Chapter 9: Server and Network Scanning

Network and server scanning is nothing but using of computer networks for gathering information related to the system of computers. This form of scanning is mainly done for assessment of security, maintenance of system and also for attacking the systems by hackers. The purposes of scanning are:

- Recognizing all the available TCP and UDP networks which are running of the hosts which are targeted
- Recognizing systems of filtering in between the host which is targeted and between the user
- Determining the OS which is in use after assessing the responses of the IP address
- Evaluating the TCP sequence number of the target host for the purpose of prediction sequence attack and for spoofing of TCP

Network scanning

When it comes to network scanning, it includes scanning of network port along with scanning for vulnerability. The scanning of network port is the method by which the data packets are sent through the network to the system of a computer with specified numbers of service ports. This is used for identifying all the network services which are available on a specific system. This method is very useful for troubleshooting of system related issues and also for gearing up the security of a system.

Vulnerability scanning is used for detecting the vulnerabilities which are present within a system of computer available right on the network. It helps in the detection of particular weak spots in the OS or software which might be used against the system for crashing down the system or for any other form of undesired attack. Both scanning of network port and scanning for vulnerability are techniques of information gathering. But, when such actions are performed by any other third party, it might turn out to be the introduction of an undesired attack.

The processes of network scanning such as ping sweeps and port scans return valuable details about the map of IP addresses which hosts live along with the services it provides. Another form of network scanning is also used which is called inverse mapping. This process gathers all the details about the IP addresses that are not capable of mapping to the live hosts and this, in turn, helps the attackers in focusing on the various advantageous addresses.

Network scanning is one of those methods which are used by the attackers for gathering relevant information about a network or the target system. At the stage of footprint, the hacker creates a designated profile of the target system or network. This includes all forms of relevant information about an organization such as the DNS of the organization, the range of the IP addresses and also the servers of email. At the stage of scanning, the attacker tries to find out all the details about a particular IP address which is accessible online, the architecture of the system, the operating systems which are used along with the services which are running on the computers of the organization. At the stage of enumeration, the attacker tries to collect all relevant data that also includes the tables of routing, network group and user names, SNMP or simple network management protocol data and many others.

Why are server and network scanning required?

Server and network scanning are very much required in this world of today where all the systems are vulnerable to the attacks of cyber criminals. With the shifting of storage from the physical database to the online version, the rate of cyber attack is also increasing day by day. The organizations are required to perform server and network scanning for preventing the following scenarios:

- Loss in the trust of the customers
- Complete disturbance of the online form of collection or generation of revenue
- Website crashing, loss of time and expenditures for the purpose of damage recovery
- The cost of securing the application on the web from further cyber attacks
- Loss of confidential data that might result in the downfall of an organization

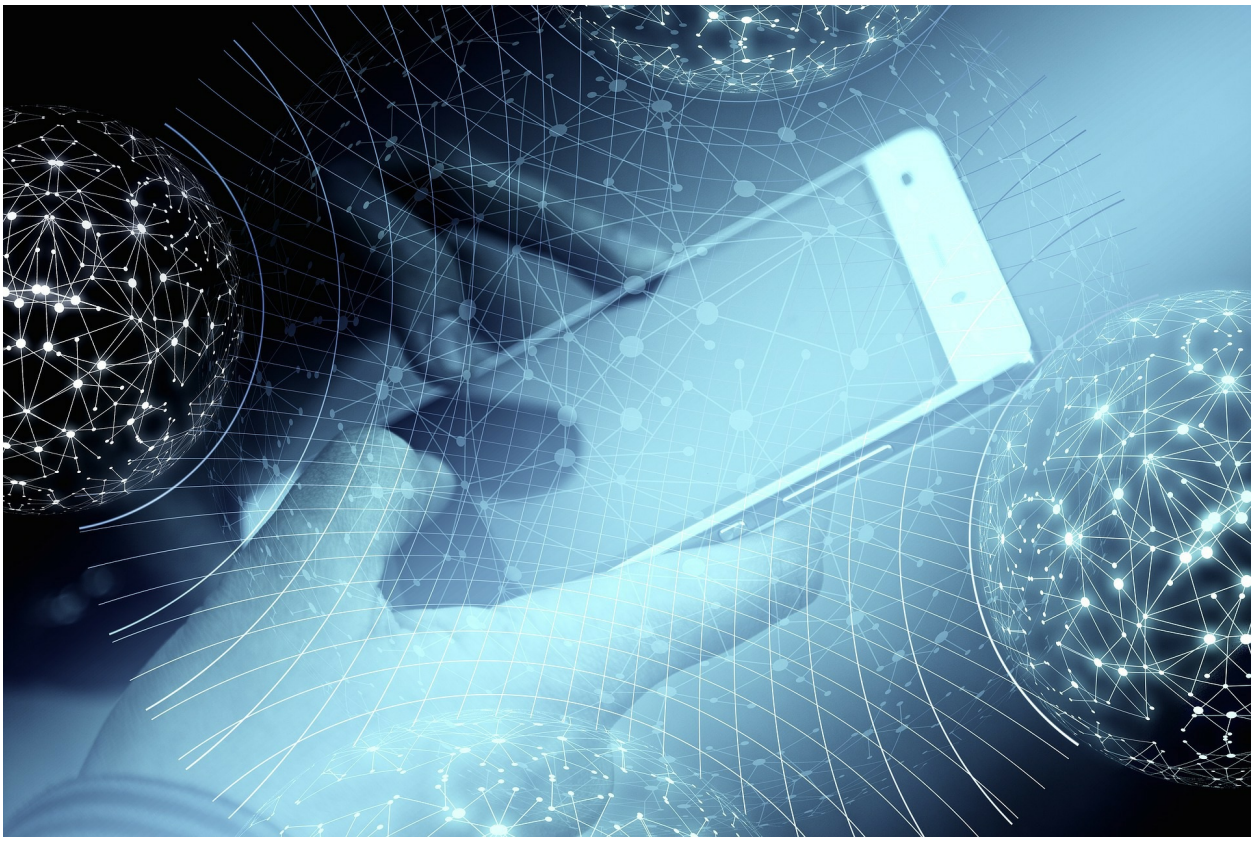
Natures of server scanning

Server scanning can be performed in a variety of ways. Let’s have a look at them.

- **Active scanning:** This is the process which is used for identifying the services of a network simply by transmitting probe packets directly towards the hosts of the network and the devices and then monitoring the same for the responses. This form of scanning is used by the attackers who try to find out the vulnerabilities of a network. This process allows the operator of the network to discover the various open services which are available within the network in a direct attempt to check all those for some of the known vulnerabilities. The probe packets which are sent to the network host can either be in generic form which will be targeting only a particular protocol in place of an application or can also be targeted which will be focused on

some accurate application by the host.

