Penetration Testing Tools: Overview and Selection Guide

By: Sagar

Note: This document is not created by a professional content writer so any mistake and error is a part of great design

Disclaimer

This document is generated by VIEH Group and if there is any contribution or or credit, it's mentioned on the first page. The information provided herein is for educational purposes only and does not constitute legal or professional advice. While we have made every effort to ensure the accuracy and reliability of the information presented, VIEH Group disclaims any warranties or representations, express or implied, regarding the completeness, accuracy, or usefulness of this document. Any reliance you place on the information contained in this document is strictly at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. also we highly appreciate the source person for this document.

Happy reading !

Content Credit: Sagar

Introduction

Hello dear hackers welcome back to my another blog, hope you all are good, happy and enjoying your life.

Penetration testing, also known as ethical hacking, simulates real-world cyber attacks to uncover weaknesses in a system's defenses. While this process requires a skilled and knowledgeable professional, having the right tools at their disposal can greatly enhance the efficiency and effectiveness of their efforts.

In this blog post, we will provide an overview of some of the most popular penetration testing tools available today.Whether you are a security professional looking to expand your toolkit or an organization seeking guidance on selecting the appropriate tools, this comprehensive selection guide will help you navigate the complex world of penetration testing.

Before start writing the blog, I have such a small request to all of you, I always right articles on cyber security, ethical hacking, penetration testing. So if you didn't follow, then follow me first and clap on this article, because that's give me a motivation to write something new !!

1. Network & Vulnerability Scanning Tools:

Network scanning tools are used to discover active hosts, open ports, and services running on a network. They provide essential information for further testing and vulnerability assessment. Some popular network scanning tools include.

1. **Nmap:** Nmap is a widely-used network exploration and security auditing tool.It helps in discovering hosts and services on a network, providing valuable insights into network inventory and vulnerabilities. With its extensive range of scanning techniques and scripting capabilities.
2. **Zenmap:** Zenmap is a graphical user interface (GUI) for Nmap, a powerful network scanning tool.It provides an intuitive interface for configuring and running Nmap scans, making it easier for users to conduct network exploration, host discovery,and vulnerability scanning.
3. **Nessus:** Nessus is a robust vulnerability assessment tool that helps in identifying vulnerabilities and misconfigurations in networks and systems.It performs thorough security scans, including host discovery, vulnerability detection.

4. **Wireshark:** Wireshark is a powerful network protocol analyzer that allows users to capture and inspect network traffic in real-time.It provides detailed insights into network communications, helping in network troubleshooting, analysis, and security investigations.
5. **Socat:** Socat is a versatile networking tool that allows for bidirectional data transfer between two endpoints.It provides a wide range of functionalities, such as creating virtual connections, port forwarding, and encryption.
6. **Netcat:** Netcat, also known as Swiss Army Knife of Networking, is a versatile command-line networking utility.It can read from and write to network connections, making it useful for port scanning, file transfers, and network troubleshooting.
7. **Netstat:** Netstat is a command-line tool used for displaying active network connections, listening ports, and routing tables on a host. It provides information about established connections, network statistics, and open ports, aiding in network monitoring, troubleshooting, and security analysis.
8. **Netdiscover:** This is a network scanning tool used for discovering active hosts on a network. It sends ARP (Address Resolution

Protocol) requests to determine the IP and MAC addresses of active hosts.

9. **Ncat:** This Tool is a versatile networking utility that allows for reading, writing, and manipulating network connections. It offers advanced features such as port scanning, debugging network protocols, and establishing secure connections, making it a valuable tool for network administrators and security professionals.

10. **Nikto:** Nikto is a web vulnerability scanner designed to identify security flaws in web servers and applications. It performs comprehensive tests for outdated software, misconfigurations, and potentially risky files or scripts.

11. **Skipfish:** Skipfish is a web application security scanner that performs a thorough analysis of web applications and identifies potential vulnerabilities.It crawls through the application, mapping its structure and testing for security flaws like SQL injection and cross-site scripting (XSS).

12. **OpenVAS:** OpenVAS (Open Vulnerability Assessment System) is a powerful open-source vulnerability scanner.It performs comprehensive vulnerability assessments on

networks and systems, providing detailed reports on security weaknesses.

