Journal of Basic and Applied Engineering Research
p-ISSN: 2350-0077; e-ISSN: 2350-0255; Volume 2, Issue 22; October-December, 2015, pp. 1884-1886
© Krishi Sanskriti Publications
http://www.krishisanskriti.org/Publication.html

# Hacker Attack Networks: Techniques & Tactics

**Harpreet Kaur[1] and Shivam Maini[2]**

*[1,2]Dept Of Computer Science S.R. Govt. College (W), ASR*
*E-mail: [1]harpreetsethi.27@gmail.com, [2]sh_asr@yahoo.co.in[2*

**Abstract—***Hacking strategies to gain malicious access to systems and attack your network, making it difficult for organizations to develop and implement the proper policies and procedures necessary to prevent hacker attacks. Hacker attack techniques and tactics will provide insight inside the mind of a hacker and help you to understand a malicious attacker's motives. You will receive advice on how hackers target specific information and what policies and procedures every organization should have in place to protect sensitive data. You will receive information on an array of specific hacker techniques and tactics, such as system fingerprinting and probing, which allow hackers to obtain access to your network systems or files. You will learn how to thwart hacker tactics and techniques with a variety of procedures and defenses, including intrusion prevention and detection technology.*

**Keywords***: Malicious, Tactics, Fingerprinting, Array, Sensitive Data, Intrusion Detection, Intrusion Prevention.*

## 1. INTRODUCTION

**This research paper valuable efforts on the** importance of securing your network endpoints and will teach you how to mitigate the threat of hackers connecting to your computers via open network ports.We use the different stratigies to prevent your system and how to know if you system has been compromised by a malicious hacking attempt, how to keep your wireless network secure and best practices for end-user education on current threats and preventative measures.Serious hackers don't shoot in the dark when attempting to penetrate a system. Instead, they will use hacker techniques such as operating system fingerprinting and probing to systematically identify what systems and services your company is running to determine your weakest link.

## 2. TECHNIQUES TO DEFENDING AGAINST ATTACKS

A typical hacker attack is not a simple, one-step procedure. It is rare that a hacker can get online or dial up on a remote computer and use only one method to gain full access. It is more likely that the attacker will need several techniques used in combination to bypass the many layers of protection standing between them and root administrative access

### 2.1 Firewalls

The first step in defending against hacker techniques designed to access your systems is to block unnecessary, incoming firewall ports. The ports that remain open should be protected by patching the services that use those ports, such as Web services, email and FTP. Your software vendors should be able to provide their most up-to-date patches. CERT lists vulnerability information about services you may be running. Additionally, Cassandra is an excellent online vulnerability database, freely available to assist you in identifying which vulnerable services you are running, and includes many applications not listed elsewhere.

### 2.2 IPS/IDS

To determine if someone is using such tools to probe and fingerprint your operating systems, you'll need to implement at least one type of logging tool that will record port scans, fingerprinting, failed login attempts, etc. Ideally, any open ports should be monitored with an intrusion prevention system (IPS), which will detect and prevent most attacks before they reach your systems. A common free and open source intrusion detection system (IDS), which only detects attacks and does not prevent them, and IPS is Snort. A quick Google search will yield plenty of free support and add-ons for Snort.

### 2.3Wirelessa Acess Points

WAPs present a special challenge because an intruder can access your network through one without ever having to pass through a firewall or a remote access server. Fortunately, there are several things you can do to guard against wireless intrusions.

Make sure to enable WEP encryption. There are several flavors of WEP available. Just about every wireless access point made in the last year supports 128-bit WEP encryption. Some of the newer devices support up to 152-bit WEP encryption. Therefore, use the highest level of WEP encryption you can. Remember that you must adhere to the lowest common denominator. For example, it does you no good to implement 152-bit encryption if your wireless client's NIC cards support only 128-bit encryption.