- **Passive scanning:** This method is used for identifying the services of a network by simply observing the generated traffic by the clients and the servers as it keeps on passing a point of observation. For the purpose of establishing passive monitoring, specialized form of hardware or software can also be inserted at the point of monitoring and can also be installed at the point. Many of the routers can replicate the ports in which the copies of the probe packets will be sent out of some other interface to the host of monitoring. Various hardware taps like the optical splitters will be adding no extra hardship on the router. However, it requires some detailed interruption for installation. The detection of both UDP and TCP with the use of passive scanning is pretty simple and straightforward. For the detection of TCP, host of monitoring requires only to capture the TCP setup message of connection. After the completion of three-way handshake, it will clearly indicate that the service is accessible. The services of UDP can also be identified with traffic observation. But, because UDP is a type of protocol which is connectionless, the overall concept behind client and server is not clear without the information of application protocol.



Chapter 10: Inspection of Wireless Networks

In this era of unique technological innovations, it is of utter importance to opt for wireless networks or WLAN testing and inspection. It needs to be done for ensuring that the involved system meets all the requirements of performance along with security. There are lots of factors that come into play while inspecting WLAN. Therefore, all that you need is proper planning along with documentation of the test.

Considerations along with planning for WLAN inspection
While you plan for WLAN inspection, it is a crucial part to consider the available varieties of the areas of testing. It includes:

- **Testing of signal coverage:** It makes sure that the levels of signal are enough for supporting the performance levels that the users require throughout the coverage areas of WLAN.
- **Testing of performance:** This certifies the capabilities of the

WLAN for meeting the needs of the users while using some particular applications over the network.

- **In-motion testing:** This helps in determining that whether the network of WLAN allows all the users for successfully using the applications at the time of moving across various areas of coverage.
- **Testing of security vulnerability:** This helps in certifying the network security by authenticating the application of the mechanism of security which is required along with the proper protection degrees from the access which are unauthorized.
- **Testing of verification or acceptance:** It offers a type of insurance to the organizations which hires various contractors for the implementation of WLAN after ensuring that the overall system has the required coverage of signal, capacity, performance along with security. It is a process which is kind of formalized that also takes into account the various practices of installation, documentation of system along with the various procedures of maintenance.
- **Simulation testing:** This helps in providing a proper visualization along with the representation of the behavior related to WLAN right before it is being deployed. It offers deep insights into the network design's effectiveness in relation to the activity of traffic, software and hardware. It also takes into account any form of potential issue in the performance.
- **Testing of prototype:** It has been designed for specifically assessing the parts of the product or the system of WLAN which are not familiar in nature in the environment of a lab right before the deployment of the same.
- **Pilot testing:** This involves the installation of WLAN in its real version with some specific facilities just before implementation of the system in the whole organization. This testing can provide with various outcomes which can offer detailed insights into the potential issues of performance and realistic usage.

Testing of signal coverage

This method uses up a signal coverage tester which is also known as signal meter for properly measuring the signals of WLAN across the overall area of coverage. The main purpose of this type of testing is to make sure that the level of signal is up to the mark for supporting high level performance which is required by the user while using various web applications on WLAN.

- **Wireless survey of site coverage:** The testing of coverage of signal often involves survey of wireless site. It is generally performed right before the installation of WLAN. It is carried on by proper positioning of access test point across different locations. The locations are situated throughout the area of WLAN coverage. It uses the signal meter for the purpose of measuring the values of signals within the area of the access point of testing. The result of such survey helps in deciding the location of the final installation of the points of access.

Testing of performance

This form of WLAN starts with the testing of association. This test ensures that the device types of the clients associate properly with one single or more than one points of access which act as parts of the system which is installed. This is regarded as a beginner's test for ensuring whether the devices of the clients are capable of establishing wireless connections. You need to confirm enough association prior to moving forward with the other tests. This testing is of utter importance as sometimes the devices of the clients turn out to be non-compatible with the WLAN points of access.

Test of network connection

For proper communication between the devices of the clients and the web application, the systems of wireless network use either UDP or TCP. In both the cases, it is ensured that the device of the client has connected successfully with the WLAN and also possesses an IP address which is valid in nature. This is typically done by observing the table of association which can be found easily in the points of access. It is a great mode of testing that will ensure that the device of the client is capable of reacting to a generated ping from the subnet which is of similar nature in which the application dwells.

The result of the ping needs to indicate that the device of the client properly reacts to the generated ping sufficient delays along with no timing out. In case the test of network connection shows a problem, make sure that the device of the client comes with a valid IP address and the firmware of the client's device is upgraded along with the points of access.

Test of application connection

It is to be ensured that each type of device of the client connects in a proper way with the application. With the help of wireless implementation of IP phone, it can be made sure that the phone registers in the proper way with the software of call manager and also receives the phone number which is applicable. In case the phone fails proper registration, try to check again that the device is actually having a convenient IP address, primary gateway, subnet mask and also settings of DNS. You need to keep in mind that the phone might connect to any point of access without being able to attain a proper IP address. The device IP address needs to correspond along with the plan of address for the particular location where the device is establishing a connection with the network.

Chapter 11: Testing of Wireless Network Security

Wireless communication is an invisible form of communication which is invisible in nature and is also omnipresent. It allows seamless flow of data in and out from homes and from business organizations through various devices and infrastructure of wireless connection. Most of the modern form of business organizations has set up some form of wireless networking, mainly Wi-Fi within their organization. However, proper implementation of such services is not able to see the type of attention that it actually requires. Various segments of networking such as VLAN routing, segmentation of network and SSID controls are required to be defined in clear form and also set up. It will allow the users to easily connect with the network and use the related services along with keeping away the intruders and the third parties, much away from the network.

Regardless of the fact that a lot of or very less consideration has been entitled for the setting up of the wireless network, the organizations are required to

hunt out any form of weakness within the wall of security of the network for the purpose of avoiding any form of unethical and unauthorized access to the resources of the network and prevention of data leakage.

Wireless network penetration testing

Penetration testing or pentesting of wireless network is nothing but scanning a network for any form of discrepancy within the security wall. In case when an organization fails to adapt proper pentesting for the wireless networks, it results in data theft as well as unauthorized access to all the resources of the network. Proper security measures can help in preventing all forms of data leakage along with ensuring the data security of a business.

Steps to be taken at the time of wireless network pentest

The steps that need to be taken will depend completely on the standards which are being followed for the penetration testing along with the methods agreed to by the company and the areas of testing. In general terms, the process of pentesting begins with the gathering of information and intelligence. It will be creating a map of heating for the area which is tested. It will track the footprint along with the size of the signal which is being broadcasted by the wireless network. Various other forms of information such as total number of SSIDs which are being broadcasted, configuration of the network, installed hardware and many others are also required to be collected. You can also start by creating a proper site map of the network.

The second step is to find out the form of threats which a company can be vulnerable to. It will be based on the hardware which is installed on the site, the network equipment visibility right behind the infrastructure of Wi-Fi and the distance to which the signal of Wi-Fi can be detected outside the property of business. Questions such as are there any open file shares which can is accessible over the network of Wi-Fi and many others are the basic questions that a pentester needs to begin with.

The analysis of vulnerability test is carried out using specialized tools which

are used by the pentester that will easily inform the tester about the form of exploitation to which the organization is susceptible to. In case, any form of susceptibility is identified, it needs to be exploited right away and then use the same to a point that will breach the security. The pentester can easily show the client about the susceptibility extent with this step. With proper pentesting, it can also be identified that what type of tool was used for attacking the wireless network.

