VAPT Practical — Metasploitable vsftpd Backdoor Exercise

Title: Metasploitable Lab — vsftpd Backdoor Exploitation (Kali attacker)

Author: Vinayak Chauhan

Team / Course: IBM Faculty Practice —Practical

Date: [2025-10-10]

Environment / Lab:

- Attacker: Kali Linux VM (isolated)
- Target: Metasploitable VM (isolated, intentionally vulnerable)
- Network: Host-only / internal virtual network (no Internet exposure)
- Authorization: Exercise performed under instructor-approved lab environment only.

---

1. Executive Summary

A short summary (2–4 sentences) describing the exercise objective and top-level findings.

This lab exercise demonstrates exploitation of the known vsftpd backdoor in the Metasploitable VM using an authorized Kali Linux attacker VM. The goal is educational: to observe exploitation vectors, practice detection and containment, and produce mitigations for hardening FTP services. The test was conducted in an isolated lab; no production systems were targeted.

---

2. Objectives

- Demonstrate identification of a vulnerable FTP service (vsftpd) on Metasploitable.
- Execute an authorized exploitation exercise in the lab to gain proof-of-concept access (non-persistent, controlled).
- Observe attacker behavior and capture network/host artifacts for detection and logging practice.
- Produce actionable remediation and detection recommendations.

---

3. Rules of Engagement & Authorization

- Exercise approved by: [ANAND GUPTA SIR] on [2025-10-10].
- Target: Metasploitable VM belonging to the lab environment.
- Scope: host-only/internal network only. No lateral movement beyond the lab VM.

- Limitations: No data exfiltration, no persistence or pivoting to other infrastructure, and no publication of exploit payloads or private keys. All sensitive outputs were redacted before inclusion in this report.

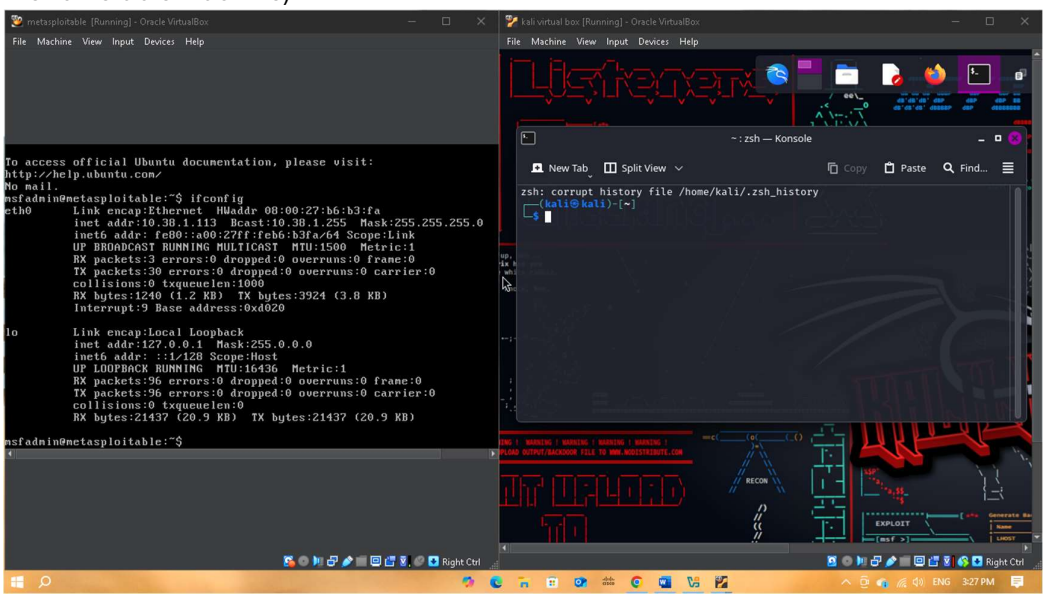
Ethics note: These techniques have real-world impact if used without authorization. This report omits step-by-step exploit commands and payloads—details necessary to reproduce attacks on real systems are intentionally non-actionable.

