



VILNIAUS GEDIMINO TECHNIKOS UNIVERSITETAS

FUNDAMENTINIŲ MOKSLŲ FAKULTETAS

INFORMACINIŲ SISTEMŲ KATEDRA

METASPLOIT

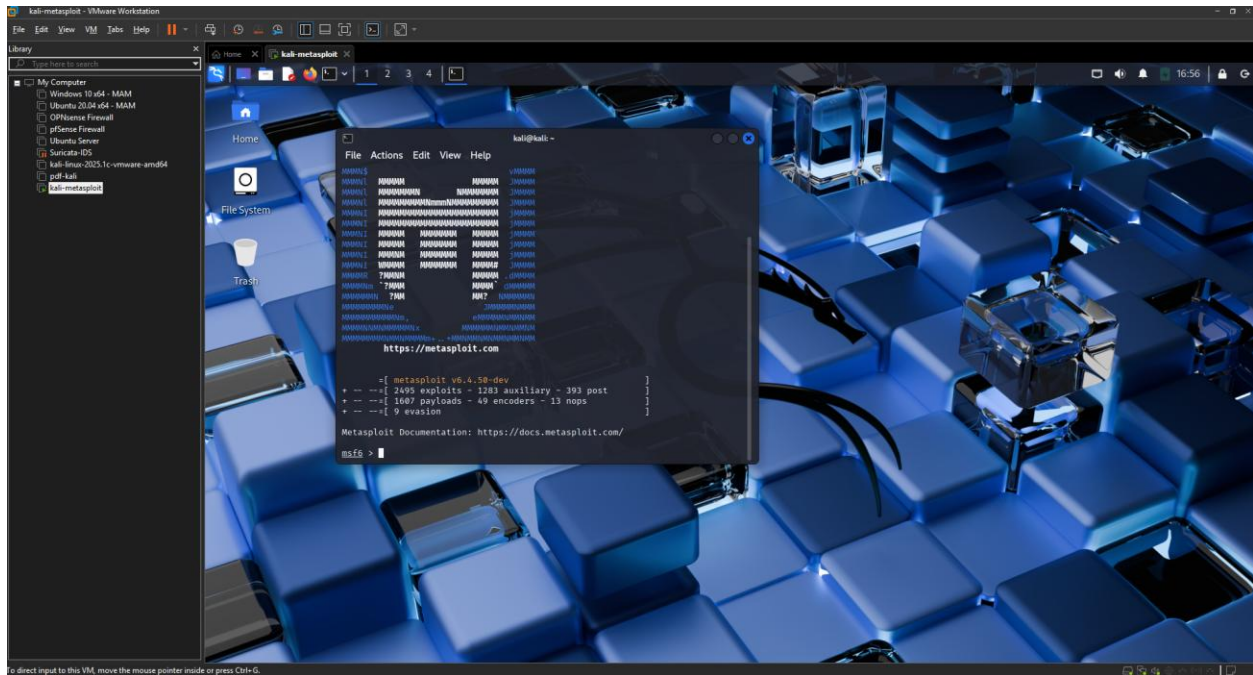
Saugumo patikros ir etiško įsilaužimo technologijų laboratorinis darbas nr. 3

