Cairo University
Faculty of Computers and Artificial Intelligence
Technical Writing

Cyber Security & Hacking

#26

Student Name	ID
ASALA EHAB MOHAMED	*20201020*
DINA OSMAN EMAM	*20200173*
GAMAL MOHAMED GAMAL	*20200123*
AYA ASHRAF MOHAMED	*20200106*
ABANOUB MORRIS NOSHI	*20200001*
HABIBA AYMAN AL_TAHRY	*20200140*
ZAHRAA AHMED ABDELKAFI	*20201082*
KHALED OSAMA ABDALLAH	*20200166*

Under supervision: Dr Ihab Elkhodary

TABLE OF CONTENTS

LIST OF Figure

Summary

In this report, we discussed one of the most important areas in the world of digital computers, which is Hacking and cybersecurity, which is one of the most prominent current areas, as it is expected to become the most prominent in the future because this is the era of cyber warfare.

In this report we will learn the definition of hacking, the importance of hacking, sequence of hacking steps and types of hacker such as (black hat hacker, white hat hacker, and more)

Also, we will discuss threats of hacking and we will learn the types of cyber-attack such as (malware attack, man-in-the-middle attack, and more) and the technique of each and the targets of each and we will know the strongest and most dangerous Hacking groups such as (APT 28, Dragonfly, and more)

In this report, we show ethical intruders, who are they and what are the conditions for a person to be called an "ethical intruder"? Then we discuss the mechanism of their work and the steps they follow, and how they are very important in the field of cybersecurity.

We then learn about the field of cybersecurity, what it is and what is formed and what is the largest institution in it, and we show what this field represents to the ordinary user and various institutions and technology in general, and how it contributes to protecting sensitive data and information from penetration? In this book, you will learn about the most important preliminary procedures that you as a user must take to protect your personal data from Hacking.

Chapter 1: introduction

1.1 scope

We will start the definition of hacking, and taking about his importance, compare between his types and taking about sequence of hacking steps, after that we will take about the danger of hacking, top ten hacking groups and the companies that had been hacked. After that we take about the Entrance to Ethical Hacking by declare the concept of Ethical Hacking, the Ethical Hacking and penetration testing. Finally, we will take about cybersecurity field by taking about his definition, explain the importance of it and the common ways to keep your data safe.

1.2 purpose

We aim to give the reader an overview about the hacking by make him know his definition, types, his importance and sequence of hacking. Making the reader became aware of the danger of hacking by give him examples of the companies that had been hacked and top ten hacking groups. Making the reader know about Ethical Hacking by explain his concept and terms. Finally, we want to make a reader became aware of cybersecurity which protect his information and know the common ways to make his data safe.

1.3 procedure

We chose our address and topics after we extracted the main sub-addresses in relation to the primary address. We choose the main important topics that will help people know more about cybersecurity and hacking, and how to protect their devices, data and information in very easy way. Also, to know more about the importance of it in our daily lives. We gathered much information from different websites and books to cover every single title in the report.

1.4 Background Statement

By the increasing of using technology and much data is transferred from one device to another or even by the internet, the idea of hacking and cybersecurity is aware by a lot of people to protect their data and information, and it has many types and many ways to protect them, also the idea of Bael hackers, data theft and fraud began to appear. And there were many ways helping you to steal data and information from normal people or even important authorities, so it become very important for anyone to protect their devices from hacking, and the awareness of that topic has finally spread among people.

Chapter 2: Introduction to hacking

2.1 the definition of Hacking

it is controlling computer network systems in an unauthorized way for illegal purpose. this process is done by professional programmers by using programs that help to hack.

2.2 importance of hacking

Hacking could be important in many ways

Hacking could help in some situations, when a system loses data by locking it could be recovered, this will help if the lost data is a password.

Hacking prevent data from falling into enemy hands and protect them, with hacking you can Strengthening your network and your data

Hacking can save the country from terrorist attacks, which helps in security and safety

Hacking could be used to prevent hacking

2.3 types of hacker

2.3.1 black hat hackers

this type of hackers is computer users who steal other people's computer system for personal gain. they have different experiences from simple malware spreading to stealing financial or personal data. they often use malware to breaking through security protocols and get information

2.3.2 white hat hackers

they are a new type of hackers. they hack systems to secure company's information. it is a different method and it has a new concept which is that if you want to arrest criminals you must think like them to be one step ahead. they were called this name because of the old western movies where the good man can be identified by the white hat.

2.3.3 Grey hat hackers

they are hackers between white hat hackers and black hat hackers. they hack the system in order to detect errors and disclose them to the owner of the system. sometimes they ask for a small fee to fix the problem. If the owner refuses, they will post the newly found exploit online

2.3.4 red hat hackers

they are very similar to the white hat hackers but they have a different style and more cruel. they want to eliminate the black hat hackers not to report them like white hat hackers

2.3.5 Green hat hackers

they are beginner hackers and make a great effort to learn. sometimes they cause a lot of damage to systems due to their lack of experience. they are also called beginners

2.3.6 Blue hat hackers

they work as hackers for revenge only and have no desire to upgrade their skills

2.3.7 script kiddie is the troublemaker in websites

they are people who are not good at hacking. they use available software and tools developed by other people to hack systems. therefore, they are considered the most dangerous type of hackers

2.3.8 suicide hacker is determined, despite knowing what will happen

despite knowing they will be arrested they insisting to hack for specific purpose

2.3.9 hacktivist is dominators on web sites

a group of hackers who learn hacking to hack government's systems for a social, political, personal goal

2.3.10 multifarious is one of means in social media hacker

their only job is to hack social media and they are very similar to black hat hackers.

2.4 Sequence of hacking steps

2.4.1. Search for information:

It is the first stage of piracy in which the hacker begins by identifying the hacker and collecting information about it like (network, host, people involved) To attack him in the right way. (the hacker will use search engines to collect that information)

2.4.2. using tools based on the information:

At this point, some tools are used such as scanners, network diagrams, sweepers, vulnerability scanners, etc. Hackers tip to get more information like IP address and user accounts and scanning the target to find weakness that could be exploited so they can launch the attack at their desired time.

