International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 1 –NOVEMBER 2014.

ETHICAL HACKING TOOLS

V.Teja Priya

Lecturer, Dept of Computer Sciences. K.B.N. College, Vijayawada

tejapriya1988@gmail.com

Abstract— A hacker is who maliciously breaks into systems for personal gain. Technically, these criminals are crackers. Crackers break into systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

Ethical hacking also known as penetration testing or white-hat hacking involves the same tools, tricks, and techniques that hackers use, but with one major difference: Ethical hacking is legal. Ethical hacking is performed with the target's permission. The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It's part of an overall information risk management program that allows for on-going security improvements. Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate.

If you don't have the right tools for ethical hacking, accomplishing the task effectively is difficult, Many tools focus on specific tests, but no one tool can test for everything. For the same reason that you wouldn't drive in a nail with a screwdriver, you shouldn't use a word processor to scan your network for open ports. This is why you need a set of specific tools that you can call on for the task at hand. The more tools you have, the easier your ethical hacking efforts are. Make sure you that you're using the right tool for the task.

I. INTRODUCTION

UNDERSTANDING THE PURPOSE OF ETHICAL HACKING:

Ethical hackers are usually security professionals or network penetration testers who use their hacking skills and tool sets for defensive and protective purposes. Ethical hackers who are security professionals test their network and systems security for vulnerabilities using the same tools that a hacker might use to compromise the network. Any computer professional can learn the skills of ethical hacking.

The term cracker describes a hacker who uses their hacking skills and tool set for destructive or offensive purposes such as disseminating viruses or performing denial-of service (DoS) attacks to compromise or bring down systems and networks. No longer just looking for fun, these hackers are sometimes paid to damage corporate reputations or steal or reveal credit card information, while slowing business processes and compromising the integrity of the organization.

Hackers can be divided in to three groups:

White Hats: Good guys, ethical hackers

Black Hats: Bad guys, malicious hackers

Gray Hats: Good or bad hacker, depends on the situation.

Ethical hackers usually fall into the white-hat category, but sometimes they're former gray hats who have become security professionals and who now use their skills in an ethical manner.

White Hats

White hats are the good guys, the ethical hackers who use their hacking skills for defensive purposes. White-hat hackers are usually security professionals with knowledge of hacking and the hacker toolset and who use this knowledge to locate weaknesses and implement counter measures.White hats are those who hack with permission from the data owner. It is critical to get permission prior to beginning any hacking activity. This is what makes a security professional a white hat versus a malicious hacker who cannot be trusted.

Black Hats

Black hats are the bad guys: the malicious hackers or crackers who use their skills for illegal or malicious purposes. They break into or otherwise violate the system integrity of remote systems, with malicious intent. Having gained unauthorized access, black-hat hackers destroy vital data, deny legitimate users service, and just cause problems for their targets. Black-hat hackers and crackers can easily be differentiated from white-hat hackers because their actions are malicious.

Gray Hats

Gray hats are hackers who may work offensively or defensively, depending on the situation. This is the dividing line between hacker and cracker. Gray-hat hackers may just be interested in hacking tools and technologies and are not malicious black hats. Gray hats are self-proclaimed ethical hackers, who are interested in hacker tools mostly from a curiosity standpoint. They may want to highlight security problems in a system or educate victims so they secure their systems properly.

II. ETHICAL HACKING TERMINOLOGY

Being able to understand and define terminology is an important part of a CEH's(Certified Ethical Hackers) responsibility. This terminology is how security professionals acting as ethical hackers communicate.

Threat An environment or situation that could lead to a potential breach of security. Ethical hackers look for and prioritize threats when performing a security analysis.

Malicious hackers and their use of software and hacking techniques are themselves threats to an organization's information security.

Exploit A piece of software or technology that takes advantage of a bug, glitch, or vulnerability, leading to unauthorized access, privilege escalation, or denial of service on a computer system. Malicious hackers are looking for exploits in computer systems to open the door to an initial attack. Most exploits are small strings of computer code that, when executed on a system, expose vulnerability.

Vulnerability The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system. Exploit code is written to target vulnerability and cause a fault in the system in order to receive valuable data.