Darbą atliko: Simonas Riška

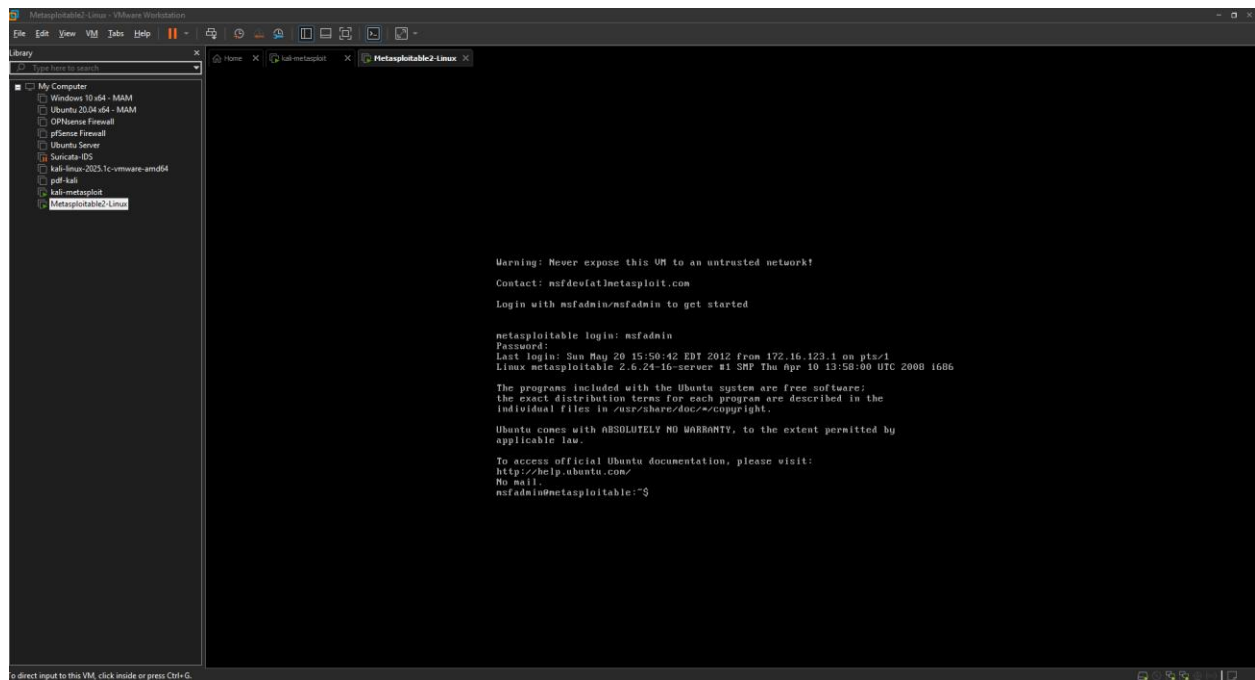
Darbą tikrino: lekt.



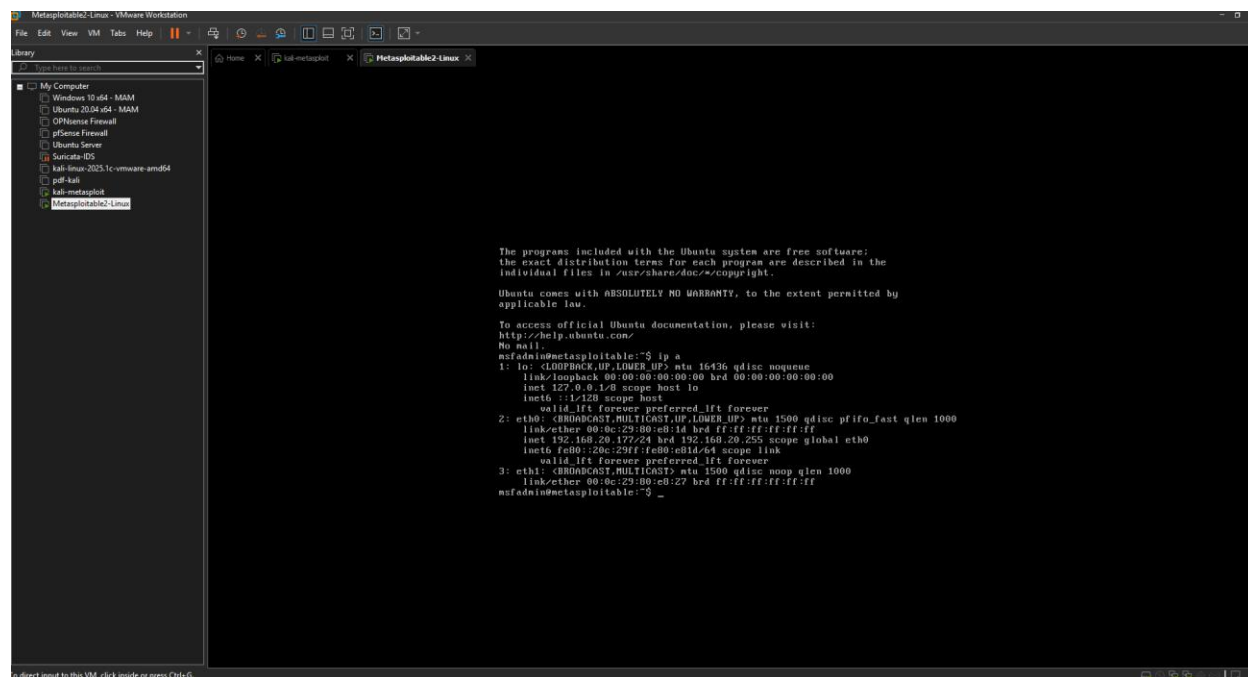
Šiame laboratoriniame darbe nusprendžiau naudoti Kali Linux operacinę sistemą VMware aplinkoje. Kali Linux turi jau įdiegtą Metasploit Framework, todėl papildomos diegimo procedūros nereikėjo. Įrodymui paleidau msfconsole komandą terminale, kuri parodė sėkmingą Metasploit Framework inicializaciją. Žemiau pateiktas ekrano vaizdas rodo veikiančią Metasploit aplinką:



