Metasploitable2

By: zyad Mohamed

Webpage_lap: the page

Install Machin : Installing

Tryhackme

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.
```

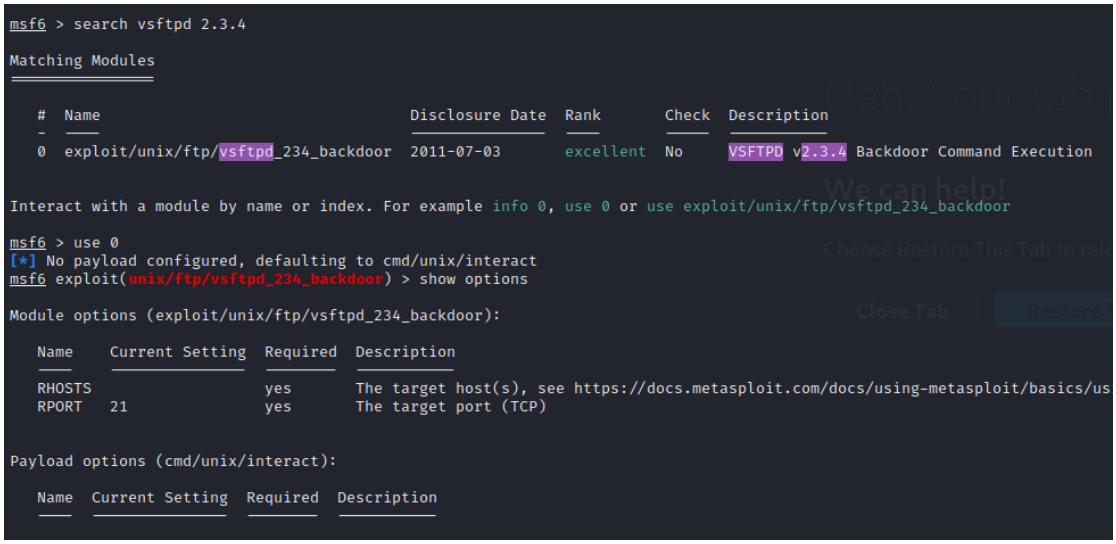
After that we will scan using Nmap as

```
┌──(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=O
| 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

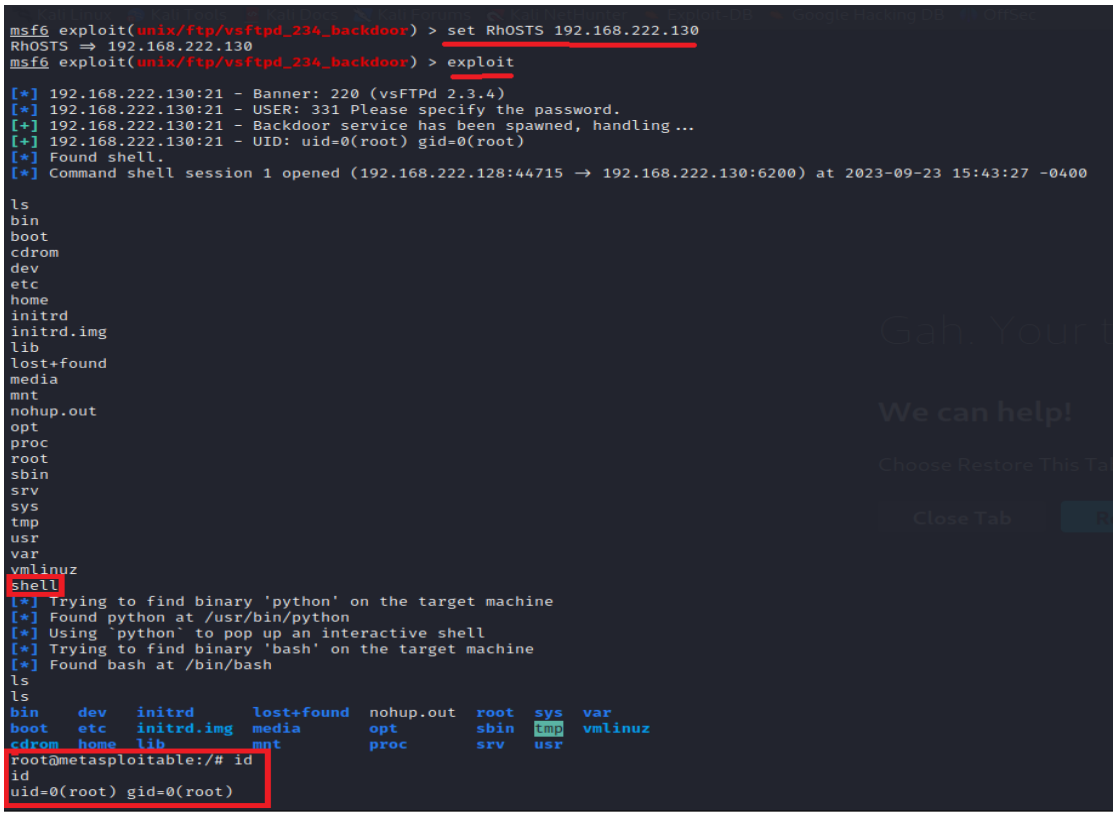
And we have a version if we want use Metasploit or anther tool or framework to exploit

