MJRET

OPEN ACCESS

Multidisciplinary Journal of Research in Engineering and Technology

www.mjret.in

eISSN:2348-6953

Comparative study of Ethical hacking tools

[1]Chinmayee Dhanu, [2]Chetana Achar
[2]Student, [1] Professor Dept. of Institute of Computer Science,
MET Institute of Computer Science
Bandra(W), Mumbai, India.

Abstract: *Ethical hacking - also referred to as penetration testing or intrusion testing or red teaming has become a serious concern for businesses and governments. Companies are worried about the likelihood of being "hacked" and potential customers are worried about maintaining control of private information. This paper compares different hacking tools based on their performance and penetration testing.*

Keywords: *Ethical hacking, security, penetration testing, vulnerability analysis, exploitation.*

1. INTRODUCTION

Hacking refers to gaining access to a computer to obtain information stored on it with help of password cracker software or any other technique to get data. This is done to either point out the loop holes within the security or to cause intentional sabotage of the computer.
Security professionals who use their hacking skills for defensive purposes are called ethical hackers. Ethical hackers work as an information security expert. They try to interrupt the safety of a computing system, network, or applications. To strengthen security, ethical hackers use their skills to find vulnerabilities, document them, and suggest ways to rectify them.
Companies that provide online services or those which are connected to the web, must perform penetration testing by ethical hackers. Penetration testing can be performed manually or through an automation tool.

Phases of hacking

Reconnaissance: Reconnaissance is the act of gathering preliminary data in order to better plan for your attack. Reconnaissance is often performed actively (directly touching the target) or passively (meaning that your recon is being performed through an intermediary).
Scanning: In Scanning, the appliance of technical tools is used to gather further intelligence on the target, but during this case, the intel being sought is more commonly about the systems that they have in place. For example, the use of a vulnerability scanner on a target network.
Gaining Access: Owning systems requires taking control of one or more network devices in order to either extract data from the target, or to use that device to then launch attacks on other targets.
Zombie system: Maintaining Access requires taking the steps involved in being able to be persistently within the target environment in order to gather as much data as possible. The attacker must remain stealthy during this phase, so as to not get caught while using the host environment.
Evidence removal: The final phase of covering tracks simply means that the attacker must take the steps necessary to remove all semblance of detection. Any changes that were made or authorizations that were escalated, all must return to a state of non-recognition by the host.

Fig 1: Hacking phases

2. WHY DO WE NEED TOOLS?

a) Saves your effort and time - a well-known vulnerability will take a significant amount of time to be identified. Tools will identify them and you can work on the subsequent stage.

b) Will be more accurate with findings; there will be false positives, but that can be minimized over a period of time.

c) A penetration tester cannot be an expert altogether phases of the test. Thus, tools will be of much help.

d) They help in generating the reports that are easy to understand and can be used by the business teams and executive management. Most of the tools offer various reporting formats which can be used by developers, testers, management or fed to other tools for further usage.

e) Automates the manual tasks- teams can focus on skilled work rather than redundant tasks.

f) The tool will gather a lot of raw data which will be reported to the tester; this data might not be exploitable always, although it offers a lot of knowledge. The data is used by internal teams to make strong architecture.

3. WEAPONS OF ETHICAL HACKERS

Metasploit

Metasploit is an exploitation framework that has been full of various capabilities. Metasploit Framework is an open source tool which can be downloaded for free. Whereas Metasploit Pro is a commercial product. With Metasploit Pro, you can leverage the power of the Metasploit Framework and its exploit database through an interactive UI to perform security assessments and vulnerability validation.

It can be used to scan for open ports and services, exploit vulnerabilities, pivot further into a network, collect evidence, and create a report of the test results. Here are the general steps it follows to perform a penetration test.