Tuomet atsisiunčiau Metasploitable2 iš SourceForge ir importavau .vmx failą į VMware Workstation. Paleidau virtualią mašiną ir prisijungiau su naudotoju msfadmin. Žemiau pateikta ekrano nuotrauka įrodo, kad Metasploitable2 veikia tinkamai.



Norėdamos įsitikinti, kad virtualios mašinos gali komunikuoti tarpusavyje, iš Metasploit (Kali Linux) sistemos atlikau ping komandą į Metasploitable2 IP adresą. Metasploitable2 IP adresas buvo nustatytas su komanda `ip a - 192.168.20.177`. Iš Kali Linux (Metasploit) atlikta komanda `ping 192.168.20.177`. Rezultatai rodo sėkmingą ICMP atsakymą – tinklas tarp VM veikia puikiai:



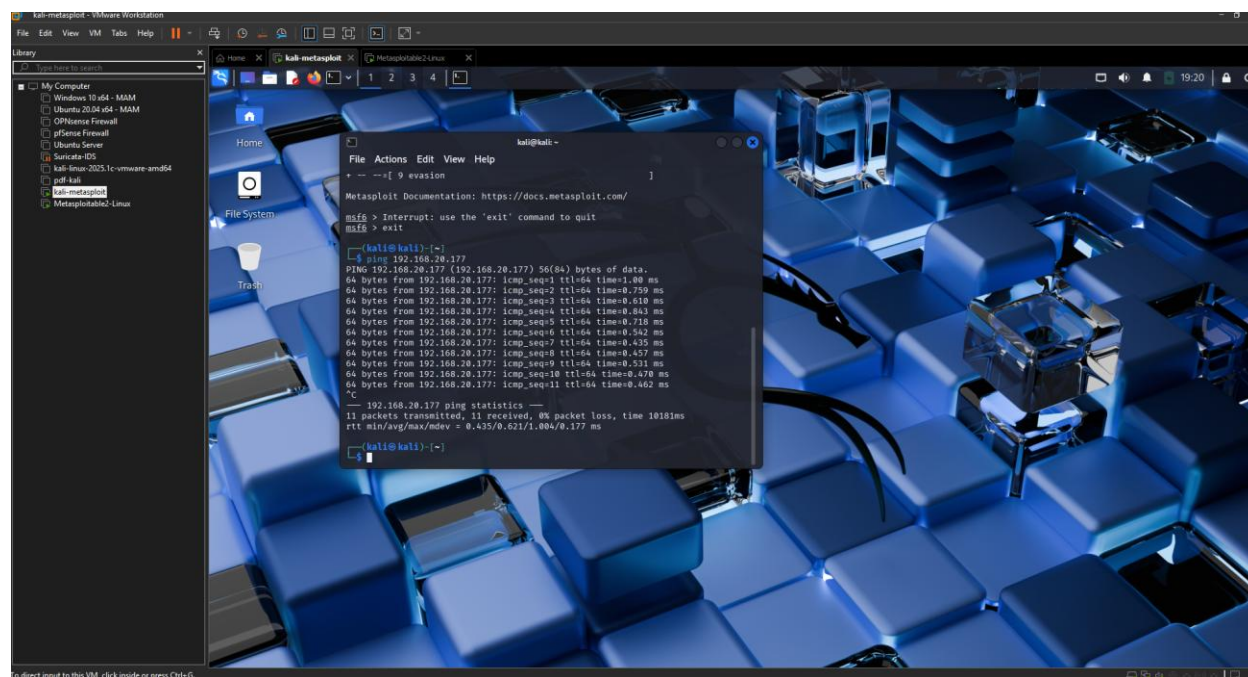
```
Metasploitable2-Linux - VMware Workstation
File Edit View VM Tabs Help
Library
Type text to search
My Computer
  Windows 10 x64 - MAM
  Ubuntu 20.04 x64 - MAM
  OPNsense Firewall
  pSense Firewall
  Ubuntu Server
  Suricata-IDS
  kali-linux-2025.1c-vmware-amd64
  kali-kali
  kali-metasploit
  Metasploitable2-Linux

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.

msfadmin@metasploitable2:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16384 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:1f:1e08:e01a/64 scope link
    inet 192.168.20.177/24 brd 192.168.20.255 scope global eth0
        inet6 fe80::20c:291f:1e08:e01a/64 scope link
            valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:1f:1e08:e01a/64 scope link
msfadmin@metasploitable2:~$
```