13. **Uniscan:** Uniscan is a feature-rich web vulnerability scanner that helps in identifying potential security issues in web applications. It employs various scanning techniques like fingerprinting, file discovery, and input validation testing.

14. **Unicornscan:** Unicornscan is a high-speed network scanning tool known for its speed and efficiency in port scanning and service detection. It can quickly scan large networks, providing valuable information about open ports and services running on target hosts.

15. **Cain and Abel:** this is a windows based multi-purpose network security tool used for password recovery, network sniffing, and various types of attacks.

16. **TCPdump:** The given tool is a command-line packet analyzer used for capturing and analyzing network traffic.It provides a wide range of options for capturing and filtering packets, allowing users to examine network communications at a low-level.

17. **Tshark:** This is a command-line tool that serves as the console version of Wireshark.It offers similar packet capturing and analysis capabilities as Wireshark but without the graphical interface.

18. **Acunetix:** Acunetix is a web application vulnerability scanner that helps in identifying security flaws in web applications. It scans for common vulnerabilities such as cross-site scripting (XSS), SQL injection, and more.

19. **smbclient & enum4linux:** smbclient is a command-line tool used to interact with SMB/CIFS (Server Message Block/Common Internet File System) shares on Windows and Samba servers. It provides file and printer sharing functionalities, allowing users to access shared resources. enum4linux is a penetration testing tool used to enumerate information from Windows and Samba systems. It gathers data such as user and group details, share information, password policies, and more.

20. **Traceroute:** Traceroute is a network diagnostic tool used to trace the route packets take from the source to a destination host. It provides insights into the network path, showing each hop along the way and the response times.

21. **Curl:** Curl is a command-line tool used for making HTTP requests. It can retrieve and send data to servers, test APIs, and perform network-related tasks. It supports various protocols and provides options for specifying request methods, headers, data, authentication, output handling, and more.It is commonly used for tasks like fetching web pages, downloading files, and interacting with web services.

2.Web Application Testing Tools:

Web application testing tools are specifically designed to assess the security of web applications.They help identify common vulnerabilities like SQL injection, cross-site scripting (XSS), and insecure session management.Some notable web application testing tools are.

1. **Burp Suite:** Burp Suite is a powerful web application security testing platform.It consists of various tools that aid in discovering and exploiting vulnerabilities in web applications.With features such as web scanning, proxy interception, and vulnerability scanning.
2. **OWASP ZAP:** OWASP ZAP (Zed Attack Proxy) is an open-source web application security scanner.OWASP ZAP offers a user-friendly interface, scripting capabilities, and a wide range of features for web security testing and analysis..

3. **Sqlmap:** Sqlmap is a popular open-source tool used for automated SQL injection and database takeover. It helps in identifying and exploiting SQL injection vulnerabilities in web applications, allowing attackers to gain unauthorized access to databases.

4. **NoSQLMap:** NoSQLMap is a penetration testing tool designed for detecting and exploiting security vulnerabilities in NoSQL databases. It supports various NoSQL database platforms, such as MongoDB, CouchDB, and Redis, and helps in identifying weaknesses and unauthorized access to NoSQL databases.

5. **Sqlninja:** This tool is a tool specifically designed for exploiting SQL injection vulnerabilities in databases. It enables attackers to execute arbitrary SQL queries, retrieve data, escalate privileges, and even take control of the database server.

6. **WPScan:** WPScan is a specialized security scanning tool for WordPress websites. It assists in identifying vulnerabilities, misconfigurations, and weaknesses in WordPress installations, themes, and plugins.

7. **XSSer:** XSSer is a specialized tool used for detecting and exploiting Cross-Site Scripting (XSS) vulnerabilities in web

applications. It automates the process of identifying and exploiting XSS flaws, helping security testers in evaluating the security of web applications.

8. **FFUF:** (Fuzz Faster U Fool) is a fast web fuzzer designed for discovering hidden files and directories on web servers. It uses a combination of brute-forcing and pattern matching techniques to identify non-publicly accessible content.

