

---

## 1. HACKING

Hacking is the act of finding and exploiting entry points that exist in a computer system or network. Hacking is performed to obtain unauthorised access to the computer system in view to steal sensitive information or harm the computer system or network. The purpose of ethical hacking is to test the computer system and network for potential security vulnerabilities and provide solutions for those vulnerabilities before an ill-intentioned hacker finds them and exploits those loopholes.

Hence, whilst hackers are usually “malicious” guys who try to compromise a computer systems or computer network in view to steal important information or to harm the computer network, ethical hackers are usually “good” guys who try to find weaknesses, in a legal manner, in a computer system or computer network for testing purposes. Through the knowledge gathered in finding the security vulnerabilities, the ethical hackers can provide solutions in order to re-enforce the computer system or computer network.

### 1.1 CLASSIFICATION OF HACKERS

#### 1.1.1 Classification based on Intent

Hackers can be classified into three groups based on their intent of hacking the system, as follows:

White Hat Hackers	A white hat hacker is a computer security specialist who breaks into computer systems and networks with the intention to test and asses their level of security. White hat hackers are also known as <u>Ethical</u> Hackers since their intent is to never harm the computer system and network. Ethical hacking is not illegal since such hackers are granted permission by the organisation which employs them to look for security vulnerabilities in the computer system.
Black Hat Hackers	A black hat hacker is a hacker who violates the computer system security in view to gain unauthorised access to the computer system and network in order to steal sensitive data or harm the

	system. Black hat hacking is illegal because the hacker has a bad or malicious intention since he/she will either steal information, compromise the privacy, damage the computer system and network or block communication, among others.
Grey Hat Hackers	The grey hat hacker is a mixture of both black hat and white hat hackers. These hackers sometimes violate laws or typical ethical standards but they act without a malicious intent to exploit the security vulnerabilities of the computer system and network without the owner's permission or knowledge. Their intention is to draw the attention of the owners to the security vulnerabilities and thus improve the security of the computer system and network.

### 1.1.2 Classification based on Hacker's Mode of Operation

Besides the three main groups of hackers, there are other categorises of hackers based on what they hack and how they perform the hack:

- **Red Hat Hackers:** they hack government agencies, top-secret headquarters in order to gain sensitive information.
- **Suicide Hackers:** hackers who are not afraid of going to jail or facing any sort of punishment.
- **Script Kiddies:** unskilled hackers who use real hackers' tools and programmes.
- **Cyber Terrorists:** hackers having religious or political beliefs with the motive of creating a large-scale fear.
- **State-Sponsored Hackers:** hackers engaged by governments.
- **Hactivists:** hackers promoting a political agenda or a social change.
- **Neophyte:** a person new to hacking and who does not possess any skills, knowledge and experience in this area.

## 1.2 WHY HACK A COMPUTER SYSTEM AND NETWORK?

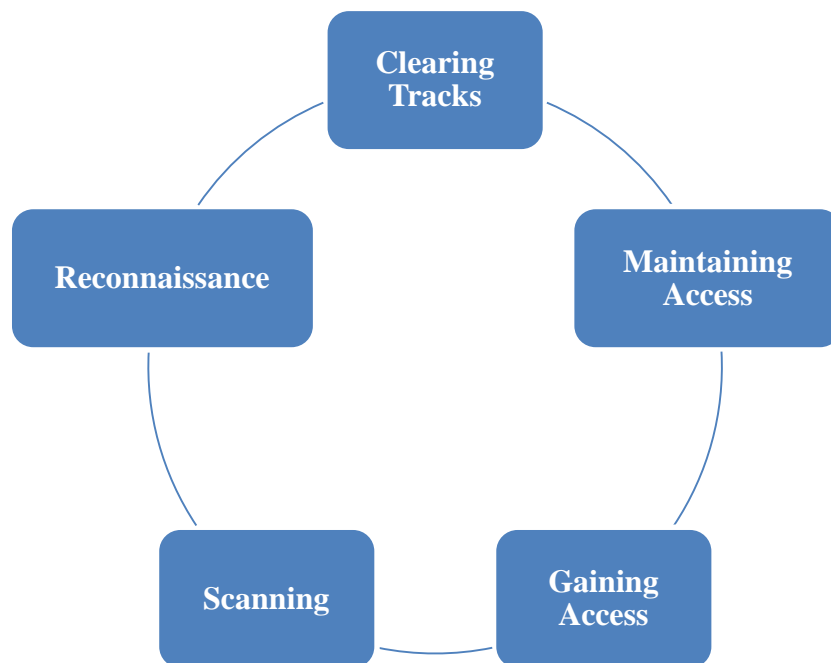
The essence of ethical hacking stems from: “To catch a thief, think like a thief”. Hacking exploits the weak computer security procedures and undisclosed vulnerabilities. Security systems such as firewalls, encryption and virtual private networks do not always guarantee secure systems. They provide only a high level security against virus and traffic but not against how a hacker works. Attacking your own system will ensure that eventually your computer systems and network become more secure and will also guard against a hacker’s common strategy. Below is a list of hacking attacks performed on computer systems and networks:

Operating Systems Attacks	Hackers like to attack operating systems. This is because every device (computer systems, mobile phones, servers, network devices) possesses an operating system in which hackers can exploit vulnerabilities. Operating systems such as Windows and Linux are often under hackers’ attacks because hackers exploit vulnerabilities in the operating system protocol implementation, file-system security, in-built authentication systems and, password and encryption mechanism.
Application Attacks	Applications are hacked almost every day or every hour. Application programmes such as email, website application and software are hacked. <ul style="list-style-type: none"><li>• Email hacking involves getting unauthorised access to an email account without the owner’s permission. This can be carried out by exploiting the Simple Mail Transfer Protocol.</li><li>• Website hacking involves obtaining unauthorised access to the web server (and eventually to the website) and involves making modification to the database and to the graphical user interface. Such attacks are also termed as <i>phishing</i> where there is an attempt to obtain sensitive information such as the username, password and bank details.</li><li>• Malicious software are introduced in computer systems and network to exploit software vulnerabilities. Examples are malwares such as viruses, worms and Trojan horses.</li></ul>

Network Attacks	<p>Hackers attack network infrastructure because a network infrastructure is easily accessible everywhere around the world through the Internet. Network system related attacks include the following:</p> <ul style="list-style-type: none"> <li>▪ Exploiting flaws in the protocol stack of the TCP/IP model;</li> <li>▪ Using networking tools or network analyser such as Telnet, Ping, Netstat, Wireshark to gather network information in view to harm the infrastructure or to capture packets to obtain confidential information;</li> <li>▪ Creating denial of service (DoS) to overwhelm the network such that it cannot process legitimate request;</li> <li>▪ Hacking wireless network in order to access the network.</li> </ul>
-----------------	---

### 1.3 HACKING PROCESS

To hack a computer system and a network, a hacker goes through the hacking process which comprises of the reconnaissance, scanning, gaining access, maintaining access and cleaning tracks, as per diagram below.



**Figure 5.1: The Hacking Process**

(Adapted from <http://searchsecurity.techtarget.com/tip/Understanding-footprinting-as-a-predecessor-to-cyberattacks>. Accessed 04 April 2018)

The steps are described as follows:

1. **Reconnaissance:** Reconnaissance is the preparation stage. In this stage, the hackers try to gather as much information as possible on the targeted computer system and network.
2. **Scanning:** Scanning is the pre-attack stage; it is done on the basis of information gathered during the reconnaissance phase. This phase includes the usage of tools such as port scanners and net mappers. Information extracted by the attacker during this phase include live machine, OS details.
3. **Gaining access:** Gaining access is the stage where the attacker gets access to the computer system or the application.
4. **Maintaining access:** Maintaining access is the process of sustaining accessibility to the computer system once access has been gained
5. **Cleaning tracks:** Clearing tracks are hiding one's malicious acts to prevent being uncovered.