```
Kali-metasploit - VMware Workstation
File Edit View VM Tabs Help
Library
Type text to search
My Computer
  Windows 10 x64 - MAM
  Ubuntu 20.04 x64 - MAM
  OPNsense Firewall
  pSense Firewall
  Ubuntu Server
  Suricata-IDS
  kali-linux-2025.1c-vmware-amd64
  kali-kali
  kali-metasploit
  Metasploitable2-Linux

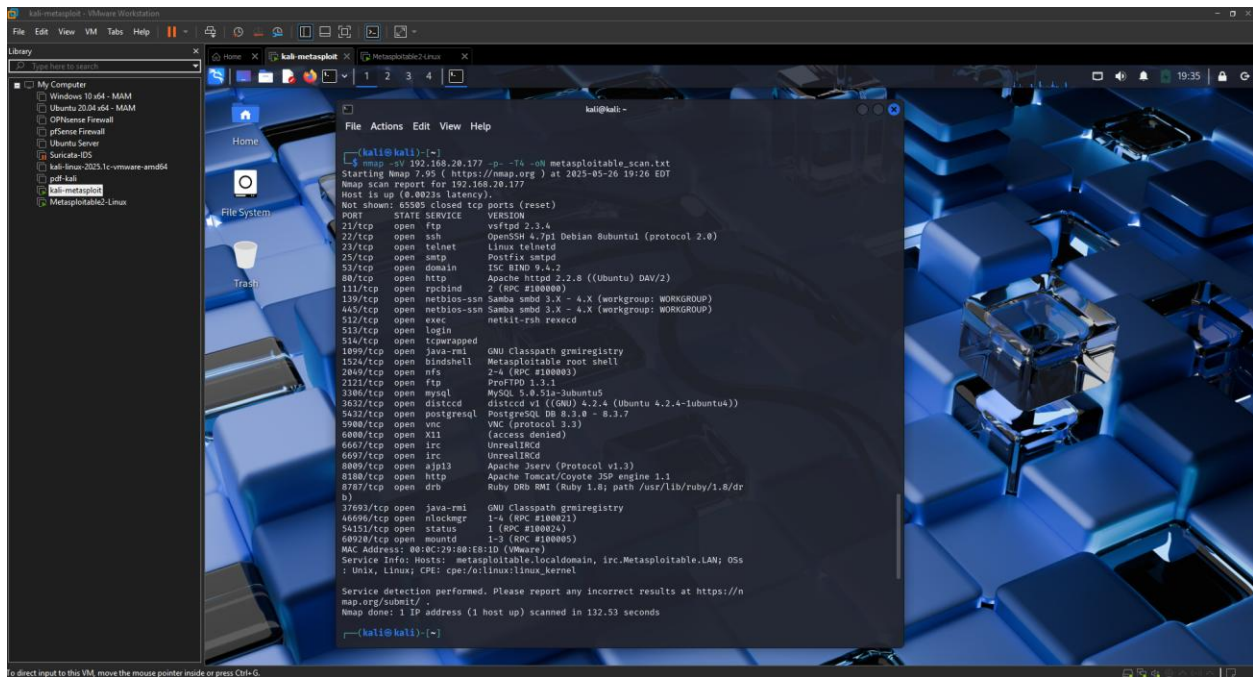
Home
File System
Trash

File Actions Edit View Help
-- [ 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
msf6 > Interrupt: use the 'exit' command to quit
msf6 > exit

kali@kali:~$ ping 192.168.20.177
PING 192.168.20.177 (192.168.20.177) 56(84) bytes of data:
64 bytes from 192.168.20.177: icmp_seq=1 ttl=64 time=1.00 ms
64 bytes from 192.168.20.177: icmp_seq=2 ttl=64 time=0.790 ms
64 bytes from 192.168.20.177: icmp_seq=3 ttl=64 time=0.610 ms
64 bytes from 192.168.20.177: icmp_seq=4 ttl=64 time=0.843 ms
64 bytes from 192.168.20.177: icmp_seq=5 ttl=64 time=0.718 ms
64 bytes from 192.168.20.177: icmp_seq=6 ttl=64 time=0.542 ms
64 bytes from 192.168.20.177: icmp_seq=7 ttl=64 time=0.435 ms
64 bytes from 192.168.20.177: icmp_seq=8 ttl=64 time=0.457 ms
64 bytes from 192.168.20.177: icmp_seq=9 ttl=64 time=0.531 ms
64 bytes from 192.168.20.177: icmp_seq=10 ttl=64 time=0.470 ms
64 bytes from 192.168.20.177: icmp_seq=11 ttl=64 time=0.462 ms
^C
--- 192.168.20.177 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 1018ms
rtt min/avg/max/ndev = 0.435/0.621/1.004/0.177 ms

kali@kali:~$
```