---

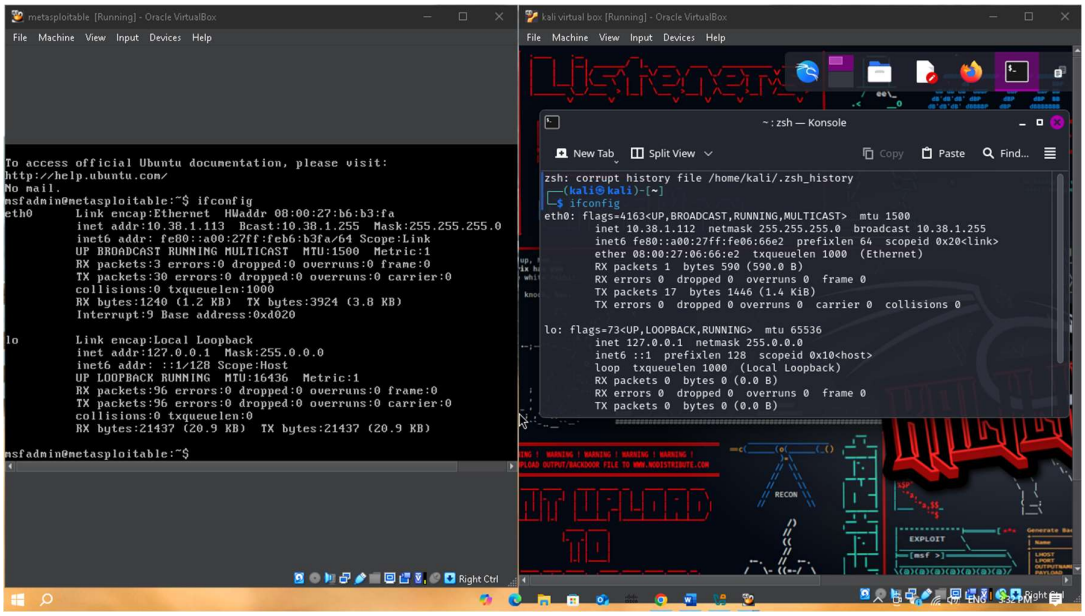
4. High-Level Methodology (Non-actionable)

This section describes the *what* and *why* of the approach without providing detailed exploit commands.

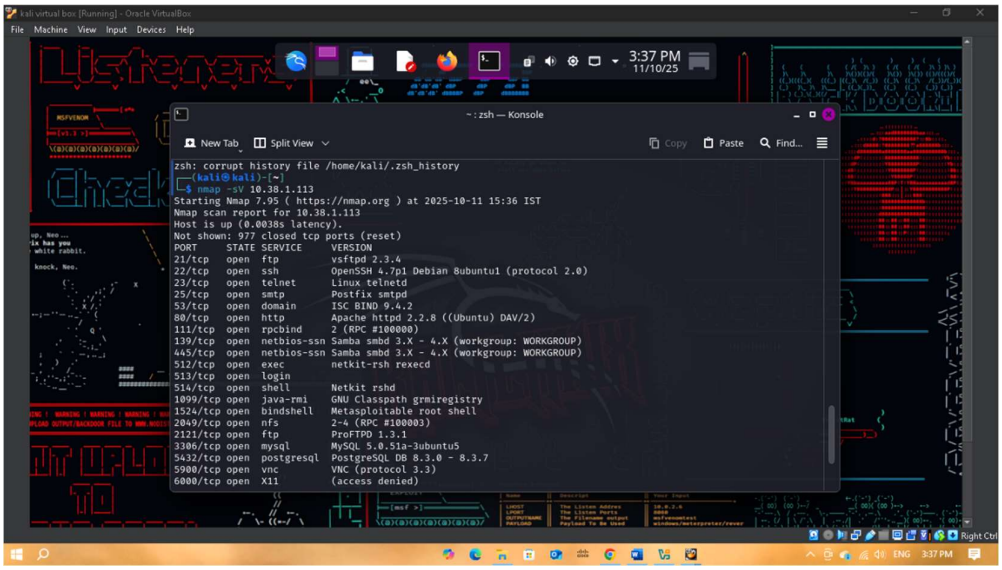
Step1) open both the virtual machines (kali Linux: - the attacker machine && Metasploitable: - the vulnerable machine).



Step 2) on vulnerable machine and kali Linux type the command: - “ipconfig” to check the internal connection stabilities on both the device.