2.4.3. prepare the target network diagram

The hacker begins Setting up the target network diagram depending on the data he collected, now hacker uses information about weakness to gain access, hacker can be connect with(local area network, LAN, wired or wireless) ,now the hacker has some options to access the network so for example, the hacker may decide to infiltrate from the IT department, now a message will be sent to the target (the victim), this message contains a site in On the surface, the victim is asked to log into a new google portal using their reliable and reliable data. As for the real significance, the link collects the victim's login information and passwords.

2.4.4. the process of maintaining control:

The hacker has succeeded in accessing, but now he is trying to maintain this access and begins taking some measures, for example, the hacker may create a personal account for himself as a precautionary measure or lie may search for accounts that have not been used for a while and are assumed to have been forgotten or not to be used as a secondary account, There will be no problem with the hacker as long as there is no evidence of discovery, so lie leaves the victim to think that everything is okay, then the hacker starts making copies of all the mail, appointments and contacts he will need later

2.4.5. scanning process effects:

In this process, the hackers will not carry out the attack directly. Instead, hackers will change their MAC address and activate the device's VPN and delete all evidence to help them cover up their identities. Hackers cover paths (clear mail messages, clear server logs, modifying registry values, uninstalling all applications he used and deleting all folders it created. etc.). there are many examples of this phase such as (attack include steganography, the use of tunneling protocols, and altering log files.)

Chapter 3: The Danger of Hacking

3.1 cyber threats

It is intended to explore methods to penetrate and exploit security flaws, existing in computer systems belonging to persons with a security characteristic or security agencies and institutions, with the aim of harming these persons or security services.

3.1.1Phishing attack

It is an attempt to obtain sensitive information, such as usernames, passwords, and credit card details. It is one of the cyber-attacks related to social engineering attacks, where the attacker performs a cyber trick such as (downloading an attachment or clicking on the link) to reach the target. It's the logical trick of having him click on the URL or an attachment from an email message. This type of deception is easy to pick up, and it's not as effective as it used to be, so some hackers have left the old ways.

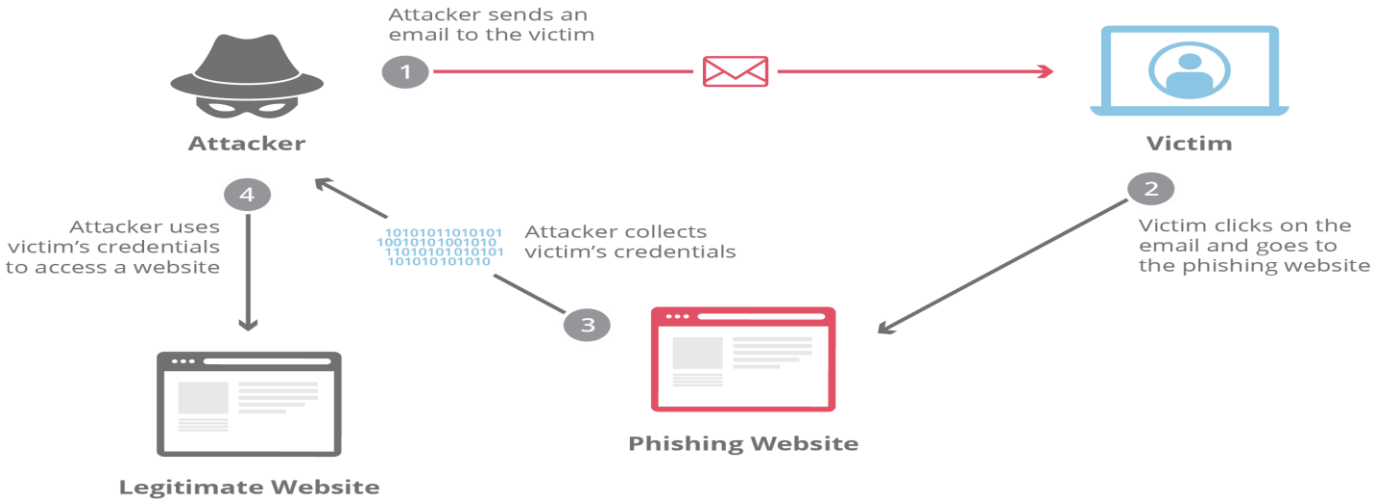

Figure 3.1 phishing attack

3.1.1.1 Types of phishing attacks

3.1.1.1.1 Spear phishing

It is one of the effective types of phishing because it uses real information to deceive the target, and that information was obtained through free sources on the Internet, such as social media, where the attacker can through these means know real information about the organization that is hacked and all its employees from a high degree to Low and the attacker sends an email that causes the target to click on it, which helps the attacker access and steal sensitive information in the organization.

3.1.1.1.2 whaling phishing

It is a specific form of phishing that targets senior managers, and differs from spear phishing in that whaling, emails or web pages presenting fraud take a formal form and usually target a person in particular, the goal is to deceive someone into the position of the top manager to disclose About confidential information about the company.

3.1.1.1.2 Clone Phishing

Where a legitimate email address was previously delivered, containing a link, and its address was used and used to create a matched or semi-cloned email, the attachment or link in the email is replaced with a malicious copy and then sent from a fake email address, to appear as if it were from the sender. the original.

3.1.2 SQL injection attacks

It is a programmatic attack on applications that contain databases, and is characterized by SQL injection in an application that is executed in the database layer for such an application, and this process is considered one of the most dangerous types of attacks against websites in particular.

figure 3.2 what is SQL injection

3.1.2.1 Types of SQL injection attacks

3.1.2.1.1 in- band SQL injection

Depends on unauthorized input, relies on wrong messages that came from the database, and the attacker can obtain information about the database structure. Consolidation Based on this technology, the attacker relies on the "UNION" operator ("UNION" is a file SQL) to combine the two "SELECT" statements that will return one result, which will be the HTTP response.