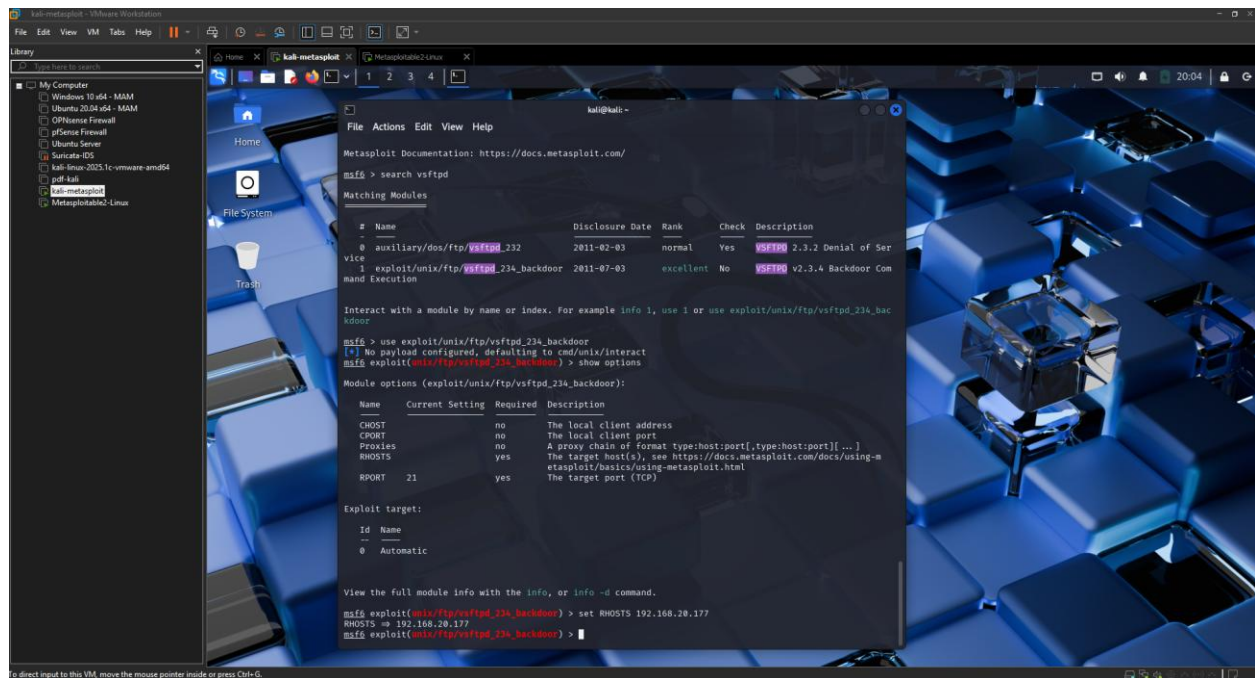
Tuomet atlikau pilną „nmap“ skenavimą prieš Metasploitable2 virtualią mašiną naudodamas Kali Linux terminalą. Naudojau komandą `nmap -sV -p- -T4` tam, kad identifikuočiau visus atvirus prievadus bei jų veikiančius servisus ir versijas. Gauti rezultatai leidžia nustatyti potencialiai pažeidžiamas paslaugas.