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



We choice the bath for exploit and we show options

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



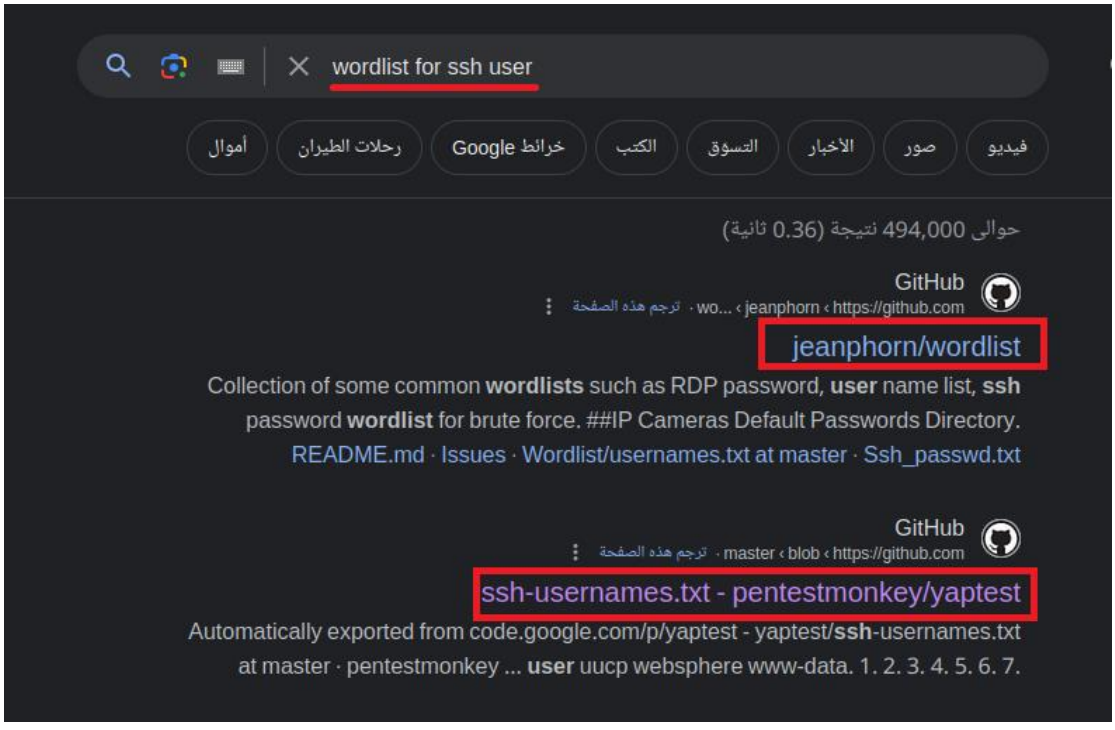
After we set ip we run and we gain access on victim I convert to shell

