ICCECIP 2020
2nd International Conference on Central European Critical Infrastructure Protection
November 16-17, 2020. Budapest, Hungary

ÓBUDA UNIVERSITY
BÁNKI DONÁT FACULTY OF MECHANICAL AND SAFETY ENGINEERING

HACKING TOOLS USED BY ETHICAL HACKERS

[1]Sanja Maravić Čisar, [1]Robert Pinter, [1]Igor Fürstner and [2]Petar Čisar

1 Subotica Tech – College of Applied Sciences, Subotica, Serbia
sanjam@vts.su.ac.rs, robert.pinter@vts.su.ac.rs, ifurst@vts.su.ac.rs

2 University of Criminal Investigation and Police Studies, Belgrade, Serbia
petar.cisar@kpu.edu.rs

Introduction

Ethical hacking is an integral part of the information technology industry, which deals with testing the security of computer systems. It is common practice for many companies to hire or form teams of ethical hackers, who are experts in the field of information technology, and above all trusted persons, who are engaged in testing the security of computer systems.
Ethical hackers use the same techniques and methods as potential attackers, check and assess the security of the system and, based on the detected data and omissions, propose changes to achieve better protection and greater data security.
Using ethical hacking tools, an ethical hacker surpasses the threats and malware by searching the weak points of the system. Some different tools and techniques help in hacking. Furthermore, we can use these tools to secure our systems and data.

Top 10 Hacking Tools Used By Ethical Hackers

Given below is a list of the most popular Hacking Software that is available in the market.

#1 Kiuwan Code Security (SAST)

Price: Free trial. One-time scans are $599.
Kiuwan Code Security is a vulnerability scanning tool. It identifies vulnerabilities in source code using the most stringent security standards including OWASP, CWE, SANS 25, HIPPA, and more. Kiuwan supports all major programming languages and integrates with leading DevOps tools.
Features:
❑ Automatic creation of action plans to remediate vulnerabilities.
❑ Integrates with leading IDEs including Eclipse, Visual Studio, IntelliJ IDEA, Phpstorm, Pycharm, and Webstorm.
❑ Supports 20+ programming languages for desktop, web, and mobile apps.
Best For: Finding and fixing vulnerabilities in source code during development. Kiuwan also has a tool called Insights that reports on vulnerabilities in open source components and helps manage license compliance.

#2 Nmap

Price: Free
Nmap is a security scanner, port scanner, as well as a network exploration tool. It is an open source software. It supports cross-platform. It can be used for network inventory, managing service upgrade schedules, and for monitoring host & service uptime. Nmap can work for a single host as well as large networks. It provides binary packages for Linux, Windows, and Mac OS X.
Features:
❑ Data transfer, redirection, and debugging tool (Ncat),
❑ Scan results comparing utility (Ndiff),
❑ Packet generation and response analysis tool (Nping),
❑ GUI and Results viewer (Nping)
Using raw IP packets it can determine:
❑ The available hosts on the network.
❑ Their services offered by these available hosts.
❑ Their OS.
❑ Packet filters they are using.
Best for: Nmap is best for scanning network. It is easy to use and fast as well.

#3 Netsparker

Netsparker is a dead accurate ethical hacking tool, that mimics a hacker's moves to identify vulnerabilities such as SQL Injection and Cross-site Scripting in web applications and web APIs.
Netsparker uniquely verifies the identified vulnerabilities proving they are real and not false positives, so you do not need to waste hours manually verifying the identified vulnerabilities once a scan is finished. It is available as a Windows software and an online service.

4 Intruder

Price: 30 days trial
Intruder is a fully automated scanner that finds cybersecurity weaknesses in digital estate, and explains the risks and helps with their remediation.
More then 9,000 security checks available. Its security checks include identifying misconfigurations, missing patches, and common web application issues such as SQL injection & cross-site scripting.
Intruder also integrates with major cloud providers as well as Slack & Jira.

#5 Acunetix

Acunetix is a fully automated ethical hacking tool that detects and reports on over 4500 web application vulnerabilities including all variants of SQL Injection and XSS.
The Acunetix crawler fully supports HTML5 and JavaScript and single-page applications, allowing auditing of complex, authenticated applications.
It bakes in advanced Vulnerability Management features right-into its core, prioritizing risks based on data through a single, consolidated view, and integrating the scanner's results into other tools and platforms.

#6 Metasploit

Price: Metasploit Framework is an open source tool and it can be downloaded for free. Metasploit Pro is a commercial product. Its free trial is available for 14 days.
It is the software for penetration testing. Using Metasploit Framework, you can develop and execute exploit code against a remote machine. It supports cross-platform.
Features:
❑ It is useful for knowing about security vulnerabilities.
❑ Helps in penetration testing.
❑ Helps in IDS signature development.
❑ You can create security testing tools.
Best for: Building anti-forensic and evasion tools.

#7 Aircrack-ng

Price: Free
Aircrack-ng provides different tools for evaluating Wi-Fi network security. For Wi-Fi security, it focuses on monitoring, attacking, testing, and cracking. It supports Linux, Windows, OS X, Free BSD, NetBSD, OpenBSD, Solaris, and eComStation 2.
Features:
❑ Aircrack-ng can focus on replay attacks, de-authentication, fake access points, and others.
❑ It supports exporting data to text files.
❑ It can check Wi-Fi cards and driver capabilities.
❑ It can crack WEP keys and for that, it makes use of FMS attack, PTW attack, and dictionary attacks.
❑ It can crack WPA2-PSK and for that, it makes use of dictionary attacks.
Best for: Supports any wireless network interface controller.

#8 Wireshark

Price: Free
Wireshark is a packet analyzer and can perform deep inspection of many protocols. It supports cross-platform. It allows you to export the output to different file formats like XML, PostScript, CSV, and Plaintext. It provides the facility to apply coloring rules to packet list so that analysis will be easier and quicker.
Features:
❑ It can decompress the gzip files on the fly.
❑ It can decrypt many protocols like IPsec, ISAKMP, and SSL/TLS etc.
❑ It can perform live capture and offline analysis.
❑ It allows you to browse the captured network data using GUI or TTY-mode TShark utility.
Best for: Analyzing data packets.

#9 Ettercap

Price: Free.
Ettercap supports cross-platform. Using Ettercap's API, you can create custom plugins. Even with the proxy connection, it can do sniffing of HTTP SSL secured data.
Features:
❑ Sniffing of live connections.
❑ Content filtering.
❑ Active and passive dissection of many protocols.
❑ Network and host analysis.
Best for: It allows you to create custom plugins.

#10 John the Ripper

Price: Free
John the Ripper is a tool for password cracking. It can be used on Windows, DOS, and Open VMS. It is an open source tool. It is created for detecting weak UNIX passwords.
Features:
❑ John the Ripper can be used to test various encrypted passwords.
❑ It performs dictionary attacks.
❑ It provides various password crackers in one package.
❑ It provides a customizable cracker.
Best for: It is fast in password cracking

Conclusions

Automated tools are changing the way hacking is evolving, making ethical penetration testing easier, faster and more reliable than ever. Penetration testing and reporting activities now play a crucial role in the process of identifying security flaws in remote or local software — enabling company owners to quickly prevent vulnerabilities from running wild all over the Internet.