ROAD MAP

VULNERABLE MACHINES

Cyber Evangelists

Table of Contents

INTRODUCTION

The vulnerable machine is a deliberately created system with intentionally introduced security vulnerabilities. These machines are used for educational and training purposes in the field of cybersecurity. By exploiting the vulnerabilities in these machines, individuals can gain hands-on experience, develop their skills, and understand the real-world implications of security weaknesses. Vulnerable machines simulate realistic scenarios and allow users to apply their knowledge practically. They are used for learning, skill development, security awareness, and training, and as targets for penetration testing and red teaming. However, using vulnerable machines responsibly, with proper authorization, and within legal and ethical boundaries is essential.

PLATFORMS

These are the following platforms that provide free or paid vulnerable machines, so students can learn real-world implications of security weaknesses and enhance their skills by exploiting the vulnerabilities.

- Try Hack me
- Hack the Box
- Vuln Hub
- Metasploit
- Damn Vulnerable Web Application (DVWA)

VULNERABLE MACHINES

The machines were intentionally created vulnerable, so the pen tester exploits their vulnerability by using their knowledge practically and developing their skills to get hands-on experience on real-world security weaknesses. Many platforms provide vulnerable machines from beginner to high levels that students learn properly in a safe and controlled environment through making mistakes and ultimately become proficient in identifying, exploiting, and mitigating security vulnerabilities.

Beginner Level

- Machine: Metasploitable
- Objective: Learn about basic network vulnerabilities and exploit them using the Metasploit framework.
- Topics: Scanning, enumeration, exploiting common vulnerabilities (e.g., weak passwords, outdated software), privilege escalation.
- Description: Exploit vulnerable services like FTP, Telnet, or SSH using available exploits to gain remote access, and for privilege escalation exploit weak configurations, default credentials, or vulnerabilities in the installed services to escalate privileges on the system.

- Machine: TryHackme (RootMe)
- Objective: Learn about basic network vulnerabilities and exploit hidden directories.
- Topics: Scanning, enumeration, exploiting common vulnerabilities (e.g., finding directories), privilege escalation.
- Description: Beginner friendly Machine focused on CTF basics, Port scanning, finding hidden directories, in uploads page uploading PHP reverse shell to gain an initial foothold, for privilege escalation finding file which is running with root privileges, and using it to read root files and escalate privileges.

- Machine: TryHackme (Pickle Rick)
- Objective: Learn about basic network vulnerabilities and exploit hidden directories, command injection.
- Topics: Scanning, enumeration, exploiting common vulnerabilities (e.g., finding directories, viewing source code, command injection), privilege escalation.
- Description: The Pickle Rick machine is a great way to learn the basics of web application penetration testing. Machine focused on CTF, Port scanning, finding hidden directories, viewing source code, gaining username and password to gain an initial foothold, for privilege escalation application is vulnerable to command injection perform directory traversal for root access.

- Machine: TryHackme (LazyAdmin)
- Objective: Learn about basic network vulnerabilities and apply brute force and MySQL Backup.
- Topics: Scanning, enumeration, exploiting common vulnerabilities (e.g., brute forcing, SQL backup), privilege escalation.
- Description: Machine focused on Port scanning, directory brute forcing tool to find directory, exploit CMS vulnerability, and access to MySQL backup file to gain credentials and PHP reverse shell to gain an initial foothold, for privilege escalation just type sudo -l access as a root.

Intermediate Level

- Machine: Damn Vulnerable Web Application (DVWA)
- Objective: Understand web application vulnerabilities and exploit them.
- Topics: SQL injection, cross-site scripting (XSS), cross-site request forgery (CSRF), and file inclusion vulnerabilities.
- Description: Identify and exploit common web vulnerabilities like SQL injection, cross-site scripting (XSS), or command injection through the DVWA web interface to initial foothold, for privilege escalation DVWA focuses on web vulnerabilities rather than privilege escalation. However, additional challenges may involve exploiting the server or misconfigurations to escalate privileges.

- Machine: Kioptrix Level 1
- Objective: Explore network vulnerabilities and privilege escalation techniques.
- Topics: Network sniffing, password cracking, remote code execution, kernel exploits.
- Description: Enumerate the network, identify open ports, and exploit vulnerabilities like weak passwords, insecure services, or misconfigurations to gain initial access, and for privilege escalation search for misconfigured file permissions, vulnerable services, or weak configurations to escalate privileges on the system.

- Machine: VulnHub's FristiLeaks
- Objective: Discover and exploit vulnerabilities in a fictitious company's web infrastructure.
- Topics: Command injection, directory traversal, insecure file upload, server-side request forgery (SSRF).
- Description: Exploit web application vulnerabilities like command injection, directory traversal, or file upload to gain initial access, and for privilege escalation: Identify misconfigured file permissions, weak user configurations, or insecure database connections to escalate privileges.