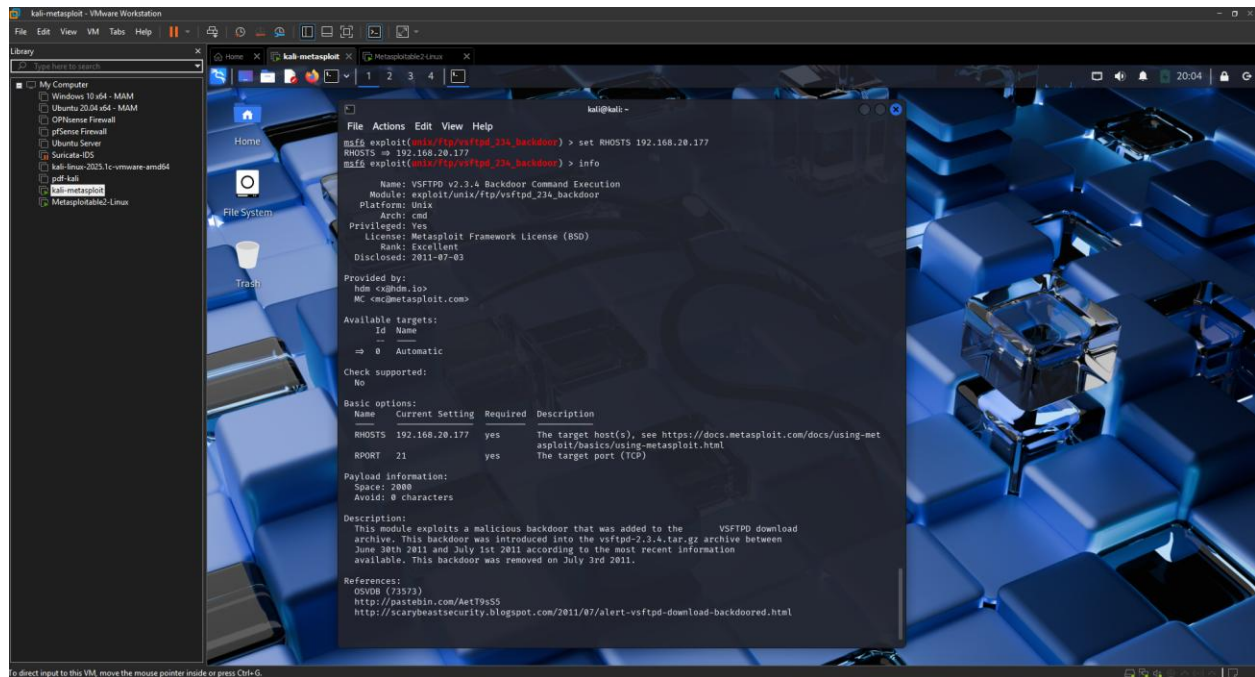
```
File Actions Edit View Help
kali@kali:~$ nmap -sV -p- -T4 -uN metasploitable2.scan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2023-05-20 19:26 EDT
Nmap scan report for 192.168.20.177
Host is up (0.0023s latency).
Not shown: 65503 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  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  smb
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi
1524/tcp  open  bindshell
2049/tcp  open  nfs
2112/tcp  open  ftp
3186/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5988/tcp  open  vnc
6080/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  irc
8080/tcp  open  ajp13
8180/tcp  open  http
8787/tcp  open  drb
37493/tcp open  java-rmi
46696/tcp open  nlockmgr
54151/tcp open  status
60928/tcp open  mountd
1-65535/tcp open  1-65535 (TCP #100000)
MAC Address: 08:0C:29:88:E8:1D (VMware)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OS: Linux, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 132.53 seconds
kali@kali:~$
```

