Muhammad Tashfeen Shinwari

Cyber Criminology

The Mentality, Vision and Aim behind Cybercrime

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

12 December 2015

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Muhammad Tashfeen Shinwari Cyber Criminology The Mentality, Vision and Aim behind Cybercrime 51 pages 12 December 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Software Engineering and IT security
Instructor(s)	Kimmo Sauren, Senior Lecturer

The goal of the project is to gain a good understanding of what kind of different cyber-attacks are carried out in modern times and how by being cautious, one can avoid becoming a victim. This study will also shed some light on what mentality lies behind these attacks and what the most common intensions are for these types of attacks.

The economic effect of computer crime is often overlooked. Only by knowing some fundamental principles, one can better prepare oneself against these crimes and also protect personal assets from these threats.

The project is also aimed to give some useful guidelines which can be benefited from not only by users who are using computers for their daily lives but also by nontechnical people in general. Nowadays more and more tasks are dependent upon computers and keeping up with the security issues on the Internet cannot only save people from losing data on a personal level but also help companies protect their assets.

Different printed and electronic media were used in order to gather the facts and figures about cybercrime. A few software were also used to mimic some of the attacks on my personal network in order to gain in depth information.

The findings in the thesis indicate that there exists no perfect protection against cyber threats. However, many of the cyber-attacks that are mentioned in the thesis are carried out successfully because a normal computer user lacks the necessary information regarding computer security.

Computer user, not only on a personal level but also on an organizational level, should be trained to adopt safety measures against cybercrime. Also, the end point user awareness should be encouraged as it can be the strongest defence against such cyber-attacks.

Keywords	cyber attack, hackers, viruses, malware, security

Contents

1 Introduction 1

2 Brief History of Cybercrimes 2

3 Types of Hackers 3

4 World of Malware 4

4.1 Computer Viruses 5
4.2 Worms 7
4.3 Trojan Horses 10
4.4 Spyware 13
4.5 Scareware 14

5 Network Attacks 15

5.1 Active Attacks 16
5.1.1 Denial-of-Service(DoS) 17
5.1.2 Man-In-The-Middle 18
5.1.3 Session Replay 19
5.1.4 Identity Spoofing 20
5.1.5 Password Based Attacks 21

5.2 Passive Attacks 22
5.2.1 Wiretapping 22
5.2.2 Port Scanner 24
5.2.3 Idle Scan 27

6 Database Attacks 29

6.1 SQL Injection 30
6.2 Excessive Privilege Abuse 33
6.3 Privilege Elevation 35
6.4 Weak User Authentication 35
6.5 Weak Audit Trail 36
6.6 Exposure of Backup 37

7 Tools of the Trade 38

8 Conclusion 39

References 41

Terms

Backdoor	A means of accessing a computer that bypasses security mechanism
Black hat hacker	People who illegally exploit vulnerabilities in systems for personal gains
Cybercrime	Illegal activity that uses a computer as a primary means of commission
Data Integrity	Accuracy and consistency of data without any unauthorised alteration
Encryption	Conversion of data into cipher text not easily understood by anyone else except the authorized parties
Firewall	A network device which restricts access to the network
Grey hat hacker	People who exploit weakness in systems to bring awareness to the owners without any malicious intent
Hacker	A person who exploits weaknesses in a computer system
Malware	Malicious software designed to infect a computer system
SQL injection	An attack which is used to penetrate database systems using unauthorised SQL commands
Virus	A program or a code written to be installed illegally on the system often to cause damage to the system
White hat hacker	Security experts dedicated to expose vulnerabilities and fix them before malicious hackers can exploit them.
Zero day vulnerability	A security hole in software unknown to the vendor

Abbreviations

DoS	Denial-of-Service
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IPS	Intrusion Prevention System
MBR	Master Boot Record
MITM	Man-In-The-Middle
RAT	Remote Access Trojan
RDBMS	Relational Database Management System
SQL	Structured Query Language
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VBR	Volume Boot Record
Wi-Fi	Wireless Fidelity

1 Introduction

Technology has a big influence on our daily lives. Electronic devices, computers and mobile phones have become a necessity. The Internet especially is used as a means of communication with the rest of the world. It has become a tool not only for communication but also for sharing information, shopping, socializing and many more activities. Like many other inventions, the Internet has its drawbacks such as scamming, stealing, user privacy issues, blackmailing and spamming. These drawbacks are used by the hackers as a source of amusement and also as means of income. In order to overcome these issues, and make the Internet a safer place, there is a constant battle in the community. On the one side are the security firms and on the other, the hackers. Security firms try to provide protection against hackers while on the other hand the hackers try to infiltrate the security measures and compromise computer systems by exploiting these vulnerabilities.

Computer viruses, worms, Trojan horses and many other such tools are used by the attackers to carry out crimes. Organizations are spending billions of dollars every year to protect themselves against such threats. Day by day these attacks are getting more and more sophisticated so people need to be up to date on security policies in order to be less vulnerable on the Internet. Modern malicious programs are harder to detect and can easily infect computers because like security firms, there are professional criminal organizations spending a great deal of money to invent new ways and techniques to compromise the systems.

The purpose of this project is to educate computer users about attackers, their ways of targeting people/computer systems and of ways of preparing a computer user against the attacks that can change their lives forever. While some solutions can be easily implemented and are well-known practices, computer users and many organizations still disregard them and solely rely on their antivirus programs to protect them against all the possible cyber-attacks. While antiviruses are good practise, they are nowhere near providing a complete secured system. It is up to the users to make small changes in their working habits. Although it might seem as an extra effort at the time, it can save them from all problems that lie ahead if proper measures are not taken.

2 Brief History of Cybercrime

Cybercrime started out as hackers tried to gain illegal access to computers either for the purpose of thrill or for accessing sensitive and classified information. Eventually the hackers started using viruses for phishing scams and credit card thefts on both personal and business levels.

In the early 1970's a computerized phone system became a target. John Draper, a computer programmer and a phone phreak, figured out the correct codes and tones to make a free long distance call [1].

In January 1986, the first computer virus called **Brain** was released. It was a virus for MS-DOS and infected the boot sector of storage media [2]. The viruses between the 1980's and the early 1990's were only spreading on floppy disks and these viruses would jump from one PC to another only by physically moving the floppy disk between the computers. However, most of these early viruses such as **Brain**, **Stoned**, **Cascade** and **Form** were not written for any benefitting purposes. Many of them were created as a joke e.g. **V-sign**, **Walker** and **ELVIRA** viruses, which would display an animation on the victim's display to let him/her know that the PC had been infected. They did not cause damage to PCs unlike the **Michelangelo** virus in 1992 which would override everything on the victim's hard drive on a certain date and was considered a destructive virus [3].

Later in the 1990's, the computer viruses became more advanced. In 1995 came viruses which would not infect the floppy disks or the program files but the user documents. The **Concept** virus (Macro virus) was the first of its kind which would affect the word documents, meaning every time the victim would share a word file with someone else, the virus would be shared as well [4].

Another well-known example is the **Happy99** virus, which is the first email virus in history. It would greet its victim happy new year 1999 and then email itself further. Then came the viruses which were a combination of the Macro virus and the email virus e.g. the **Melissa** virus, which would infect a word document and then forward the infected file to other people on the victim's address book [5].

In 2003, **Fizzer** virus gained popularity as it was the first of its kind of virus that was written in order to actively make money by taking over the infected computers and use them to send spams. Other viruses at the time were for example, **Sobig, Mydoom** (email worm), **Bagel** (email worm), **Netsky**, **SDBot**, **Cabir** (the world's first mobile phone virus) and **Storm** worm [6].

Stuxnet, a computer worm, discovered in June 2010 is looked upon as a game changer in the history of cyber-attacks. It is one of the most sophisticated malware and the first case of cyber sabotage ever seen [7].

From the years 1980's to the year 2015, malware have advanced and are becoming more sophisticated day by day. Nowadays, it is almost impossible to detect some malware and many of the malware are being detected to have zero day vulnerabilities. In other words, hackers have managed to find security holes in the software, unknown to the vendor of that software. Security experts are on a constant battle against these cyber criminals, trying to make the internet a safer place for all of its users.

3 Types of Hackers

The word hacker has a different meaning for different people. Usually the definition affiliated with the term hacker is a person who secretly gets access to a computer system in order to gain some sensitive information and causes damage to/through the system. However, it is important to understand that not all hackers have criminal intentions. There are hackers who are working day and night just to keep a user's sensitive and personal information safe and protect the irreplaceable data that can be priceless to the user.

One needs to be aware of which hackers can be trusted and which hackers can be the cause of a distress. Listed below are a few types of hackers that might have an effect on a user's life and should be distinguished.

White Hat Hackers are security experts who are responsible for making sure that a company's and its client's sensitive data is secure and out of the reach of the people who can use that information illegally for personal gains. These IT professionals are fighting daily against the threats of the hackers called Black Hat Hackers.

Black Hat Hackers are actually the cyber criminals and one needs to be aware of them. The term hacker is mostly used to refer to black hat hackers. Black hat hackers are professionals who are highly trained and qualified to carry out cyber-attacks against the community. They are responsible for breaking into computer systems/networks and creating computer viruses in order to meet some set goals. Mostly their intensions are financial benefits. However, their goals vary from trying to make some money by stealing a person's credit card information to company espionage and even to government surveillance.

Grey Hat Hackers also referred to as crackers. They are IT professionals who possess skills of a black hat hacker but use those skills for good purposes. They try to exploit vulnerabilities in the system and fix them before black hat hackers could get to them and take advantage of them.

Script Kiddies are amateur hackers trying to make names for them. They use borrowed programs to hack into weak computer systems/networks and websites. However, the mentality behind such attacks is not financial benefits but a little fame for themselves.

Hacktivists are motivated to hack into systems for political, religious and other social purposes. Their intensions are not to make money but to expose their targets for better or worse.

Cyber Terrorists are by far the most dangerous of all hackers and are highly trained with a wide range of skills and goals. Usually their goals are to disrupt the critical infrastructures for religious or political beliefs.
[8].

4 World of Malware

The word malware stands for "Malicious Software". It is a collective term for viruses, worms and Trojans that get installed on the victim's computer without his/her consent. They can be used for a wide range of purposes, from crashing victims devices to monitoring and controlling their online activities. Malware are used by cyber criminals to steal personal information, commit frauds and send spams. Over time, malware have

become more sophisticated and harder to detect. A few of the most basic malware are explained below.

4.1 Computer Viruses

“A Computer Virus is a small program designed to cause some kind of damage in the infected computer, by deleting data, capturing information, or by altering the normal operation of the machine”[9].

A computer virus does not spread on its own. It needs human interaction in order to spread and causing destruction. A computer virus can range from being slightly disturbing to causing a total destruction. Depending upon its purpose and ways how it is transferred from one PC to another, computer viruses can be broadly divided into three categories.

Boot Virus or a boot sector virus, also known as a memory virus, is most commonly spread using physical media e.g. through an infected floppy disk or a USB drive. This virus stays in the boot sector of the floppy and in the Master Boot Record (MBR) of hard disks. The MBR is responsible for selecting which Volume Boot Record (VBR) to load based on the instructions or the user input. A boot virus will run itself before the operating system is loaded [10]. A typical operation of the boot sector virus is shown in figure 1.