3.1.2.1.2 blind SQL injection

Blind SQL injection differs from generic SQL injection, in that blind injection is usually not available from the rendering result page, so the injection result is unknown. Like chatting with a robot, it knows a lot but only answers (yes or no)

3.1.2.1.3 Out-of-band SQL injection

the attacker uses an out-of-range attack when it becomes more difficult for the attacker, and in this attack the attacker executes the attack by formulating the SQL command, and a connection occurs between the database and another server that is carrying out the attack and is able to control it, and then he can insert, request or update data from the database.

3.1.3 cross-site scripting

Cross-site scripting is a security attack, in which the target is not directly attacked It occurs by entering web security through the app with a code, when the customer makes an entry the injected web browser executes the transcoding. A cross-site scripting attack uses third-party web resources to run the scripts, and most attackers do Java Script as a web programming language for writing XSS code, and also it can be any web language Used to carry out this attack.

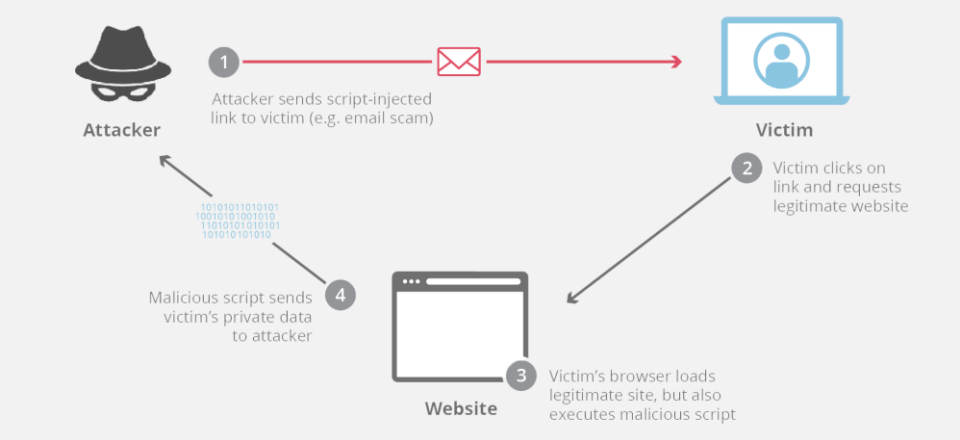

Figure 3.3 what is cross- site scripting

3.1.3.1 Types of cross-site scripting attacks

3.1.3.1.1 Reflected XSS

Reflected XSS It is also called Non-persistent XSS, and it occurs when the hacker exploits one of the site's entries without the need to store the script in the database, then sends the website link combined with a mined script to the victim via an email, for example, or by posting this link on a site or on Social media sites, and when the victim clicks on the link, he will go to the site and the built-in script will be executed, thus the hacker will get what he wants, either by stealing cookies, through Key Logging, or other operations.

3.1.3.1.2 Persistent XSS

Persistent XSS, also called stored XSS: This vulnerability occurs when the hacker exploits one of the website entries and sends a script that is stored at the site server level and often in the database, such as sending the script from the comment box on the site, or in the form of a message, or from Any place on the site allows values to be stored in the database, and when a visitor comes to browse the page that contains the values coming from the database, this script is executed. For example, you programmed a blog in order to publish articles on it, in one of your articles the hacker entered and instead of writing a comment for you he wrote a script, this script will be stored in the database, and therefore when a visitor comes to view your article, the comments will be downloaded from the database with the comment Mined.

3.1.3.1.3 Dom-based XSS

This attack depends on security gaps that made in the client side scripts, in this attack in the bad script doesn't execute in the website / application, it only delivers the bad script using the gap found on the client side scripts the difference between the Dom Based XSS attack and the Other Two attacks is that the website / application does not serve the script.

It is also very similar to Reflected XSS, except that it mainly relies on controlling Dom-based XSS by executing a script where a specific value is sent.

3.1.4 Man-in-middle attack

Man-in-middle attack is a common attack that’s is used by the attacker to spy on two targets

The attacker infiltrates interacting interlocutors into a network without each of their knowledge and the attacker gets or receive the message from one of them and reply to the other

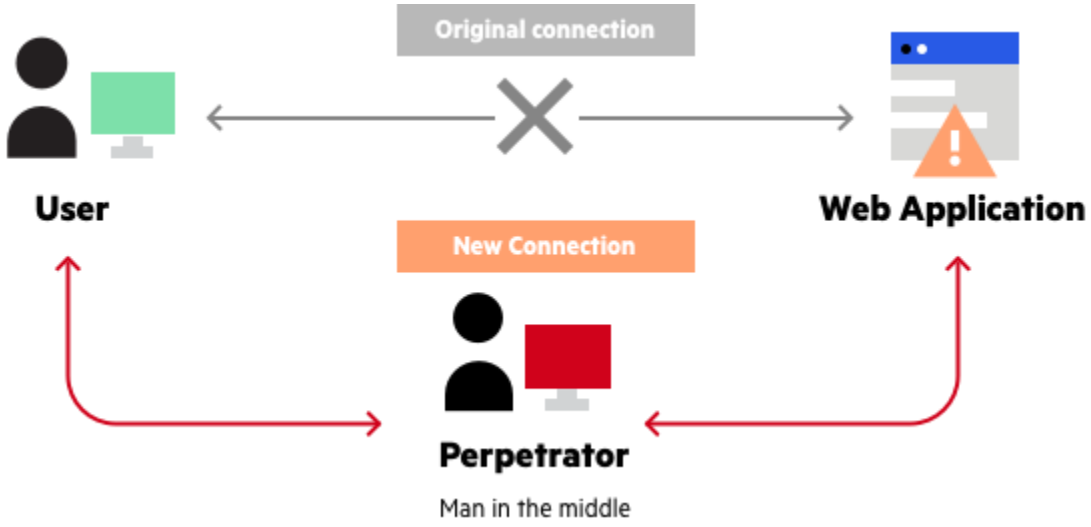

Figure 3.4 what is man-in-the-middle attack

3.1.4.1 Types of man-in-middle attack

3.1.4.1.1 Rouge access point

the attacker targets with the new devices which have long range wireless devices that have an auto connect option to the strong signal, the attacker start his own wireless access point, tricking the device to enter the access point, when the device connect the attacker will be able to control the device the attacker doesn't need, he only need to be close to the device range.