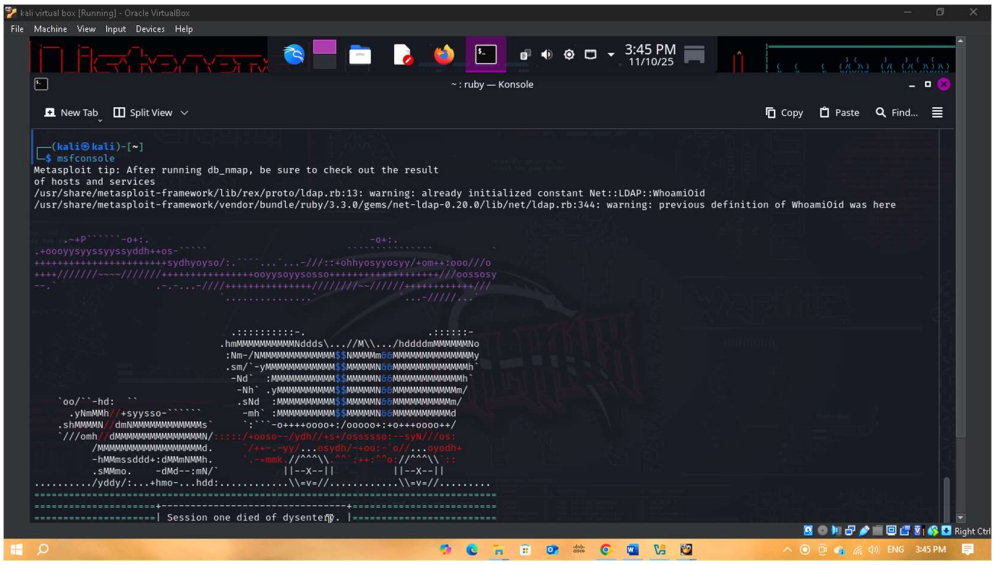


Step 3) after conformation open the terminal in kali Linux open the tool “NMAP” (NETWORK MAPPER) and run the command “Nmap -sV <the vulnerable machine Ip>., this command will -sV tells Nmap to perform **service/version detection** on open ports it finds. Instead of just reporting *that* a port is open (like 80/tcp open), -sV probes the service running on that port to identify **which application**, **version**, and sometimes **extra details** (like protocol, product string, or CPE identifiers).



Step 4) IN this scenario we will work with vsftpd 2.3.4 vulnerability (The backdoor would open a shell listening on **TCP port 6200** when a specially-crafted username (the “smiley face” username :)) was used. This is tracked as **CVE-2011-2523**.)

Step5) open Metasploitable frame work (we will use Metasploit framework to gain access to the system using the backdoor).



Step6) follow the commands along to exploit the machine: -

msfconsole

msf > search vsftpd

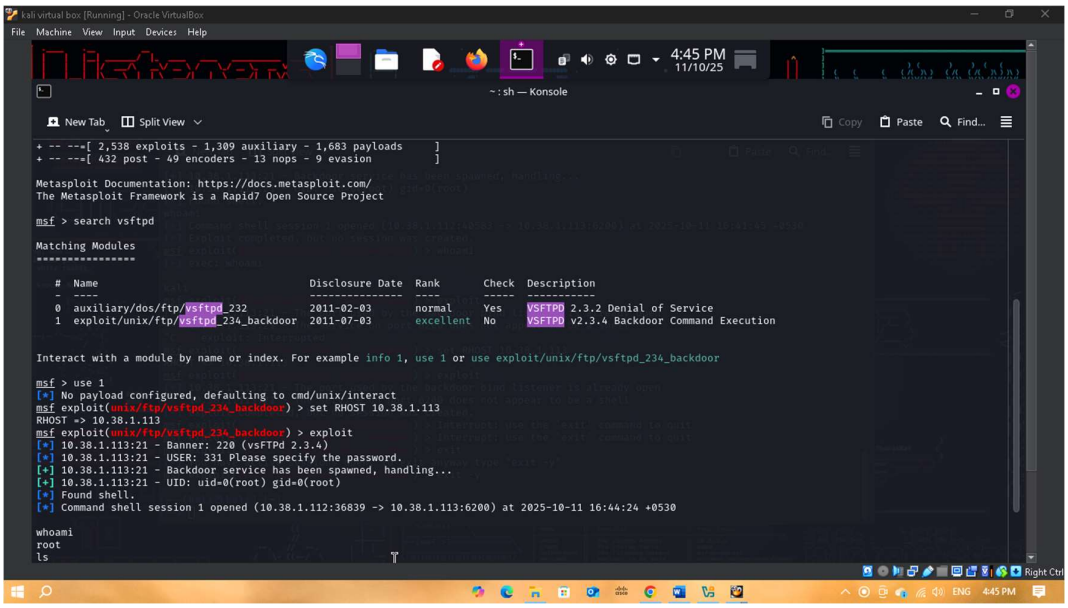
msf > use <vsftpd_backdoor_module>

msf exploit(vsftpd_234_backdoor) > set RHOST 10.38.1.113

msf exploit(vsftpd_234_backdoor) > exploit

after session opens

Whoami → ls.