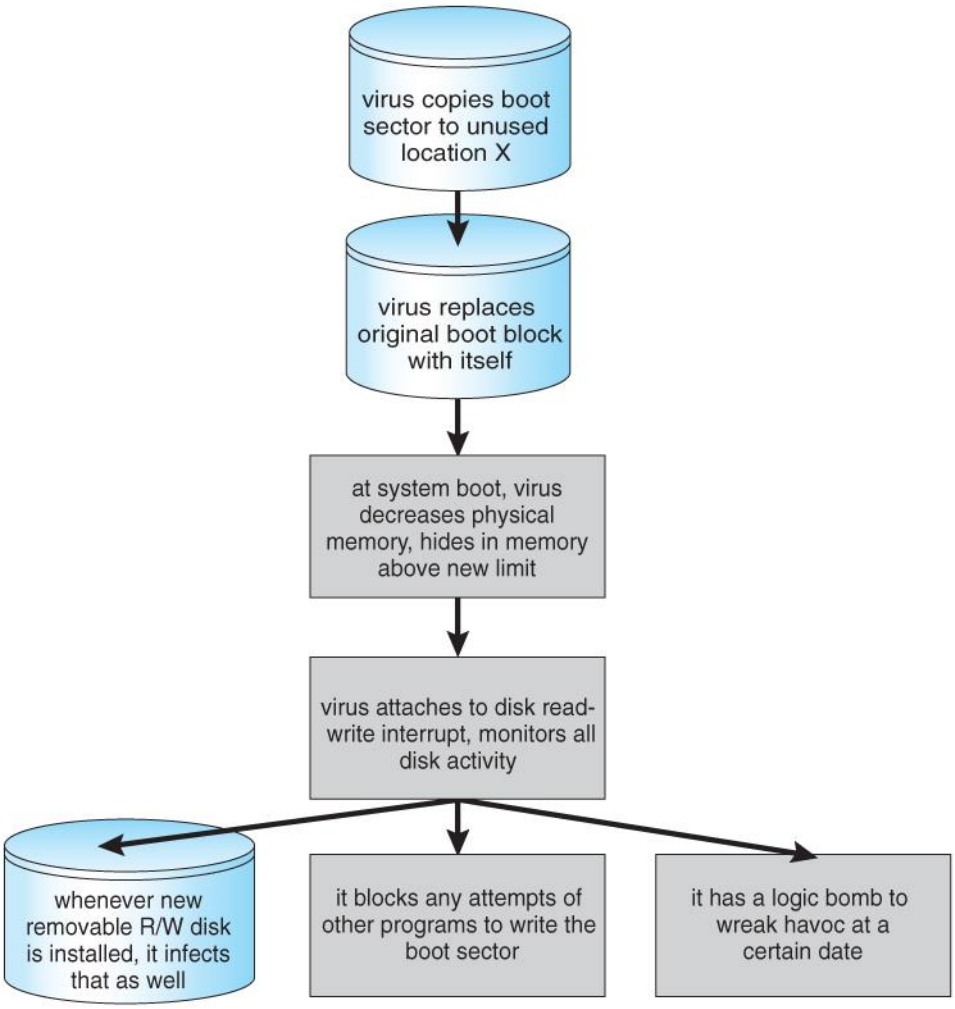


Figure 1. Operation of a boot sector virus [10]

Figure 1 illustrates that the boot sector virus is installed in the boot sector of the computer system. Once the user starts the system, the virus prevents it from running the default operations i.e. loading the operating system and runs its own instructions and causes damage to the system. It also transfers itself to any removable disk and infects the computers on which the disk has been used. Boot viruses are very difficult to detect and the victim very often does not know about their existence unless he or she runs a virus scan. However, the boot sector virus will not infect the computer if the virus is introduced after the boot-up or when the computer is already running the operating system. The most common examples of boot sector viruses are **Brain** virus, **Polyboot.B** virus and **Mebroot** rootkit [11]. In order to avoid being effected by a boot sector virus, it is advised to continuously update the antivirus protection program and preferably choose antiviruses that have a large list of boot virus definitions in the registration. If

all the efforts of removing the virus result in vain, the hard drive may need a reformatting in order to get rid of the infection.

Macro Viruses are the most commonly used viruses that exist as macros (scripts) that run automatically by certain macro-capable programs to infect and duplicate the documents. These viruses are generally made for Microsoft Office and exist in word processing documents and spreadsheets e.g. Concept Virus and Melissa Virus [12]. A user can realize the existence of a virus e.g. if the computer is running more slowly than normally or if a user is prompted for a password on a file which does not need a password or if the documents are saved as template files. There are various ways how a user can avoid getting effected by such viruses. One safe way is to use a digital signature. These signatures will confirm if the file is coming from the source (the author) or if it is a tempered file. Of course updating the security virus program will also help in providing a better protection for the system.

Program Viruses infect executable program files usually with extensions ".BIN", ".COM", ".EXE", ".OVL", ".DRV (driver)" and ".SYS (device driver)". These programs are loaded in the memory during execution, along with the virus. Usually the program viruses hide themselves under the name of other legitimate programs and the victim, thinking that he/she is installing a particular program, is deceived and a malicious program in installed instead. A common example of such viruses are **Sunday** Virus and **Cascade** Virus.

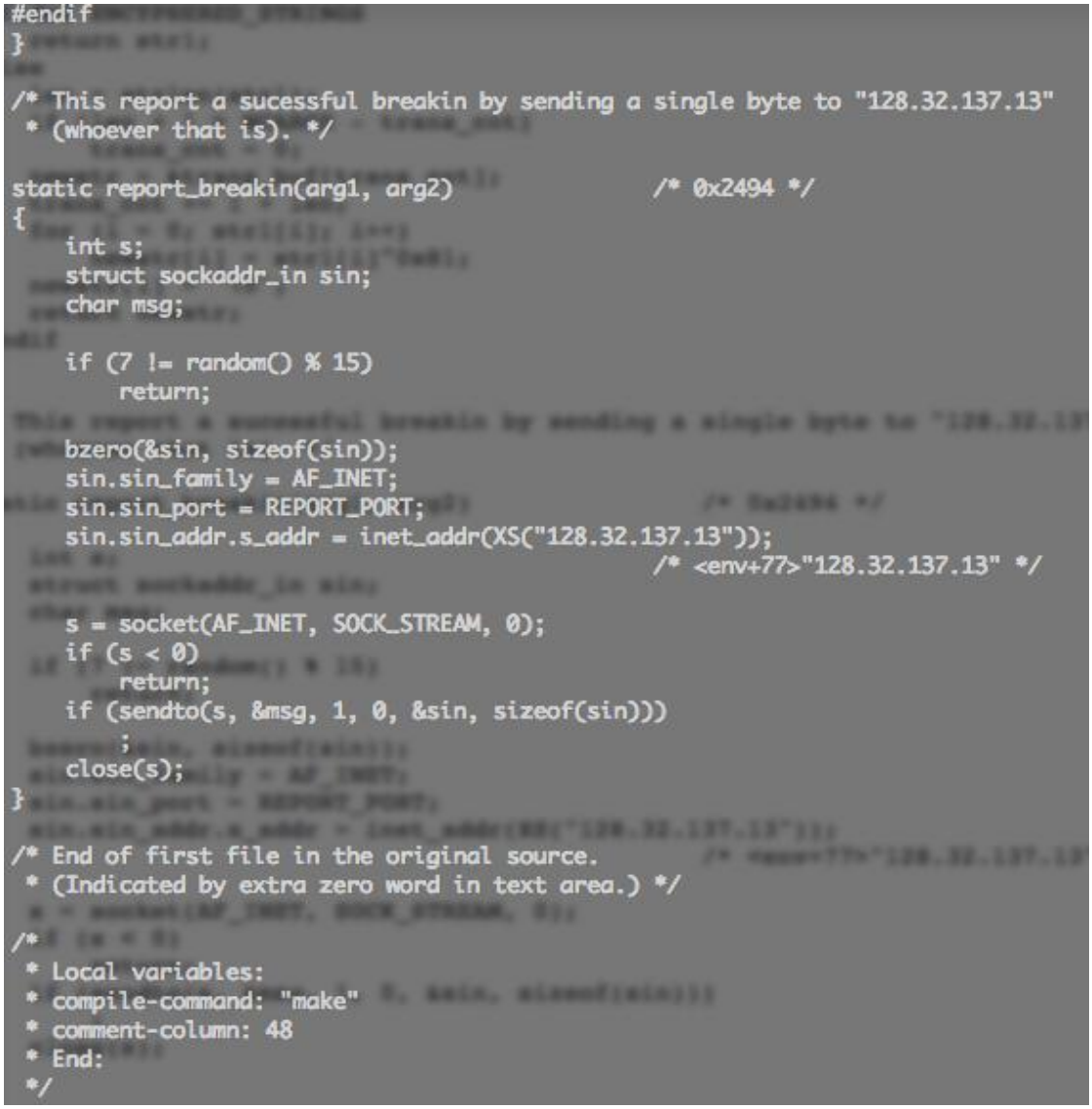
A good practice is to avoid running any executable files, which are from unknown sources and check the certificates before running any file. It is also advised to create a system restore point before installing any new program because even if the malicious program compromises the system, the user could choose to go back to the settings before the installation of the program. On Windows machines, one should always install windows updates in order to patch the vulnerabilities.

4.2 Worms

Worms are very often mistaken for viruses. However, unlike viruses, worms do not require any human interaction and are more dangerous than viruses. An infected computer, rather than sending out a single worm, can send hundreds and thousands of computer worms causing devastating damages to society.

Computer worms are self-replicating malicious codes that spread across computers which are vulnerable and infect them. They do that by attacking the computer network and then spread to the computers which have weak security policies. They are responsible for causing harm to systems from deleting files to forwarding them by emails and by consuming bandwidth to installing backdoors in the computer system. A backdoor is a means of accessing the computer system by bypassing the security mechanism. Worms can also open TCP ports in order to create a network security hole for the other applications to take advantage.

A particularly notorious incident occurred in 1988 when a computer worm named the **Morris** worm was created by Robert Tappan Morris. A copy of the Morris code is shown below in figure 2.



```
#endif
}

/* This report a sucessful breakin by sending a single byte to "128.32.137.13"
 * (whoever that is). */

static report_breakin(arg1, arg2)                /* 0x2494 */
{
    int s;
    struct sockaddr_in sin;
    char msg;

    if (7 != random() % 15)
        return;

    bzero(&sin, sizeof(sin));
    sin.sin_family = AF_INET;
    sin.sin_port = REPORT_PORT;
    sin.sin_addr.s_addr = inet_addr(XS("128.32.137.13"));
                                                 /* <env+77>"128.32.137.13" */

    s = socket(AF_INET, SOCK_STREAM, 0);
    if (s < 0)
        return;
    if (sendto(s, &msg, 1, 0, &sin, sizeof(sin)))
        ;
    close(s);
}

/* End of first file in the original source.
 * (Indicated by extra zero word in text area.) */

/*
 * Local variables:
 * compile-command: "make"
 * comment-column: 48
 * End:
 */
```

Figure 2. Example of the Morris code [13]

It is argued that the Morris worm was released either accidently or prematurely. The Morris worm was not written for destructive purposes and it only caused the computer to slow down because of all the unnecessary processing caused by it [13]. However, it infected 6000 university, military and research center computers and caused hundreds of thousands of dollars' worth of damage [14]. The worm was designed to be undetectable but due to a design flaw, it made far more copies of itself than initially anticipated by the developer.

A series of measures should be considered in order to ensure a worm free system. Scanning any suspicious files with a good antivirus program helps accomplish that goal. Keeping the antivirus up to date and performing a periodic scan is also recommended.

4.3 Trojan horses

Trojan horses are malicious computer programs that can perform actions on the victim's computer without their consent. Even though Trojan horses cannot self-replicate as viruses and worms, they can cause as much damage to computer systems. There are a number of actions that a Trojan horse can perform on the victim's computer, including blocking data, modifying data, deleting data, copying data or even disrupting the performance of the computer system/network.

The Trojan horse is generally the malicious code that is hidden inside a safe legitimate program. In some cases, Trojan horses are spread deceiving the user into believing that they are programs that will remove viruses from the computer but when run by the victim, they instead become installed and allow the hacker to get control of the victim's computer. Trojan horses can be subcategorized according to the actions they perform on the victim's computer. Out of many, a few types are the following.

Backdoor (Remote Access Trojans) also known as Remote Access Trojan (RAT), allows the hacker to remotely control the infected computer. Very often, backdoor Trojans are used to unite a group of infected computers and form a botnet/zombie network, which is then used for criminal purposes by hackers.