3.1.4.1.2 ARP spoofing

Here the attacker uses the ARP which converts the IP address to MAC address in local networks. Attacking attackers can respond to another host's requests by not responding to their MAC address, with some tricks, the attacker can break thought the private traffic between two host, then from this link he can access the host application accounts or extract sensitive information

3.1.4.1.3 Multicast DNS spoofing

Multicast DNS is similar to DNS, but it’s dona on a local network similar to ARP.

The local name resolution system simply configurate network devices, devices make use of IP in trusted networks, which leads to make the attacker get use of any app request from these devices to respond on it with fake data, redirecting it to an address under his control, because devices keep the local cache of address here the attacker's devices will be trusted for the target for a time.

3.1.4.1.4 DNS spoofing

DNS spoofing similar to the way ARP convert IP addresses to MAC addresses on a local network. DNS convert domain names to IP addresses. When using a DNS spoofing attack provides a corrupted DNS cache to a host to access another host with the other domain name, this makes the target send the sensitive information to the attacker's host.

3.1.4.2 Man-in-the-Middle Attack Techniques

3.1.4.2.1 Sniffing

In this technique the attacker using specific wireless devices to find packets at low level, these devices are allowed to be monitoring or promiscuous mode, which help the attacker to see all packets like other hosts packets

3.1.4.2.2 Packet injection

The attacker can also use the devices used in sniffing to inject a malicious packet in data communication streams, the packets can marge with valid data communications streams and appearing to be part of the communication.

This technique includes first sniff to determine how the packets will be.

3.1.4.2.3 Session Hijacking

The attacker only needs to get the session token from the targets. He does not need to spoof. Session token is used in most web application to let the user use the web application without asking him for the password on every page, if the attacker hijack the session token, he will be able to make requests as the user.

3.1.4.2.4 SSL stripping

The attackers use SSL stripping to block packets and redirect their HTTPS-based address request to go to the end point of the HTTP, which forces the host to make requests to the server and the information will leak.

In this technique the attacker does not use ARP and DNS spoofing because this couldn't attack HTTPS.

3.1.5 Malware attacks

One of the common cyber-attacks is malware attack, malware is bad software that could be (ransom software, spyware, command and control and more).

For example, a famous malware attack is the WannaCry ransomware this malware works when it's downloaded to the system, then it starts to execute some commands to upload data and frozen application and prosses on the system, asking to pay for data. Attackers use malware for a certain goal.

Figure 3.5 Ransome example

3.1.5.1 Most Common Malware Goals

3.1.5.1.1 Exfiltrate information

here the attacker uses the malware to get a sensitive information, credentials and payment information from the target's system

3.1.5.1.2 Disrupt operations

this attack making errors and problems on the OS of the targeted, it can also block operation int the system or make a system unusable by target a critical file in OS, it can also make a self-destruction for a system, the damage varies in this attack.

3.1.5.1.3 Demand payment

Here the attackers use scareware software which uses empty threats to scare the target to paying some money and the attacker creates a ransomware that block the target from accessing his data until the target pay to the attacker.

3.1.5.2 Types of malware attack vectors

3.1.5.2.1 Trojan horse

Trojan horse is a malware that appears like a game or useful software, this only require the target to download the game or software

3.1.5.2.2 Virus

Virus is a type of malware that inject itself into software virus has injection codes that spread to other application and infect them

3.1.5.2.3 Worm

Worm differ from virus because a worm actively works to infect other targets, worms could attack targets with any action of them.

3.1.6 Denial of service (Dos) and distributed denial of service (DDOS) attack

3.1.6.1 Denial of service (Dos):

This occur because Fortis turnout at same time such as turnout websites. Denial of service attack all system's resource, but it is launched from a large number of other host machines that controlled by the attacker. Exist some attacks such as attackers that are designed which help attacker to increase access. Denial of service has indirect ways to benefit to provide benefit to attackers. Attackers will benefit from resources which attacked and belonged to a business competitor. This is real enough. (Dos) attack has another benefit such as take system offline. Exist some examples which explain different types of attack will be launched. Examples such as session hijacking. There are different between Dos and DDOS attack. The difference is TCP syn flood, teardrop attack, surf attack, Ping of Death attack and botnets.

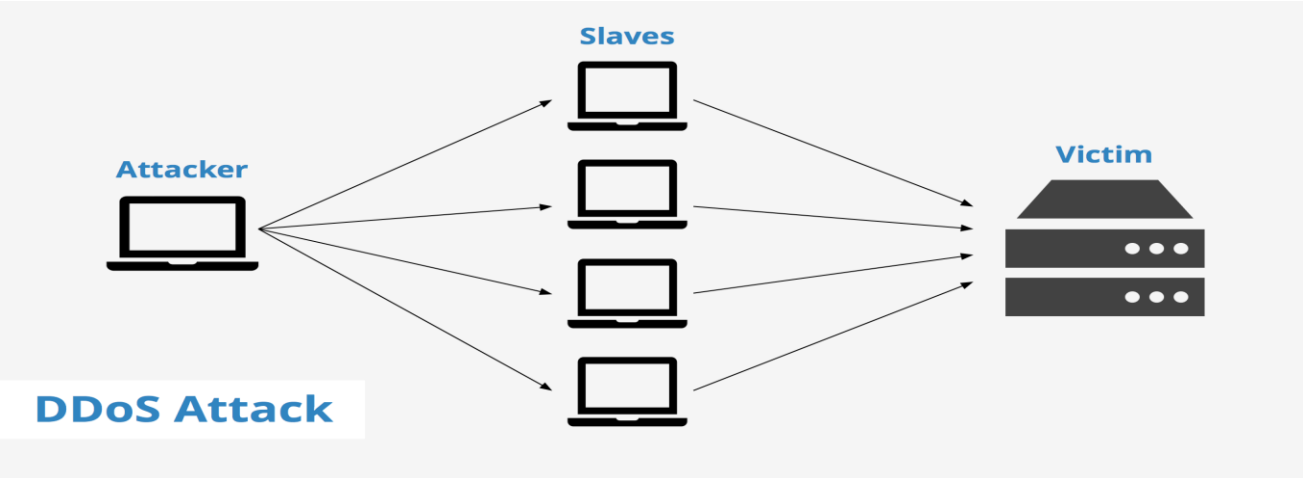

Figure 3.6 DDoS attack

3.1.6.2 TCP syn flood attack:

In this attack, an attacker makes use of buffer space during a transmission control protocol. Exist in the attacker's device small biding spar. Which targeted with connection requests, but it is not respond when respond to the target system to these requests. The result of this: the target system will stop during biding response from the attacker's device. Exist some countermeasures which used to a TCP syn flood attack:

1_put servers behind the dike of protection to stop syn.