### 2.4 DHCP

To securing your perimeter is to make sure that you aren't giving anything away. Avoiding the use of wireless DHCP services is one example of this, since you want to avoid giving a hacker an IP address, DHCP server number, and so on. However, the idea of not giving anything away goes way beyond mere IP configuration information

## 3. HACKERS ATTACKS TACTICS

### 3.1 Social Engineceering

Social engineering can be a fruitful tactic for hackers, and it takes less time than trying to identify or bypass a firewall or an IPS. Unfortunately, or fortunately, depending on whom you ask, the security administrator can't screen everyone's calls or ask for ID from every person who steps foot into your company. It's up to the rest of your staff, those non-configurable human beings, to filter out malicious requests that come in through the doorways and over the phone lines. Are they up to the task? The best way to prepare them is to educate them on the social engineering hacker attack tactics they may encounter, both on and off the job.

### 3.2 Disable Unused Ports

Although you’ve probably heard this a million times, the first thing you should do is to disable all TCP and UDP ports that aren’t absolutely necessary through your firewall —especially ports 135, 137, 139, and 445. An ideal arrangement would be to enable only TCP ports 80 and 443, but your own individual business needs may require you to open more ports. For example, it’s probably necessary for you to open ports 110 and 25, the ports associated with POP3 and SMTP, to have e-mail

### 3.3 Remote Access Servers

Once you’ve secured your firewall(s), turn your attention to your remote access servers. There are many techniques for securing remote access servers. Some of the most common techniques include requiring callbacks to preset numbers, recording caller ID information to log files, denying dial-up access to everyone except those who have a legitimate business need for it, and limiting the times and days when employees can dial in.

### 3.4 Rogue Modems

In most organizations, the firewalls and remote access servers are the main perimeter access points. However, there are other perimeter holes that you might not have thought about. Any PC with a modem could potentially act as a remote access server. Ideally, you should know from your hardware inventory which PCs on your network have modems and how those modems are configured. At every network administration job I’ve ever had, I’ve discovered at least one unauthorized modem. Unauthorized modems represent a serious security risk. Basically, if you don’t know that a modem exists, you can’t control how it’s used.

There are a couple of ways of spotting rogue modems. One technique involves maintaining an automated hardware inventory. The inventory software can send you an e-mail message when hardware changes occur.

Another technique that works well is to maintain a list of every telephone number that the company owns. You can then configure a PC to call every single number (preferably late at night) to search for rogue modems. Bear in mind that I’ve also known of hackers using this technique to call every number in a company to look for modems.

### 3.5 Secure Remote Acess Points

Hackers love poorly configured remote access points, and why shouldn't they? Many times they represent an open door into a network without having to fuss with firewalls and intrusion detection/prevention systems (IDS/IPS) at the Internet border. Considering the threat that these misconfigured devices pose, all organizations should secure remote access points and configure remote connections to prevent a hack. The fact is that most networks have remote access points, and most of those access points don't employ adequate security. Remote access points most often come in the form of dialup modem banks and VPN concentrators, and it doesn't take much to discover the phone number or IP address.

Most remote access points require only a static user ID and password to log on to the network. If your remote access point doesn't require strong authentication, you should probably count on the fact that somewhere out there, maybe an employee or vendor, has setup a remote connection to your network with a saved user ID and password. This means your network is available to anyone who opens that connection, including your employee's neighbor whose computer was used to check email a month ago, and that vendor's employee who quit last week and took all his clients' remote access passwords with him.

#### 3.5.1 How To Secure Remote Access And Configure Remote connections

To remedy this problem, it is best to implement some type of strong authentication, requiring a user ID and a single-use password or biometric. There are a number of vendors that sell remote access keychain tokens, which generate a new single-use passcode every few seconds. Additionally, your suppliers and vendors could be required to call your operations department to obtain a passcode for remote access, thus adding another layer of security when dealing with outsiders. By implementing a strong authentication system, saved passwords for remote connections will no longer represent an information security risk.

Additionally, most remote access points don't inspect the remote computer for viruses or hacking software, and they usually don't watch the network traffic coming from such computers. If a user with a virus-infected PC or a hacker were to remotely log on to your network with such software, the network could be on the receiving end of a server compromise or a virus outbreak. To help prevent a remote connection hack, it is best to have an IDS or IPS sitting inline between your remote access point and your internal network. Such a system should be capable of catching network-based attacks from hackers or hybrid viruses. Some systems will even prevent users from connecting to your network if their antivirus software is not up to date. It is also best to limit the number of ports allowed access into your internal network.

