Hacking Techniques in Wired Networks

Dr.Amer Salem,*Marwa Nagim Mansur Idrees[1]

1) Dr.,University of Information Technology and Communications, Baghdad ,Iraq.
2) Programmer., University of Information Technology and Communications, Baghdad ,Iraq.

What is Hacking?

In computer networking, hacking is any technical effort to manipulate the normal behavior of network connections and connected systems. A hacker is any person engaged in hacking. The term "hacking" historically referred to constructive, clever technical work that was not necessarily related to computer systems. Today, however, hacking and hackers are most commonly associated with malicious programming attacks on the Internet and other networks

INTRODUCTION

Nowadays, wired networks, especially the Internet, have already become a platform to support not only high-speed data communication, but also powerful distributed computing for a variety of personal and business processes every day. However, the principles for designing and developing a network mainly targeted at providing connection and communication capabilities, until a series of security “disasters” happened on the Internet recently as shown in Figure 1. As a result, without making security an inherent part of the network design and development process, existing networks are very vulnerable to cyber attacks because of various security vulnerabilities. Such vulnerabilities, when being exploited by the hacker, can motivate the development of a variety of hacking techniques. These hacking techniques directly lead to cyber attacks; and these cyber attacks have become a more and more serious threat to our society.

*Corresponding Author mar918wa5@yahoo.com

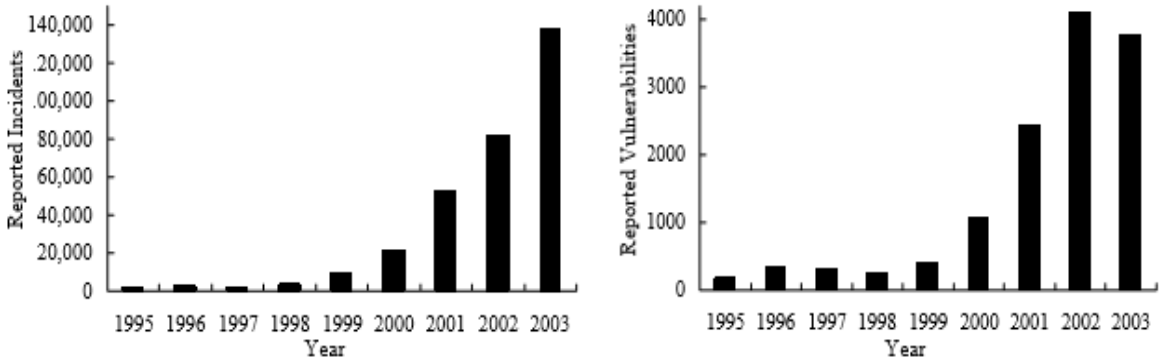

Figure 1. Reported Incidents and Vulnerabilities from 1995 to 2003 [11]

PRINCIPLES OF HACKING

In this article, attacks and hacking techniques are two different concepts that are, nevertheless, closely related to each other. An attack typically goes through several steps or phases. In each phase, some attack actions will be carried out by the hacker, and these attack actions will typically involve the use of one or more

hacking techniques. The hacking techniques involved in different attack phases could be different. Moreover, an attack or hacking (software) tool may cover several phases of an attack and involve multiple hacking techniques.

Seven Steps of Hacking

No matter how to hack or attack a network, the attacker always takes certain procedures to accomplish his objectives. In general, these procedures fall in one of the following seven steps reconnaissance, probe, toehold, advancement, stealth, listening post, and takeover, where each step is enabled or helped by its previous steps and prepares for its following steps. These seven steps can serve as a procedural classification of hacking techniques because the hacking techniques used in each step are for the same purpose and share many common characteristics.

Common Network Hacking Techniques

Hacking on computer networks is often done through scripts or other *network programming*. These programs generally manipulate data passing through a network connection in ways designed to obtain more information about how the target system works. Many such pre-packaged scripts are posted on the Internet for anyone, typically entry-level hackers, to use. More advanced hackers may study and modify these scripts to develop new methods. A few highly skilled hackers work for commercial firms with the job to protect that company's software and data from outside hacking Cracking techniques on networks include creating worms, initiating denial of service (DoS) attacks, or in establishing unauthorized *remote access* connections to a device.

Effective hacking requires a combination of technical skills and personality traits:

- ability to work with numbers and background in mathematics - hacking often requires sorting through large amounts of data, code and computer algorithms
- memory recall and logical reasoning - hacking involves assembling small facts and details (sometimes from many sources) into a plan of attack based on the logic of how computer systems work).
- patience - hacks tend to get very complex and requite large amounts of time to plan and execute .

You're using a wireless access point that has encryption so you're safe, right? Wrong! Hackers want you to believe that you are protected, so you will remain vulnerable to their attacks.

Here are 4 things that wireless hackers hope you won't find out, otherwise they might not be able to break into your wireless network and/or computer:

1. WEP encryption is useless for protecting your wireless network. WEP is easily cracked within minutes and only provides users with a false sense of security.

Even a mediocre hacker can defeat Wired Equivalent Privacy (WEP)-based security in a matter of minutes, making it essentially useless as a protection mechanism. Many people set their wireless routers up years ago and have never bothered to change their wireless encryption from WEP to the newer and stronger WPA2 security. Updating your router to WPA2 is a fairly simple process. Visit your wireless router manufacturer's website for instructions.

2. Using your wireless router's MAC filter to prevent unauthorized devices from joining your network is ineffective and easily defeated.