“ACCESS GRANTED TO THE MACHINE “

---

5. Findings (Summary Table)

Finding ID	Title	Severity	Affected Asset(s)	Evidence	Recommendation
M-001	Exposed vsftpd with known backdoor	High	Metasploitable VM — FTP service	Screenshot: evidence-01.png (service banner); PCAP: evidence-02. pcap	Replace vsftpd with supported FTP solution or disable FTP; apply patches/configuration hardening

Severity Guidance: High = immediate patching / isolation; Medium = remediate within 30 days; Low = monitor and plan.

---

6. Detailed Finding — Example

M-001 — Exposed vsftpd with known backdoor (High)

Description: The target host runs an outdated vsftpd version containing a known backdoor vulnerability (intentionally present in Metasploitable). In the lab, this vulnerability allowed a proof-of-concept access to the target in a controlled manner.

Evidence:

- Service banner and enumerated version (see evidence-01.png).
- Network capture showing the exchange leading to PoC (see evidence-02. pcap).
- Screenshots of the attacker terminal and target process list post-exploit (redacted) in screenshots/.

Impact: An unauthenticated remote attacker could achieve unauthorized access to the FTP server process and may execute commands or retrieve files.

Root cause: Use of intentionally vulnerable vsftpd version in the VM; lack of hardening and monitoring.

Recommendation (priority):

1. Disable or remove legacy FTP services in production if not required. Prefer SFTP (SSH) or FTPS (FTP over TLS) with strong configuration.
2. If FTP is required, ensure the service is a supported, patched version and enforce TLS.
3. Restrict access to FTP via network segmentation and firewall rules.
4. Implement detection rules for suspicious FTP commands and unusual service behavior.

---

7. Artifact Collection & Evidence (Appendix)

- evidence-01.png — Screenshot: FTP service banner and port scan output (redacted).
- evidence-02. pcap — Network capture of the demonstration attack (redacted).
- evidence-04.txt — Extract of system logs showing FTP connections and timestamps (redacted).

How to attach: Rename your screenshots and PCAPs as above and include them under practice-03_vstp-backdoor/screenshots/ in the repo. Remove or redact any sensitive artifacts before committing.

---

8. Detection & Logging Recommendations

- **Network detection:** Create IDS/IPS signatures to flag anomalous FTP command sequences and patterns associated with the known backdoor behavior. Monitor for new connections to unusual ports and suspicious payloads.
- **Host detection:** Monitor for unexpected child processes spawned by the FTP daemon, unusual binaries in writable directories, and changes to /etc./ configuration.
- **Logging:** Ensure FTP server logs are centrally collected and correlated. Add timestamped alerts for anonymous logins or rapid command sequences.

---

9. Remediation Roadmap (Suggested)

Immediate (0–7 days):

- Isolate affected VMs; ensure no further exposure to production networks.
- Disable FTP service if not required.

Short term (1–4 weeks):

- Patch or replace vulnerable FTP server software.
- Enforce TLS and disable anonymous logins.
- Configure network ACLs to limit access to FTP from only required hosts.

Long term (1–6 months):

- Implement periodic vulnerability assessments and patch management.
- Deploy host-based EDR and network monitoring with tailored detection rules.
- Conduct red-team/blue-team exercises and tabletop incident response drills.

---

10. Safety, Ethics & Responsible Disclosure

- This report documents a lab-only exercise performed with explicit authorization. The details intentionally avoid step-by-step exploit instructions to prevent misuse.

- If you discover similar issues on production systems, follow responsible disclosure and internal incident response procedures. Do not attempt exploitation on systems for which you lack authorization.

---

11. Appendix — Commands & Tools (Non-actionable list)

- Tools used (examples): Nmap (for discovery), Metasploit Framework (lab PoC only), Wireshark/tcpdump (network capture), and system utilities for host inspection.
- Note: The report does not include exploit payloads or step-by-step Metasploit commands. If you need to reproduce this exercise for approved lab training, consult your instructor for an in-lab walkthrough or use the lab materials provided by the course.

---

12. References

- Metasploitable project documentation (lab intentionally vulnerable VM).
- Vendor/security advisories describing vsftpd historical vulnerabilities.
- NIST and SANS guidance on secure FTP configuration and network segmentation.

End of report.