2_decreasing time on opening connections.

3.1.6.3 Teardrop attack:

This attack leads to overlap the length of fields and dismemberment both on Ip.

Ip is limitations of internet protocol. The target system will be broken down because the system which attacked try to rebuild bale during the process, but it is filed.

This attack leads to use target cheat with traffic. IP requests targeted ICMP addresses. This attack way uses ICMP echo requests targeted at broadcast IP address. If the address of victim is 10.0.0.10. The attacker will cheat an ICMP echo requests from 10.0.0.10 to the broadcast addresses 10.255.255.255. to back IP and this request will move on to all addresses and all answers to 10.0.0.10 this process is repeatable.

Protecting your device from this attack: Directed broadcast throughout IP will be broken down. This enables us to prevent the ICMP echo broadcast request at network device.

3.1.6.4 Ping of death attack:

This attack uses Ip with volume exceeds 65,535 and is ping. So, the attacker apportions IP. It so important to system to recycle the collection of bales.

Protecting from ping of death attack: by using firewall which check bale to know the maximum size of IP.

3.1.6.5 Botnets:

It’s uses Reboot's system and Botnets is term about a lot of systems which infected by harmful programming. This programming is patronage attacker for carrying out attacks. Botnets has many locations so that it is difficult for attackers to trace.

Decreasing from Botnets:

-filtering that deny traffic from addresses and enable to follow traffic to a real source.

-Black hole filtering which deny undesirable traffic before it enters to a protected network

3.1.7 Password attack:

This attack is used to get password; it has two types of attacks.

3.1.7.1 Brute force

In this attack the attacker uses a software to try each combination of numbers and letters until it finds password

3.1.7.2 Dictionary attack

In this attack the attacker uses software to guess the password from a dictionary of passwords, today this attack does not efficient as it was in the past because the people start to use more complex password, also security system has been improved

3.1.8 Eavesdropping attack

By eavesdropping, the attackers can get on passwords and information which sent this occur when interception of network traffic

Eavesdropping has two types

Passive Eavesdropping

Active Eavesdropping

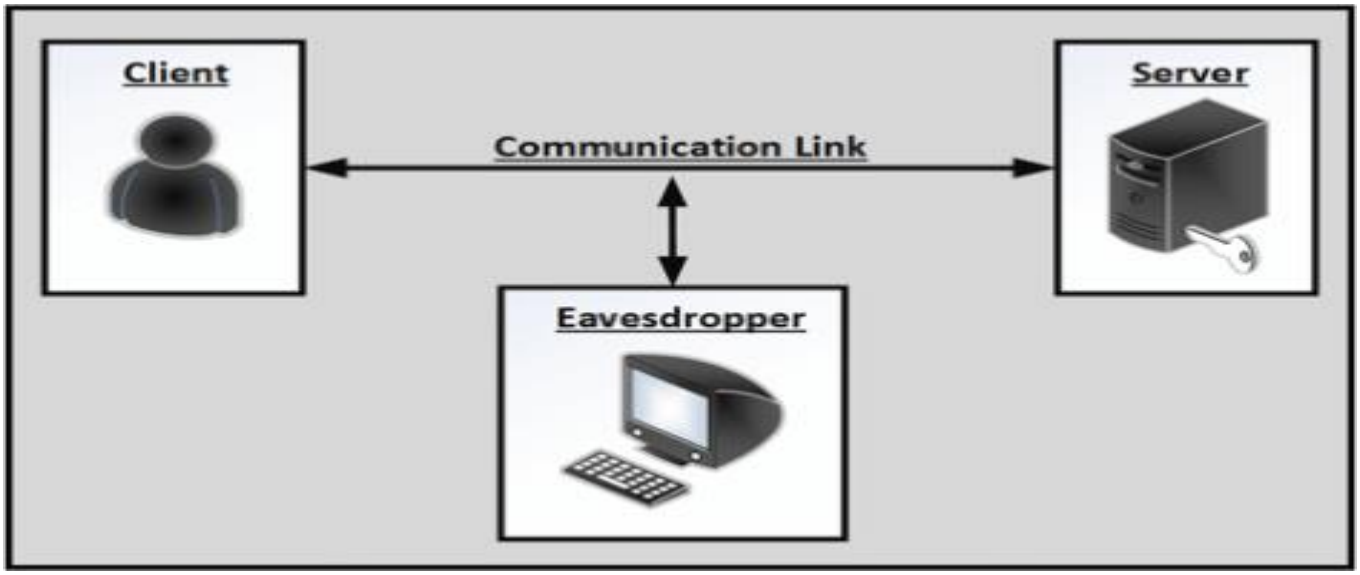

figure 3.7 eavesdropping attack

3.1.8.1 Passive Eavesdropping

The attacker detects the information by listening to the message transmission in the network

3.1.8.2 Active Eavesdropping

A hacker uses probing tempering which enable hacker to disguise himself as friendly unit.

Detecting passive eavesdropping attack is considered more important than spotting active one because active attackers require to get more knowledge of the friendly unit by conducting passive eavesdropping before.

Protecting from eavesdropping: this occurs by encryption and this is considered best counter measure for eavesdropping

3.1.9 birthdays attack:

hashing algorithms play vital role in our life software. They are used to check the integrity of a message software or digital signature. After processing a message which has fixed length. Exist MD which distinguished perfectly. There is in MD randomly two messages which form same MD and we will process this message by hash function. ATTACKER can replace the user's message with his, the receiver will not be able to discover the replacement, and the user will not discover if he compares.