## 1.4 THE ETHICAL HACKING PROCESS

The Ethical hacking process is put in place in order to overcome the hacking process and to test a computer system and network before a malicious attacker hacks the system. Ethical hacking process involves

- Planning
- Tools Selection
- Plan Execution
- Result Evaluation

### 1.4.1 Planning Step

The first step in ethical hacking is to firstly seek the necessary approval from the organisation, decision makers or the owner of the computer system and network to allow you to perform the hack. Then a detailed plan needs to be designed in which all the testing procedures to be performed on the computer system and network are enumerated. The detailed plan may include the following:

- The different computer systems and network which will be tested
- The timeline for the test
- The strategic of the test
- The different deliverables to be produced.
- A risk assessment plan, i.e. what happen if the computer system crash during the test.
- A contingency plan

### 1.4.2 Tools Selection

After having identified the computer system and network to hack, the appropriate tools need to be selected for that purpose in order to discover the weakness in the system. There are different commercial and open source security tools available to perform the hack. For example, to test a website, tools such as WebInspect could be used instead of Wireshark which is a network analyser. Below is a list of tools which can be used for ethical hacking:

- **Nmap** ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing (Nmap.org, 2018).
- **SuperScan** is a free connect-based port scanning software designed to detect open TCP and UDP ports on a target computer, determine which services are running on those ports, and run queries such as whois, ping, ICMP traceroute, and Hostname lookups (Wikipedia, 2018).
- **WebInspect**: Finds and prioritises web application vulnerabilities
- **QualysGuard**: Qualys Cloud Platform or QualysGuard consists of integrated apps to help organisations simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for all your IT assets – on premises, in clouds and on mobile endpoints (Qualys, 2018).

- **NetStumbler** (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards (NetStumbler, 2018).
- **Wireshark** is an open source packet analyser which is used for troubleshooting network, analyse packets and their associated network protocol.
- **Kismet** is a wireless network detector, sniffer, and intrusion detection system. Kismet works predominately with Wi-Fi (IEEE 802.11) networks, but can be expanded via plug-ins to handle other network types (Kismet, 2018).

### **1.4.3 Plan Execution**

Once all the necessary tools have been selected, it is time to execute the plan. However while executing the plan, it is important that privacy and confidentiality are maintained while the hacking is being performed. It may happen that during the hacking process, sensitive information are obtained and hence it is important not to disclose the information or it will be better to encrypt these information or files or password-protect them.

### **1.4.4 Result Evaluation**

Once the test or hack has been performed, all the security weaknesses uncovered should be assessed. Counterpart solutions and alternatives security solutions should be proposed (such as upgrades, security patches, new encryption mechanism). In case further investigation is required, this should be proposed as well. All the results, weaknesses and proposed recommendations should be documented and provided to the organisation or owner of the computer system and network. Furthermore, recommendation of another test should be proposed once the recommendation has been applied to test whether the security weaknesses have been resolved.

## **2. MALWARE THREATS**

### **2.1 Introduction**

Malwares are one of the biggest threats which all computer systems face in a daily manner. There are different types of malware ranging from Viruses to Worms and passing through Trojan horses. Those malwares keep evolving and it is important to always keep testing the computer system for these types of threats since they are backdoors for hackers to enter and cause maximum damage to the computer system. We shall now introduce how malwares are distributed, and the ways to detect and combat them.

### **2.2 Malware Threats**

Malwares are one of the biggest threats to your computer system and network. They are one of the preferred ways hackers adopt to cause maximum security damage to your system. Recently the Ransom malware re-invented by the hackers caused lots of inconveniences to computer system owners; they operate by blocking documents and these documents are only unlocked after payment has been effected: otherwise, if payment is not made, the documents will be automatically deleted.

Malwares propagate easily since they do not require user intervention. They are distributed through email attachments which once downloaded attack the computer system. The malware exploits the computer system vulnerabilities. Sometimes having an up-to-date antivirus does not necessary protect the computer system from new forms of malware (meaning that a fix will be found after the discovery of the malware but not right-away); however they certainly protect from older versions of malware. Unfortunately most owners of computer systems do not regularly update their antivirus or system patches to guard against malware.

