TRYHACKME ROADMAP TO CLEAR OSCP

AKASH BASFOR

VIEH GROUP

TryHackMe learning paths:

Beginner's Path:

- Description: Start with the basics of cybersecurity, networking, and essential tools used in ethical hacking.
- Skills:
  - Basic Linux commands and navigation.
  - Understanding of TCP/IP, OSI model, and network protocols.
  - Familiarity with common hacking tools (Nmap, Nikto, Netcat, etc.).
  - Basic web application vulnerabilities (SQL injection, XSS, etc.).

Web Application Penetration Testing:

- Description: Focus on web application security and common vulnerabilities found in web applications.
- Skills:
  - In-depth knowledge of web application security (OWASP Top Ten).
  - Hands-on experience exploiting web vulnerabilities in different applications.
  - Familiarity with Burp Suite for web application testing.

Network Penetration Testing:

- Description: Dive into network penetration testing and understanding network vulnerabilities.
- Skills:
    - Proficiency in using scanning tools (Nmap, Netdiscover, etc.) for network reconnaissance.
    - Exploiting network-level vulnerabilities (SMB, FTP, SNMP, etc.).
    - Understanding of privilege escalation techniques in a network environment.

Privilege Escalation:

- Description: Focus on privilege escalation techniques to gain higher-level access in compromised systems.
- Skills:
    - Understanding Linux and Windows privilege escalation methods.
    - Identifying misconfigurations and vulnerabilities that lead to privilege escalation.
    - Practical experience in escalating privileges on different operating systems.

Buffer Overflows:

- Description: Learn about buffer overflows, a common vulnerability often tested in the OSCP exam.
- Skills:
    - Understanding of memory management and stack-based buffer overflows.
    - Hands-on experience in developing and exploiting buffer overflow exploits.

Advanced Exploitation Techniques:

- Description: Enhance your exploitation skills with more complex scenarios and techniques.
- Skills:
    - Bypassing security mechanisms (ASLR, DEP, etc.).
    - Exploiting custom applications and complex systems.
    - Practice with Metasploit and understanding when it's allowed in the OSCP exam.

Post-Exploitation and Pivoting:

- Description: Focus on maintaining access and pivoting through networks after initial exploitation.
- Skills:
    - Privilege escalation on compromised systems.
    - Post-exploitation enumeration and lateral movement techniques.
    - Understanding of tunneling and proxying through compromised systems.

Vulnerability Assessment and Report Writing:

- Description: Learn how to document your findings and write comprehensive penetration testing reports.
- Skills:
    - Creating detailed reports of vulnerabilities and exploitation steps.
    - Effective communication of technical findings to non-technical stakeholders.

CTF Challenges and Practice Labs:

- Description: Engage in various Capture The Flag challenges and hands-on practice labs.
- Skills:
    - Apply your skills in real-world scenarios and different environments.
    - Improve problem-solving abilities and time management.

Wireless Network Penetration Testing:

- Description: Learn about wireless network security and how to identify and exploit vulnerabilities in Wi-Fi networks.
- Skills:
    - Understanding of different Wi-Fi encryption protocols (WEP, WPA, WPA2).
    - Cracking Wi-Fi passwords and exploiting weak configurations.
    - Practical experience in conducting wireless network assessments.

Client-Side Attacks and Social Engineering:

- Description: Explore social engineering techniques and client-side attacks to compromise systems through human interaction.
- Skills:
    - Phishing and spear-phishing attacks.
    - Creating malicious documents and exploiting client-side vulnerabilities.
    - Gaining access through social engineering scenarios.

Reverse Engineering and Binary Exploitation:

- Description: Delve into reverse engineering and understanding binary code to exploit applications at a deeper level.
- Skills:
    - Debugging binaries and understanding assembly language.
    - Analyzing and exploiting vulnerabilities in compiled programs.
    - Dealing with packed and obfuscated code.

Cryptography and Steganography:

- Description: Gain knowledge of cryptographic concepts and hiding information within files using steganography techniques.
- Skills:
    - Understanding cryptographic algorithms and weaknesses.
    - Decrypting messages and solving cryptographic challenges.
    - Identifying hidden information in images, audio, and other files.

Red Team Operations:

- Description: Get a glimpse into real-world red team engagements and how to emulate adversary tactics.
- Skills:
    - Emulating APT (Advanced Persistent Threat) behaviors.
    - Maintaining persistence and avoiding detection.
    - Utilizing various tools to achieve red team objectives.

Active Directory (AD) Exploitation:

- Description: Focus on understanding Active Directory environments and exploiting misconfigurations and vulnerabilities.
- Skills:
    - Enumeration and reconnaissance of Active Directory domains.
    - Exploiting AD trust relationships and misconfigurations.
    - Privilege escalation in AD environments.

Threat Hunting and Incident Response:

- Description: Develop skills to detect and respond to security incidents in a networked environment.
- Skills:
    - Identifying indicators of compromise (IOCs).
    - Analyzing logs and network traffic for suspicious activities.
    - Developing incident response plans and procedures.

TryHackMe rooms to practice and prepare for OSCP:

Basic Pentesting:

- Difficulty: Easy
- Description: This room covers the basics of penetration testing, including web application vulnerabilities and privilege escalation.