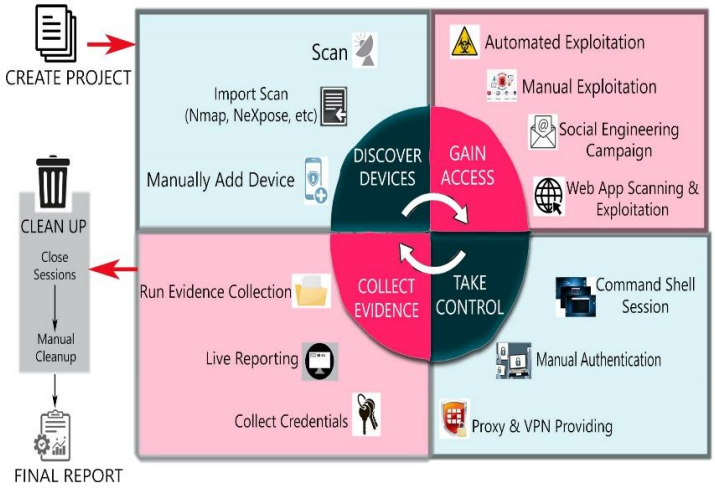

Fig 2: Typical workflow

Metasploit helps to identify the weakest point to exploit a target and prove that a vulnerability or security issue exists. It can easily automate all phases of a penetration test, from choosing the right exploits to streamlining evidence collection and reporting

Nmap

Nmap ("Network Mapper") - is a free, open source tool for network exploration and security auditing. It was written by security expert Gordon Lyon in 1997, and the solution is openly available under the GNU General Public License.

Nmap uses raw IP packets in novel ways to determine characteristics, such as;

a) what hosts are available on the network?
b) what operating systems and OS versions those hosts are running?
c) what application name and version (or services) they are offering?
d) what type of packet filters/firewalls are in use?

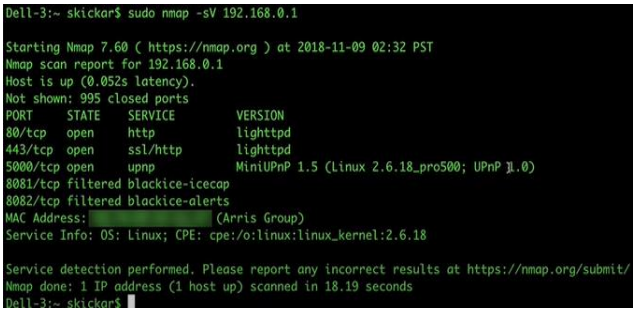

Fig 3: Nmap version scan

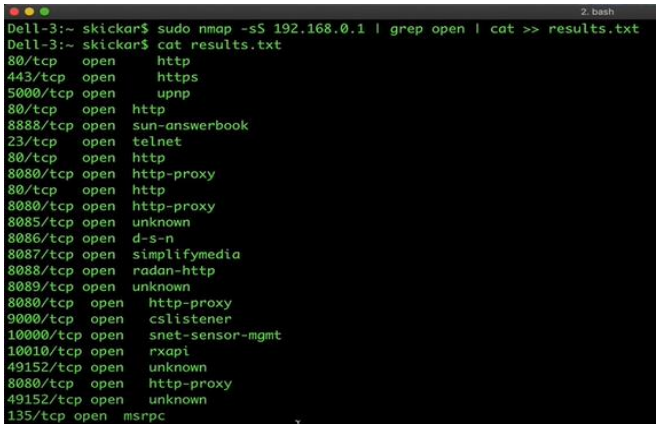

Fig 4: Nmap port scan

Here are few options for scanning:
-sS: Port scan
-sP: Ping scanning.
-sT: A TCP connect() scan.
-sU: Sends a UDP header to every port.
-sV: version scan.
-O: OS scan.

It was designed to rapidly scan large networks, but also works fine against single hosts. It runs on all major computer operating systems such as Windows, and Mac OS X, and provides official binary packages for Linux.