Malwares have the ability to

- Log your keystrokes
- Delete or lock files
- Steal passwords
- Manipulate systems file
- Control webcams and microphones



### 2.3 Types of Malware

Trojan Horses	A Trojan Horse is a malicious computer program which conceals its malicious intention as a legitimate program with the goal to infect the computer system. For example, a user may be conned to download an email attachment which is in fact a malicious program which when clicked upon, will work in the background without the user's knowledge. Thus the Trojan horse will capture information, steal password or other details and remotely send the information to the hackers.
Viruses	Viruses are computer programs that are self-replicating (i.e., they can make several copies of themselves) and attach to executable files, delete files and crash the computer system whenever the user or computer system runs the program.
Worms	Worms are self-propagating programs that travel around the Internet at lightning speed. They load up in memory, effectively exploit known software vulnerabilities, and often end up crashing the systems.
Rootkit	A rootkit is a collection of computer software, typically malicious, designed to enable access to a computer or areas of its software that would not otherwise be allowed (for example, to an unauthorised user) and often masks its existence or the existence of other software (Wikipedia, 2018). Rootkits are mostly found on UNIX systems but are becoming popular on the Windows platform. Rootkits are sets of programs that either masquerade as typical administrator command-line programs or integrate into the kernel, or core, of the operating system (Beaver, K., 2004.)
Spyware	Spyware is a software that aims to gather information about a person or organisation without their knowledge, and then may send such information to another entity without the consumer's consent; it can also assert control over a device without the consumer's knowledge (Wikipedia, 2018).

Spyware is mostly classified as: adware, system monitors and tracking cookies.

## **2.4 Symptoms of an Infected Computer System**

Malwares work in various ways. Some malwares will run whenever the computer system is up and running while others will remain active as long as the application it is attached to is running.

Below are some common symptoms of an infected computer system:

1. The computer system has a slow response time.
2. Software in the computer systems are not working properly.
3. Disk drives or USB peripherals become inaccessible.
4. Strange and unusual error messages start appearing.
5. Websites or graphical user interfaces become distorted.
6. Software cannot be installed.
7. The computer system crashes and reboots each time.
8. Some folders become hidden.
9. Windows Explorer stops working.

## **2.5 Exploiting Operating System Programming Interfaces**

Malwares are designed to exploit the programming languages which the operating system supports. For example the Flashback (Trojan) malware affects both Windows and Mac OS X computer system. It exploits the Java (programming language) Security vulnerability to download additional malicious codes in the infected computer system so as to create a backdoor for hackers to steal files, execute command without the consent of the user and to delete files.

Another example is the ActiveX controls which are Windows-based programme that are exploited by hackers to exploit a computer system.

JavaScripts and VBScripts are also programming interfaces which are exploited by malware to gain access to the operating system of the computer system. JavaScripts and VBScripts are principally run on Web Browsers found on the user's computer system. If a user runs malicious JavaScripts and VBScripts on the web browser, they will cause harm to the user's computer system.

## 2.6 Malware Process Life Cycle

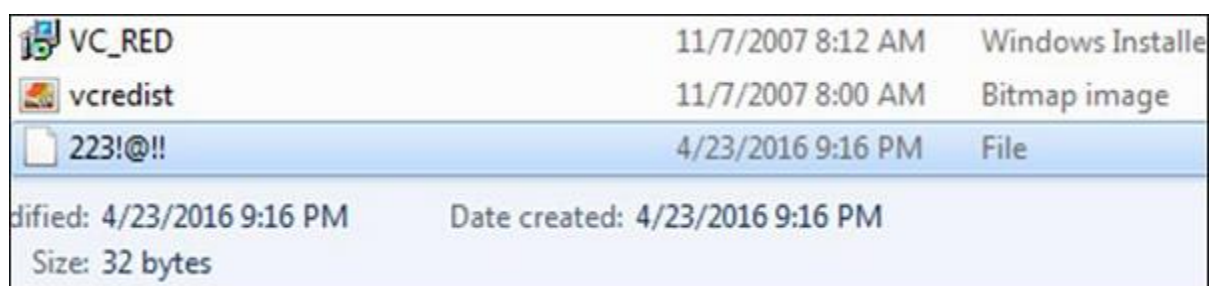
Malwares have the following characteristics:

- They cannot auto-start.
- They cannot propagate themselves by using non-executable files.