Once the threats have proved to work, the pentester continues scanning the overall network and then establish the extent to which the threat will be able to exploit the permissions of the users along with data breach. After all, these have been done, a report is presented to the client with the details of the threats and the security holes within the system. The client is supposed to modify the security measures according to the report. The pentester tests the network again with the same form of exploits to check whether the modified security forms are able to defend the attacks or not.

In general, the wireless penetration testing is carried on in two phases: active and passive. In the passive phase, all sort of information is collected and in the active phase, the threats are tested for the network. This whole thing can also be done by an attacker who is trying to target an organization for data breaching.

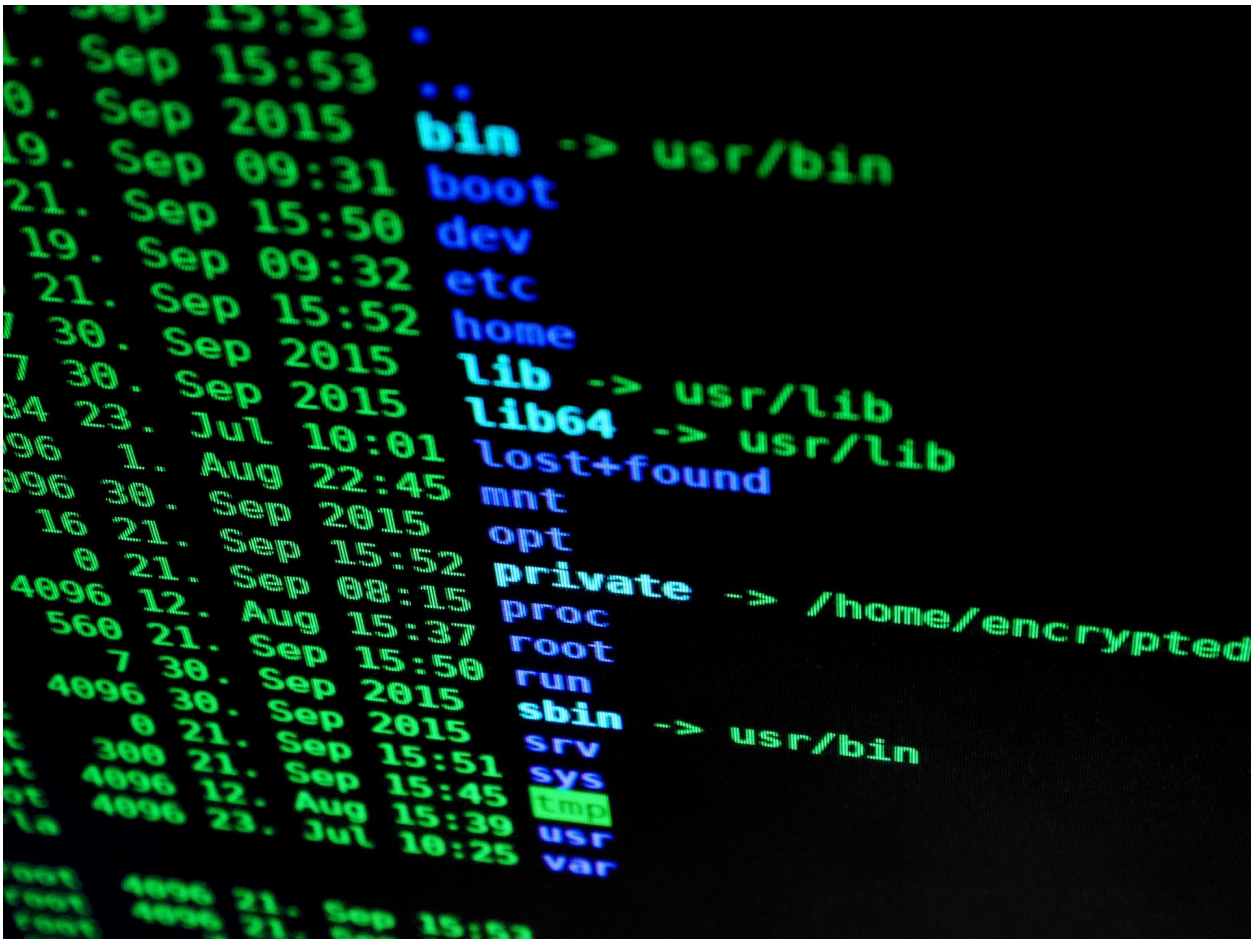
Tools used for wireless network scanning

There are various tools which are being used today for the scanning of wireless network against all forms of vulnerabilities. Some of the most commonly used tools are:

- **Kali Linux:** Kali Linux can be used for testing the breach within a network. It is a hacking tool that also provides various security tools for the systems such as penetration testing. It is regarded as a very helpful tool.
- **Wireless card:** If you want to use Kali Linux as your Virtual Machine, wireless card of the PC can be directly used within the VM. It helps in detecting any form of threat within a network and also returns significant results of security testing.

Benefits of penetration testing

The biggest benefit of pentesting is the benefit of knowledge. In case your organization is susceptible to any form of threat via the wireless network, it is always better to detect the same as early as possible rather than repenting later. With the help of pentesting, the assessing of the current Wi-Fi state can be easily determined and the required changes in the wireless network configuration can be applied. In case the report of penetration testing is detailed enough, it can help the organizations to determine what strategies of wireless security they are required to adopt for improvement of the wireless network. The whole concept of pentesting ultimately helps in building up and improving various security measures that can help in preventing data leakage. It is also beneficial for finding out whether the present security measures are enough for the wireless networks or not.



Chapter 12: Management of Linux Kernel and Loadable Kernel Modules

All the operating systems that can be found today are composed of the two most important components. The first component and the most important one out of all is the kernel. The kernel functions as a prime constituent of any form of OS. It is situated right at the center of your OS. It comes with the power of controlling each and every functioning of the operating system that also includes the function of CPU control, memory management along with control of the content that a user can see on the screen. The second most important element within an operating system is the user land and it constitutes of everything else.

The kernel of an operating system has been designed in a way to perform as a privileged or protected area which is possible to access by any other form of account which is privileged as well or by root. This whole protection thing is

only for the good. This is because, with unlimited access to the kernel can result in providing all forms of unauthorized access to the functioning of an operating system. So, in the real world, majority of the operating systems which are available in the market provide all the users along with the access to the services only at the access land. In the access land, the users can easily have access to everything they want without the need of taking the operating system under control.

Kernel access by the users provides them with the ability of changing the looks of the operating system, the method of working of the operating system and also the way in which the operating system feels to use. The users who get access to the kernel can also crash a whole operating system and thus making the whole system dead or unworkable. In spite of such risks involved with the kernel of an operating system, the administrators of the systems sometimes are required to access the operating system kernel for the purpose of security as well as operational reasons.