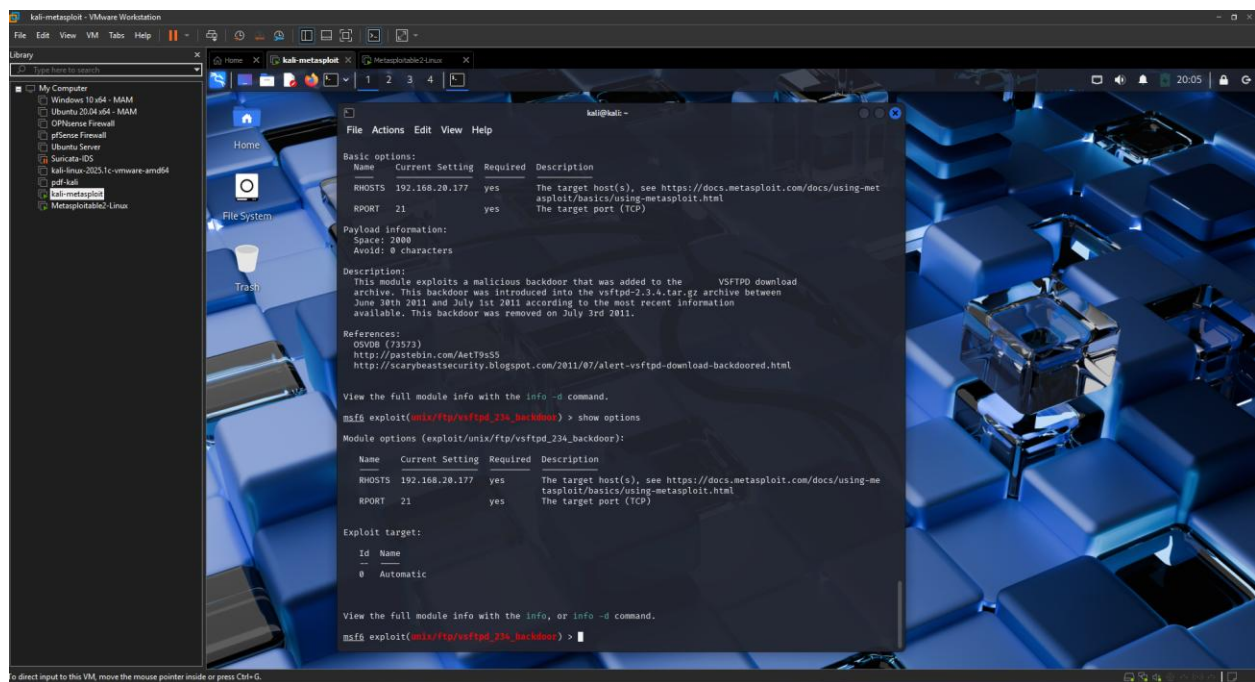
Metasploit aplinkoje atlikau komandą `search vsftpd`, kuri parodė kelis galimus modulius, susijusius su FTP paslauga. Pasirinkau modulį `exploit/unix/ftp/vsftpd_234_backdoor`, nes Metasploitable2 turi šią pažeidžiamą versiją (2.3.4). Atlikau komandą `use exploit/unix/ftp/vsftpd_234_backdoor` ir sukomandavau `show options`, kad pamatytčiau reikalingus nustatymus. Nustačiau taikinio IP adresą: `set RHOSTS 192.168.20.177`.