By giving some attention to the authentication process and the traffic coming from remote users, you will greatly reduce the risk of your remote access points being a source of unwelcome company.

### 3.6 Securing Your Web Server

Your company's website is one of the first places a malicious hacker will look for misconfigurations, poorly written code and vulnerable services. If you house your own Internet-facing Web server, and it's connected to your internal network, it's worth your time to ensure the process of securing your Web sever is a corporate priority, and investigate the security controls in place for Web server protection. This is even more critical if your company has an online store or account management system.

When operating system patches are released and tested in your environment, Web servers should be the first servers patched to prevent a Web server hack. Exploit code is becoming more readily available to anyone within days of a vulnerability discovery. A few days after it's been in the hands of hackers, a scripted attack is likely to take place that could successfully attack your unpatched Web server. This gives little time to test and install patches for such vulnerabilities, so it's important to devise a deployment plan prior to patch release.

Looking at Web code itself, there are several ways hackers can manipulate the URL of a website to perform SQL injection, directory traversals, buffer overflows, etc. There are two common methods to defend against these types of vulnerabilities. One is to have your Web code reviewed by a person or a tool in an effort to identify and correct vulnerabilities. Or you can install an application firewall that examines user input to verify that it is not malicious or malformed before allowing it to pass to the backend application. Blue Coat Systems Inc. and Sanctum Inc. are two vendors that offer such products, which may be worth looking into, especially if you don't think you can retrain your programmers to write secure code.

### 3.7 Media Access Control

Most radio access points also allow you to restrict network access by the Media Access Control (MAC) address, a hardware address that uniquely identifies each node of a network. But be aware that this can be defeated using a passive wireless sniffer that can capture the MAC address of a device that is allowed on the network. Once acquired, the hacker can spoof his MAC address and is no longer restricted to that level. Restricting MAC addresses does add one more layer that must be compromised, so it's worth considering

## 4. CONCLUSIONS

In every hacker's tool bag are a variety of free system probing and fingerprinting tools, the purpose of which is to identify specifics about your hardware and software configurations. Some of these tools will undoubtedly check for open ports on routers and firewalls and identify what system services are available for exploitation. To get an idea of what a hacker would see, download and run some of these tools against your own network. Be sure  when these tools are being run, in case there are performance issues when certain scans are launched, and always test them against a few non-critical machines first.

## REFRENCES

[1] J. Danish and A. N. Muhammad, “Is Ethical Hacking Ethical? “ , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011..

[2] Sarah Granger, Social Engineering Fundamentals, Part I: Hacker Tactics, SECURITYFOCUS, at http://www.securityfocus.com/infocus/1527 (last updated Dec. 18, 2001)

[3] SANS INSTITUTE, July 26, 2000, at http://www.giac.org/practical/GSEC/John_Palumbo_GSEC.pdf).

[4] Snort is a common open source tool that can be used as a sniffer, packet logger, and network intrusion detection system allowing network traffic to be analyzed. http://www.snort.org

[5] Pythonvariantof“WftpdstatCommandRemoteVulnerabilityExploit”byOYWin, submitted by Security Team Oseen (o5een@hotmail.com) on March 3, 2004. Retrieved from http://archives.neohapsis.com/archives/bugtraq/2004-03/0020

[6] edia.techtarget.com/searchNetworking- Introduction to ethical hacking-Tech Target. [7] H.M David, “Three Different Shades of Ethical Hacking: Black, White and Gray,” in GSEC Practical Assignment, Version 1.4b, Option 1, Feb 23, 2004.

[7] D. Manthan “Hacking for beginners”, 254 pages, 2010.

[8] Ajinkya A., Farsole Amruta G., Kashikar Apurva Zunzunwala"Ethical Hacking", in 2010 International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 10 David Melnichuk," The Hacker’s Underground Handbook ", at http://www.learn-how-to-hack.net