9. **Dirbuster:** This tool is a directory and file brute-forcing tool used for web application testing and enumeration.It helps in discovering hidden directories, files, and sensitive information by systematically scanning web applications and attempting to locate directories that may not be publicly visible.

10. **Gobuster:** This is a directory and DNS brute-forcing tool used for website and subdomain enumeration.It helps in discovering hidden directories, files, and subdomains by brute-forcing them systematically.

11. **BeEF:** (Browser Exploitation Framework) is a powerful penetration testing tool that focuses on exploiting vulnerabilities in web browsers. It allows security professionals to assess the security of web browsers and their vulnerabilities.

12. **Vega:** Vega is an open-source web application vulnerability scanner and testing platform. It helps in identifying security vulnerabilities in web applications by scanning for common vulnerabilities like cross-site scripting (XSS), SQL injection, and more.

13. If you want's to know more about web recon tools then I written a blog on it.

Complete Bug Bounty Recon Fundamentals.
Hello beautiful hackers, welcome back to my new blog, I hope so you all are good !!
So today, in this blog, we are…
imshewale.medium.com

3. Password Cracking Tools:

Password cracking tools are used to test the strength of passwords and assess their susceptibility to brute-force or dictionary attacks.They are essential for evaluating the effectiveness of password policies.Some widely used password cracking tools include:

1. **John the Ripper:** John the Ripper is a popular password cracking tool known for its speed and versatility.It supports various attack modes, including dictionary attacks, brute force

attacks, and hybrid attacks, making it effective in cracking a wide range of password hashes. John the Ripper is commonly used for password auditing and recovery tasks.

2. **Hashcat:** Hashcat is a powerful password recovery tool capable of cracking a wide range of password hashes. It supports GPU acceleration, making it highly efficient for password cracking tasks. Hashcat is widely used in security assessments and forensic investigations to recover lost passwords or test the strength of hashed passwords.
3. **Hydra & Hydra gtk:** Hydra is a powerful and popular password-cracking tool used for online password attacks. It supports various protocols such as HTTP, FTP, SMTP, and more, allowing for brute-forcing of passwords by trying different combinations.
   Hydra gtk provides a graphical user interface (GUI) for hydra.
4. **Medusa:** Medusa is a powerful and fast network password cracking tool. It supports various protocols like SSH, FTP, Telnet, and more, allowing for brute-force and dictionary attacks on login credentials.
5. **Ophcrack:** Ophcrack is a popular offline password cracking tool that specializes in cracking Windows passwords. It uses rainbow

tables to precompute hash chains, making the cracking process faster.

6. **RainbowCrack:** RainbowCrack is a general-purpose password cracking tool that utilizes rainbow tables. It can crack hashed passwords for different operating systems and applications by leveraging precomputed tables.
7. **Crowbar:** Crowbar is an online brute-forcing tool specifically designed for cracking RDP (Remote Desktop Protocol) passwords. It leverages a list of known usernames and performs a dictionary attack to guess the password.
8. **jSQL:** jSQL Injection is a lightweight application used to find database information from a server. It's free, open source and cross-platform for Windows, Linux and Mac and it works with Java from version 11 to 20.

4. Wireless Network Testing Tools:

Wireless network testing tools help assess the security of Wi-Fi networks by identifying vulnerabilities like weak encryption, rogue access points, and misconfigurations.Two popular wireless network testing tools are:

1. **Aircrack-Ng:** Aircrack-Ng is a network security tool used for assessing the security of wireless networks.It specializes in capturing packets, analyzing network traffic, and cracking WEP and WPA/WPA2-PSK keys.
2. **Kismet:** Kismet is a wireless network detector, sniffer, and intrusion detection system. It can detect hidden networks, collect network packets, and identify devices and their vulnerabilities.
3. **Wireshark:** Wireshark is a powerful network protocol analyzer that allows users to capture and inspect network traffic in real-time.
4. This blog which I written before, it will help you to know more about wireless pentesting tool.

Top 15 Best WiFi Hacking Tools.
Hello hackers, welcome back to my new blog, hope you all are good. Today in this blog we are going to discuss about…
imshewale.medium.com

5. Payload Generator and Exploitation Tools:

Payload makes and exploitation are mostly used to get access over your target system. It content lots of payloads to use. Here are some following tools to use.