Wireshark

Wireshark is a packet sniffer that performs deep inspection of many protocols. Wireshark can be used for monitoring the attack and analyzing the data packet exchange over a network wired or wireless. Although it won't directly tell anything but it might alert users to a possible threat.

Wireshark works in three major steps:

a) Collection: In this step Wireshark capture the raw binary data from the network, so that it can sniff all the traffic.
b) Conversion: Once the data is been captured it is converted into a human readable form.
c) Analysis: This is the final step in where the converted data is analyzed by the user to get the required information, depending on how well the user interprets the data.

Following figures show, how the Wireshark captures the data over TELNET protocol and convert back into a human readable format.

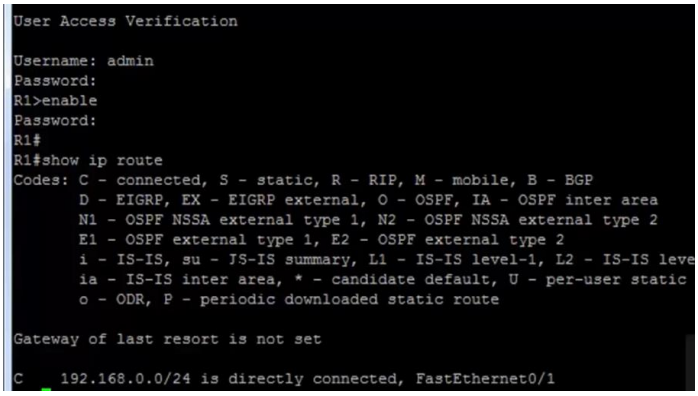

Fig 5: Executing commands.