After knowing the actual power of kernel, you can easily figure out that in case a hacker gets access to the kernel of an operating system, he can actually control the entire system and that might turn out to be dangerous as well. Also, for some advanced form of attack such as MITM or main in the middle attack, the attacker might also need to alter the functioning of the kernel also.

What is kernel module?

Just like human beings perform all their functions with the help of the CNS or central nervous system, the kernel can be regarded as the central nervous system of the operating system. It controls every functioning of the operating system and also includes the management of interaction in between the components of hardware and the starting of required services. Kernel functions in between the applications of the users that you can actually see and between the components of hardware that performs everything such as hard disk and memory along with CPU.

Linux is an imposing type of kernel that allows the adding up of the kernel modules. In general, the modules can be removed or added right from the kernel according to the user need. Occasionally, the kernel of an operating system might also require some updates which require the installation of

some new form of device drivers such as Bluetooth devices, video cards and USB devices and drivers of the file system. While updating the kernel, it might also require installation of some system extensions. For being functional in its full form, the drivers are required to be embedded within the kernel.

There are some operating systems, in which, for the purpose of adding one driver for the update, the user needs to completely rebuild, assemble and reboot the whole kernel of the operating system. However, in Linux, it comes with the capability of adding up kernel modules to the system kernel without performing this whole process. Such modules are known as LKMs or loadable kernel modules. LKMs are powered with the access of kernel to the lowest levels and that too by necessity. This makes the LKMs a very easy target for all the attackers. There is a very particular form of malware which is known as rootkit. This malware inserts itself into the operating system's kernel and mostly through the LKMs. In case a malware like rootkit ingrains itself into the kernel, the attacker will be able to have complete control over the functioning of the OS.

In case an attacker gets access to the admin of Linux for the purpose of loading up new modules into the operating system kernel, the attacker will not only gain access to the controlling of the target system but will also control each and everything that the system which has been targeted reports in relation to the ports, space of hard drive, processes, services etc., in short everything that a kernel handles. This is mainly because the attackers will be functioning at the level of kernel of the OS. SO, it can be said that when an attacker is able to induce an admin of the Linux into the installation of drivers such as video driver that comes with rootkit ingrained in it, the attacker will be able to take the complete control of the kernel along with the OS.

Management of kernel modules

Linux comes with two varied ways in which kernel modules can be managed. The first one is by using a command group which is built in the suite of insmod which stands for insert module. It has been made up for dealing with module management. And then comes the modprobe command which is the second method. This command is used for management of the LKMs. For adding a kernel module using modprobe, you need to use the command with -

a switch. For removing a kernel module, you need to use-r along with the command. The command of modprobe comes with an added benefit when compared to insmod. The command of modprobe can understand all the options and procedures of removal or addition just before making any change in the kernel.

Chapter 13: Security and Hacking of the Web

Web Hacking

With the pace of time, the attacks of the web hackers are also increasing day by day. There is not a single day when someone hasn't been the victim of a hacking attack. This becomes more terrifying you act as the owner of a website. It might happen that all the work that you have done on your website gets wiped out the next day or it has been altered completely. This happens only when your website gets attacked by a web hacker. The news of data breaching and hacks are all over the new in today's world. You might also think that why would the hackers attack a small website of business? Well, nothing depends on the size of a website. It has also been found that 43% of data breaching is done from small business websites. So, it is clear that the attackers can victimize anyone they like.

The hackers are turning out to be more sophisticated in their operation within a community of close-knitted web hacking. The hackers try to target the new intrusions of web application. This is because when a new intrusion is found, it takes some time for the developers to apply the counter measures. The

hackers take advantage of such situations and attack the business websites. The intrusions which are discovered newly are posted on various hacking forums which inform the hackers about the intrusions and the sites. The most common form of attack is infecting the website with some sort of malicious code. Ultimately, the websites which are infected turn out to be the attack launching sites for the hackers and installs the malware on those systems of computers those who visit that site.

Hacking of websites can be regarded as the result of adoption of technologies which are web-based for carrying out e-business. The applications on the web allow the organizations to seamlessly connect with the customers and with the suppliers. However, the vulnerability of such applications on the web has also opened up new doors for the attackers. The hackers opt for the vulnerable websites for various reasons such as data breaching, stealing of confidential information and many more.

Web hacking for stealing sensitive data

When someone conducts online business, the website is bound to function with a wide collection of applications such as submission forms, shopping carts, dynamic content, login pages and many others. The web applications are constructed in such a way that allows the customers to submit and also retrieve various forms of dynamic content that includes different levels of sensitive as well as personal data. Such sensitive data is stored in the databases of the websites. As such websites need to be accessible 24*7 from any location in the world, the web applications which are insecure in nature opens up the doors for the web attacks on the corporate databases. In case the attacker gains access to the credit card and bank details of the customers, the business might turn out to be in great danger.

Web hacking for implementing phishing sites

It might happen that the database of a business is not online or is secured already. However, in spite of such facts, it does not make the web site less susceptible to the attacks. Hackers trace out weak and small sites for the purpose of injecting malware into the sites. They also look out for vulnerable applications for tricking the users and then redirecting them to the phishing sites. Phishing sites are used for retrieving the bank details of the users. Such

attacks which are mainly targeted against the services of online payment can turn out to be the result of either SQL injection or any other type of hacking that can also be performed when the database and the servers contain no susceptibilities.

Securing websites from hackers

There are various ways in which the websites can be protected from the hacking attacks. You can start by installing plug-ins of security on your website. The website security plug-ins helps in improving the security of a website and also prevents any form of attempt of hacking. There are various forms of security plug-ins which are meant for websites of different formats such as Sucuri for WordPress, Amasty for Magento and RSFirewall for Joomla. Make sure that the website that you are constructing comes with HTTPS as SSL certificate is essential for protecting the details of the users such as personal data and credit card information.

Google Hacking

Also known as Google Dorking, is a technique which is used by hackers for information gathering by taking into consideration some of the prime searching techniques of Google. The search queries of Google hacking can be treated by the attackers for identifying the various vulnerabilities of security in the web applications, discovering messages of errors for disclosure of various confidential data and for discovering various files with credentials. The only way to prevent this is by checking out for regular website application vulnerabilities.

XSS Attack

XSS or cross-site scripting attack is a technique which is used by the attackers for injecting malicious form of scripts into mild and trustable websites. It occurs when a hacker takes help of a web application for sending out harmful codes in the form of side script in the browser to the end-user. The end-user will have no idea that the code is malicious in nature and will run the script without even knowing anything.

SQL Attack

It is a form of injection attack that allows the attackers to execute various harmful SQL statements. The SQL statements perform the function of controlling the servers of the database behind the web applications. The hackers can use this measure for bypassing the security measures of a web application. The attackers can also use this technique for adding, modifying and deleting various records from the database. SQL vulnerability can affect any application on the web or websites that use up database of SQL like MySQL, SQL Server, Oracle and others. The cyber attackers use this technique for gathering sensitive data such as personal data, intellectual property, customer information, secrets of trade and many more.