Target of Evaluation (TOE) A system, program, or network that is the subject of a security analysis or attack. Ethical hackers are usually concerned with high-value TOEs, systems that contain sensitive information such as account numbers, passwords, Social Security numbers, or other confidential data. It is the goal of the ethical hacker to test hacking tools against the high-value TOEs to determine the vulnerabilities and patch them to protect against exploits and exposure of sensitive data.

Attack An attack occurs when a system is compromised based on vulnerability. Many attacks are perpetuated via an exploit. Ethical hackers use tools to find systems that may be vulnerable to an exploit because of the operating system, network configuration, or applications installed on the systems, and to prevent an attack.

There are two primary methods of delivering exploits to computer systems: Remote the exploit is sent over a network and exploits security vulnerabilities without any prior access to the vulnerable system. Hacking attacks against corporate computer systems or networks initiated from the outside world are considered remote. Most people think of this type of attack when they hear the term hacker, but in reality most attacks are in the next category.

Local The exploit is delivered directly to the computer system or network, which requires prior access to the vulnerable system to increase privileges. Information security policies should be created in such a way that only those who need access to information should be allowed access and they should have the lowest level of access to perform their job function.

III. ETHICAL HACKING TOOLS

The following list runs down some of my favourite commercial, freeware, and open-source security tools:

Acunetix has a free and paid version. This hacking tool has many uses but in essence it tests and reports on SQL injection and Cross Site scripting testing. It has a state of the art crawler technology which includes a client script analyzer engine. This security tool generates detailed reports that identify security issues and vulnerabilities. The latest version, Acunetix WVS version 8, includes several security features such as a new module that tests slow HTTP Denial of Service. This latest version also ships with a compliance report template for ISO 27001. This is useful for penetration testers and developers since it allows organizations to validate that their web applications are ISO 27001 compliant.

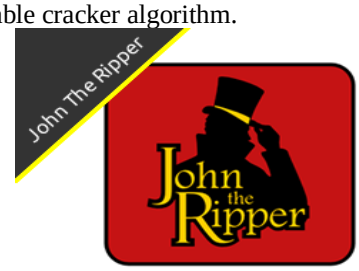
Air cracking is a comprehensive set of network security tools that includes, aircrack-ng, which can cracks WEP (wired Equivalent Privacy) and WPA (Wi-Fi Protected Access) Dictionary attacks, airdecap-ng (which can decrypts WEP or WPA encrypted capture files), airmon-ng (which places network cards into monitor mode, for example when using the Alfa Security Scanner with rtl8187), aireplay-ng (which is a packet injector), airodump-ng (which is a packet sniffer), airtun-ng (which allows for virtual tunnel interfaces), airolib-ng (which stores and manages ESSID and password lists), packetforge-ng (which can create encrypted packets for injection), airbase-ng (which incorporates techniques for attacking clients) and airdecloak-ng (which removes WEP cloaking). Other tools include airdriver-ng (to manage wireless drivers), airolib-ng (to store and manages ESSID and password lists and compute Pairwise Master Keys), airserv-ng (which allows the penetration tester to access the wireless card from other computers). Airolib-ng is similiar to easside-ng which allows the user to run tools on a remote computer, easside-ng (permits a means to communicate to an access point, without the WEP key), tkiptun-ng (for WPA/TKIP attacks) and wesside-ng (which is an automatic tool for recovering wep keys).

Cain & Abel, or just Cain for short, has a reputation of being a bit of a script-kiddie tool, but it is still awesome nonetheless. Cain & Abel is defined as being a password recovery tool. This tool allows a penetration tester to recover various types of passwords by sniffing the network, and cracking encrypted passwords using either a dictionary or brute-force attacks. The tool can also record VoIP(Voice Over Internet Protocol) conversations and has the ability to decode scrambled passwords, discover WiFi network keys and cached passwords. With the correct usage and expertise, a penetration tester can also analyze routing protocols. The security tool

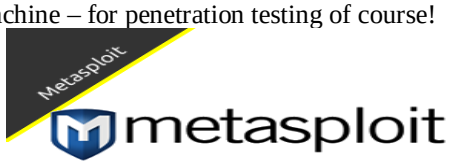
does not inherently exploit any software vulnerabilities or holes, rather it identifies security weaknesses in protocol's standards.