1. **Metasploit Framework:** Metasploit Framework is a comprehensive penetration testing tool that assists in exploiting security vulnerabilities.It provides a vast collection of exploits, payloads, and auxiliary modules, making it a go-to tool for security professionals.
2. **Searchsploit:** Searchsploit is a command-line tool used for searching and displaying exploits from the Exploit Database.It helps in identifying available exploits and their associated vulnerabilities.
3. **Revshells.com:** revshells.com is a website that provides a collection of reverse shell one-liners in various programming languages. Reverse shells are used in post-exploitation scenarios to gain remote access to compromised systems. Revshells.com simplifies the process of generating reverse shell commands for different platforms and languages.

4. **WADComs:** The WADComs project aims to simplify the process of collecting, analyzing, and visualizing data generated by web applications. It offers a range of tools and libraries that enable developers to integrate data collection mechanisms into their web applications and extract valuable insights from the gathered data. (Github)
5. **Security Focus:** Security Focus is a website that provides information on vulnerabilities, exploits, and security-related news.
6. **Packet Storm Security:** Packet Storm Security is a website that provides a wide range of security-related resources, including vulnerability disclosures, exploits, security tools, and advisories. It offers a repository of security-related documents and archives, allowing users to search for specific vulnerabilities, exploits, or tools.
7. **Google Hacking Database:** The Google Hacking Database, also known as GHDB, is a collection of Google search queries that can be used to identify vulnerable systems or discover sensitive information exposed on the internet.
8. **PayloadAllTheThings** and **FuzzDB** are valuable resources for security professionals and penetration testers.They provide

extensive collections of payloads, attack vectors, and fuzzing techniques. These comprehensive databases assist in identifying and testing vulnerabilities in various applications and systems.

6. Privilage Escalation Tools:

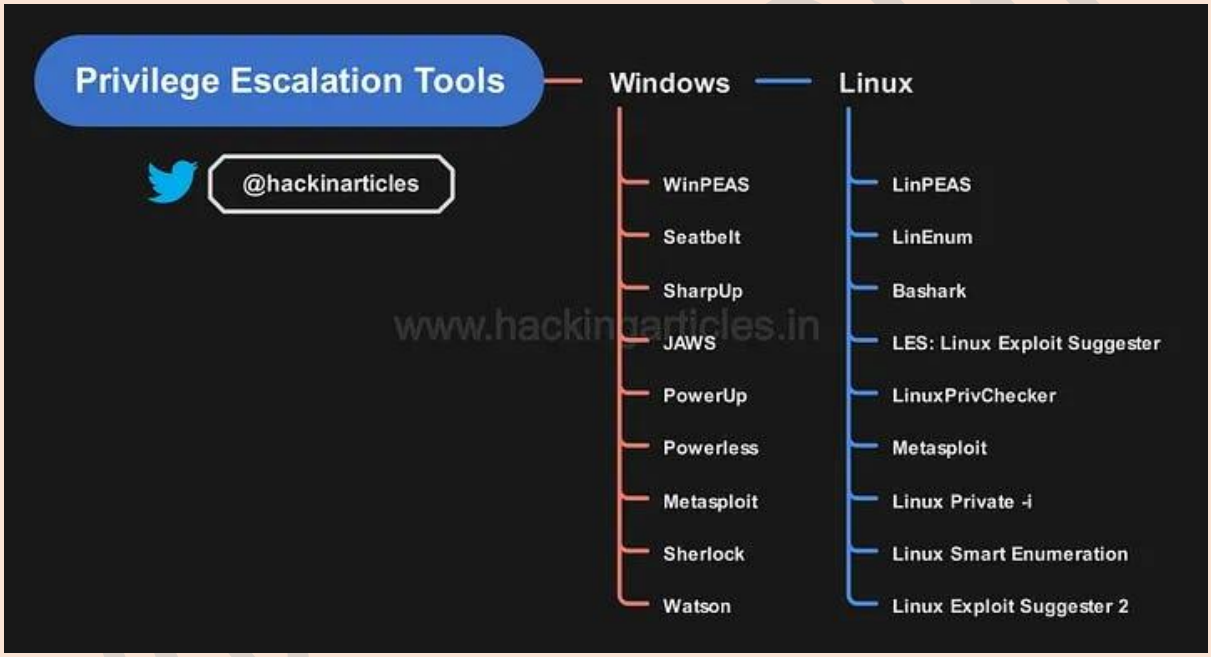
Privilage Escalation is a most important part while pentesting. It helpes you to take you control over super user privileges on your target system. There are some tools you can use to take the action.