Boooom, we are root 😊

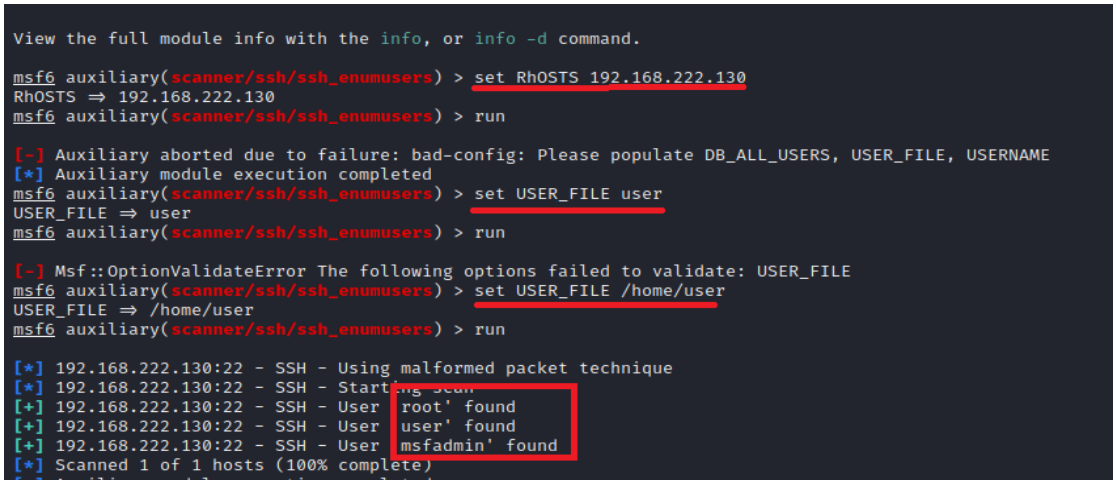
And in another way we can enumerate about ssh using Metasploit as:

```
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_creds                                    normal     No     Multi Gather OpenSSH PKI Credent
   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        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                         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        Single username to test (username spray)
   USER_FILE                      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

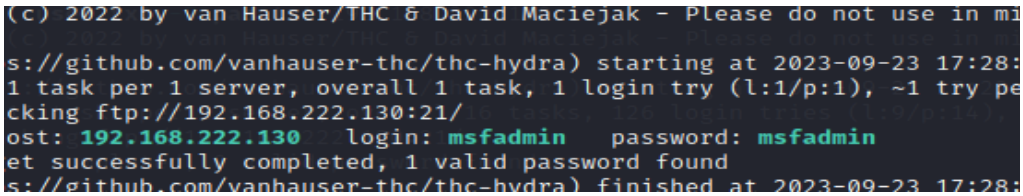


So we install and I rename it to (user) to use it in Metasploit as:

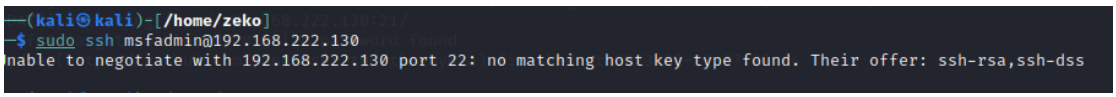


Her we find 3 users(root , user ,msfadmin)

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

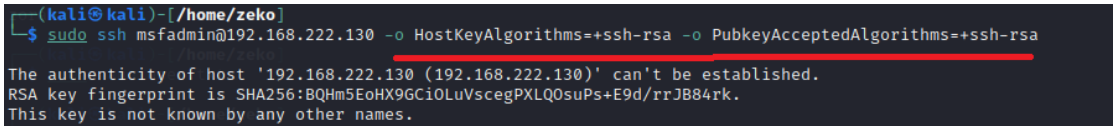


Now we will connect with ssh and try to escalate our privilege to root as

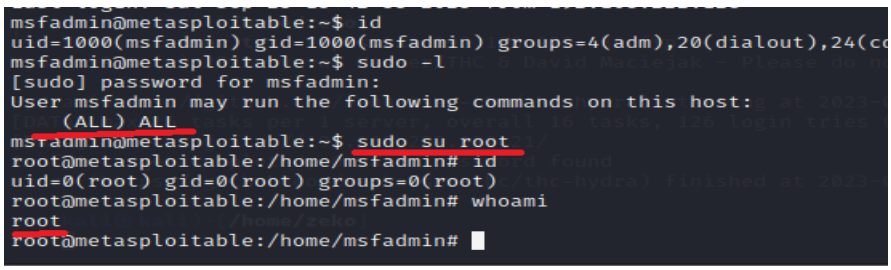


When I try to connect this massage is appear so that is search and found you must use the command to connect with ssh because the encryption

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



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



Booooooom , we are root 😊