Ettercap It is a free and open source network security tool for man-in-the-middle attacks (MITM) on LAN. The security tool can be used to analyze computer network protocols within a security auditing context. Ettercap has four methods of functionality:Security scanning by filtering IP-based packets, MAC-based: whereby packets are filtered based on MAC address, (this is useful for sniffing connections through a gateway). ARP-based scanning by using ARP poisoning to sniff on a switched LAN between two hosts (known as full-duplex). PublicARP-based functionality: Ettercap uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (known as half-duplex).

John The RipperIt was written by Black Hat Pwnie Winner Alexander Peslyak. This very popular security tool, often abbreviated just to "John" is a free password cracking software tool. Originally created for the UNIX operating system, it currently works on every major operating system. By far, this tool is one of the most popular password testing and breaking programs used by information security professionals. The penetration testing tool combines various password crackers into one concise package which is then able to identify password hash types through its own customizable cracker algorithm.



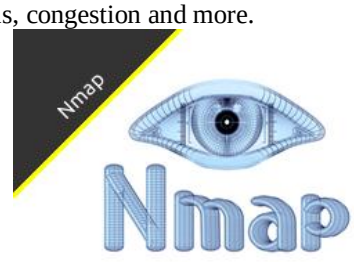
Metasploit is huge. Developed by Rapid7 and used by every penetration tester and ethical hacker in the world. The Metasploit Project is a security project which delivers information about security vulnerabilities and helps penetration testing and Intrusion detection. The open source project – known as the Metasploit Framework, is used by security professionals to execute exploit code against a remote target machine – for penetration testing of course!



Nessus is another giant – a security tool that focuses on vulnerability scanning. There is a free and paid version – free for personal use. Started in 1998 by Renaud Deraison is has evolved into one of the world's most popular security tools – particularly as a vulnerability scanner. The organization behind Nessus, Tenable Security, estimates that it is used by over 75,000 organizations worldwide.

Essentially Nessus scans for various types of vulnerabilities: ones that check for holes that hackers could exploit to gain control or access a computer system or network. Furthermore, Nessus scans for possible misconfiguration (e.g. open mail relay, missing security patches, etc.). The tools also scans for default passwords and common passwords which is can use execute through Hydra (an external tool) to launch a dictionary attack. Other vulnerability scans include denials of service against the TCP/IP stack.

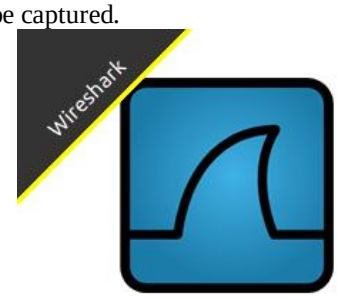
Nmap (Network Mapper) It is the defacto(legal) security scanner which is used to discover hosts and services on a computer network. To discover hosts on a network Nmap sends specially built packets to the target host and then analyzes the responses. The program is really sophisticated because unlike other port scanners out there, Nmap sends packets based upon network conditions by taking into account fluctuations, congestion and more.



Kismet is a wireless network detector, sniffer, and intrusion detection security penetration testing tool. Kismet can monitor

and sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic. There are many sniffing tools out there but what makes Kismet different and very popular is the fact that it works passively – meaning that the program does not send any loggable packets whilst being able to monitor wireless access points and wireless clients. It is open source and widely used.

Wireshark Wireshark has been around for ages and is extremely popular. Wireshark allows the penetration tester to put a network interface into a promiscuous mode and therefore see all traffic. This tool has many features such as being able to capture data from live network connection or read from a file that saved already-captured packets. Wireshark is able to read data from a wide variety of networks, from Ethernet, IEEE 802.11, PPP, and even loopback. Like most tools in our 2013 Concise Courses Security List the captured network data can be monitored and managed via a GUI – which also allows for plug-ins to be inserted and used. Wireshark can also capture VoIP packets and raw USB traffic can also be captured.



IV. REFRENCES

[1] CEH(Certified Ethical Hackers)2010V6.
[2] Hacking Wireless Networks For Dummies.
[3] Ethical Hacking and Countermeasures- Web Applications and Data Servers.
[4] HACKING: THE ART OF EXPLOITATION
[5] http://www.concise-courses.com/security/top-ten-pentesting-tools/
[6] http://media.techtarget.com/searchNetworking/downloads/hacking_for_dummies.pdf
[7] http://bedaone.blogspot.in/p/chapter-1-introduction-to-ethical.html
[8] http://www.ehacking.net/2011/06/top-6-ethical-hacking-tools.html