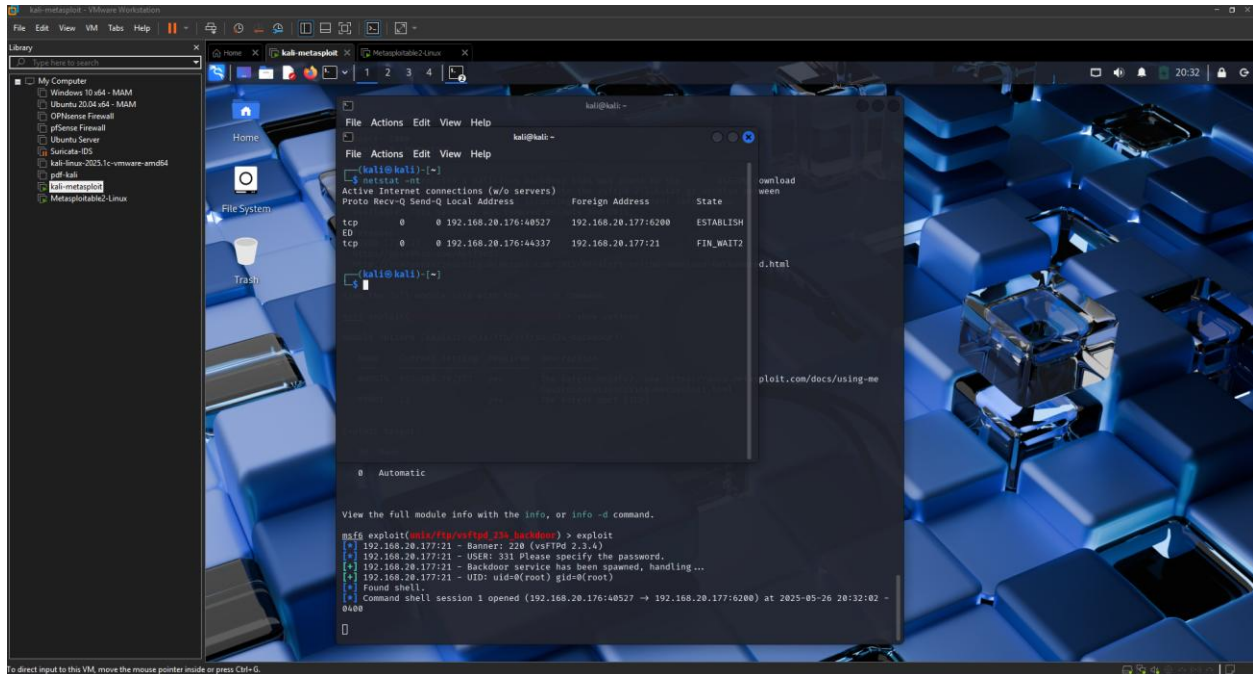
Tuomet patikrinau informaciją apie modulį naudodamas info komandą.



Ir taip pat patikrinau reikiamus parametrus naudojant new options komandą.



vsftpd_234_backdoor išnaudojimas pasinaudoja kenkėjiškais galinėmis durimis, kurios buvo tyčia įtrauktos į FTP serverio (vsftpd) versijos 2.3.4 išeities kodą. Kai naudotojo vardas yra suformuotas su šypsenėle :, serveris atidaro shell sesiją per 6200 prievadą. Tai yra klasikinis tiekimo grandinės pažeidimo (supply chain compromise) pavyzdys. Suaktyvinus šį pažeidžiamumą, buvo paleista shell sesija su root privilegijomis – tai parodo, kaip užkrėsti dvejetainiai failai gali būti panaudoti neteisėtai prieigai gauti su minimaliomis pastangomis.



Wireshark buvo naudojamas tinklo srautui užfiksuoti vykdamas vsftpd 2.3.4 galinių durų (backdoor) pažeidžiamumo išnaudojimą. Fiksuotas TCP trijų žingsnių rankos paspaudimas (three-way handshake) per 21 prievadą, po kurio seka galinių durų paleidiklis (naudotojo vardas su simboliais :) ir atidaroma shell sesija per 6200 prievadą. Tai patvirtina, kad išnaudojimas pavyko ir kenksmingas kodas (payload) buvo perduotas per užmegztą ryšį su galinėmis durimis.