VulnHub: Mr. Robot CTF:

- Difficulty: Easy/Medium
- Description: Based on the TV show "Mr. Robot," this room offers a real-world experience in CTF-style challenges.

Web Fundamentals:

- Difficulty: Easy
- Description: Focuses on web application security fundamentals, such as SQL injection, XSS, and more.

Nmap:

- Difficulty: Easy
- Description: Learn about network scanning and enumeration using Nmap.

Blue:

- Difficulty: Easy/Medium
- Description: Emulates a Windows environment with vulnerabilities, including EternalBlue.

Simple CTF:

- Difficulty: Medium
- Description: A beginner-friendly CTF-style room with a variety of challenges.

Kenobi:

- Difficulty: Medium
- Description: Practice Linux privilege escalation techniques on an intentionally vulnerable machine.

Lian_Yu:

- Difficulty: Medium/Hard
- Description: A challenging room that covers multiple skills, including enumeration, exploitation, and privilege escalation.

Advent of Cyber (series):

- Difficulty: Medium
- Description: A series of Christmas-themed rooms covering a range of cybersecurity topics.

Brainstorm:

- Difficulty: Hard
- Description: A challenging room that includes web application security, privilege escalation, and more.

Offensive Pentesting:

- Difficulty: Hard
- Description: An advanced room focusing on various exploitation techniques and privilege escalation.

Post Exploitation Basics:

- Difficulty: Medium
- Description: Learn about post-exploitation techniques, file transfer, and privilege escalation.

HackPark:

- Difficulty: Medium
- Description: Simulate hacking into an amusement park system with various challenges.

Relevant:

- Difficulty: Medium/Hard
- Description: A room that covers web application security and exploitation techniques.

Pickle Rick:

- Difficulty: Medium/Hard
- Description: Based on the TV show "Rick and Morty," this room involves various challenges related to privilege escalation and enumeration.

Wgel CTF:

- Difficulty: Hard
- Description: A challenging room with a Capture The Flag (CTF) format and a focus on enumeration and exploitation.

HA Joker:

- Difficulty: Hard
- Description: Simulate a CTF-like environment with various challenges and vulnerabilities.

Resolute:

- Difficulty: Hard
- Description: Practice Active Directory enumeration and exploitation techniques.

Ice:

- Difficulty: Hard
- Description: An advanced room focusing on exploitation and privilege escalation in a Windows environment.

OSCP Exam-like Practice:

- Difficulty: Very Hard
- Description: A room designed to simulate the format and challenges of the OSCP exam. This is excellent for final exam preparation.

DarkCTF Labs (series):

- Difficulty: Very Hard
- Description: A series of challenging labs designed for CTF enthusiasts and advanced learners.

Symfonos:

- Difficulty: Very Hard
- Description: A challenging room that covers web application security, privilege escalation, and lateral movement.

Skynet:

- Difficulty: Very Hard
- Description: A highly realistic room that simulates real-world scenarios, including Active Directory exploitation and advanced privilege escalation.

Blaster:

- Difficulty: Easy
- Description: Focuses on open-source intelligence (OSINT) and information gathering.

OhSINT:

- Difficulty: Hard
- Description: An advanced room focusing on exploitation and privilege escalation in a Windows environment.

LazyAdmin:

- Difficulty: Easy
- Description: A beginner-friendly room covering web application vulnerabilities and privilege escalation.

Advent of Cyber 2 (series):

- Difficulty: Medium
- Description: A follow-up to the original Advent of Cyber series, with new challenges to practice various cybersecurity skills.

Metasploit:

- Difficulty: Medium
- Description: Learn about Metasploit framework and its usage in penetration testing.

Brainpan:

- Difficulty: Hard
- Description: A challenging room that involves binary exploitation and buffer overflow techniques.

Vulnversity:

- Difficulty: Hard
- Description: Practice web application vulnerabilities and privilege escalation in a Linux environment.

Game Zone:

- Difficulty: Hard
- Description: A CTF-like room with a variety of challenges to test your penetration testing skills.

Writeup:

- Difficulty: Hard
- Description: Based on a real-world scenario, this room covers web application security, lateral movement, and more.

Tokyo Ghoul:

- Difficulty: Very Hard
- Description: A highly challenging room with multiple complex steps to complete the objectives.

Cyber Apocalypse (series):

- Difficulty: Very Hard
- Description: A series of rooms with a post-apocalyptic theme, featuring advanced challenges across different topics.

As you progress through these rooms, take the time to analyze your weaknesses and areas where you need improvement. Focus on understanding the methodologies behind the challenges and learning from your mistakes. Always try to solve problems independently before seeking hints or solutions.

Remember, OSCP is not just about passing the exam; it's about gaining hands-on experience and becoming a capable penetration tester. Stay persistent, keep learning, and don't hesitate to seek help from the community or mentors if needed. Good luck on your OSCP journey!

VIEH GROUP

Join our community: t.me/viehgroup
Social media: @viehgroup

AKASH BASFOR

LinkedIn: https://www.linkedin.com/in/akashbasfor/