Destructive Trojans at times are used just for the purpose of causing inconvenience to the victim. They also help to make some financial benefits for the hacker in the process. E.g. Ransom Trojan can encrypt a user file in a way that the owner of the file is no longer able to access the file. Upon receiving the ransom, the hacker promises to restore the file or the computer system to its normal behavior. An example of one ransomware is shown in figure 3.

Figure 3. An example of Ransomware [15]

Figure 3 is one of many examples of ransomware where the personal files of a user are encrypted and the user is not allowed to access the files unless he or she pays the attacker to decrypt his/her files. Another common ransomware which I myself have come across is called the Poliisi virus. The Poliisi virus can be distributed through several means. Malicious websites or a legit website that has been hacked can infect the victim's machine by exploiting the vulnerabilities in the system. It can also be sent as an email attachment and upon opening, can infect the system. A screenshot of the Poliisi virus is shown in figure 4.

Figure 4. Poliisi Virus screenshot [16]

This ransomware locks the screen of the computer and does not allow the user to access his/her computer and displays a message with a demand to pay 100€ to unlock

the machine. It uses a bogus message in order to scare its victim into paying. It also has the ability to access the victim's webcam. Even though there are different ways found on the Internet to get rid of this ransomware, users are advised to avoid opening attachments or links from unknown senders and avoid visiting websites that look fishy.

Another example of destructive Trojans is the security software disabler, where the Trojan takes out as many security programs as it can and leaves the victim unprotected and vulnerable for the next attack.

Proxy Trojans allow the hacker to use the infected computer as a proxy server. It provides the hacker with the possibility of committing frauds such as stealing credit card information or even to launch malicious attacks against other networks using the infect computer.

4.4 Spyware

Spyware are computer programs that gather user information of the infected PC and send that information through the Internet to the hacker. Spyware are most commonly spread bundled with some free programs which are available online.

Spyware are similar to Trojan horses as they are installed unwittingly by the user while trying to install something else. Once installed on the computer, spyware can monitor keystrokes, read cookies, snoop chat programs or scan files on the hard drive and send the information back to the hacker. The information collected is then used by the hacker either for advertising or for selling it to the third parties.

A common example is the Elf Bowling game introduced in the 1990's. It was packed with a spyware which reported the user information to its developer [17]. Another example is CoolWebSearch (CWS) spyware. This spyware was introduced in May 2003 and it infected the Windows Operating system. Once installed on the PC, it would change the browser's homepage to websearch.coolwebsearch.info as shown below in figure 5.

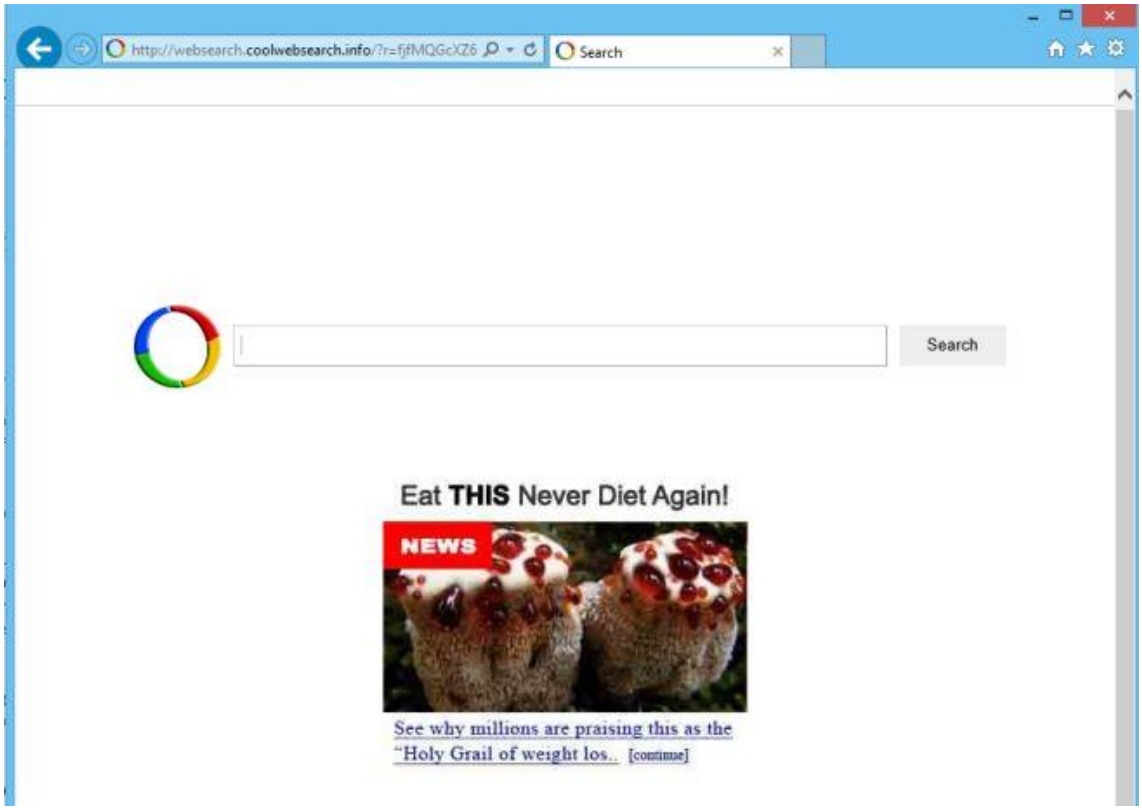


Figure 5. Example of CoolWebSearch homepage [18]

Coolwebsearch spyware had the capability of creating pop-up ads that would redirect the user to other websites, collect sensitive and private information of the user and would also slowdown the infected computer.

A number of anti-spyware programs are available on the Internet e.g. Spybot and Malwarebytes, which are worth buying. Some other commonly used programs as anti-spware include Webroot Spy Sweeper and eTrust Pest Patrol. Users should be careful while opening emails from unknown sources and should try to stay away from ill-reputed websites. A good firewall should also be used in order to hide a user's PC from attackers who would try to access the system through the Internet.

4.5 Scareware

Scareware, also known as smitfraud or rogue security software, is designed to trick its victims into buying or downloading potentially dangerous software. It displays a message on a pop-up screen such as infected files have been found on the system and the user must click to remove those files. However, when a user clicks on the screen, unwittingly the malware can be installed on the computer. At times the software asks the

user to buy a program to remove those viruses and that program not only causes the user to lose money but also contains real malware. A common example is shown below in figure 6

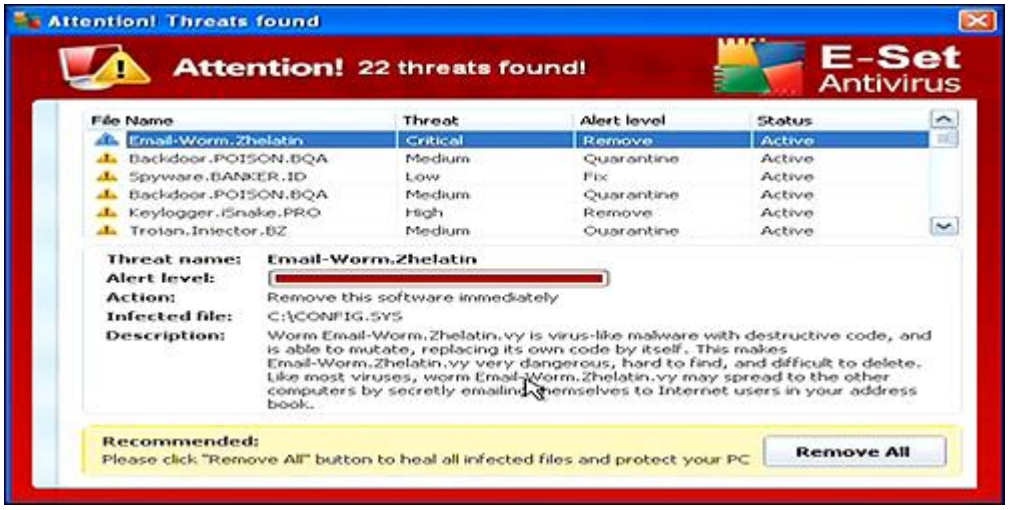


Figure 6. An example of the pop-up screen of scareware [19]

Figure 6 illustrates a typical scareware example where the screen pops up appearing as if it was from the antivirus installed on the computer. However, in reality it is just scareware and will either install malware on the computer or will ask the user to purchase a program and then install the malicious program, thus infecting the computer.

A totally secure system is hard to accomplish, but in order to be best protected, the system should be updated for patches. Programs like Adobe reader, flash player and Java should be updated with the latest releases as many times as these programs are used to compromise a system.

5 Network Attacks

Over the passage of time, hackers have learned ways of compromising not just a single computer but an entire network using one infected computer. Therefore, network security is a fundamental component while designing a network. A network security defines the user privileges of what a user can and cannot do with the network component and resources. Therefore, it is of utmost importance to be aware of the security threats that might compromise the entire network because of one compromised system. In the unlikely event of an attack, a system must limit the damages and should be able to recover as quickly as possible.

Network attacks are very common nowadays and based on the type, they can be classified into two wide categories, active attacks and passive attacks. A typical operation of both types of attacks is shown in figure 7.

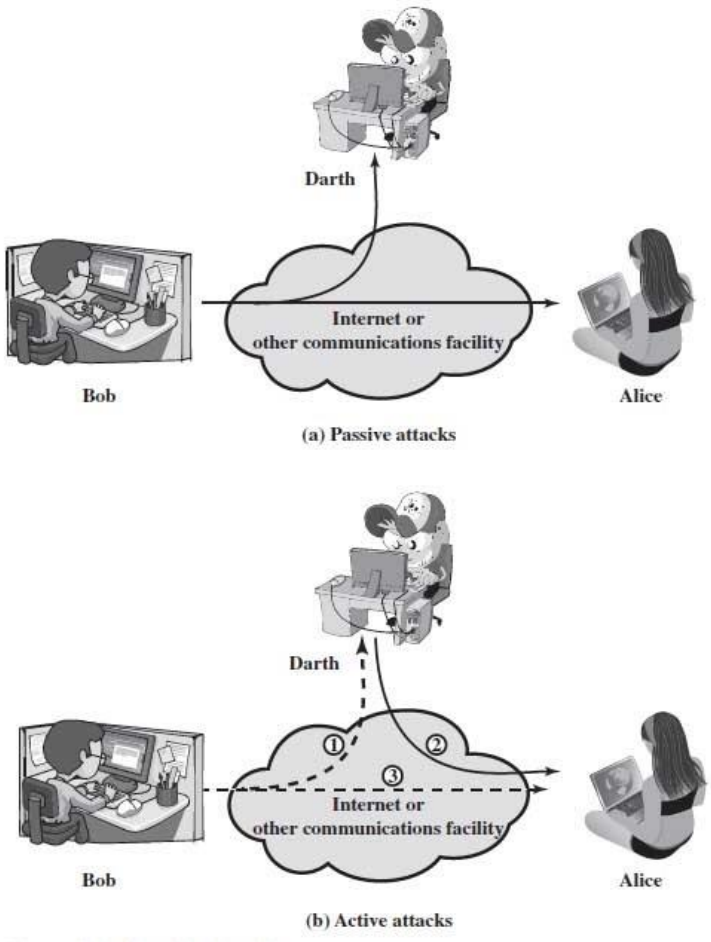


Figure 7. Active and passive attacks in practice [20]

As shown in figure 7, passive attacks only monitor the network traffic whereas active attacks try to modify the data sent through the network.

5.1 Active attacks

An active attack is a network exploit where the hacker attempts to modify the data on the target computer or modify it while it is on the way to the target computer. This requires the attacker to be able to transmit data to one or both parties. An attacker can be located in between the talking parties and can stop all or parts of the communication depending upon his or her intensions. If there are no integrity checks on the system,

the system will not realize that the data has been tempered. These attacks can be carried out through viruses, worms or Trojan horses. Active attacks are subcategorised below, based upon the type of action they perform.