Every piece of IP-based hardware, whether it's a computer, game system, printer, etc, has a unique hard-coded MAC address in its network interface. Many routers will allow you to permit or deny network access based on a device's MAC address. The wireless router inspects the MAC address of the network device requesting access and compares it your list of permitted or denied MACs.

This sounds like a great security mechanism but the problem is that hackers can "spoof" or forge a fake MAC address that matches an approved one. All they need to do is use a wireless packet capture program to sniff (eavesdrop) on the wireless traffic and see which MAC addresses are traversing the network.
They can then set their MAC address to match one of that is allowed and join the network.
3. Disabling your wireless router's remote administration feature can be a very effective measure to prevent a hacker from taking over your wireless network.
Many wireless routers have a setting that allows you to administer the router via a wireless connection. This means that you can access all of the routers security

settings and other features without having to be on a computer that is plugged into the router using an Ethernet cable. While this is convenient for being able to administer the router remotely, it also provides another point of entry for the hacker to get to your security settings and change them to something a little more hacker friendly. Many people never change the factory default admin passwords to their wireless router which makes things even easier for the hacker. I recommend turning the "allow admin via wireless" feature off so only someone with a physical connection to the network can attempt to administer the wireless router settings.

4. If you use public hotspots you are an easy target for man-in-the-middle and session hijacking attacks.

Hackers can use tools like Firesheep and AirJack to perform "man-in-the-middle" attacks where they insert themselves into the wireless conversation between sender and receiver.

Once they have successfully inserted themselves into the line of communications, they can harvest your account passwords, read your e-mail, view your IMs, etc. They can even use tools such as SSL Strip to obtain passwords for secure websites that you visit. I recommend using a commercial VPN service provider to protect all of your traffic when you are using wi-fi networks. Costs range from $7 and up per month. A secure VPN provides an additional layer of security that is extremely difficult to defeat. Unless the hacker is extremely determined they will most likely move on and try an easier target.

Classifications of Hacking Toolkits

Attacks against the Internet Infrastructure
Attacks against DNS Attacks against TCP/IP
Attacks against BGP

Attacks against End Systems of the Internet

Morris Worm
Melissa
Sadmind

Code Red I and Code Red II
Nimda
SQL Slammer
W32/Blaster

Attacks against Enterprise Network Systems

Attacks against Private Networks
Attacks against Private Networks with Web Service
Attacks against Firewalls and Virtual Private Network

Top 10 Hacker Tools and Techniques

By understanding how hackers gain access to systems, organizations can stay a step ahead and ensure information availability, integrity, and confidentiality. Listed below is Altius IT's list of the Top 10 Hacker Tools and Techniques:

Reconnaissance. Hackers use tools to get basic information on your systems. Tools like Netcraft and PCHels to report on your domain, IP number, and operating system.

Network Exploration. The more information the hacker knows about your system the more wanys he can find vulnerabilities. Tools such as NMap identify your host systems and services.

Probe Tools. Some tools were initially designed to be used by system administrators to enhance their security. Now, these same tools are used by hackers to know where to start an attack. Tools like LANguard Network Scanner identify system vulnerabilities.

Scanners. Internally, sniffer tools analyze network performance and applications. Hacker reconnaissance tools such as AET Network Scanner 10, FPort 1.33, and Super Scan 3 scan your devices to determine ports that are open and can be exploited.

Password Cracker. Password tools are used by security administrators to find weak passwords. These tools may also be used by hackers. Password crackers include LC5, John The Ripper, iOpus Password Recovery XP, and LastBit.

Remote Administration Tools. Tools such as AntiLamer and NetSlayer are used by hackers to take partial or complete control of the victim's computer.

Backdoor. Backdoor tools and Trojan Horses exploit vulnerabilities and open your systems to a hacker. KrAIMer and Troj/Zinx-A can be used by hackers to gain access to your systems.

Denial of Service (DoS). Denial of service attacks overload a system or device so it can't respond or provide normal service. Hackers use tools such as Coldlife and Flooder overload a system.

Recover deleted files. Once hackers are inside your perimeter, they can use tools like Deleted File Analysis Utility to scan your hard drive partitions for deleted files that may still be recoverable.

Web Site Tools. Hackers use tools such as Access Diver and IntelliTamper to index your web site pages and directories. These tools can download your site to the hacker's local hard drive. Once on his system, the hacker analyzes the web site to identify and exploit security vulnerabilities.

Network security audits help organizations identify, manage, and reduce their risks from hackers and their emerging tools. Formal and documented policies ensure a top down approach to managing network security risks.

CONCLUSION

In this article, we discussed a variety of hacking techniques. From the functionalities, objectives, and principles of different hacking techniques, we can summarize that vulnerabilities of a network or system always come from two major factors, technical factor and human factor. The technical factor refers to those imperfect designs of networks and systems, such as unencrypted data, unprotected communications, buffer overflow problems and software bugs. These deficiencies provide holes through which intruders can penetrate into the system. The human factor is another important perspective. For example, users' incautious talk can become the source to disclose critical information about

network and system. Inappropriate use of the system may let attackers sneak in. Insiders may be the most serious threats to the system.

References

1. Qijun Gu, Pennsylvania, Peng Liu, Pennsylvania, Chao-Hsien Chu, Pennsylvania State University, University Park https://s2.ist.psu.edu/paper/hack-wired-network-may-04.pdf
2. AndyO'Donnell,October05,2016 https://www.lifewire.com/secrets-wireless-hackers-dont-want-you-to-know-2487647

[٣] Bradley Mitchell ,February26,2016 https://www.lifewire.com/definition-of-hacking-817991

4 http://www.altiusit.com/files/blog/Top10HackerTools.htm