3.1.10 Drive by attack:

In drive by attack the attacker search for a poor security site and start to attack it with bad scripts, these scripts will directly install malware to the system using the user browser this unlike other types of cyberattacks as it can happen without the user interaction, this could be happened on websites, popups or an email message,

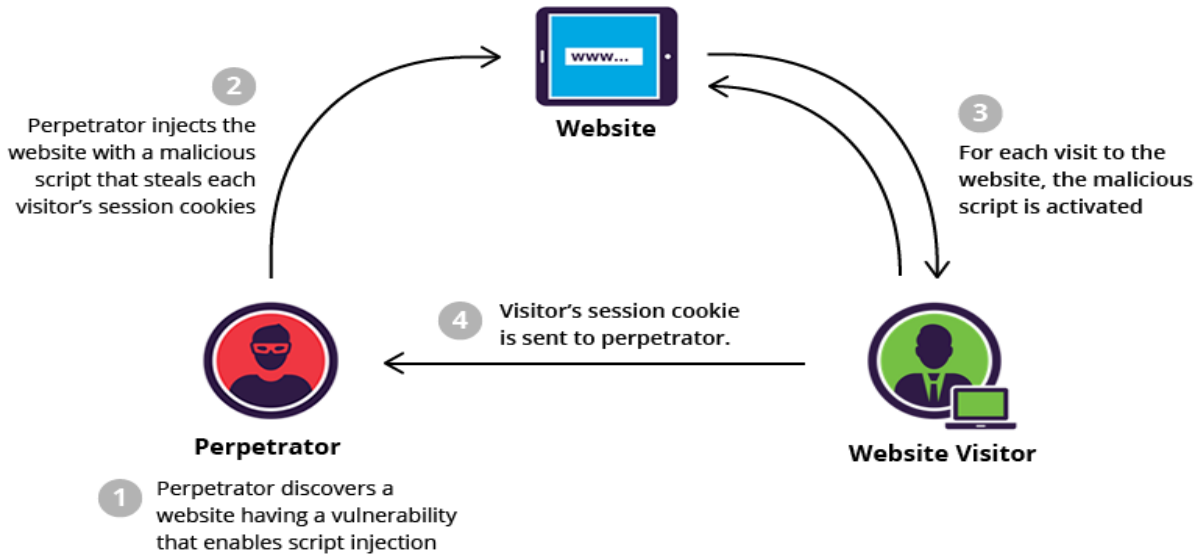

Figure 3.8 drive by attack

3.2. top ten hacking groups

3.2.1 the level seven crew

(The Level Seven Crew) This group is one of the strongest piracy groups. In 1999, it penetrated nearly 60 computer systems, including Sheraton hotels, the First National Bank of America, NASA, and the location of the US embassy in China.

This group was abolished in 2000

3.2.2 Tailored Access Operations, NSA

One of the most dangerous groups known is TAO. TAO has the best capabilities in the world, which enabled it to collect US phone data.

TAO also owns (QUANTUMSQUIRREL) that enables them to appear online anywhere and like anyone.

PRIDE also owns, it is a program that can work in iPhone and Android phones, which enables them to operate and control phones remotely, and operate the phone's microphone and listening, using manipulation programming, their programming and the geographical location. Thanks to Edward Snowden.

3.2.3 Dragonfly

It is a group from outside Europe and Russia, and it is possible that the state will support it, for its work such as the energy industry, electrical networks and control systems in the United States and Europe, and therefore it is designated as (APT).

Common attacks include Spear phishing and Water hole attacks.

3.2.4 APT28

APT28 They are a Russian group; all of its targets are linked to the Russian government.

This group uses very well-known penetration methods, but they use it with great success

. They broke into the Organization for Security and Cooperation in Europe, the location of the Polish government, the ministries of Georgia and NATO.

This group operates in no-extradition areas in the United States, so it is completely fortified

3.2.5 Anonymous

Anonymous is one of the most well-known groups. It originated in 2003 on the Fortune site, and now it has become a large group on the Internet.

Among its campaigns are the occupation movement, anti-child pornography, and anti-church Scientology. And they have certain group symbols like Guy Fawkes' masks.

3.2.6 Tarh Andishan/Ajax

The State of Iran was not satisfied with (Stuxnet) because it exposed it to some dangers, and therefore Iran decided to increase its cyber capabilities, and they did so by creating a group to be sponsored by the state, which is (Tarh Andishan), and consulting with (Stuxnet) and renting it.

(Tarh Andishan) managed to control the airport gate systems in South Korea, Pakistan and Saudi Arabia, and also penetrated the oil, communications and gas companies.

3.2.7 Morpho

Morpho is one of the prominent groups known since 2011 for their penetration of pharmaceutical, investment and technology companies.

It is a well-funded group.

They were able to access companies like Microsoft, Facebook, Apple Twitter.

It is possible that it is a small, sophisticated group that includes multiple malwares, authentication code, multi-stage command and control networks, and encrypted virtual devices.

It is also possible that you are not under state sponsorship, not hackers usually steal information from the inside to earn money

3.2.8 Syrian Electronic Army

The Syrian Electronic Army is a group of electronic pirates that deals with the Syrians and links them to Iran and Hezbollah.

Among the most famous breakthroughs that they did and showed some offensive capabilities is that they distorted many of the major western news windows, and they also succeeded in locating the opponents through some of their programs.

This group is distinguished because of its style.

Also controversial about her identity is her knowledge of colloquial English humor.

The Times reported that the Syrian Electronic Army was most likely Iranian.

Figure 3.9 Syrian electronic army

3.2.9 Chaos Computer Club

Chaos Computer Club is one of the oldest groups, it was founded in 1981 by a group of Germans.

It is now a large group of German-speaking hackers.

This group conducted many penetration operations, but after consulting legal experts first to blind themselves in a legal scope, this desire to work legally was a reason for its survival.

Among the operations it carried out was the theft of 134,000 German marks They returned the money the next day

3.2.10. Bureau 121

Bureau 121 is the main group of hacker groups present in Korea, with about 1,800 people working all over the world, and because NK's Internet infrastructure is very weak, most of the group's activity focuses on South Korea.