5.1.1 Denial of Service (DoS)

Denial of service, or Distributed denial of Service (DDoS), is one of the most common attacks when it comes to network attacks. This kind of attack is target-specific. It is an attempt to make a network resource unavailable to its intended users and is done by flooding the network with useless traffic until to the point where the network shuts down because of the overload. An example of how an attacker would overflow the resources is shown below in figure 8.

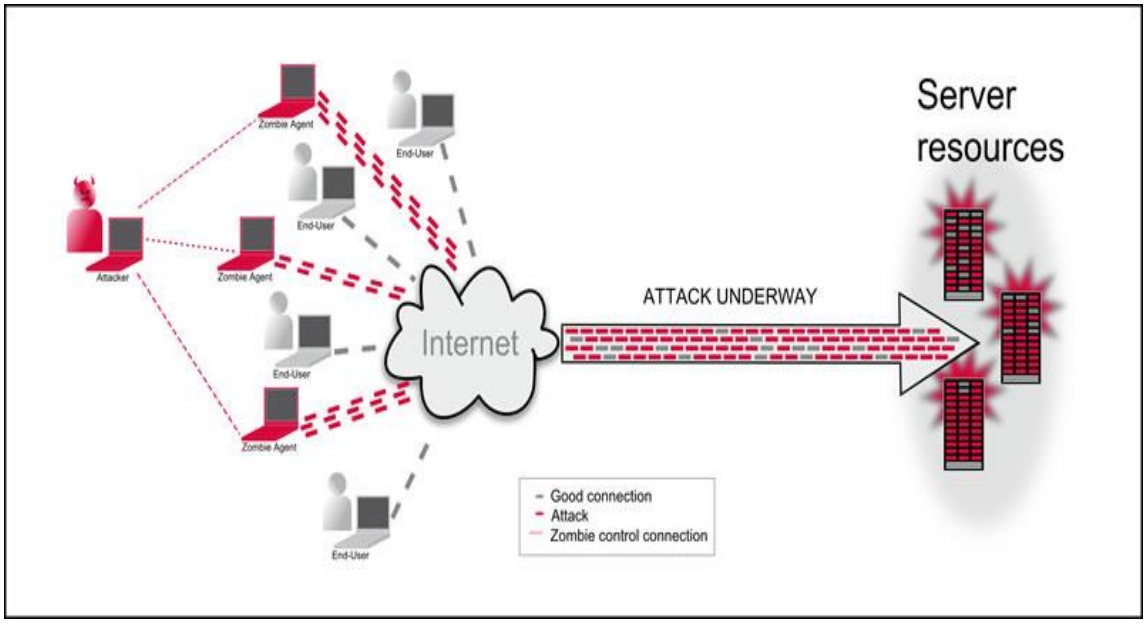


Figure 8. Anatomy of DDoS attack [21]

The figure illustrates how an attacker uses zoombie computers to flood the network traffic and the server resources such that the legitimate users can no longer use the services they are entitled to, and as a consequence the network shuts down due to the traffic overflow.

Although DoS attacks do not cause any theft of information, they can cost the victim a great deal of time and money. For example a DoS attack could force a website or a

server to shut down causing the service providers to be unable to provide services to the entitled customers/users.

While there are no easy tricks to fight against this kind of attack, it is worth using some simple practises to ensure a safer environment. Computers within a network should be secured and in case of any malicious activities, they should be cut off from the rest of the network. Since any computer system can be used for performing a DoS attack, the most effective solution is a global cooperation effort to ensure a secured Internet. System administrators should understand the vulnerabilities of their system and should try to fix them and take proper backups just in case there is a breach in the system.

5.1.2 Man-In-The-Middle (MITM)

A man-in-the-middle attack is a kind of eavesdropping cyber-attack where the attacker secretly gets access to communication between the two parties and can record, change or send information that never existed to the parties, pretending the information was sent from the other communication party. This kind of attack breaks the integrity of the messages being sent between the two parties. An example of an MITM is shown below in figure 9.

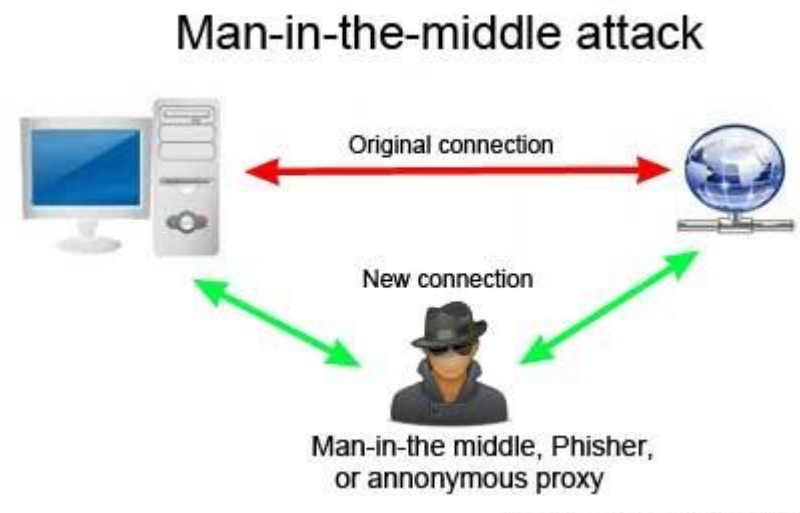


Figure 9. An illustration of MITM attack [22]

As the figure illustrates, the attacker inserts him/herself in the communication between the two parties and instead of messages sent directly from one party to another, they go through the attacker and the attacker forwards the altered or his/her own message

to the reciever party without the parties acknowledging that the message has been altered. For example, if a buyer purchases an item and the communication between the buyer and the seller is compromised, an attacker could modify the item amount or the shipping address for the item causing trouble both for the buyer and the seller.

Prevention against MITM attack is either on the server side or on the routers. Strong encryption methods can be used between the two parties in which case the communication parties can be identified by their digital certificates. Any mismatch would be a sign of tempered data. Another method of preventing an MITM attack is to avoid using open WiFi routers directly. There are various cryptographic algorithms that are available to protect the users from this type of attack.

5.1.3 Replay Attack

When a user logs into a website, to identify the user and the privileges that the user has, user is assigned a session id which serves as his/her identity. In a replay attack, an attacker steals the user's login information by stealing the session id. The attacker then has the same rights as the authorised user on the website.

In networks, this attack is used to maliciously delay or repeat the data transmission without authorization. An authorized user of the network transmits some messages but the attacker records those messages and can send the same messages at a different time without knowing the passwords and the keys. This could have bad consequences such as redundent orders of the purchased items.

An example of the replay attack is shown in figure 10.

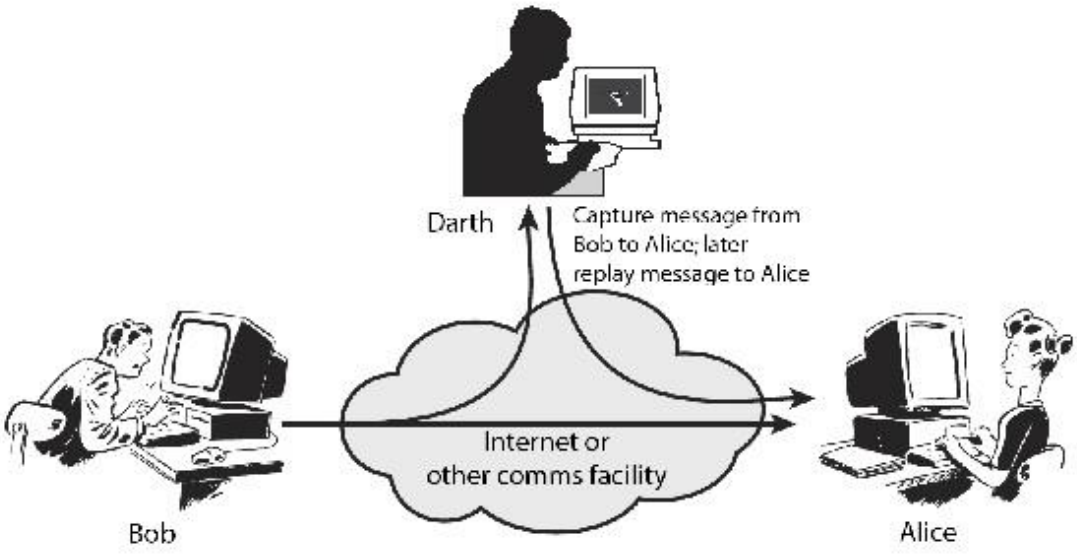


Figure 10. Example of a Replay Attack [23]

In the example, Bob and Alice play the role of two friends who want to transfer a message between themselves. Darth on the other hand plays the role of an attacker. Bob tries to send a message to Alice but Darth intercepts the message and later sends the message to Alice and makes it appear as if Bob just sent a message to Alice.

One approach to possibly avoid this kind of attack is that Bob can add a timestamp to the message so that it could indicate the time when the message was sent and if the timestamps do not match, it is an indication that there was a third party involved in the communication.

5.1.4 Identity Spoofing

Identity spoofing also known as masquerading, is an attack where the attacker pretends to be a particular authorized user in order to gain more privileges. After a successful attack, the attacker compromises the system and use it for his/her own good. It can be attempted through the use of stolen passwords, finding security loops in the system or by bypassing the security mechanism. An attacker can trick the victims into reveiling their passwords or sensitive personal information.

Another type of spoofing attack is the email spoofing where the attacker disguises as someone else usually as a person the victim might know or might be interested in knowing. For example, an attacker could send someone a malicious link by email and

try to deceive the receipient into thinking that the email was sent by their friends or family members or by someone they know. This allows the attacker to gain trust of the victim and as soon as the victim clicks the link, without his/her knowledge, the system is compromised.

5.1.5 Password Based Attacks

Passwords are secret words used for the authentication of an identity. While many users still choose some simple words in order to remember their passwords easily, e.g. their date of birth or their pet's name, using a secure password which is hard to guess can actually help them to be less vulnerable to these kind of attacks.

When an attacker hacks a user's account by hacking his/her password, he/she gains access to the same rights as the user and if the account hacked has the administrator rights, it means that the attacker has full control over the system and can perform actions on the system according to his/her liking.

Different approaches are used by hackers in order to compromise a user account. One of the most common types is password guessing. Attackers use both a manual and an automatic approach to guess user passwords. The easiest targets and the most vulnerable users in this case are the ones who have an easy to guess or a commonly used password e.g. 1234 or "password".

Another type of password attack is the dictionary attack where the attacker uses all the words found in the dictionary to check if there is a match and see if he/she gets access to a system. Dictionary attacks work because many users and organizations still use simple words as their passwords in order to avoid the complexity of creating a strong password and then remembering it.

Sometimes attackers also use password resetting programs in order to avoid the hasle of guessing passwords. This approach is useful only when an attacker just wants to get access to a system. However, resetting a password invites undesired attention and that is the reason attackers prefer password crackers by using password hashes and converting them into plain text formats instead of password resetters [24].

Password hashing is a process where a clear text which is used as a password is changed to give completely different values by applying some algorithm on it. This helps to protect a user from a dictionary-based attack as the password has been changed to some non-normal value instead of some plain words found in a dictionary.

While one can never garuntee a 100% secure password, using complex and strong passwords is always recommended as it reduces the chances of being compromised. As a general strong password, it is recommended to use 8-character long passwords along with some numbers and special characters in order to maximize security and minimize the chances of being compromised [25].

5.2 Passive Attacks

Unline an active attack, a passive attack is a network attack where the target system is monitored and scanned for vulnerabilities. The purpose of this kind of attack is to gather information about the victim's system without changing any data on it. Since passive attacks do not make any changes to the system or the data on it, they are very difficult to detect. Based on the intention, passive attacks are further divided into different categories.