As a result, a malware needs a certain trigger to start acting. Therefore, to propagate a malware, emails are used. A hacker makes use of email attachments to attach the malware and sends the email to users. Unsuspecting users will click on the attachment thinking it is a genuine attachment and when the malware is clicked upon, it will either copy or delete local files, or try to use the user's email address contact to propagate itself to other users.

Once the malware has infected the computer system, it will reside in the computer system memory and will start as soon as the program to which it is attached starts running. Once the malware has started, it will start self-replicating itself and will also modify itself such that it is difficult to be found by an antivirus.

Afterwards it will hide in the operating systems by using encryption mechanism. Below is an example of how a malware encrypts itself using symbolic names.



VC_RED	11/7/2007 8:12 AM	Windows Install
vcredist	11/7/2007 8:00 AM	Bitmap image
223!@!!	4/23/2016 9:16 PM	File
Modified: 4/23/2016 9:16 PM		Date created: 4/23/2016 9:16 PM
Size: 32 bytes		

**Figure 5.2: Symbolic Names Attribution by a Malware (Malwares, 2018)**

## 2.7 Malware Detection Tools

This section shows the different investigation which can be done in order to detect a malware.

### 2.7.1 Malicious Port Detection

While investigating for malware in a computer system, one must screen for ports number which malwares will use to send and receive data.

For example NetAV (F-Secure, 2018) is a worm which propagates via emails. Once downloaded and run, this worm will look for .DOC files and will randomly pick one .DOC files on every Tuesday and transmit the file on port number 12345 and 12346. Hence screening those port numbers and monitoring the activities on these ports will show whether the computer system is infected or not.

Below is a list of common malware ports number (TechNet, 2018):

<b>Trojan Name</b>	<b>Port</b>
VooDoo Doll	1234
Trojan Cow	2001
NetMetro	5031
BladeRunner	5400
Portal of Doom	9872
SubSeven	27374
Back Orifice	54320

**Table 5.1: Malware Ports**

In order to monitor and screen activities on ports number, Netstat can be used. It shows all the active ports on the computer system. Using the command, netstat -a will display all the active port on the computer system. However Netstat will not tell us which program is using this port. But Netstat is a tool which is used to initiate the detection of malware.

```
C:\Users\Avi>netstat -a

Active Connections

Proto Local Address           Foreign Address         State
TCP   0.0.0.0:135             Avinash:0              LISTENING
TCP   0.0.0.0:445             Avinash:0              LISTENING
TCP   0.0.0.0:5357            Avinash:0              LISTENING
TCP   0.0.0.0:5800            Avinash:0              LISTENING
TCP   0.0.0.0:5900            Avinash:0              LISTENING
TCP   0.0.0.0:6646            Avinash:0              LISTENING
TCP   0.0.0.0:49664           Avinash:0              LISTENING
TCP   0.0.0.0:49665           Avinash:0              LISTENING
TCP   0.0.0.0:49666           Avinash:0              LISTENING
TCP   0.0.0.0:49668           Avinash:0              LISTENING
TCP   0.0.0.0:49669           Avinash:0              LISTENING
```

**Figure 5.3: Netstat**

### 2.7.2 Port Mapper

In order to map a program to its port on a local computer, a port mapper can be used. Examples of port mapper are Portmap (a Linux utility), rpcbind (a Solaris utility) and Startup Status (for Windows compatible utility). Below is an example of rpcbind (Wikipedia, 2018): it displays the program associated with the port number which is useful in order to track a specific malware.

```
$ rpcinfo -p
program vers proto  port
100000  2    tcp    111  portmapper
100000  2    udp    111  portmapper
100003  2    udp    2049 nfs
100003  3    udp    2049 nfs
100003  4    udp    2049 nfs
100003  2    tcp    2049 nfs
100003  3    tcp    2049 nfs
100003  4    tcp    2049 nfs
100024  1    udp    32770 status
```

**Figure 5.4: Portmap**

### 2.7.3 Registry Folder

Usually malware resides in the registry folder and they are initiated from the registry folder.