Among the attacks they did, were the bad games applications targeting South Korea, the destruction of bank data and broadcasting companies, and the penetration of the website of the South Korean president.

Among the groups that might be an agent of Bureau 121 are (Guardians of Peace) who hacked Sony Pictures, which cost her about $ 15 million.

3.3. Companies had been Hacked

3.3.1 (Dubai's Careem) Cyber attacks' effect

Careem is one in all the biggest firms within the Middle East and competition for Uber. In city on Jan fourteen, the corporate was attacked by information regarding fourteen million users. Such firms have some computers to store client information, and these computers are compromised. And not solely client information, however additionally drivers' information. The names of the shoppers, their emails, their itinerant numbers, furthermore because the flight locations are acknowledged.

3.3.2. (T-Mobile) Stolen Personal Data

on August 20, the cybersecurity team discovered that T-Mobile had some shortcomings in the information of some customers. Fortunately, this information did not include any financial data, such as social security numbers or credit cards, and no passwords were known, but it is expected that any of these elements were disclosed: name, phone number, email address, account number, account type. A spokesperson for the company said that about 3% of the company's clients were hacked, but the exact number was not announced. He added that he did not know whether this attack was from criminals or from the government.

3.3.3 Sony Pictures Hack 2014

One of the biggest breakthroughs in history is the penetration of the Sony Pictures Entertainment company, specifically the film industry division, due to the hand of a group of hackers called (guardians of peace). This break remained for a year in secret until the company learned about it in November 2014. The hackers were able to obtain the data of most of the employees in the company and the salaries of the most senior officials. They also managed to obtain 1 TB of films, including the movie (Fury) starring (Brad Pitt) and it was published on the Internet. The US government accused the North Korean government of this attack, after they

announced the movie (the interview), which was dirty from North Korean leader Kim Jong-Un, and the Internet was cut off from North Korea for several hours. The company's revenue decreased during this period by 11.7% to $ 1.63 billion, due to weak sales for home entertainment and theater, after the number of hackers' theaters exported to the movie (The interview). The losses were eventually estimated at 15 million dollars.

3.3.4 (Cathay Pacific Airways) Passenger Data Hacking

on Wednesday, in the airline (Cathay pacific), data about 9.4 million passengers were hacked. The company said in a report that 8600,000 passport numbers have been reached, and about 245,000 Hong Kong identification cards numbers, 403 expired credit card numbers. The company has informed the Hong Kong police of what happened, and it was observed that there was no misuse of any of these data.

Chapter 4: Ethical Hacking

4.1. The concept of Ethical Hacking:

Ethical Hacking identifies the vulnerabilities or weaknesses in a computer system or a network and devises a strategy for protecting those vulnerabilities.

Hacking is process of identifying and exploiting vulnerabilities in computer and network systems to gain access to these systems. Password Cracking is a type of hacking used to gain access to the system. Hacking is a fraudulent act that allows criminals to invade a system, steal personal date, or perform fraud in any manner via digital devices.

4.2. The Ethical Hackers:

A person who finds and exploits vulnerabilities in a network or a computer system is called a hacker. He or she may have very a Devance'd skills in programming and a working knowledge of network or computer Security Hackers can be categorized into six types:

(white hat hacker, black hat hacker, and more)

4.2.1 Benefits of Ethical Hacking:

The sudden rise in the demand for ethical hacking that is being noticed is a result of technological advances that lead to many threats in the technology sphere in the world. An ethical hacker serves as an organization by protecting their system and its information from illegal hackers as cyber-attacks and cyber terrorism is greatly growing.

4.2.2. Beneficiaries of the Ethical Hacker:

With the increase in multinationals in a place where the danger has increased, especially for large companies and government institutions, terrorist organizations are financing to breach data systems and then losing confidence and information to the victim or extortion in huge sums, so any government institution now or a large company knows how much and the importance of moral infiltration, so it cannot be Safety Once your doors are closed, the beneficiary here is the one who employs the ethical intruder that he has maintained customer confidence and preserved his information from penetration and extortion.

4.3. Important terms in Ethical Hacking:

4.3.1. having Authorization:

Authorization is a security mechanism to determine access levels or user/client privileges related to system resources including files, services, computer programs, data and application

features. This is the process of granting or denying access to a network resource which allows the user to various resources based on the user's identity.

4.3.2 Identity Confirmation:

You can make a strong argument that the entire field of cyber security rests almost completely on identity verification and access control. Without those two functions, almost no other security technique matters. Every other element of security depends on the system identifying the user and validating their permissions to various objects.

4.3.3. Vulnerability Assessment:

It is the process of identifying vulnerabilities in the computer systems networks, and the communication channels. It is performed as a part of auditing and also to defend the systems from further attacks. The vulnerabilities are identified, classified, and reported to the authorities so that necessary measures can be taken to fix them and protect he organization.

4.3.4. Gap Assessment & Testing:

The process also gives you a more in depth look at your business practices which can help you discover new opportunities for improvement. In short, a gap analysis provides the information and resources needed to meet your unique business goals and reach your full potential.

4.4 Phases of penetration testing:

4.4.1 Planning and Define:

Defining the scope and goals of a test, including the systems to be addressed and the testing methods to be used. Gathering intelligence (e.g., Network and domain names, mail server) to better understand how a target works and its potential vulnerabilities.

4.4.2 Scanning:

The next step is to understand how the target application will respond to various intrusion attempts.

This is typically done using:

1-Static Analysis:

Inspecting an application's code to estimate the way it behaves while running.

2-Dynamic Analysis:

Inspecting an application's code in running state.

4.4.3 Gaining Access:

This is stage uses web application attacks, such as cross-site scripting, SQL injection and backdoors, to uncover a target's vulnerabilities. Testers then try and exploit these vulnerabilities, typically by escalating privileges, stealing data, intercepting traffic.

4.4.4. Maintaining Access:

The goal of this stage is to see if the vulnerability can be used to achieve a persistent presence in the exploited system -long enough for a bad to gain in- depth access.

4.4.5 Analysis the result:

The results of the penetration test are then compiled into a report detailing:

1-Specific vulnerabilities that were exploited.

