A Comparitive study on Tools for Ethical hacking.

Mani Thakur[1],
Mohd Aalim[2],
Manisha[3],
Sachin singh[4]
[1]Scholar CCSIT,TMU Moradabad,
[2]Scholar CCSIT,TMU Moradabad
[3]Assistant Professor CCSIT TMU Moradabad
manithakur88007@gmail.com,
8899733714a@gmail.com,
manisha244221@gmail.com,
singh.sachin1986@gmail.com

Abstract-

Ethical Hacking so often called as dissemination Testing is an act of intruding/penetrating into system or networks to find out threats, vulnerabilities in those systems which a malicious attacker may find and exploit causing loss of data, financial loss or other major damages. The purpose of ethical hacking is to improve the security of the network or systems by fixing the vulnerabilities found during testing. Ethical hackers may use the same methods and tools used by the malicious hackers but with the permission of the authorized person for the purpose of improving the security and defending the systems from attacks by malicious users.

Introduction-

Best open source online Ethical Hacking Tools used by hackers:

If hacking is performed to identify the potential threats to a computer or network then it will be an ethical hacking.

Ethical hacking is also called penetration testing, intrusion testing, and red teaming.

Hacking is the process of gaining access to a computer system with the intention of fraud, data stealing, and privacy invasion etc., by identifying its weaknesses.

Ethical Hackers:

A person who performs the hacking activities is called a hacker.

There are six types of hackers:

- The Ethical Hacker (White hat)
- Cracker
- Grey hat
- Script kiddies
- Hacktivist
- Phreaker

A security professional who uses his/her hacking skills for defensive purposes is called an ethical hacker. To strengthen the security, ethical hackers use their skills to

find vulnerabilities, document them, and suggest the ways to rectify them.

Companies that provide online services or those which are connected to the internet, must perform penetration testing by ethical hackers. Penetration testing is another name of ethical hacking. It can be performed manually or through an automation tool.

Comparision of various Hacking Tools-

Hacking Tools are computer programs and scripts that help you find and exploit weaknesses in computer systems, web applications, servers and networks. There is a variety of such tools available on the market. Some of them are open source while others are commercial solution.

In this list we highlight the top 20 tools for Ethical Hacking of web applications, servers and networks

1) Netsparker

Netsparker is an easy to use web application security scanner that can automatically find SQL Injection, XSS and other vulnerabilities in your web applications and web services. It is available as on-premises and SAAS solution.

Features

- Dead accurate vulnerability detection with the unique Proof-Based Scanning Technology.
- Minimal configuration required. Scanner automatically detects URL rewrite rules, custom 404 error pages.
- REST API for seamless integration with the SDLC, bug tracking systems etc.
- Fully scalable solution. Scan 1,000 web applications in just 24 hours.

2) Acunetix

Acunetix is a fully automated ethical hacking solution that mimics a hacker to keep one step ahead of malicious intruders. The web application security scanner accurately scans HTML5, JavaScript and Single-page applications. It can audit complex, authenticated webapps and issues compliance and management reports on a wide range of web and network vulnerabilities.

Features:

- Scans for all variants of SQL Injection, XSS, and 4500+ additional vulnerabilities
- Detects over 1200 WordPress core, theme, and plugin vulnerabilities
- Fast & Scalable – crawls hundreds of thousands of pages without interruptions
- Integrates with popular WAFs and Issue Trackers to aid in the SDLC
- Available On Premises and as a Cloud solution.

3) Probely

Probely continuously scans for vulnerabilities in your Web Applications. It allows its customers to manage the life cycle of vulnerabilities and provides them with some guidance on how to fix them. Probely is a security tool built having Developers in mind.

Features:

- Scans for SQL Injections, XSS, OWASP TOP10 and over 5000 vulnerabilities, including 1000 WordPress and Joomla vulnerabilities
- Full API - All features of Probely are also available through an API
- Integration with your CI tools, Slack and Jira
- Unlimited team members
- PDF Reports to showcase your security
- Diverse scanning profiles (ranging from safe to aggressive scans)
- Multiple Environment Targets - Production (non-intrusive scans) and Testing (intrusive and complete scans)

4) Burp Suite:

Burp Suite is a useful platform for performing Security Testing of web applications. Its various tools work seamlessly together to support the entire pen testing process. It spans from initial mapping to analysis of an application's attack surface.