5.2.1 Wiretapping

The history of wire tapping goes back to the days of telegraph when it was first used by the law enforcement in the New York City in the 1890's [26]. At that time, it was used by FBI, NSA and even business owners to monitor the activities of criminals, terorrists and office employees [27]. However, due to the advancements in techonology, the term wiretapping no longer stands for monitoring telephone calls only but is a term also used for the surveilance of the Internet communication. The term is still used even if no physical wire is used for the communication between two parties. While passive wiretapping does not involve modification of the data being transferred, it poses a big threat to the confidentialiy of communication.

A common tool used for wiretapping nowadays is called a Packet Sniffer. Everything done on the Internet, e.g. checking emails, browsing the Internet, chatting or transferring files, the data is always converted into packets. A packet sniffer can legitimately or illegally monitor the data packets sent over a network. Packet sniffers

help administrators of the network to monitor the network traffic and see bottlenecks if any. However, the same tool can be used by attackers to analyze the network traffic and to use that information for destructive purposes. One of the most commonly used tools for packet sniffing is Wireshark which captures the data packages which can later be viewed in detail as shown below in figure 11.

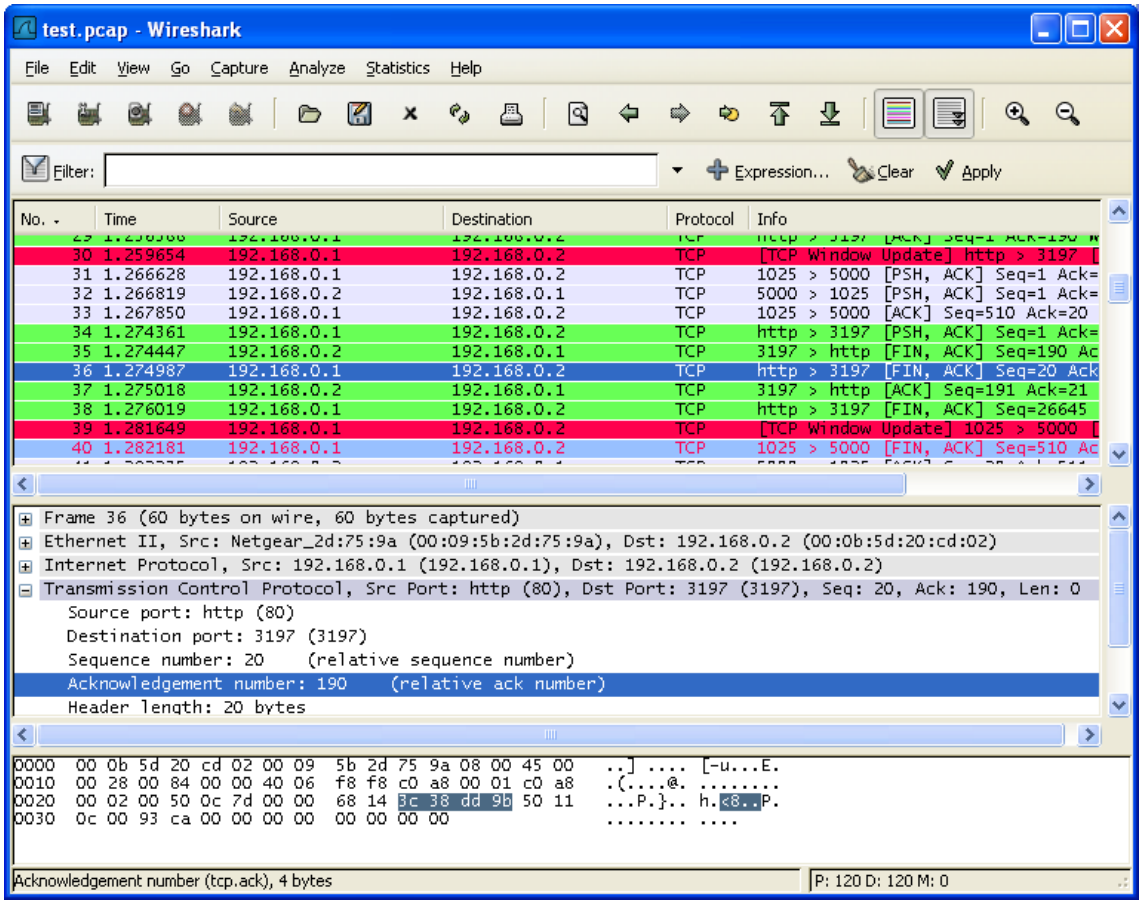


Figure 11. Capturing packet data using wireshark [28]

The figure shows a TCP packet selected for viewing. Wireshark is used as a tool for this purpose as it shows the time, name of each packet, source ip address, the destination ip address and more information in order to maximize the efficiency of a network. However, if used by wrong people, it can cause harm.

It is recommended that every network administrator knows how to use these tools in order to make sure that the network is not compromised in any way and the information of the clients is securely handled.

From a user's point of view, it is important to use HTTPS websites only, instead of HTTP, because HTTPS uses encryption algorithms, meaning that both the sending party and the receiving party agree upon a secret "code" and change their documents into random looking strings. This allows the user's information to be securely transferred over the Internet, thereby reducing the chances of any data breaches.

5.2.2 Port Scanner

Port serves as a communication endpoint in an operating system. It is a point where the information goes into and out of a system. A port is associated with an ip address and the type of the protocol used for the communication.There are specific port numbers defined for different services. HTTP serivce, for example, has a default port value of 80. A list of a few common port numbers is shown below in figure 11.

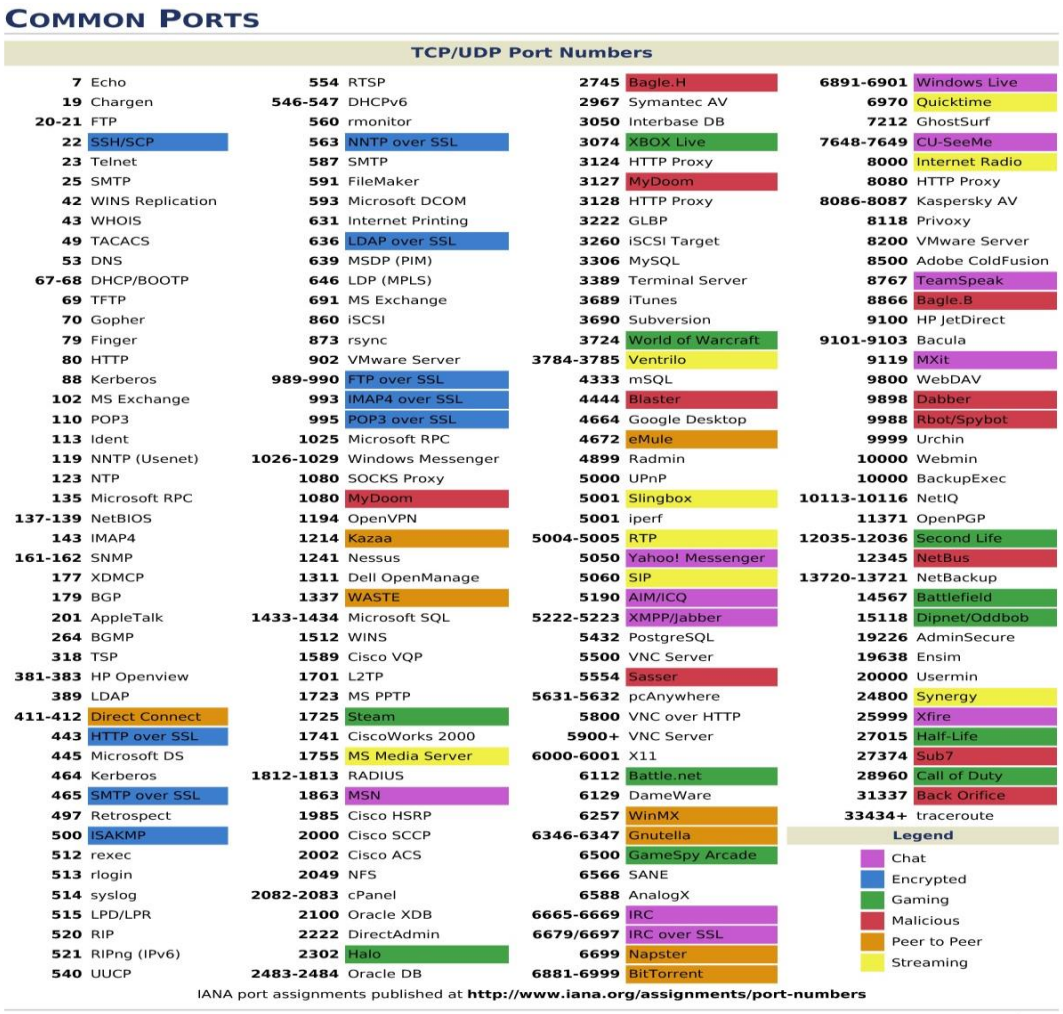


Figure 11. Common TCP/UDP port numbers [29]

A port scanner, like the Wireshark, is a tool which is used both by the network administrators and the hackers for monitoring the network. However, the intensions are quite different. Network administrators usually use port scanners to verify their network policies and improve their overall security while the attackers on the other hand try to use port scanning as a vehicle for reconnoissance, hereby allowing them to gain more information about the network.

One of the most commonly used tools for a port scanner is called NMap (Network Mapper). NMap among many other things can scan for open ports in a network and allow the user to see which ports are currently open in their network and are not being used for any special tasks at that particular moment. From network administrator's point of view, the open ports which are not being used should be closed as the attackers try to access the system using those open ports. Figure 12 shows the GUI (Graphical User Interface) of a network scan where the open ports are listed.

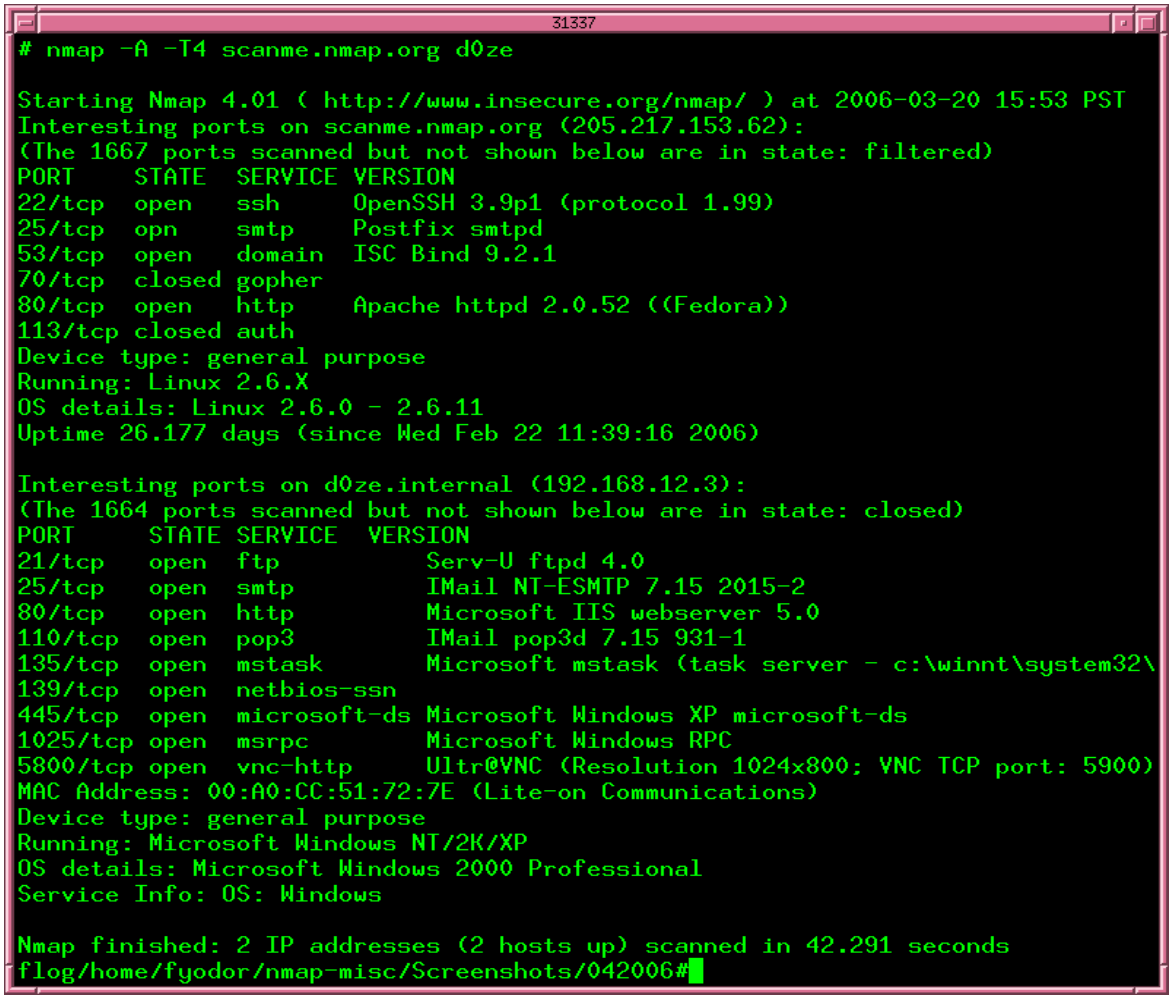


Figure 12. Viewing open ports using NMap [30]

Generally, the idea behind port scanning is to find open ports on a network host. When a burglar wants to target a house, the first thing he or she looks for is an open door or a window. The port scanner works in a similar way where the ports act as the doors and windows of the victims computer. The attacker tries to run a scan and see which ports on the computer system are open and which can be used to compromise the system. The attacker might not use those open ports right away but he or she would know an easy access to the system when he/she would need to break into the system. In some cases, the attackers can open ports themselves on the target computer in order to get get access to the system.