Chapter 14: Exploitation of Computer Systems

With the increase in the use of computer systems day by day, the percentage of attacks by third parties on the systems is also increasing gradually. There were days when people used to store all their data and confidential information in the form of physical copies. But, today most of the people prefer their confidential information in the computer systems and that is what gave birth to the attacks on computer systems. Exploitation is nothing but a programmed script or software which allows hackers to gain control over the entire system and then exploit the same for the benefit of the hackers.
The exploitation attacks try to take advantage of any form of weakness in an OS of the user, in the application or in any other form of software code that also includes plug-ins of the applications or of the libraries of software. The owners of such codes issue a patch or fix in response. The system users or the users of the applications are completely responsible behind obtaining the patch. It can be downloaded from the developer of software which is readily available on the web or it can also be downloaded by the OS automatically or

by the application that needs the same. In case the user fails to install the required patch for a specific problem, it will expose the user to the exploitation of the computer system and might also lead to breaching of security.

Computer exploits and its types

Computer exploits can be categorized into two different types:

- **Remote exploits:** Remote exploits are those exploits types where it is not possible to access a network or remote system. Such exploits are generally used for gaining access to the systems which are remote in nature.
- **Local exploits:** Local exploits are used for those systems which are having local system access. The attackers use this for over-passing the rights of the users of the local systems.

The security exploits can come in all forms of size and shape. However, there are certain techniques among the lot which are more often used than the others. The most common vulnerabilities which are web-based are XSS or cross-site scripting, SQL injection along with cross-site request forgery. It also includes abuse of authentication codes which are broken in nature or other misconfigurations of system security.

Zero-day exploit

The exploits of computer systems can be differentiated in various ways that will depend on the process of working of the exploits along with the attack type that it can accomplish. The most common form of exploit is zero-day exploit. This form of exploit takes ultimate advantage of the zero-day susceptibility. Zero-day susceptibility takes place when a software that might also be an application or an OS, consists of some critical form of vulnerability in the security measures that the vendor is also unaware of. The system vulnerability can only be detected when any hacker is detected with exploiting the susceptibility of the system. That is why it is known as zero-day exploit. After such an exploit takes place, the system which is running the software is also left vulnerable to all forms of attacks until and unless the software vendor releases the required patch for the correction of the system

vulnerability.

The computer exploits can also be characterized according to the expected form of an attack like the execution of remote code, delivery of malware, escalation of privilege, denial of service and various other harmful goals. The exploits can be characterized according to the vulnerability type which is being exploited that also includes code injection, exploits of buffer overflow and various other attacks of side channel and vulnerabilities of input validation.

How does exploit take place?

It is a fact that exploits can take place in various ways. However, one of the most common methods of all is exploits being launched from the websites which are malicious in nature. The victim of such exploits generally visits the malicious websites by mistake. The victim might also be tricked into surfing or clicking on a malicious site link that can come attached with a phishing mail or in the form of advertisement of malicious nature.

The malicious websites which are being used for the computer exploits come equipped with various toolkits of software and exploit packs which can be used easily for unleashing the attacks against the various vulnerabilities of the browser right from a harmful website. It might also be from a hacked website. Such form of attack generally attacks the software which is coded in JAVA, browser plug-ins and the browsers which are unpatched. It is used for planting malware into the computer system of the targeted victim.

The automated form of exploits which are generally launched by various malicious websites are designed with two components: exploit code and shell code. Exploit code is a software which tries to exploit a known form of vulnerability. The payload of the exploiting software is the shell code which has been designed for running one single time when the breaching of the system is complete. The name of shell code comes from the very fact that many of the payloads open up command shell which is used for running the commands in opposition to the system of the target. However, all shell codes are not capable of opening a command shell.

Shell code

Shell code acts as a tiny piece of code which is used as the payload in the process of software exploitation. The shell codes are written in the form of machine codes. Download and execute is a form of shell code that performs by downloading and then executing some malware from directly on the targeted system. This form of shell code do not generate shell but instructs the target machine for downloading a form of an executable file which will be off the network, then save the same into the disk and execute the file. This form of shell code is most often used in drive download form of attack in which the victim clicks on a malicious website link and the shell code downloads the malware and installs the same on the system of the targeted victim.

Chapter 15: Firewall Security

As the rate of cybercrime is increasing every day and is also threatening all form of business all over the world, it is a known fact that each and every organization of today are in need of firewall security. The term ‘firewall’ originates from the word wall which can be constructed for preventing the spread of fire. That is why it came to be known as firewall. However, the fire in the world of computer and networking is referred to as the sudden third-party attacks on the systems. Firewall security helps in blocking some specific form of network traffic and forms a barrier in between trusted and untrusted networks. It can be compared to a physical wall in the way that it tries to prevent spreading of malicious computer attacks.

Types of firewall

There are various types of firewall that can be found today.

Packet filtering firewall

This firewall type comes with a list of rules for firewall security and is capable of blocking internet traffic completely based upon IP address, IP protocol and port number. This firewall management program allows all types of web traffic along with the ones that can bring about web attacks. In such a situation, the user needs prevention of intrusion along with firewall security. In this way, it can easily differentiate among good and bad web traffic. However, a packet filtering firewall cannot tell the proper difference between various forms of web traffic. It also comes with an additional drawback in which the firewall cannot differentiate between a return packet which is legitimate in nature and a return packet which acts like being a part of an established form of connection. So, this form of firewall will allow both types of return packets into your network.

Stateful firewall

This type of firewall is somewhat similar to that of the packet filtering firewall but it is more intelligent in nature. It can easily keep a track of all the connections which are active so that the user can customize the rules of firewall management as such by allowing only those return packets which are actually the part of an established connection. However, just like the packet filtering firewall, the stateful firewall cannot also differentiate between good and bad traffic and this needs prevention of intrusion for detecting and then blocking the malicious web attacks.

Firewall with deep packet inspection

This form of firewall examines the data packets in actual and thus can also look after the attacks of the application layer. This form of firewall is similar in nature to the technology of intrusion prevention. So, it is capable of performing some of the functions of intrusion prevention. It comes with three admonitions. Firstly, the explanation of “deep” inspection for some of the vendors extends to a specific depth within the packets and therefore, do not examine the packet entirely. This can ultimately result in missing out some of the major forms of attacks. Secondly, as it depends on the capacity of hardware, it might not have the processing power which is required for handling the deep inspection of the packets. As a user, you need to make sure about the bandwidth capacity that the firewall can easily handle at the time of inspection. Thirdly, the technology of embedded management of firewall

might not have the required flexibility for handling all forms of attacks.

Application-aware firewall

This form of firewall is similar in function with the deep packet inspection firewall. However, this type of firewall can understand various protocols and can also define them so that the rules or signatories can address specific sections in the protocol. Application-aware firewall provides flexible firewall protection to the computer systems and also allows the rules for being both comprehensive and particular. This firewall management system does not come with any form of drawback as in general, it will improve the functioning of deep packet inspection. However, some of the attacks might get unnoticed by the firewall as the defining of routines by the firewall is not potent enough for handling the variations in actual world traffic.

