Professional Penetration Test Report

Rohan Jadhav

1. Executive Summary

This section is for non-technical stakeholders (management, decision-makers). It should be concise (one page maximum) and focus on the business risk.

- Objective: Briefly state the scope (e.g., external, internal, web application test against Cap.htb).
- Overall Risk: A quick assessment (e.g., High).
- Key Findings: List the top 3-5 most critical vulnerabilities.
    - *Example:* Unauthenticated FTP access leading to credential discovery.
    - *Example:* Privilege escalation vulnerability allowing full root access.
- Recommendation: A high-level, immediate action plan.

2. Scope and Methodology

This section details *what* was tested and *how*.

Component	Target IP/URL	Description
Target System	Cap.htb	Ubuntu Linux System
Services Tested	SSH, FTP, HTTP (Web Dashboard)	Standard services identified by Nmap.
Timeframe	October 22, 2025	Based on timestamps in images.
Methodology	Black Box (External)	Started with no prior knowledge of the internal network.

3. Detailed Findings

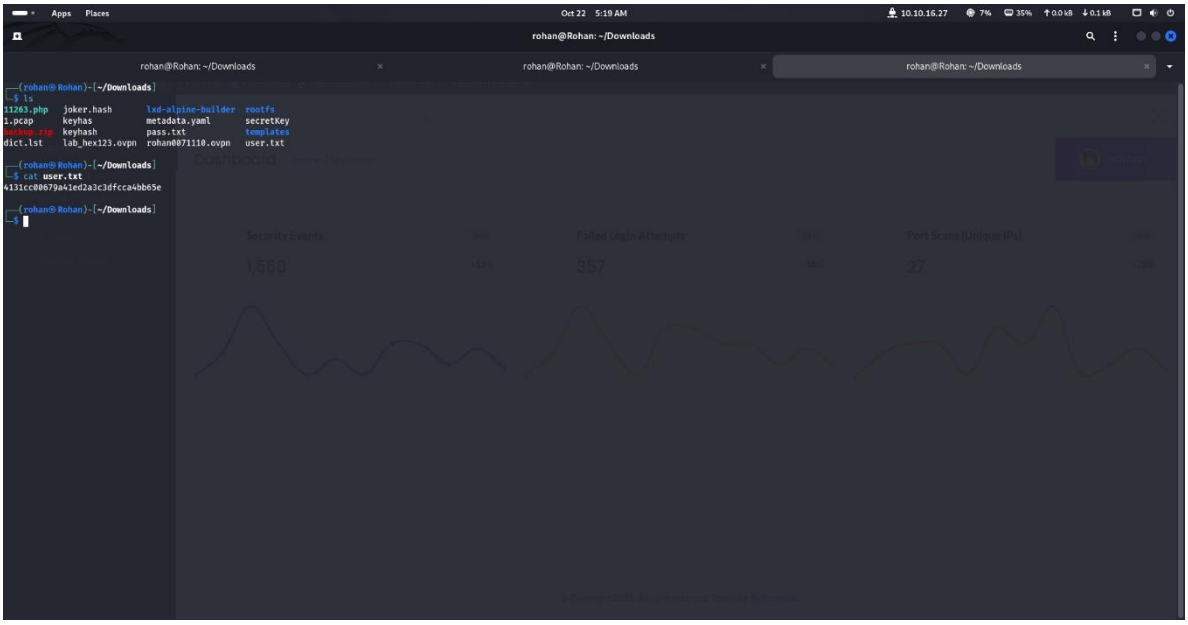
This is the core of the report, detailing each vulnerability found. Each finding must include the following sub-sections:

Finding 3.1: Unauthenticated Information Leak via FTP (Critical)

- Vulnerability Description**:** The target system is running an FTP service that allows anonymous login, which exposed a file containing potential user credentials.
- **Impact:** An attacker gained unauthorized access to sensitive files, leading to lateral movement via SSH.

Proof of Concept (PoC):

1. **FTP Service Identification and Access:** Nmap identified the FTP service ($21/tcp). Access was gained using the anonymous username.



2. **Credential Retrieval:** The file user.txt was downloaded and contained what appears to be a password hash (413cc08879b4e1a2d3fcfc1a4b8d5e).

Recommendation: Disable anonymous FTP access. Implement strong authentication, and ensure that sensitive files are not stored in accessible directories.