Although tools like NMap are freely available on the Internet, network administrators can actually use these tools to find vulnerabilities in their system and secure their system from any possible attacks. As a countermeasure for attacks such as port scanning, the network administrators could define rules in their firewalls, e.g. to look for

malicious behaviour if many ports of their network are being scanned per minute. Another way to ensure security is to close any unnecessary services on the target system. In reality all the systems are vulnerable to port scanning. However, the best offense is a good defense [31]. Network administrators should take a few necessary steps in order to avoid any catastophic damages in the future.

5.2.3 Idle scan

An idle scan, also known as zoombie scanning, is the stealthiest TCP scanning technique often used by an attacker. Even though it is another way to scan for open ports, this technique is used on servers or networks which have strong firewalls, which makes it very difficult for an attacker to get access to a system. The way this scan differs from other port scanners is that an attacker can perform this scan on the target system with his or her own real ip address and still manage to get away with it. This is done using a zoombie (idle) machine on the network.

Every IP packet on the Internet has a fragment identification number (IP ID). Many operating systems simply increment this number for each packet being sent, probing for the IPID can tell an attacker how many packets have been sent since the last probe [32]. In order for idle scan to work, an attacker first tries to make a connection with the zoombie computer which is part of the network of the target computer. The attacker sends a SYN/ACK (Session request acknowledgement) to the zoombie computer. The zoombie computer not expecting the SYN/ACK, sends back a RST(reset), thereby disclosing its IPID. Since the zoombie machine is part of the network, it lies within the trust zone of the target system. The attacker then uses the IP address of this zoombie computer and sends a SYN (session establishment) packet to the target system. If a port is open, the target sends back an acknowledgement to the zoombie machine SYN ACK (session request acknowledgement) or RST(reset) if a port is closed [32]. The process is shown below in figure 13.

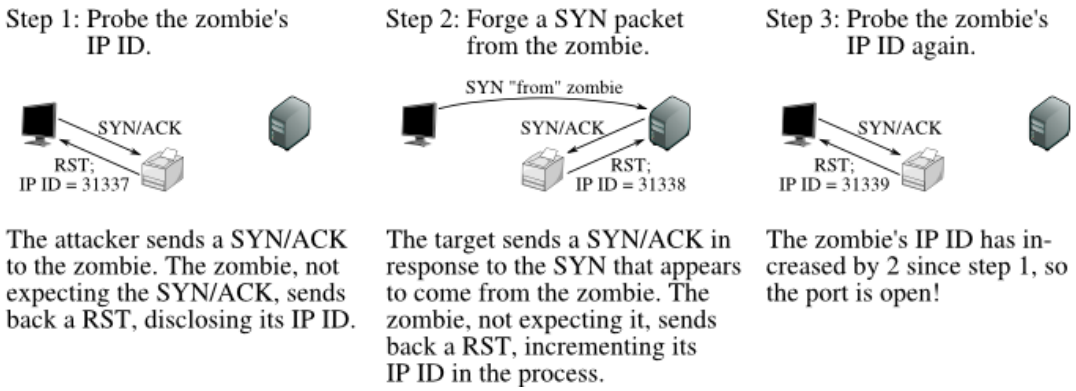


Figure 13. Scanning of an open port [32]

However, when a port is closed and an attacker scans the port, the behaviour is as follows in figure 14.

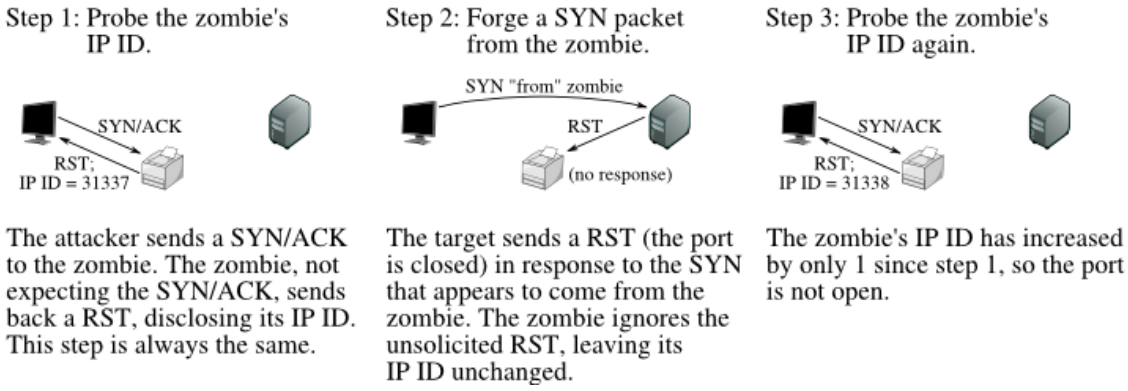


Figure 14. Scanning of a closed port [32]

Idle scanning, like port scanning can be easily done using the tool Nmap. After several bogus requests, network or system administrators might realize that someone is scanning their network but not only the attacker goes unidentified but also the attacker manages to map the network.

Luckily there are some defence mechanisms that the administrators can adapt in order to secure their network from idle scanning. Idle scanning works with zoombie (idle) machines. In other words, if the machine is not idle and there is communication between the zoombie machine and the system, idle scanning cannot work. Also when the attacker tries to use a zoombie machine, he or she is hoping that the zoombie machine has more rights to the system then they do. A good practise is to not put any public host in front of the firewall. The firewall should also be able to maintain a state-on connection, meaning that it can determine if someone is making any phony session

requests without a target host response. Also ingress and egress filters can be used on the network in order to become less easy targets for the attacker [33].

6 Database attacks

Databases are very often a key target for cybercriminals due to the fact that they carry sensitive and valuable information. Whether that information is private, governmental or business-related, attackers can always use that information to make some money for themselves. Usually the more sensitive the information, the more money for cybercriminals. While database attacks are very common, database developers and administrators are said to be responsible for providing such an environment where hackers can easily breach security and get access to databases [34].

Databases are of utmost importance to many organizations. They are used to store customer information and other confidential business data. Databases are also the backbones of many web applications. However, at times due to poor programming skills and failure to provide strong user validation methods by the web application developers, databases can be compromised.

Many times databases are tested to see if they do what they are supposed to do but administrators fail to achieve the security aspect, i.e. to check if databases do not do what they are not supposed to do. Attackers take advantage of these circumstances. Therefore, safety aspects must be considered from the very beginning phase of an application using databases, from development to the updating and the maintenance phases. The next figure 15 graphically shows the data breaches over different periods of time.

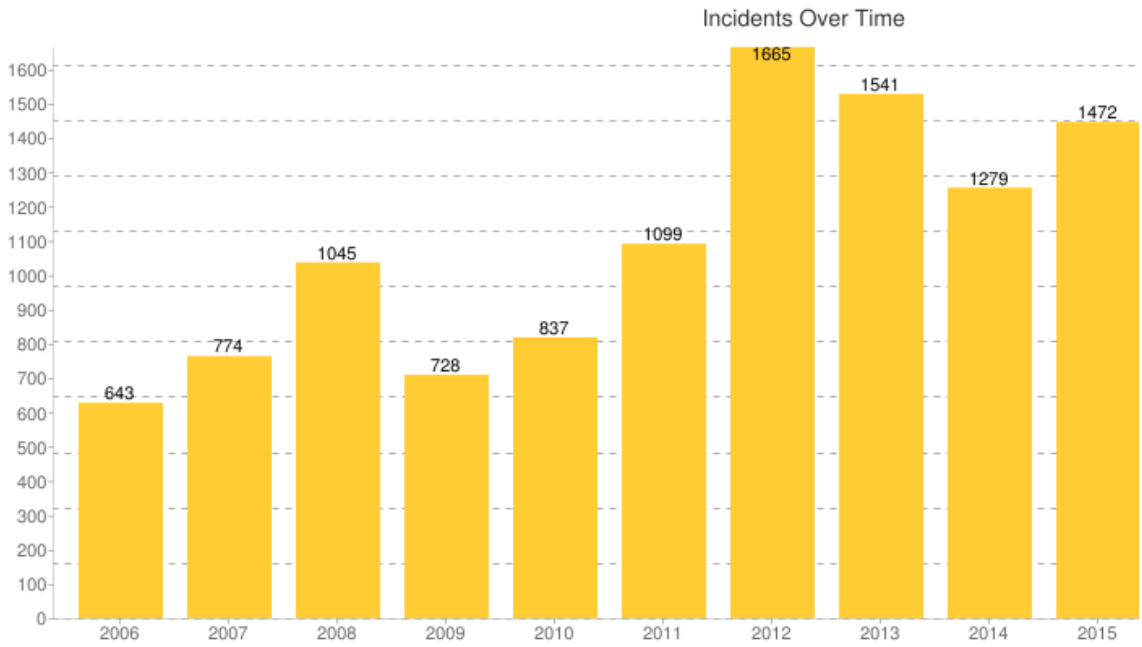


Figure 15. Data breaches from 2006-2015 [35]

Figure 15 graphically represents data breaches from the year 2006 to 2015. The maximum number of data breaches were in 2012 as seen from the figure.

On an average it takes an attacker less than 10 seconds to hack in and out of a database [36]. This is due to this fact that many database attacks go unnoticed until later when the compromised data has been leaked to the public. According to Noel Yuhanna, principal analyst with The Forrester Group, “The typical database may have 15,000 to 20,000 connections per second. It’s not humanly possible to know what all of these [connections] are doing.” [36]. While it might seem like hackers were using some complex hacking tools to get access to a database, in reality even nowadays, there exist so many application vulnerabilities that they can be easily exploited using simple hacking methods. A few of the database hacking methods most commonly used by hackers are discussed below.

6.1 SQL injection

SQL stands for Structured Query Language and it is a computer language that is used to manage data in the RDBMS (Relational Database Management System). An SQL injection is a database attack where the attacker penetrates the database by using unauthorised SQL commands. The primary targets of this kind of attack are the applications or servers which have big backend databases and which carry confidential

and sensitive information. Since this attack can be used against all the databases which are based on SQL, it is one of the oldest, most prevalent and dangerous of all attacks. Using an SQL injection, an attacker can take advantage of the vulnerabilities of an application and use queries to fetch all the usernames and passwords from the database. This also allows the attacker to see all the data fields in the database and create, modify and delete the fields if he or she pleases. Over different periods of times, Sony Pictures, PBS, Microsoft, Yahoo and even CIA have been targets for this kind of attack. Below figure 16 illustrates an overview of the SQL injection attack.