Application proxy firewall

Application proxy performs as the mediator for some applications like web, traffic or HTTP that intercepts all the requests and also validates all of them before allowing them. Application proxy firewall also comes with certain features of intrusion prevention. However, the application of complete application proxy is actually difficult and each proxy is capable of handling a single protocol only like incoming email or web. For getting the ultimate firewall protection from an application proxy firewall, it needs to completely accept the protocols and for enforcing blocking of the protocol violations.

Importance of firewall security

Firewall security is of utmost importance for the computer systems of today's world. The attackers are always looking out for the vulnerable form of devices which are connected with the internet. The attackers can easily gain access to the system by implementing malware or any other form of malicious script into the system through the internet. It can lead to data breaching and also loss of sensitive data. Firewalls can provide ultimate security to the systems and are important because:

- It can protect the computer of the user from unauthorized access.

- It can easily identify and then block unwanted and harmful contents.
- It can help in preventing viruses, worms and malware from entering the system.
- It can create a secure environment of network for multi-person usage of the system.
- It can help in securing all sorts of sensitive and confidential information.

Firewalls come with the capability of blocking some particular online locations. This feature might turn out to be very beneficial for the purpose of security and also for blocking various sites that might contain content which is not suitable. Filtering of content is useful for the parents, schools and corporations. Firewall can easily block the access to malware, however, it cannot detect any malware in the system and get rid of the same. So, it is always recommended to install an anti-virus software along with the system firewall protection right in place. Anti-virus software is capable of detecting any form of malware in the system and can also help in blocking the same.

Chapter 16: Cryptography and Network Security

With a rapid increase in the rate of cyber attacks, it is of utter importance to protect all forms of confidential data as much as possible. Data leakage can lead to serious loss for various businesses and can also turn out to be a threat for an individual person where the credit card, as well as bank details, are breached. The term cryptography is linked with the technique used for converting plain and ordinary text into unintelligible form. With this method, transmission and storage of sensitive data become a lot easier. Only those to whom the message is intended can process the text and read it. It is not only helpful in protecting data from breaching or theft but it is also useful for data authentication.

In the world of computer science, cryptography is associated with securing all forms of information along with the techniques of communication which are derived from the concepts of mathematics. It uses a definite set of ruled calculations which are known as algorithms. The algorithms are used for

transforming the messages in such a way that it becomes very hard to decipher the same. Such algorithms of deterministic character are used in the generation of cryptographic keys along with digital signing for protecting the privacy of data, browsing various websites on the internet and for sensitive communications like email and credit card or bank transaction details.

Techniques of cryptography

The technique of cryptography is often linked with the characteristics of cryptanalysis and cryptology. The technique of cryptography includes the usage of various techniques like merging of words with various images, microdots and several other techniques which are used for hiding that information which is in transit or in storage. However, in the world of computer today, the technique of cryptography is often linked with the process of scrambling ordinary text or cleartext. Such form of ordinary text is known as plaintext. The plaintext is converted into ciphertext with the process of encryption and then back to the original form with the help of decryption. The people who specialize in the field of cryptography are called cryptographers.

Objectives of cryptography

The modern-day objectives of cryptography are as follows:

- **Confidentiality:** Confidentiality is the act of keeping all forms of personal and sensitive data protected for the concerned people. The information which is being transmitted or stored cannot be analyzed or understood by any third party for whom it was not at all intended.
- **Integrity:** The data or information which is being transmitted or stored cannot be changed or altered between the sender and the receiver who is intended to receive the data. In case any form of alteration is made, the sender and receiver will both be notified.
- **Non-repudiation:** The sender, as well as the creator of the data or information, will not be allowed to deny his/her intentions at a later stage during the creation or transportation of the data or information.

- **Authentication:** Both the parties in communication who are the sender and the receiver will have the capability of confirming the identity of each other along with the origin and final destination of the data.

The protocols and the procedures that meet all of the mentioned objectives and criteria are called cryptosystems. The cryptosystems are often taken as only referring to the procedure of mathematics and programs of computer only. However, in actual, they also comprise of human behavior regulation like logging off from the systems which are not used, choosing strong and difficult to guess passwords while logging in and not discussing any form of sensitive data and procedure with the outside world.

Algorithms of cryptography

The cryptosystems work along with a bunch of procedures called ciphers or cryptographic algorithms. It is being used for the purpose of encrypting as well as for decrypting the messages for securing up the communications among smartphones, applications and other computer systems. A suite of cipher uses up one single algorithm for the purpose of encryption, one more algorithm for authentication of messages and another algorithm for exchange of keys. This whole process is embedded within the protocols and is written within the programming of software which runs on the OS along with the computer systems which are based on the network. It also involves generation of public as well as private key for the process of encryption as well as decryption of data, verification for the purpose of message authentication, digital signing along with the exchange of keys.

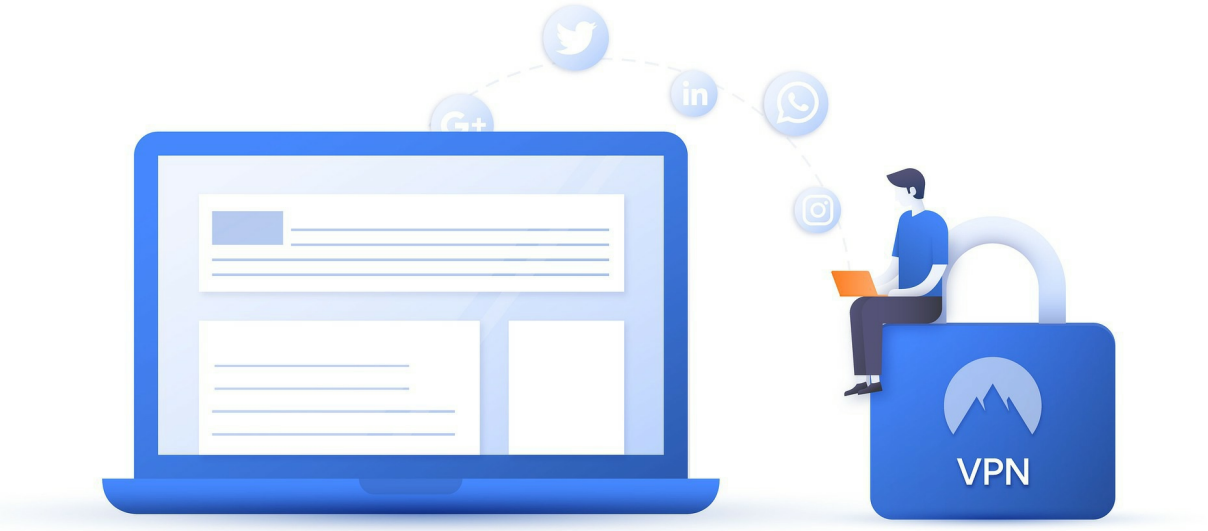
Cryptography and its types

There are various types of cryptography which are being used today.