2-Sensitive data that was accessed.

3-The amount of time the pen tester was able to remain in the system undetected.

This information is analyzed by security personnel to help configure an enterprises WAF setting and other application security solutions to patch vulnerabilities and protect against future attacks.

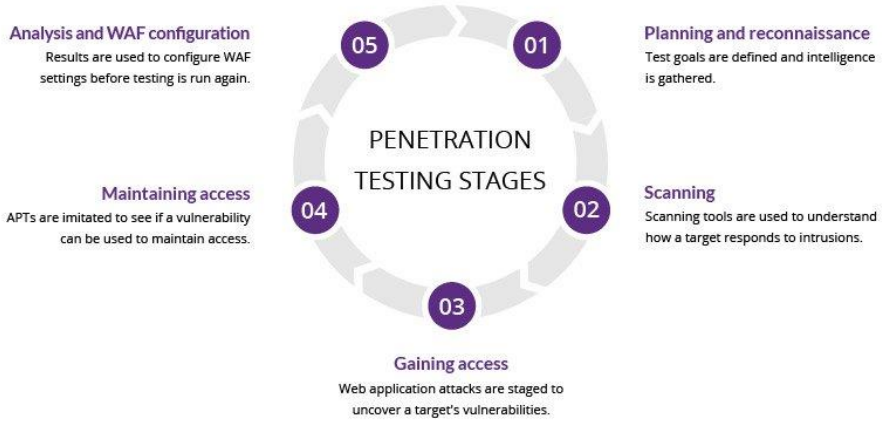

figure 4.1 Penetration testing stages

Chapter 5: Cybersecurity field

As we all know that cyber security became an important field in our life because it reduces the quantity of dangers that we will face if our sensitivity information be attacked

Many organizations have emerged in cybersecurity field, which works to protect people by protecting their devices and their digital accounts, and the most important of these organizations are CISSP and CISCO

figure 5.1 CISCO

5.1 Definition of cyber security

It's known that cyber security working on protecting our data, computer systems and networks from hacking attempts and preventing hackers from access to sensitive information.

An effective cyber security system consists of several protection applications that are distributed consistently to provide the necessary protection for user data and related networks, and this happens in all organizations, so individuals and digital devices must work together to build an effective defense and security against cyber-attacks.

5.1.1 Cybersecurity for people

There is user who must understand basic data in cybersecurity such as choosing strong password, be careful from any attachment with an e-mail, learn more about basic of cyber security and obey rules to protect your accounts.

5.1.2 Cybersecurity processes

in any organization it must have rules to deal with any successful attack, to be able to recover their data after successful attacks and close gaps.

5.1.3 Cybersecurity technology

as we know that technology is an important thing because it given the individuals and organization tools to deal with attacker and it Is known that we must protect three main entities

End points like (computers, smart device)

Networks

5.2 The importance of cyber security

Cyber security is concerned with protecting networks, systems and programs from cyberattacks. These cyber-attacks mostly aim to spy on or destroy confidential information or extort money from users of electronic devices; for this time everyone today relies on information security programs. On an individual level, cyber security attacks can result in everything from identity theft, attempts Blackmail, loss of important data like family photos.

5.3 common ways to keep your data safe

5.3.1Enable Tow-factor authentication

We use it to make sure of the protection of our account, because if even somebody knows your password, they won't be able to access your account or get your Information Also,

there are many apps help us to use it such as

LastPass

Microsoft

Authy

5.3.2 Using the right WIFI

There are steps enable people the choose the right WIFI and router such as, the router should be dual-band or more. It should have a mulit-core processor. Verify online the real-life speed of the router buy. Router naming conventions should not take into account when making your buying decision.

5.3.3 Using effective password

Your password is very important so it must be very confidential because if you reach anyone else's hand this could ruin your life, there are ways to choose an effective password that protects you from hacking such as,

never reuse one

Choose a long and strong password and it should be easy to remember

Let a password manager do it for you

Don’t update it regularly unless you are forced to

Skip the secret question

5.3.4 Anti-malware

Microsoft has released a program that comes with the computer called (Windows Defender), an application that works like anti-virus programs, but it is also the first program to get updates and defenses against viruses and hackers.

5.3.5 Use the latest version

Regardless of your operating system, you need to download the latest version

Recommendation

-you must know how to protect against piracy to maintain information security.

-there are many types of hackers and each has a different mission.

-you can learn about many programs to protect information and how to deal with it.

-learn about the protection programs and how they were programmed.

-take advantage of ethical piracy to secret information.

-knowing about malware attacks will help you avoid them.

-you will know cyber security processes to prevent your information from being compromised.

Conclusion

- Hackers are clever people who exploit the vulnerabilities of computers to penetrate them

- hacking is useful in many ways, such as: hacking a program and identifying the gaps in it to avoid them

- Hackers are trying in various ways to obtain sensitiveity data

- There are many types of hacking, most notably 1- white hat hacker
and 2-Black hat hacker

- There are many types of hacker risks such as: The hacker obtaining very senstivity data, such as a bank account

- We got to know the top 10 hackers that are not only dangerous for people or individuals, but even for major companies

- ethical hacker is a person trying to find and fix holes in any program

- Cyber security is one of the most important areas in the current era to increase the number of devices that an individual use and to increase their risks, such as: data theft and digital fraud

References

What is hacking? Introduction & types

https;//www.guru99.com/when-is-hacking-an-introduction,html

What is hacking

http;//www.malwarebytes/hacker/

Types of cyber security

https;//www.educba.com/types-of-cyber-security/

What is cybersecurity

https;www.forcepoint.com/cyper-edu/cybersecurity

Types of hacking

https:www.digitalvidva.com/blog/types-of-hacking/

Five phases of hacking

https://www.geeksforgeeks.org/5-phases-hacking/

Top ten group of hacking

https://turbofuture.com/internet /most-powerful-active-hacking-groups

Types of cybersecurity attacks and hacking techniques

https://www.rapid7.com/fundamentals/types-of-attacks/

What is ethical hacking

https://www.eccouncil.org/ethical-hacking/

Books

Penetration testing

Hacking the art of exploitation

Cybersecurity