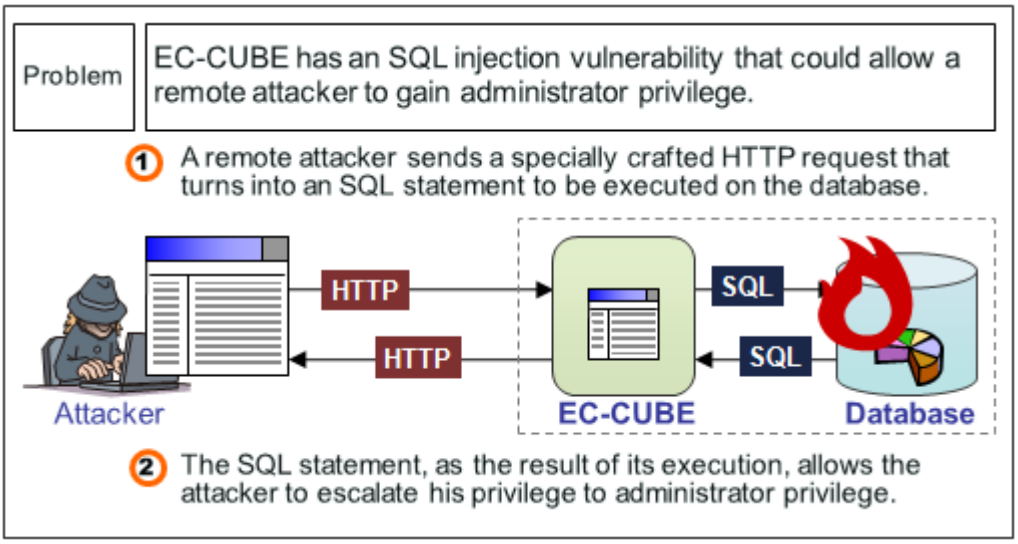


Figure 16. An example of SQL injection [37]

Hackers use easy tricks to gather information about a database. The easiest way to notice an SQL injection is to put **'** into the input field and if the field is vulnerable to the SQL injection, an SQL error will be displayed. The hackers actually gather information using this SQL error. A simple query for the SQL injection is as follows.

SELECT fields FROM aTable
WHERE field = ‘ $EMAIL’:

where $EMAIL is the email address which a user provides through a web form. The attacker does not know the email and instead provides a value

dummy ‘ OR ‘1’=’1

So the resulting SQL query will be

SELECT fields FROM aTable
WHERE field=’dummy’ OR ‘1’=’1’:

Here 1=1 plays an important role. Since 1=1 is a true statement, the web application is tricked into displaying every item in the “aTable” field of the database. In the same manner any other true statement can also be used instead of 1=1 for instance, 9=9 or a=a. Some common tools used for an SQL injection are Sqlninja, Sqlmap and Paros Proxy.

There are different vulnerability phases for an SQL injection.

- Finding a vulnerability.
- Finding out the type and version of SQL server.
- Finding out the type of vulnerability.
- Resolving the structure of databases.
- Stealing or changing information.
- Using the stolen information.
- Taking control of server and installing backdoors in the server for later use.

Sometimes, a web application is developed properly by taking into account the security measures. The application does not output any data which normally would be used by attackers to gain information about the database. In such cases an attacker can use a Blind SQL injection. A Blind SQL injection is somewhat similar to an SQL injection but the difference is in the way data is fetched from the database. In a Blind SQL injection, the attacker asks a series of True or False questions from the database and expects the database to answer the questions, thereby giving out confidential information to the attacker. Using a Blind SQL injection to exploit database vulnerability is not easy and careful reading of the outcomes is needed in order to be able to find the differences between True and False results.

SQL injections have been around for a while now but still they are a danger that many big organizations fear. For example, one major SQL injection attack was in March 2008 where Heartland Payment System became the target and 134 million credit cards were exposed [38].

While SQL injections at times can be hard to detect, there are ways how administrators can avoid being easy targets for them. Web application developers should possess good programming skills and be familiar with SQL injection attacks and their consequences. The code that has been written should be reviewed properly keeping security

aspects in mind. Also some automated tools should be used to test the application and make sure that there are no open vulnerabilities in the system.

The application should use some kind of encryption algorithms in order to store usernames and passwords, e.g. SHA-1, and avoid storing passwords in plain text form. Simple security precautionary steps should be taken. If someone tries, for example, to access the password table, the administrator should be informed by email or by some other means of communication. The user should not be allowed to enter all characters into the fields. The user input should be filtered to allow some characters and disallow certain others.

Another good practise is to create multiple database user accounts instead of one database with each having a minimum level of privilege for their environment. For example, the login page can have a separate database. In that case, even if there is a breach in the system; the entire database will not be compromised.

Any of the above defences, when applied, can provide better security for a database. However, as the best practise, all the above techniques should be used at least in order to ensure a safer database.

6.2 Excessive Privilege Abuse

Whenever a user is granted some privileges to use an application, the administrators should make sure that the user is not given more privileges then he or she requires. Very often, those privileges are used for malicious purposes. For example, if an office worker has the administrative rights just because he or she could update the names of the employees in the database, these rights can also allow him or her to see other personal details of each employee, e.g. salaries and home addresses. According to statistics, excessive privileges have been the top database threat in the year 2015 as shown in figure 17.

Ranking	2015 Top Threats
1	Excessive and Unused Privileges
2	Privilege Abuse
3	Input Injection
4	Malware
5	Weak Audit Trail
6	Storage Media Exposure
7	Exploitation of Vulnerabilities and Misconfigured Databases
8	Unmanaged Sensitive Data
9	Denial of Service
10	Limited Security Expertise and Education

Figure 17. Top ten database threats in 2015 [39]

Abuse of Excessive Privilege is often due to the fact that database developers do not have extra time to define and maintain access privileges for each user. Consequently, users are granted some default privileges that might exceed their job requirements. Large organizations spend a lot of money and effort on protecting themselves from the outside world but fail to secure themselves from within. It is not unheard of that a rogue employee of an organization still has access to the system and can cause devastating loss to the company. Many organizations even nowadays do not have a proper process for updating user rights.

Attackers have become smarter and faster. They learn the weaknesses of organizations. The attackers understand the fact that in order to compromise an organization's network, illegal access to a computer from within the network, could help to carry out the attack with less effort and in a time efficient manner. Once the attacker has access to a computer with excessive or administrative rights from within the network, he or she can abuse those privileges according to his or her needs. While excessive privilege attack is not a new concept, many users/organizations even today fail to take the necessary steps in order to avoid these kinds of attacks.

In order to avoid users from having excessive privileges to a database and thus to reduce the chances of an attacker compromising the user account and abusing the user rights, one solution is query-level access control. The mechanism behind this approach is that it limits database privileges to the minimum required SQL operations, e.g. SELECT, UPDATE etc. This approach would allow the office worker described in our pre-

vious example, to change the name of the employees in the organization but not to access any other information. If he or she tries to access some other data fields, an alert would be generated. Limiting the user privileges can also help to control the damage caused by an attacker when a user account is hacked.

6.3 Privilege Elevation

Sometimes, even if all the privileges are assigned correctly to users by using some security policies, attackers can manage to change the user rights. Attackers may do that by taking advantage of the vulnerabilities of the database platform software. These vulnerabilities might be found in the stored procedures or protocol implementation or even in SQL statements. An attacker can exploit such vulnerabilities to change a normal user account into an administrator user account.

In order to protect against such an attack, traditional intrusion prevention systems (IPS) can be used. IPS is often used to identify a known malicious vulnerability in network traffic. IPS can also be used to block access to all the procedures which are considered malicious. Unfortunately, IPS alone is not enough to fight against such attacks. Query-level control should also be used alongside IPS in order to maximize the defence mechanism.

6.4 Weak User Authentication

Authentication plays a very important role in security. When a user logs into a system, the username and password are used to confirm the identity of that user and after being identified, the system assigns the user specific privileges. There are many different forms of user authentication. A few are mentioned below.

- Basic Authentication: Uses cleartext usernames and passwords.
- Digest: Mostly the same as basic authentication but the passwords are scrambled.
- Form-based: Uses a custom form and allows the user to enter username and password which are then verified on the backend during the login process.

Providing fingerprint, using smart cards, voice pattern sample and retinal scan are a few other methods that are used for user authentication.

Many times people avoiding to learn different and complex passwords, choose some simple, and easy to remmeber words and even use one password for everything. While this approach might be convenient, it puts a great danger on the security of the system and provides the attacker with a welcoming environment.

Some corporations implement effective security mechanisms around their databases, only to have the rights compromised due to a weak authentication mechanism. In such environments where passwords are the only defence against attackers, password strength plays a key role. Instances where default usernames and passwords are used is a sign of weak user aunthentication.

Originally SQL servers were shipped with a null as default password for the administrative account “sa” [40]. This information can be easily used by the attacker to get access to the database server and own it. An attacker can also use social engineering to hack the password and very often this technique shows promising results. The human nature of trying to be helpful allows attacks like social engineering to be carried out almost effortlessly. A simple phone call, for example, made by the attacker pretending to be a higher authority can trick people into revealing sensitive information.

In order to protect ourselves from weak authentication attacks, it is recommended to change the default passwords right away. Strong passwords should be used which are not easy to guess and should be changed after every fixed period. In order to provide better security, more than one authentication method should be considered for high privileged users, e.g. passwords along with retina scan or voice sample or finger prints. While one can never be too secure, the better security, the less chances of becoming a victim.

6.5 Weak Audit Trail

Weak audit trails can be no less than a terrible nightmare from which it is not easy to recover for organizations. Many times, in case of a data breach, organizations are not able to confirm what data has been accessed and who has accessed it.

A weak audit policy exposes the organization to risk on many levels, e.g. regularity risks, when organizations failing to achieve strong audit trials will often find themselves

at odds with the government regularity requirements. A detection and recovery risk is also something to consider. When an attacker manages to bypass all the other security measures, the audit mechanism is the last defense against the attacker, as it will provide the information regarding any violations in the system. Failing to use a strong audit, deprives the organization of the opportunity to detect and/or to report an attack properly.

Databases have the highest rate of breaches among all business assets. A weak audit lies is in the top five database threat categories. An attacker usually gets away with this kind of attack because proper system logs are not maintained and once there is a breach in the system, it cannot be traced back to the attacker. While database developers might argue by stating that taking logs slows down the performance of the system and occupy resources, the attackers are looking for getting their hands on such systems.

In order to protect systems from such attacks, it is important from the very beginning stage of development that developers understand what data is sensitive and needs to be protected and monitored. Clear logs should be stored when sensitive data is accessed so that in the case of any data breach, the security team could view the logs and get a better understanding of the damage done. The logs could be stored on separate systems in order to avoid occupying CPU resources. The audit duties should be separated from the administrative duties and the rights should be assigned accordingly so that in the case of a compromised administrator account, the attacker is not able to delete the log files.

While weak audit attacks are very common, taking some simple precautionary steps can ensure not only a secure database but also encourage administrators to be more aware and watch out for attackers.

6.6 Exposure of Backup

While it is a good practise to take backups, in some recent cases backups and stolen hard drives have been involved in high profile attacks. While organizations spend millions of dollars trying to protect their data and keeping it secure, sometimes the security of backup data is overlooked. Stealing backup data is more convenient for attackers at times than trying to hack the system and gain access to the system. Failing

to monitor the activities of administrators who have access to sensitive information can also put the data at risk.

Appropriate measures should be taken in order to securely save the backup data and monitor users who have access to that data. As a good practice it is recommended to encrypt backup data just in case it gets into the hands of an unauthorized user.

7 Tools of the trade

No matter where computers are being used, either at home or offices, users need to be educated and they should be aware of all the attacks that are carried out through the Internet. Users should be aware of any unusual behaviour on their system. Users should also avoid opening links or files from unknown sources and not share any sensitive information except with authorised personnel.