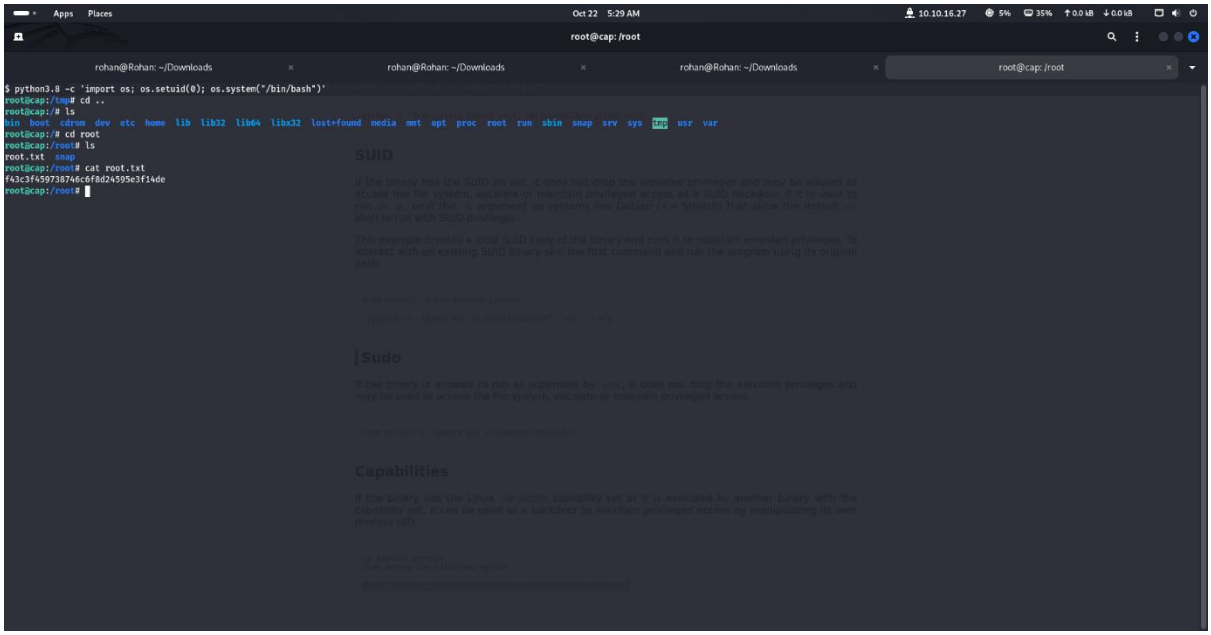
Finding 3.2: Compromised User Access via SSH (High)

- **Vulnerability Description:** The discovered password hash allowed authentication to the system via SSH using the username nathan.
- **Impact:** An attacker gained authenticated shell access, establishing a foothold within the internal network.
- **Proof of Concept (PoC):**
    - The username nathan and a password (likely derived from the hash) were used to log in via SSH. The login was successful, providing an unprivileged user shell.

- **Recommendation:** Enforce a strong password policy and implement multi-factor authentication (MFA).

Finding 3.3: Local Privilege Escalation (Critical)

- Vulnerability Description**:** Once authenticated, the attacker was able to exploit a local vulnerability (likely related to a misconfigured SUID binary or similar mechanism) to elevate their privileges to **root**.
- Impact: Complete compromise of the target system, allowing full control over all data, processes, and configuration.
- Proof of Concept (PoC):
    - A command was executed to gain a root shell. The attacker confirmed root access (root@cap:/root#) and retrieved the final proof file (root.txt).



- **Recommendation:** Audit the system for vulnerable SUID/GUID binaries, outdated kernels, and potential configuration errors. Apply vendor-supplied patches immediately. Implement robust logging and monitoring to detect suspicious process execution.

3. Risk Rating and Remediation Plan

This section summarizes all findings and provides a concise plan for fixing them.

ID	Finding	Risk Level	Remediation Effort
3.1	Unauthenticated FTP Information Leak	**Critical**	Low
3.2	Compromised User Access (nathan)	High	Medium
3.3	Local Privilege Escalation	**Critical**	High

4. Conclusion

The penetration test conducted on the target system **Cap.htb** revealed **critical vulnerabilities** that allowed for complete system compromise, escalating from an external, unauthenticated attack to full **root** access.

The attack chain began with a **High-risk information leak** through an anonymously accessible FTP service, which yielded a user credential. This foothold led directly to **authenticated access** via SSH under the username nathan. The final and most severe stage was the **Critical local privilege escalation**, which provided the tester with administrative control over the entire system, as evidenced by the successful retrieval of the root.txt flag.

The severity of the findings necessitates immediate action. The organization must prioritize remediation of the open services, particularly the misconfigured FTP and the underlying vulnerability that enabled privilege escalation, to prevent external attackers from gaining full control over this critical asset. The identified weaknesses represent a **complete failure** in the current security posture regarding external exposure and internal system hardening.