Features:

It can detect over 3000 web application vulnerabilities.

- Scan open-source software and custom-built applications
- An easy to use Login Sequence Recorder allows the automatic scanning
- Review vulnerability data with built-in vulnerability management.
- Easily provide wide variety of technical and compliance reports
- Detects Critical Vulnerabilities with 100% Accuracy
- Automated crawl and scan
- Advanced scanning feature for manual testers
- Cutting-edge scanning logic

5) Ettercap:

Ettercap is an ethical hacking tool. It supports active and passive dissection includes features for network and host analysis.

Features:

- It supports active and passive dissection of many protocols
- Feature of ARP poisoning to sniff on a switched LAN between two hosts
- Characters can be injected into a server or to a client while maintaining a live connection
- Ettercap is capable of sniffing an SSH connection in full duplex

- Allows sniffing of HTTP SSL secured data even when the connection is made using proxy
- Allows creation of custom plugins using Ettercap's API

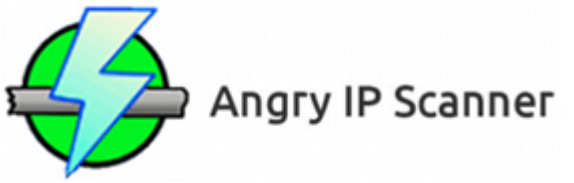
6) Aircrack:

Aircrack is a trustable ethical hacking tool. It cracks vulnerable wireless connections. It is powered by WEP WPA and WPA 2 encryption Keys.

Features:

- More cards/drivers supported
- Support all types of OS and platforms
- New WEP attack: PTW
- Support for WEP dictionary attack
- Support for Fragmentation attack
- Improved tracking speed

7) Angry IP Scanner:



Angry IP Scanner is open-source and cross-platform ethical hacking tool. It scans IP addresses and ports.

Features:

- Scans local networks as well as the Internet
- Free and open-source tool
- Random or file in any format
- Exports results into many formats
- Extensible with many data fetchers
- Provides command-line interface
- Works on Windows, Mac, and Linux
- No need for Installation

8) GFI LanGuard:

GFI LanGuard is an ethical tool that scan networks for vulnerabilities. It can acts as your 'virtual security consultant' on demand. It allows creating an asset inventory of every device.

Features:

- It helps to maintain a secure network over time is to know which changes are affecting your network and
- Patch management: Fix vulnerabilities before an attack
- Analyze network centrally
- Discover security threats early
- Reduce cost of ownership by centralizing vulnerability scanning
- Help to maintain a secure and compliant network

Conclusion-

Ethical hackers use penetration testing and other, mostly offensive, techniques to probe an organization's networks, systems and applications. In essence, ethical hackers use the same techniques, tools, and methods that malicious hackers use to find real vulnerabilities – only in this case, they

report them back to the organization for remediation…and a paycheck.

References-

[1] 1 .Challenges And Prospects Of Ethical Hacking Research Paper By Sanjay Maheshwari Sanjay@vsom.in Assistant Professor Vishisht School of Management

[2] 2.Study Of Ethical HackingBhawanaSahare1, Ankit Naik2, Shashikala Khandey3

[3] 3. A COMPREHENSIVE STUDY ON ETHICAL HACKING Suriya Begum*, Sujeeth Kumar, Ashhar INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

[4] 4 .Ethical Theory and Moral Practice An International Forum Editor-in-Chief: Th. Schramme**; M.** Düwell **ISSN: 1386-2820 (print version) ISSN: 1572-8447 (electronic version) Journal no. 10677**

[5] 5. Ida Matero Ethical Hacking: Research and Course Compilation Helsinki Metropolia University of Applied Sciences