- **Encryption using single key or symmetric key:** The algorithms of this form of cryptography create block cipher which are actually particular length of bits. The block cipher comes along with one secret key that the sender uses for encrypting the data. The same key can be used by the receiver for deciphering the information. AES or Advanced Encryption Standard is a type of

symmetric key encryption which was launched by the NIST as Federal Information Processing Standard or FIPS 197 in the year 2001. It is being used for the protection of confidential and sensitive data. In the year 2003, the U.S. government approved of AES for the purpose of classified information. AES is a form of specification which is free from royalty and is used in all forms of hardware and software in the whole world. AES succeeded DES and DES3. AES uses up longer lengths of keys for preventing attacks.

- **Encryption using public key or asymmetric key:** The algorithms for this form of cryptography uses two keys at a time in pair. One public key which is associated along with the sender and the receiver for the purpose of encrypting the information. Another private key is used for the purpose of decryption of the message. The private key is only known to the originator. There are various forms of cryptography using public key like RSA which is used all over the internet, ECDSA which is being used by Bitcoin and DSA which has been adopted as FIPS for all forms of digital signatures by the NIST.
- **Hash functions:** For the purpose of maintaining the integrity of data, hash functions are used that returns an accepted value from the value which is used as input. It is being used for mapping the data into a fixed size of data. SHA-1, SHA-2 and SHA-3 are the types of hash functions.



Chapter 17: Protection and VPN

VPN, also known as Virtual Private Network, is a technique of creating a highly secure connection with another network directly over the internet. In this world of today, VPNs are widely used now for accessing various websites which are restricted in several regions, for protecting the user's activity of browsing from the attacking eyes while using public Wi-Fi and many more. VPNs are very popular today but it is not being used for the purpose for which it was created originally. It was made for connecting to the networks of business in a secure way over the internet. It was also made with the purpose of allowing the user to access the network of business right from their home. VPNs help in forwarding all the traffic in the network which provides users with various benefits such as accessing the resources of local network remotely and bypassing of censorship on the internet. Many of the OS comes with integrated support of VPN.

How does VPN help?

The concept of a VPN is very simple. It connects the smartphone, PC or tablet of the user with another server or computer directly on the internet and also allows the users to browse the content on the internet by using the

internet connection of that computer. So, in case the computer with which the user is connecting to for surfing the internet is from a different country, it will show that the user is also from the same country as the server computer. So, the users of VPN can easily access everything that they couldn't do normally.

A VPN can be used for various purposes such as:

- Bypassing the restrictions on websites based on geography or for streaming of video and audio.
- Watching online media streaming like Hulu and Netflix.
- Protecting the user from connecting to any form of malicious hotspots of Wi-Fi.
- Gaining a little bit of privacy online by hiding the original location of the user.
- Protecting the user from being scanned while using torrent.

Most of the people today use VPN for the purpose of bypassing their geographic restrictions for watching restricted content by using the network of any other country or for torrenting. VPNs are really useful while accessing public Wi-Fi such as at coffee shops.

How to get a VPN?

You can get a VPN depending completely on your requirements. You can either create a server of VPN all by yourself or host one VPN server out of the house. You can also create a VPN from your workplace as well. But, in real-world, most of the people are looking out for a VPN server for surfing restricted content which is banned in some areas or countries, like torrent. Just for the purpose of surfing restricted online content, you can download from the various options available online and use it according to your need.

Working of a VPN

When the user connects a computer or other device like a tablet or smartphone to the VPN, the system will start acting like it is from a similar local network as of the VPN. All the network traffic will be sent across a secure connection to the VPN. As the system behaves like it is also from the

same network, it allows the users to access the resources of local network securely even when the user is at some different corner of the world. The user can also use the internet as if he/she was present right at the location of the VPN that also comes with some added benefits in case the user is using Wi-Fi of public nature or wants to access some sort of geo-restricted website.

When you are browsing the internet while being connected with the VPN, the computer will contact the website via the VPN connection which is encrypted in nature. The VPN will help in forwarding the user request and then brings back the website response through the same secure connection only. For example, if you are using a VPN based on the USA accessing content on Netflix, Netflix will be seeing your connection coming out from the USA only.

Uses of VPN

The usage of VPN is really simple and it can help the users do perform a variety of things such as

- **Accessing network of business at the time of travelling:** The most common use of VPN is by the business travelers who use it to access the network of their business along with all the resources of the local network while travelling only. The resources of the local network are not required to be directly exposed to the internet and thus it helps in improving the overall security.
- **Accessing home network at the time of travelling:** You can easily set up a VPN of your own for the purpose of accessing your network at the time of travelling. This will let you access a form of Windows remote access desktop directly over the internet. You can use it for local area file sharing, playing games on the web by acting as if you are also on the same local area network.
- **Hiding the browsing activity from the local network along with ISP:** In case you are using a Wi-Fi which is of public nature, all your activities of browsing on the websites which are non-HTTPS are visible to everyone on the same network nearby in case they know how to trace those activities. If you want to

hide your browsing activity for gaining more privacy, you can use a VPN. The network of the local area will only be seeing one single VPN connection. All forms of other traffic will be traveling from over the connection of the VPN. This can also be used for bypassing monitoring of connection by the ISP.

- **Bypassing censorship on the internet:** There are various Chinese people who use VPN for accessing the Firewall of China for the purpose of accessing the complete internet.
- **Accessing the websites which are geo-blocked:** the use of VPN increased in recent years only because of one reason which is accessing websites which are blocked according to various locations. You can use a VPN for accessing such websites and also for watching online streaming media while you are out of your country such as Netflix and many others.

Chapter 18: Ethical Hacking and Penetration Testing

There is a misconception among most people which is that they think ethical hacking and penetration testing is both the same thing. However, in reality, it is not so in actual. Not only normal human beings who are not acquainted with the world of cyber security but the cyber security experts also get confused at times between the two. Although both of them fall under the same section of offensive security, there is a thin line that differentiates both. Offensive security is composed of various objects such as penetration testing, reverse engineering of software, social engineering, ethical hacking and many more.

In the world of cyber security, both the items ethical hacking and penetration testing are of utter importance. Let’s have a look at some of the aspects of both the components.

Penetration Testing

Penetration testing, as the name goes by, can be understood that it is a process of testing whether penetration is possible or not. It looks out for all sorts of vulnerabilities, risks, malicious content and flaws within a system. By system, it can either be a computer system or an online server or network. This process is done for the purpose of strengthening the system of security in an organization for the sole purpose of defending the infrastructure of IT. It is a procedure which is official in nature and can be regarded as very helpful and not at all a harmful attempt if used wisely. Penetration testing is an essential part of ethical hacking where it is focused on the attempt of penetrating a system of information.

As it is very helpful in readily improving the overall strategies of cyber security, the process of penetration testing needs to be performed at regular intervals. Several forms of malicious content are built up for finding out the weak points within an application, program or system. The malware is spread throughout the network for testing the vulnerabilities. Pentest might not be able to sort out all forms of concerns regarding security, but it can actually minimize the chances of any attack. Penetration testing helps in determining whether an organization or company is vulnerable to any form of cyber attack or not, whether the measures of defense are on point and which of the security measures needs to be changed for decreasing system vulnerability.