1. **Linpeas:** Linpeas is a Linux Privilege Escalation Awesome Script (PEAS) used for privilege escalation in Linux environments.It automates the enumeration process, scanning for common misconfigurations, vulnerabilities, and weak file permissions.Linpeas is often used during security assessments to identify potential paths for privilege escalation. (Download)
2. **Winpeas:** Winpeas is a Windows Privilege Escalation Awesome Script (PEAS) used for privilege escalation in Windows environments. It automates the enumeration process, scanning for misconfigurations, vulnerable services, and weak file permissions. Winpeas is commonly used during security assessments to identify potential paths for privilege escalation. (Download)

3. **LinEnum :** is a shell script that performs various checks and commands to enumerate the system. It can assist in identifying misconfigurations, weak permissions, and potential security weaknesses that may exist on the target Linux machine. (Download)
4. **WinEnum :** is a Windows enumeration tool used for privilege escalation and system reconnaissance in Windows environments. It is designed to gather information about the target Windows system, including user accounts, installed software, services, network configuration, and potential vulnerabilities. (Download)
5. **Linux-Exploit-Suggester:** This tool tool by The-Z-Labs is an open-source utility available on GitHub. It is designed to assist with identifying potential vulnerabilities and suggesting relevant exploits for Linux operating systems.The tool aims to help in the process of vulnerability assessment and penetration testing.(Download)
6. **WES-NG :** works by retrieving system information, such as the operating system version, installed software, and patch level. It then compares this information against a

comprehensive vulnerability database, which includes details about known vulnerabilities and associated exploits.(WES-NG)

7. **GTFobins:** GTFobins is a curated collection of Unix binaries that can be used for privilege escalation during security assessments.It provides instructions and examples of using these binaries to gain elevated privileges or execute commands with higher privileges. GTFobins aids in the exploitation of misconfigured systems.



7. Tools Selection Process:

Tool selection processes is a most important thing that you have to know about it.

When selecting penetration testing tools, consider the following factors:

1. **Testing requirements**: Understand the scope of your testing project, including the target systems, network infrastructure, and applications you need to test.
2. **Features and capabilities:** Assess the features, capabilities, and ease of use of the tools. Look for tools that offer the functionalities you require and integrate well into your existing workflow.
3. **User-friendliness:** Consider the ease of use and the learning curve associated with the tools, as it can impact the efficiency of your testing efforts.
4. **Community support:** Consider the popularity and active community support for the tools. Active communities provide updates, bug fixes, and a wealth of resources, including tutorials and forums.

5. **Licensing and cost:** Evaluate the licensing models and costs associated with the tools. Some tools may offer free or open-source versions, while others require commercial licenses. If the tool is free then no problem.
6. **Reporting and documentation:** Check the reporting capabilities of the tools. Robust reporting features help in generating comprehensive reports that communicate the findings effectively.
7. Remember that penetration testing tools are only one component of a successful penetration testing process. The skills and expertise of the tester are equally important in effectively identifying and addressing security vulnerabilities.

Conclusion:

Penetration testing tools play a vital role in assessing the security posture of computer systems and networks.

By utilizing the right tools for network scanning, web application testing, password cracking, and wireless network testing, security professionals can identify vulnerabilities and take appropriate measures to enhance the overall security.

Remember to carefully evaluate your testing requirements and consider factors such as features, user-friendliness, community support, and cost when selecting the tools.

Stay updated with the latest tools and techniques in the field to ensure comprehensive and effective penetration testing.

I hope you guys love this blog.

If you like it, then don’t forget to follow, subscribe and claps.

I’ll see you with next article.

Thanks for reading