It is said that the safest computer is the one that is powered off and not connected to the Internet but that might not be true. Social engineering is a very powerful tool that is used for tricking users into helping the attacker carry out the attacks. A powered off computer can be powered on and can be connected to the Internet if a user has no knowledge regarding security. Such users are easy targets for the attackers. Organizations should educate their employees on security issues no matter if the employee is working with a computer or not. Many cases are known where an employee, unaware of the security issues, plugged in a USB drive found in the company's premises to the office PC and infected the system. This approach is used by attackers when they cannot get direct access to a company's PCs. Organizations should establish security policies and train their employees accordingly.

While there is no such thing as a fully secured system, there are some great tools available that would get very close. Antivirus should be installed on all PCs, no matter if it is a home PC or an office PC. Antivirus should be updated for new virus definitions and a periodic scan should be run on the entire system. Any plugin device should be scanned for viruses before opening. Users should not rely solely on the antivirus program, but they should keep an eye on the suspicious behaviour of a file or a program. Malwarebytes is another good tool that is very often used to detect malware and zero day threats.

Firewalls play a very important role when it comes to security. Antiviruses detect a malicious program that is already in the computer or is about to be installed, whereas firewall filters the data packets that come into the system and go out. A firewall is well known to keep hackers out of the network (system) and prevents any unauthorised intrusions.

Backup of any relevant data is highly encouraged. The backups should be stored possibly with an encryption to protect them in the case of any thefts. Physical security should also be taken into account while storing the backups. Data loss can cause companies a great loss of revenue. No matter what the reasons behind a data loss are, whether they are due to human errors or natural causes, crime or disasters, a right backup strategy is well worth the effort.

Whether a user is sending emails or storing data, chatting with colleagues or browsing the Internet, encryption is the best tool to ensure the integrity and confidentiality. While browsing the Internet, users should avoid going to websites that are not encrypted (HTTP).

When it comes to data encryption, there are many encryption tools available for the protection of the user data, e.g. TrueCrypt that uses complex cryptographic algorithms to encrypt the data. Even though encryption is known to affect a system performance, the benefits of encryption are far more than its disadvantages.

8 Conclusion

The aim of the project was to gain a better understanding of different kinds of cyber-attacks carried out through the Internet. Cyberspace has evolved very rapidly and along with it has changed the ways of cyber criminals to choose their victims. While these attacks most likely will increase by time, the project has suggested some guidelines which can be used in order to be better prepared. People, organizations, schools, universities and all the other communities where computers are used in the daily life, should establish strong security policies and help each other to defend against such cyber-attacks.

Achieving network security is almost an impossible task. Even with the best network administrators, network security breaches are still likely to occur and will be reported.

The way of thinking of a network administrator has a great effect on the network security.

Security awareness should not be restricted to the IT department, but should be a part of all areas of the business from the top management to the lowest level of employment in the company. Security policies that are implemented in the company should have proper guidelines and should be shared in the company and not in the IT department alone.

In an organization, proper training should be held including everyone in the company, so that the security policies that are defined in the policy formulation will be efficiently implemented. The training should encompass information not only related to the software but also the hardware usage for the employees.

Since the threats that the business may encounter evolve rapidly, up-to-date knowledge of countering threats should be disseminated to all the employees of the company. Devices that the company uses should also be kept up-to-date, for example, by installing the up-to-date patches and even the operating system.

The history of our society has shown that crime cannot be eliminated forever. However, with proper measures and precautions it can be decreased to a great extent. Computer users need to understand their duties and responsibilities. They should be able to defend themselves against all the cyber threats. Self-awareness is very often a key factor and the only difference between a failed attack attempt and a compromised system.

References

1. TRIGAUX, R. (2000). A history of hacking. [online].
   URL: http://www.sptimes.com/Hackers/history.hacking.html
   Accessed 24 March 2015.

2. Campaigns.f-secure.com, (2015). F-Secure - About Brain. [online].
   URL: https://campaigns.f-secure.com/brain/virus.html
   Accessed 7 May 2015.

3. Cluley, G. (2012). Memories of the Michelangelo virus | Naked Security. [online].
   URL: https://nakedsecurity.sophos.com/2012/03/05/michelangelo-virus/
   Accessed 11 May 2015.

4. De Forest, N. (2015). The Concept Virus. [online].
   URL: http://www.chebucto.ns.ca/~af380/ConceptMacro.html.
   Accessed 24 April 2015.

5. Wikipedia, (2015). Happy99. [online] Last modified November 6 , 2015.
   URL: https://en.wikipedia.org/wiki/Happy99.
   Accessed 9 October 2015.

6. b., David. March 25, (2012). The History and the Evolution of Computer Viruses: 2003-2008 | Privacy PC. [online].
   URL:http://privacy-pc.com/articles/the-history-and-the-evolution-of-computer-viruses-2003-2008.html.
   Accessed 8 February 2015.

7. Zetter, K. (2014). An Unprecedented Look at Stuxnet, the World's First Digital Weapon. [online] WIRED.
   URL: http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.
   Accessed 24 August 2015.

8. Siciliano, R. (2011). 7 Types of Hacker Motivations - McAfee. [online]
URL: https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/
Accessed 15 February 2015.

9. OWASP. Computer Viruses [online]. Last modified September 13, 2010
URL:https://www.owasp.org/index.php/Computer_Viruses
Accessed 12 March 2015.

10. Avi Silberschatz, Peter Baer Galvin, Greg Gagne. Operating System Concepts
URL: http://codex.cs.yale.edu/avi/os-book/OS7/os7c/slide-dir/ch15.pdf
Accessed 15 March 2015.

11. PABON, J. (2014). VIRUS DE BOOT O SECTOR DE ARRANQUE. [online]
URL: http://viruss-del-sector-de-arranque.blogspot.fi/
Accessed 8 June. 2015.

12. Kaspersky Lab United States, (2015). Kaspersky Personal & Family Security Software. [online]
URL: http://usa.kaspersky.com/internet-security-center/definitions/macro- virus#.VlRj4XYrLIU
Accessed 29 March 2015.

13. Christopher M. Kelty. The Morris Worm [online]. Issue number one: Systematic Risk
URL:http://limn.it/the-morris-worm/
Accessed 12 September 2015.

14. Wikipedia, (2015). Morris worm. [online]. Last Modified Nov 3, 2015
URL: https://en.wikipedia.org/wiki/Morris_worm
Accessed 12 September 2015.

15. Philipp Rogmann. Malware and Cybercrime as a service [online]. F-secure. July 08,2015
URL:https://business.f-secure.com/malware-and-cybercrime-as-a-service/
Accessed 08 August 2015.

16. MalwareTips. 3 easy way to remove any Police Ransom Trojan [online].
URL: https://malwaretips.com/blogs/remove-police-trojan/
Accessed 19 August 2015.

17. History of Spyware. (2012). [online]
URL: http://www.tuneupadvisor.com/history-of-spyware.aspx
Accessed 20 March 2015.

18. Stelian Pilici. Browser hijackers [online]. MalwareTips. February 20, 2015
URL: https://malwaretips.com/blogs/websearch-coolwebsearch-info-removal/
Accessed 23 April 2015.

19. TheFBI. Scareware distributors targeted[online]. June 22, 2011
URL: https://www.fbi.gov/news/stories/2011/june/cyber_062211
Accessed 12 June 2015.

20. William Stallings. Cryptography and Network Security- The basics-part-II [online]. EDN Network. May 30, 2013
URL: http://www.edn.com/design/wireless-networking/4415350/1/Cryptography-and-Network-Security-The-basics-Part-II
Accessed 12 June 2015.

21. AVNET. DDos Attack Control Service[online]. United Kingdom. 2015
URL:http://www.ts.avnet.com/uk/value_added_services/partner_services/ddos_attack_control_service/
Accessed 30 August 2015.

22. Computerhope. What is Man-in-the-middle attack? [online]. 2015
URL: http://www.computerhope.com/jargon/m/mitma.htm
Accessed 2 September 2015.

23. Susmita Mandal & Ayan Kumar Pan. Risks in Cloud Computing. April 29, 2013
URL: http://sharedopinions.devhub.com/blog/1803608-risks-in-cloud-computing/
Accessed 19 September 2015.

24. Grimes, R. (2006). Types of Password Attacks. [online] Windowsitpro.com.
URL: http://windowsitpro.com/security/types-password-attacks
Accessed 29 September 2015.

25. Columbia.edu, (n.d.). Using Strong Passwords. [online]
URL:http://www.columbia.edu/acis/security/users/passwords.html
Accessed 13 August 2015.

26. Rouse, M. What is wiretapping? - Definition from WhatIs.com. [online]. Last updated May, 2014
URL: http://whatis.techtarget.com/definition/wiretapping
Accessed 2 October 2015.

27. Itsecurity.com,DIY Wiretapping: The Ultimate Guide (and How to Fight Back) - IT Security. [online] June 17, 2008
URL: http://www.itsecurity.com/features/diy-wiretapping-061708/?PHPSESSID=7fceb5810f180e33f7a788c028b84869
Accessed 3 October 2015.

28. Wireshark.org, (n.d.). Chapter 6.Working with captured packets. [online]
URL:https://www.wireshark.org/docs/wsug_html_chunked/ChapterWork.html
Accessed 13 October 2015.

29. Stretch, J. (n.d.). Common Ports. [online] Packetlife.net.
URL:http://packetlife.net/media/library/23/common_ports.pdf
Accessed 11 October 2015.

30. Nmap.org, (n.d.). [online]
URL:https://nmap.org/images/nmap-401-demoscan-798x774.gif
Accessed 16 October 2015.

31. Sans.org, (2002). [online] Last Modified Nov 25, 2015
URL: https://www.sans.org/reading-room/whitepapers/auditing/port-scanning-techniques-defense-70
Accessed 9 June 2015.

32. Nmap.org, (n.d.). TCP Idle Scan (-sI). [online]
URL: https://nmap.org/book/idlescan.html
Accessed 13 October 2015.

33. Mullins, M. (2007). Defend your network from idle scanning - TechRepublic. [online].
URL: http://www.techrepublic.com/blog/it-security/defend-your-network-from-idle-scanning-86384/
Accessed 13 October 2015.

34. Osborne, C. (2013). The top ten most common database security vulnerabilities |ZDNet. [online]
URL: http://www.zdnet.com/article/the-top-ten-most-common-database-security-vulnerabilities/
Accessed 16 October 2015.

35. Datalossdb.org, (n.d.). Data Loss Statistics. [online]
URL:http://www.datalossdb.org/statistics?utf8=%E2%9C%93&timeframe=last_year
Accessed 13 October 2015.

36. Higgins, K. (2008). Hacker's Choice: Top Six Database Attacks. [online] Dark Reading.
URL: http://www.darkreading.com/risk/hackers-choice-top-six-database- attacks/d/d-id/1129481
Accessed 6 July 2015.

37. Sakhackingarticles.blogspot.fi, (2014). Hack Website Using SQL Injection Attack with WebCruiser | SAK Hacking Articles.[online]
URL: http://sakhackingarticles.blogspot.fi/2014/08/hack-website-using-sql-injection-attack.html
Accessed 15 July 2015.

38. Armerding, T. (2015). The 15 worst data security breaches of the 21st Century. [online] CSO Online.
URL: http://www.csoonline.com/article/2130877/data-protection/data-protection-the-15-worst-data-security-breaches-of-the-21st-century.html
Accessed 19 July 2015.

39. Imperva, (2015). Top Ten Database Security Threats. [online]
URL: http://www.imperva.com/docs/wp_topten_database_threats.pdf
Accessed 21 October 2015.

40. Kb.cert.org, (2015). Vulnerability Note VU#635463 - Microsoft SQL Server and Microsoft Data Engine (MSDE) ship with a null default password. [online]
URL: https://www.kb.cert.org/vuls/id/635463
Accessed 26 October 2015.