- Machine: TryHackme (MrRobot)
- Objective: Discover and exploit vulnerabilities in wordpress.
- Topics: Gobuster, directory traversal, Cyberchef, Python webserver.
- Description: A Machine where all flags and hashes will be redacted to prevent an easy win of the room. start with port scanning, use GoBuster for directories, use CyberChef to decode the string, try login into WordPress and set up a reverse shell and get our first foothold. For privilege escalation run a Python web server with the script we got some username and Password hashes, decoded them, and accessed them as root.

Advance Level

- Machine: VulnHub's SickOS 1.2
- Objective: Engage in a full-scale penetration test on a simulated vulnerable infrastructure.
- Topics: Exploiting misconfigurations, remote file inclusion (RFI), privilege escalation, pivoting, lateral movement.
- Description: Discover and exploit misconfigured services, insecure file uploads, or remote file inclusion vulnerabilities to gain initial access, and for privilege escalation analyze system configurations, search for weak file permissions, or exploit vulnerabilities in installed software to escalate privileges.

- Machine: HackTheBox's Blue
- Objective: Replicate an advanced real-world attack scenario by exploiting Windows vulnerabilities.
- Topics: EternalBlue exploit, MS17-010 vulnerability, Windows privilege escalation techniques.
- Description: Exploit the MS17-010 vulnerability using EternalBlue or other available exploits to gain initial access to the Windows system, and for privilege escalation analyze the system for weak configurations, unpatched vulnerabilities, or insecure services to escalate privileges on the compromised machine.

- Machine: VulnHub's Brainpan
- Objective: Exploit a custom vulnerable application and analyze memory corruption vulnerabilities.
- Topics: Buffer overflows, stack-based and heap-based exploits, reverse engineering.
- Description: Analyze the vulnerable application, identify memory corruption vulnerabilities like buffer overflows, and exploit them to gain initial access, and for privilege escalation once inside the system, search for additional vulnerabilities, weak configurations, or misconfigured permissions to escalate privileges.

- Machine: HackTheBox's OSCP-like machines (e.g., Legacy, Devel, Optimum)
- Objective: Prepare for the Offensive Security Certified Professional (OSCP) certification.
- Topics: Exploiting multiple vulnerabilities, pivoting, post-exploitation techniques, evading detection.
- Description: Perform comprehensive enumeration to identify vulnerable services, weak configurations, or potential entry points. Exploit the discovered vulnerabilities to gain initial access, and for Privilege Escalation: After gaining initial access, explore the system for misconfigurations, vulnerable services, or weak permissions to escalate privileges on the machine.

High Level

- Machine: VulnHub's Kioptrix Level 3
- Objective: Apply advanced penetration testing methodologies and techniques.
- Topics: Web application firewalls (WAF) bypass, file upload vulnerabilities, database exploitation, lateral movement.
- Description: Identify and exploit web vulnerabilities, such as bypassing a web application firewall (WAF), exploiting file upload vulnerabilities, or attacking misconfigured components, to gain initial access, and for privilege escalation search for vulnerabilities in the web application, database misconfigurations, or weaknesses in user permissions to escalate privileges and potentially perform lateral movement.

- Machine: HackTheBox'ss Active Directory (AD) labs (e.g., Forest, Bastard, Nest)
- Objective: Gain expertise in attacking Active Directory environments.
- Topics: AD enumeration, Kerberos attacks, BloodHound usage, privilege escalation in AD, persistence.
- Description: Enumerate the Active Directory environment, identify vulnerable services, weak user accounts, or misconfigured permissions to gain initial access to the AD infrastructure, and for privilege escalation exploit misconfigurations, privilege escalation vulnerabilities, or weaknesses in the AD environment to elevate privileges and gain further access or control.

- Machine: TryHackme Uranium CTF
- Objective: Gain expertise in attacking Social media accounts.
- Topics: AD enumeration, Phishing attacks on social media accounts.
  Description: Hard-level machine a Twitter account is given. The machine has an SMTP server that is vulnerable to phishing attacks. The goal of the challenge is to send an email to Hakanbey’s email address with a payload attached.

CONCLUSION

In conclusion, vulnerable machines are intentionally created systems with security vulnerabilities used for cybersecurity education and training. They offer a practical learning environment where individuals can gain hands-on experience and develop their skills in identifying, exploiting, and mitigating security weaknesses. Platforms like Try to Hack Me, Hack The Box, vuln Hub, Metasploit, and DVWA provide a range of vulnerable machines for different skill levels.

These machines simulate realistic scenarios and cover various topics such as web application vulnerabilities, network vulnerabilities, privilege escalation, and Active Directory attacks. By engaging with vulnerable machines, students make mistakes, learn from them, and gradually become proficient in cybersecurity techniques.

It is essential to use vulnerable machines responsibly, with proper authorization, and within legal and ethical boundaries. By doing so, students can enhance their cybersecurity skills, contribute to improving security practices, and make a positive impact in the field.