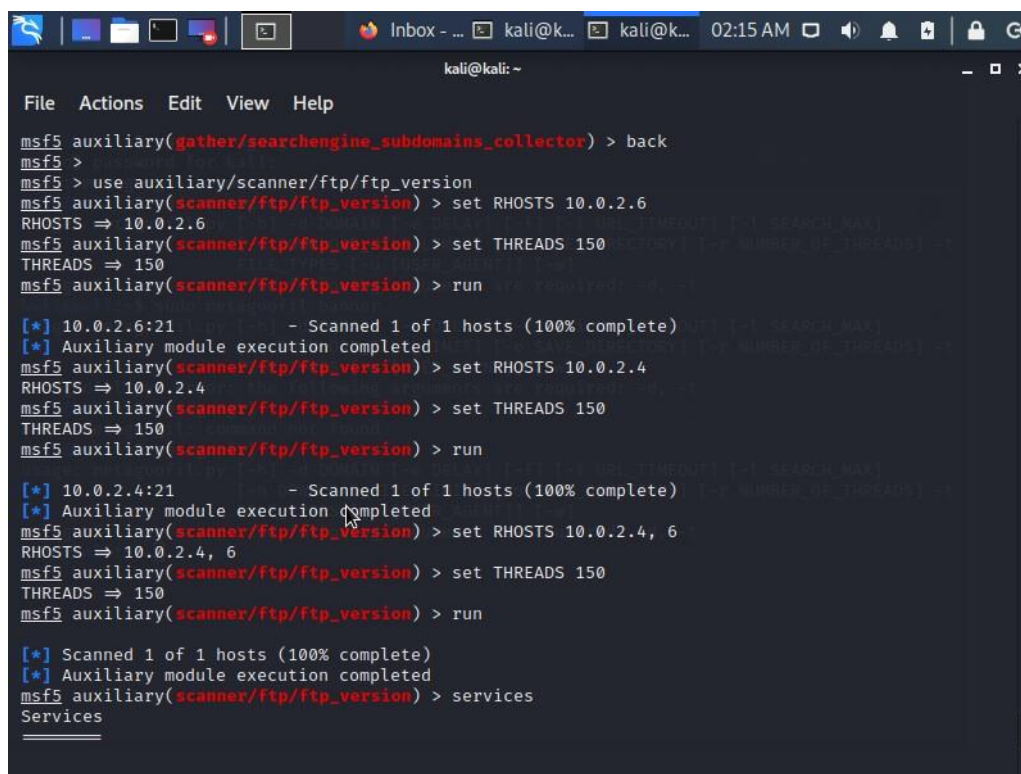
[*] Searching Bing for subdomains from domain:cisco.com
[*] Searching Yahoo for subdomains from domain:cisco.com
[*] Auxiliary module execution completed
msf5 auxiliary(gather/searchengine_subdomains_collector) > set TARGET www.cisco.com
TARGET => www.cisco.com
msf5 auxiliary(gather/searchengine_subdomains_collector) > run

[*] Searching Bing for subdomains from domain:www.cisco.com
[*] Searching Yahoo for subdomains from domain:www.cisco.com
[*] Auxiliary module execution completed
msf5 auxiliary(gather/searchengine_subdomains_collector) > set TARGET www.microsoft.com

```

We shall use Auxiliary modules like Enumerator to search for sub domains too...

We shall use Auxiliary modules like Enumerator to search for ftp too...



```
kali@kali: ~  
File Actions Edit View Help  
msf5 auxiliary(gather/searchengine_subdomains_collector) > back  
msf5 >  
msf5 > use auxiliary/scanner/ftp/ftp_version  
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.0.2.6  
RHOSTS => 10.0.2.6  
msf5 auxiliary(scanner/ftp/ftp_version) > set THREADS 150  
THREADS => 150  
msf5 auxiliary(scanner/ftp/ftp_version) > run  
[*] 10.0.2.6:21 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.0.2.4  
RHOSTS => 10.0.2.4  
msf5 auxiliary(scanner/ftp/ftp_version) > set THREADS 150  
THREADS => 150  
msf5 auxiliary(scanner/ftp/ftp_version) > run  
[*] 10.0.2.4:21 - Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.0.2.4, 6  
RHOSTS => 10.0.2.4, 6  
msf5 auxiliary(scanner/ftp/ftp_version) > set THREADS 150  
THREADS => 150  
msf5 auxiliary(scanner/ftp/ftp_version) > run  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf5 auxiliary(scanner/ftp/ftp_version) > services  
Services
```

We shall use Auxiliary modules like Enumerator to search for the users too...

We shall use SMTP for that.

To understand, Generally, SMTP uses to work with names of the users and its emails. So, we can use SMTP services to get those details.

```

kali@kali: ~
File Actions Edit View Help
10.0.2.2 2869 tcp 10.0.2.2 2869 open
10.0.2.2 3389 tcp 10.0.2.2 3389 open
10.0.2.2 4466 tcp 10.0.2.2 4466 open
10.0.2.2 5357 tcp 10.0.2.2 5357 open
10.0.2.4 135 tcp 10.0.2.4 135 open [-w DELAY] [-s] [-i URL_TIMEOUT] [-i SEARCH_MAX]
10.0.2.4 139 tcp 10.0.2.4 139 open [-w DELAY] [-s] [-i URL_TIMEOUT] [-i SEARCH_MAX]
10.0.2.4 445 tcp 10.0.2.4 445 open [-w DELAY] [-s] [-i URL_TIMEOUT] [-i SEARCH_MAX]
10.0.2.4 554 tcp 10.0.2.4 554 open [-w DELAY] [-s] [-i URL_TIMEOUT] [-i SEARCH_MAX]
10.0.2.4 2869 tcp 10.0.2.4 2869 open
10.0.2.4 5357 tcp 10.0.2.4 5357 open [-w DELAY] [-s] [-i URL_TIMEOUT] [-i SEARCH_MAX]
msf5 auxiliary(scanner/ftp/ftp_version) >
msf5 auxiliary(scanner/ftp/ftp_version) > back
msf5 > use auxiliary/scanner/smtp/smtp_enum
msf5 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf5 auxiliary(scanner/smtp/smtp_enum) > set threads 150
threads => 150
msf5 auxiliary(scanner/smtp/smtp_enum) > run
[*] 10.0.2.4:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf5 auxiliary(scanner/smtp/smtp_enum) > set threads 150
threads => 150
msf5 auxiliary(scanner/smtp/smtp_enum) > run
[*] 10.0.2.6:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smtp/smtp_enum) >

```

In Kali Linux:**MS17-010 EternalBlue SMB Remote ... in Metasploit**

We shall use this vulnerable service for scanning phase... The above stated module is called ETERNALBLUE exploit, is said to be used as part of the WannaCry ransomware attack. It is used to commence a payload and affect Windows machines without security update MS17-010 for Microsoft Windows SMB Server SMBv1 Server

We will do this next Lab...