

Boyd Aaron Sigmon

Dr. Phil Lunsford

ICTN 4040 Section 601

19 April 2009

Hacking Tools & Techniques and How to Protect Your Network from Them

Hackers today use a wide variety of tools and techniques to gain entry into networks across the globe, stealing and destroying confidential data, as well as defacing public websites, writing malicious code, and bringing systems and networks to their knees. These attacks can sometimes cost companies thousands of dollars in downtime, resources, and manpower, not to mention the possibility of having secret data stolen and leaked. The purpose of this paper is to discuss some of the most common tools and techniques hackers use today, and how you and your company can protect your infrastructure from these attacks, as well as broaden your knowledge on hacking as a whole.

The true meaning of hacking is to increase the capabilities of an electronic device, and use it beyond the original intentions of the vendor. Hacking began in the 1960's, when a group of students at MIT were tweaking electric trains to go faster and be more efficient. Then, it wasn't long before a group of these guys started using their skills in the mainframes at MIT. In the 1970's a new type of hacker emerged, called a "phreaker", who could hack telephone systems and make phone calls for free. By the 1980's, hackers were starting to use computers more and more, and started using Bulletin

Board Systems to share stolen computer passwords & credit card numbers, which led to the Computer Fraud and Abuse Act being passed by Congress in 1986. Once the internet had its surge of users in the 90's, hacking was becoming more main-stream and the number of hackers around the world started growing rapidly (Hackingalert.com).

As hacking has become more and more popular over the years, experienced hackers and security professionals have written programs that have enabled less experienced hackers, also called “script kiddies”, to easily achieve attacks on systems and networks. Most of these tools were originally designed for use by security professionals to test their networks for vulnerabilities, but have since become a double-edged sword. Identified below, are 6 of the most popular hacking tools and techniques currently used today.

1. **Port Scanners** – Port scanning, also called “Port knocking” is a technique used by hackers to find an opening in to a remote system. There are over 65535 TCP and UDP ports in the TCP/IP suite that a host can use to communicate with the Internet. A remote attacker can use a tool such as Nmap to scan for open ports and try to connect to that system using it's IP address and open port numbers by using telnet or ssh. Tools like Nmap can also detect running processes and the Operating System (OS) version that the system is using, so they could exploit vulnerabilities associated with that process or OS. Also, experienced attackers can use port scanning techniques that can easily go undetected by most Network Intrusion Detection Systems.

- 2. Vulnerability Scanners** – Vulnerability scanning is a tool & technique that can have a use that is both good and bad. It was originally designed by security professionals to find weaknesses in their network, but has since then, been used by attackers to detect those same weaknesses. Attackers can exploit a vulnerability to gain entry to a system, and obtain user to administrator level access, as well as cause the system to crash maliciously. Nessus is one of the most popular vulnerability scanners used today, and is an open source product that is available to download for free over the internet. This scanner is capable of testing services running on non-standard ports, and multiple instances of a service, as well as detecting patches and updates that have not been applied to systems.
- 3. Packet Sniffers** – A packet sniffer is a network analyzer that can either be used rightfully by a network administrator to monitor traffic on their network, or can used by an attacker to sniff out packets on a network that could contain valuable information passed in plain-text, such as usernames and passwords (Bradley). A Packet sniffer can only be used to sniff out packets on the subnet that the attacker is on, but it can also be hard to detect because of their passive nature. There are about a dozen of popular packet sniffers available today for free on the internet like Wireshark, TCPDump, and Cain & Abel, as well as wireless sniffers such as Kismet and Netstumbler, which sniff out packets on wireless networks and even look for open access points. Also, one of

the most popular Network-Based Intrusion Detection tools, called Snort can even be used as a packet sniffer.