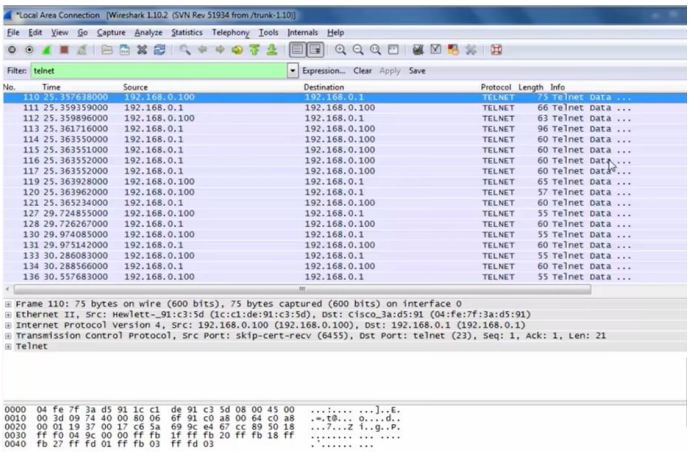

Fig 6: Capturing packets using Wireshark

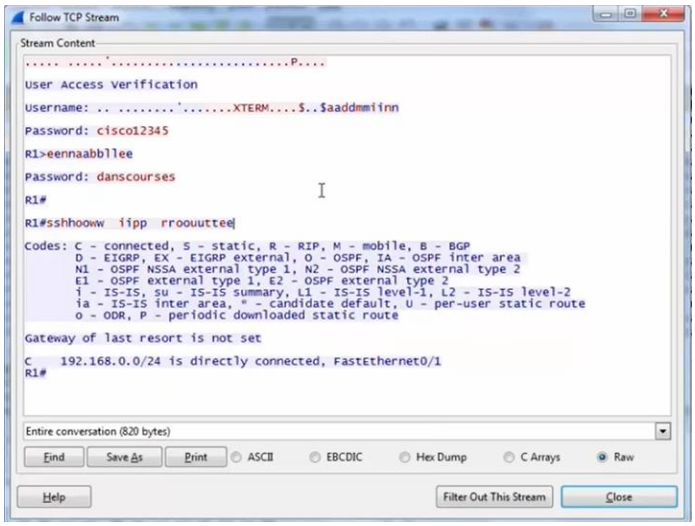

Fig 7: Converted data

4. SUMMARY

Criteria	Metasploit	Nmap	Wireshark
Technology	Penetration testing	Software vulnerability scanner	Network analyzer
Tool type	Security and exploitation	Security auditing and network management	Packet sniffer
Written in	Ruby	C, C++, Python, Lua	C, C++
Helps to	Identify weakest point to exploit a target and develop IDS signature	Rapidly scan huge networks	Find the root cause of a known problem
Most suitable for	Building anti forensic and Stealth tool	Rigorous scanning and exploiting vulnerabilities in a network	Analyzing specific timing, protocol flags, or bits over the network.
Platform	Mac OS, Linux, Windows	Linux, Windows, Solaris, Mac OS X, OpenBSD, etc.	Linux, Windows, Mac OS X, FreeBSD, NetBSD, etc.
Addition Features	• The extensible model through which payloads, encoders, no-op generators, and exploits are often integrated • allows the proper testing of an IDS and aid with the signature development. • crafting a quick and dirty exploit using the tools is available • reduces the amount of manual programming work • allows a network administrator to interrupt into his own network to spot security risks and document which vulnerabilities got to be addressed first	• Built in signature checking algorithms to guess OS & versions based on network response. • Along with the classic command-line Nmap executable, • the Nmap suite includes; Data transfer, redirection, and debugging tool(Ncat), Scan results comparing utility(Ndiff), Packet generation and response analysis tool (Nping), GUI and Results viewer (Zenmap)	• Built in decryption support for many encrypted protocols • Perform live capture & offline analysis • Decompresses the gzip files on the fly • Output can be exported to XML, PostScript, CSV, or plain text. • Facility to apply coloring rules to the packet list for quick, intuitive analysis • VoIP calls in the captured traffic can be detected.

Table 1: Comparison of Hacking tools

5. REFERENCES

[1]. Suriya Begum, Sujeeth Kumar, Ashhar: "A Comprehensive Study on Ethical Hacking. International Journal of Engineering Sciences & Research Technology." August, 2016 ISSN: 2277-9655

[2]. Najiya Sultana: "A Framework of Wireless Network Security Threats: Solution for Various Information Security Problems." IJCSMC, Vol. 8, Issue. 10, October 2019, pg.109 – 122 ISSN 2320–088X

[3]. *Pawan Kesharwani, Sudhanshu Pandey, Vishal Dixit, Lokendra Kumar Tiwari: "A study on Penetration Testing Using Metasploit Framework." International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 12 | Dec 2018 e-ISSN: 2395-0056 p-ISSN: 2395-0072*

[4]. *Carlos Joshua Marquez: "An Analysis of the IDS Penetration Tool: Metasploit."*

[5]. *Mujahid Shah, Muhammad Junaid, Sheeraz Ahmed, Hamayun Khan, Khalid Saeed, Ata-ur-rehma: "Penetration Testing Active Reconnaissance Phase – Optimized Port Scanning With Nmap Tool." International Conference on Computing, Mathematics and Engineering Technologies – iCoMET 2019*

[6]. *S.Pavithirakini,D.D.M.M.Bandara, C.N.Gunawardhana, K.K.S.Perera, B.G.M.M.Abeyrathne, Dhishan Dhammearatchi: "Improve the Capabilities of Wireshark as a tool for Intrusion Detection in DOS Attacks." International Journal of Scientific and Research Publications, Volume 6, Issue 4, April 2016 ISSN 2250-3153*

[7]. *Usha Banerjee, Ashutosh Vashishtha, Mukul Saxena: "Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection." International Journal of Computer Applications (0975 – 8887) Volume 6– No.7, September 2010*

[8]. *Haroon Iqbal, Sameena Naaz: "Wireshark as a Tool for Detection of Various LAN Attacks."* *International Journal of Computer Sciences and Engineering Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693*