Penetration testing can easily show the strengths and weaknesses of the structure of an IT system at one point of time. The pentesting process is not at all a casual process. It comes with lots of planning, granting of permission for pentesting from the management and then starting the process without preventing the normal flow of work in an organization.

Ethical Hacking

The role of an ethical hacker is somewhat similar to that of a penetration tester. But, the process of ethical hacking comes with various forms of diversified duties. Ethical hacking encompasses all the methodologies of

hacking along with all forms of methods related to cyber attack. The process of ethical hacking is targeted to the identification of vulnerabilities and also fixes all of them just before any attacker can exploit the information for the purpose of executing cyber attack. Ethical hacking is being called as ethical as all the required functions are performed only after the granting of required permissions from the authority for intruding the system of security. The ethical hackers perform their role on the ground of ethics whereas the attackers hack without any prior alarm.

The role of a professional ethical hacker is very critical as well as complex as the person who is intruding the system of security needs to perform everything without even affecting the overall functioning of the system and then locate the available vulnerabilities as well. The ethical hacker traces out the possible vulnerabilities and reports the authority about the required measures. An ethical hacker not only works with the methodologies of security but also suggests the implementation of the same. The safety of an IT infrastructure is in the hands of an ethical hacker.

Penetration testing Vs. Ethical hacking

Although the functioning of both penetration testing and ethical hacking might seem similar but both differ from each other in various aspects. The main goal of penetration testing is to look out for vulnerabilities within a specific environment. In the case of ethical hacking, it uses various types of attacks for finding out the flaws in security. Penetration testing deals with the security of a particular area whereas ethical hacking itself is a comprehensive term and pentesting is a function of the ethical hacker. For being a good pentester, past experience is required in the field of ethical hacking. Ethical hacking is one step towards pentesting. Unless and until someone knows the methodologies properly, they will not be able to carry on with a penetration testing.

Penetration testing does not require very detailed writing of reports. However, in the case of an ethical hacker, an ethical hacker needs to be an expert report writer. Paper work is comparatively less in penetration testing when compared to ethical hacking. In the case of ethical hacking, detailed paper work with legal agreements is required. Penetration testing consumes very less time which is not the case with ethical hacking. It requires a lot

more time and effort. For penetration testing, accessibility of the overall system is not required. In the case of ethical hacking, a hacker requires complete accessibility of the target system.

Bottom line

As penetration testing techniques are being used for protecting the systems from all forms of threats, the attackers are also coping up with the same and are coming up with new vulnerability points in the target applications. So, it can be said that some sort of penetration testing is not at all sufficient for protecting the system of security. This is not the case with ethical hacking as it effectively finds out the loopholes and reports about the same for further improvement. There are many cases where it has been found that when a new vulnerability has been found in a system, the attackers hacked the system immediately after the testing. However, it does not imply that penetration testing is not useful at all. It cannot prevent an attack from taking place but can help in the improvement of a system.

Chapter 19: FAQ

How often should penetration testing be done?

The organizations perform according to their own set of regulations and mandates. The standard that they follow will determine whether they need penetration testing or not. The standards of the organizations come with their own methodologies that help in describing what will be the best practice for protecting the security system. The standard will also determine that whether documentation of the tests needs to be done for compliance and purpose of auditing afterwards.

What is the rogue wireless network?

Rogue wireless network acts simply as a point of access just like a router or Wi-Fi station. It is plugged into the network of the organization; however, it

does not even adhere to with the organization’s standards for the wireless infrastructure which is in existence.

How a rogue wireless network can be installed?

This form of security threat occurs when any device has been adapted in an organization and is connected with the network, either knowingly or unknowingly. There are various types of equipment that come with activated Wi-Fi by default which is not configured at all. This means, that when the device gets turned on for the first time, it will start broadcasting signal for connection.

Can the employees of a business expose the organization to cyber threats?

Yes, they can. Any person who carries a device that has a connection with the Wi-Fi of the company might turn out to be a potential threat for the business. Malware can get into a system unknowingly via a network through laptop, tablet or smartphones. It happens when the segments of Wi-Fi are not properly locked. If the business servers are not separated on a completely different VLAN and all wireless network traffic can access the same, there is a high chance of security breaching and data theft.

Is it required to have wireless networks for businesses in spite of the associated potential risks?

Modern businesses cannot function without wireless technologies. However, the standards of technology and configuration which are applied for the wireless equipment will determine the usefulness of the wireless technologies and also the potential risks of security breach. There are various forms of businesses where the employees are required to work with tablets and scanners, especially in the manufacturing and warehousing sector. It will not be possible for such businesses to operate without the presence of a wireless network within the organization.

What are the most common types of Wi-Fi attacks?

When it comes to Wi-Fi attacks, the list is never-ending. There are several vulnerabilities, exploits and shortfall of security when it is related to wireless

attacks. But, the attackers employ certain common methods for the purpose of accessing the wireless networks.

Is MITM a serious security threat?

Also known as man in the middle, it is one of the most commonly found forms of attack and is the most used tactic as well by the attackers. The attacker tricks the victim and transmits data so that the sufferer believes that the communication is coming from a legitimate form of contact only. Using MITM, the attackers can easily target the system of the victim and control it remotely, gain access to several sensitive data such as bank details along with exploits.

What are packet analyzers?

The attackers are capable of analyzing and sniffing the data packets which are being transported through a wireless network. The attackers can also intercept various unencrypted data which is inside the packets of TCP as well. When data is gathered using this method, the attackers can easily gain insight into the internal working system of an organization which is being targeted and can also fish out valuable information that might turn out to be a huge loss for the business.

What is malware?

Malware is a form of cyber attack and is the most common form of attacks. It possesses a serious kind of threat to the networks and servers. It also comes with the power of self-propagating over various networks. It becomes very difficult to detect and stop it once it has gained access to a network segment. It can infect the system when two devices are being connected with the same network which makes the spread of infection very fast.

Can poorly configured Wi-Fi lead to cyber attack?

Yes, it is possible when the Wi-Fi is configured poorly. It is the main reason behind the infiltration of a wireless network. This becomes more serious when there are no available management tools for the IT staffs to gain a perspective of the wireless environment.

Is it okay to share the result of penetration test outside the organization?

No, you should never disclose the test report outside the organization. You can only share it with the company officials and authorities. Sharing test results with the outside world will open up vulnerabilities for the organization and might lead to a serious cyber attack.

Conclusion

After you have completed the whole eBook, you can easily develop a clear perception of the process of hacking with the help of Kali Linux. By now, you have must have understood all the requirements for setting up a secure server and network for your business. Everything depends on you. You are the one who can secure the system of security from all forms of attacks.

With the help of various tools from Kali Linux, you can have overall control over the security interface of your organization. This book is not only about Kali Linux. You have also learnt about various components of a network and the measures required for securing them up. The key benefit of using Kali Linux is that you can perform various security tests that can help in removing all forms of vulnerabilities from your IT infrastructure.

The security of your organization and network completely depends on you. Make sure to employ the various steps that you have learnt from this eBook about securing your infrastructure.

If you find this book helpful for your business in any way, kindly leave a review on Amazon.