4. **Rootkits** – Rootkits are a tool or program that can give an attacker administrator-level access on a system, as well as give them the ability to hide their intrusion by altering log files (SearchMidmarketSecurity.com). Rootkits can also contain spyware, and can be hard to detect by hiding themselves in files and directories that cannot be seen by simply browsing through a folder structure, or even by using a Host Based Intrusion Detection System.
5. **Password Crackers** – A password cracker is a tool that an attacker can use to gain access to system by using different combinations of sequences to guess usernames and passwords. There are many popular password cracking tools out there today, like Cain & Abel, John the Ripper, and THC Hydra that can perform several password cracking techniques, such as Dictionary, Brute Force, and Cryptoanalysis attacks. Also, there are wireless crackers like Aircrack-ng & Aircrack-ng that can recover encryption keys and crack wireless protocols like WEP & WPA (Insecure.org).
6. **Social Engineering** – One of the most important and common attacks to protect your network from is a social engineering attack. Social Engineering is the process of using social skills to convince people to reveal access credentials or other valuable information to an attacker (Whitman & Mattord 69). Basically, an attacker could gain access to

locked area by telling another employee that they have lost their key, or forgot their ID badge. Another scenario could be that a person calls in to the helpdesk, pretending to be an employee of the company that has lost their password, and asks the help desk to give them the password over the phone. Attackers could also go through trash or other areas that important documents could be stored or disposed of. It is extremely important to educate employees on security awareness, so that social engineering attacks cannot occur.

Some other very common attacks that hackers use today are against web servers and online databases. Web-servers are usually placed in a small sub-network between the internal network (LAN) and the internet called a DMZ, or Demilitarized Zone, so that everyone is able to access its web pages over the internet. One of the most commonly used attacks against web servers is called, “cross-site scripting”, which is a web application software vulnerability where hackers can inject malicious code into a web page, and can also be used to bypass access controls to gain access to network resources (Cross Site Scripting).

Another common attack used in web hacking is the SQL injection, where attackers can inject a SQL query or command as an input through a web page. A lot of web pages will take certain parameters from a web user, and then make a SQL query to the database. SQL Injections attack web applications, such as ASP, JSP, PHP, and CGI, and can be done over port 80 by just using a web browser. With SQL injections, attackers can send a modified user name and password field that can change the SQL query and then grant them access to other resources (SK).

Not only can hackers attack web applications, but they can also attack other applications programmed in various languages, such as C, using a “buffer overflow” attack. This causes the program to write more information into the buffer than the space has set aside in memory. Once this is done, an attacker can overwrite the data that controls the program and hijack control of the program to execute the hacker’s code instead of the original source code (WindowSecurity.com).

Defending your systems and networks from these attacks can be sufficiently achieved by using a number of tools, equipment, and industry best practices. Some of those tools include using a firewall to protect your network from outside traffic. A firewall is a device that selectively denies or accepts data flowing into or out of the company network, and protects resources on the internal network from the outside (Whitman & Mattord 204). Firewalls can be hardware appliances or server-based, and should be placed between your border internet router and internal network. An ideal solution is to place two firewalls in your infrastructure, having one as a perimeter firewall behind the border internet router, and placing another between the perimeter firewall and the internal network, isolating the DMZ.

Another critical piece of equipment and best practice for securing your network is to use Network and Host-Based Intrusion Detection Systems, such as Snort and AIDE. Snort is an open source industry leading Network Intrusion Detection System (NIDS) that uses rules to combine the advantages of signature, protocol and anomaly based examination methods (Snort.org). By using an NIDS, you can monitor traffic trying to enter your network, and based on the rule-set will be able to detect threats and suspicious activity, like scanning, sniffing, and password cracking, as well as other threats and

vulnerabilities, much like how an antivirus software works. An ideal location to place your NIDS would be between the border internet router and the firewall that blocks off the internal network, as well as behind your firewall to monitor your internal network in case of intrusion. If you have two firewalls that isolate your DMZ, then place the NIDS in your DMZ between the two firewalls to effectively protect and monitor your DNS, HTTP, FTP, and SMTP servers. In addition to using an NIDS, it would also be a good idea to use a Host-Based Intrusion Detection System (HIDS), such as AIDE, to be able to detect modified files or directories and rootkits on servers, in case they have been compromised.

The next defense from keeping an attacker from accessing critical data is to use encryption. All confidential data should be encrypted using at least Data Encryption Standard (DES) cryptography, as well as having access controls in place to prevent unauthorized user accounts from accessing files or directories. Also, only secure encrypted connections should be used, like SSH, when remotely accessing network equipment. This will prevent passwords from being passed in plain-text, in case the attacker is using a sniffer on that subnet. If users must connect to the network remotely from the outside, they should use a Virtual Private Network (VPN) connection to create a secure tunnel to transmit data.

To protect your applications and web applications from buffer overflow, cross-scripting attacks, and SQL injections you must implement application layer security, by securing the applications through input validation, session management, authentication, authorization, exception management, parameter manipulation, as well as auditing and

logging. Failure to do so can result in exploits in your applications, and cause systems to be compromised.

The last and one of the most important defense mechanisms to handling attacks on your network is to effectively train users to be aware of social engineering attacks and other forms security measures. Whether it is in the form of weekly email memos or training courses, users must be trained to prevent unauthorized users from accessing restricted areas, obtain confidential information, or give out sensitive data. User should also create strong passwords consisting of at least 8 characters, as well as change those passwords every 90 days.

In conclusion I feel that these are some of the most common hacking tools and techniques used in the computing world today. I also feel that the defense tools and best practices listed in this paper, along with properly educating other users and employees in security awareness, should adequately help you defend your systems and network from intrusion and attack.

Works Cited

History of Hacking. Hackingalert.com. 19 April 2009

<<http://www.hackingalert.com/hacking-articles/history-of-hacking.php>>

Introduction to Packet Sniffing. Tony Bradley, CISSP-ISSAP, About.com. 19 April 2009.

<<http://netsecurity.about.com/cs/hackertools/a/aa121403.htm>>

Snort – the de facto standard for intrusion detection/prevention. 2009. Snort.org. 19 April 2009

Top 100 Network Security Tools. 2006. Insecure.org. 19 April 2009.

<<http://www.sectools.org>>

Understand the CROSS SITE SCRIPTING Vulnerability. 4 April 2007. Cross Site Scripting. 19 April 2009.

<<http://www.crosssitescripting.com/>>

SecuriTeam - SQL Injection Walkthrough. 26 May 2002. SK. 19 April 2009

<<http://www.securiteam.com/securityreviews/5DP0N1P76E.html>>

Analysis of Buffer Overflow Attacks. 2009. WindowSecurity.com. 19 April 2009

<http://www.windowsecurity.com/articles/Analysis_of_Buffer_Overflow_Attacks.html>

What is rootkit? – a definition from Whatis.com. 11 March 2009.

SearchMidmarketSecurity.com

<http://searchmidmarketsecurity.techtarget.com/sDefinition/0,,sid198_gci547279,00.html#>

* Rowan Tom. “Password protection: the next generation”. Network Security, Volume 2009, Issue 2, February 2009, Pages 4-7, ISSN 1353-4858, DOI: 10.1016/S1353-4858(09)70015-7.

<<http://www.sciencedirect.com/science/article/B6VJG-4VRYF90-5/2/3c3019fc675727ea0787710d5f4a7082>>

* Potter, Bruce. "Three tips for your network". *Network Security*, Volume 2009, Issue 2, February 2009, Pages 16-18, ISSN 1353-4858, DOI: 10.1016/S1353-4858(09)70019-4.

<<http://www.sciencedirect.com/science/article/B6VJG-4VRYF90-9/2/3ece78acf98edef97bc1f2cce7fda222>>

Whitman, Michael and Herbert Mattord. Principles of Information Security. 3rd Edition. Course Technology, Cengage Learning, 2007