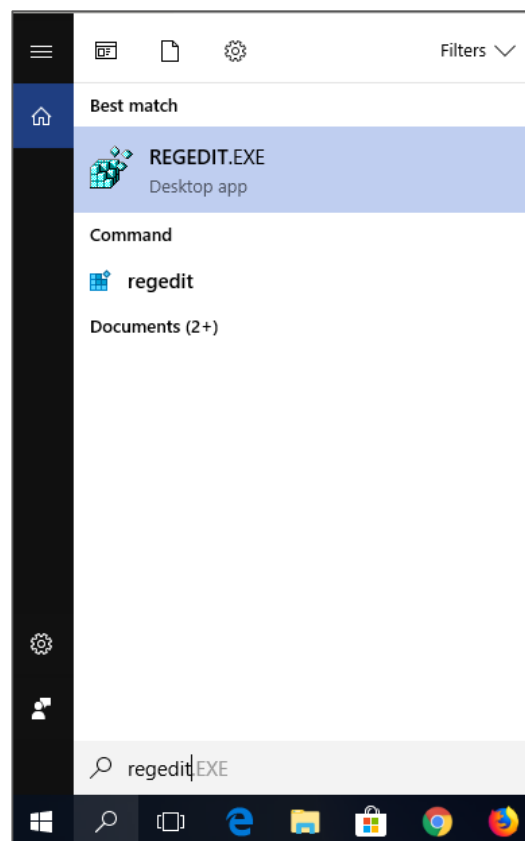
In Windows 10, the registry folder is accessed as follows:

1. Click on the search window



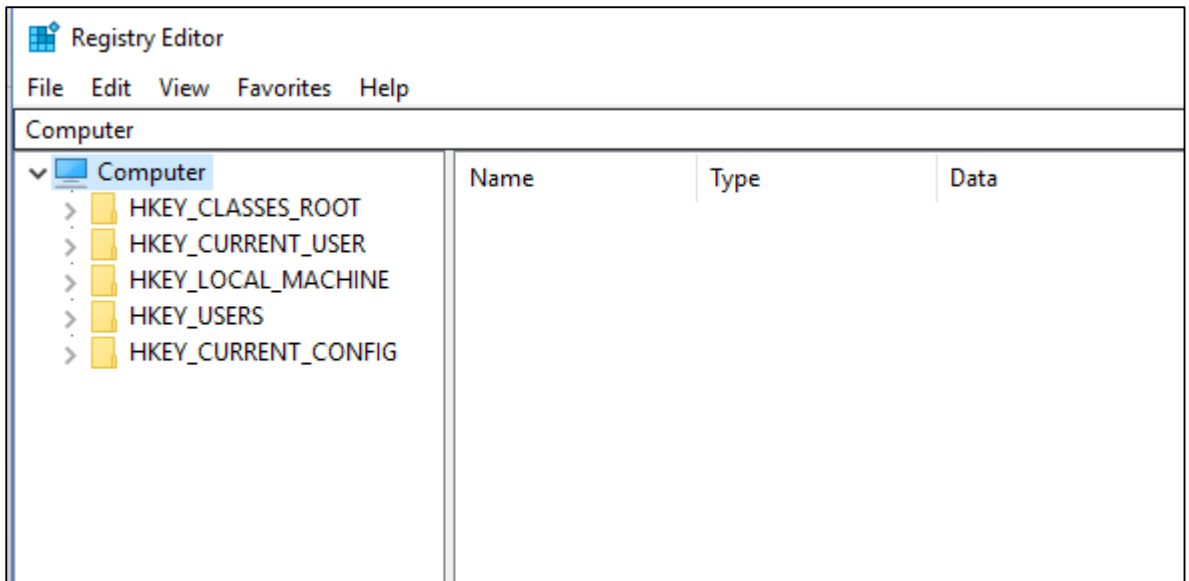
**Figure 5.5: .Search Windows 10**

2. Type regedit in the search bar



**Figure 5.6: Regedit.**

3. Click on the regedit.exe and let it run. You will be prompted for User Account Control, click Yes.



**Figure 5.7: Window Registry Editor**

4. Search in the HKEY\_LOCAL\_MACHINE for names which are weird. This can be an indication that a malware has been installed in the computer system.

Furthermore, Windows provides a list of utilities which can be downloaded to detect malware or to start preliminary investigation of malwares. Example of those downloaded utilities are Autologon, LogonSessions, NewSID, PsLoggedOn, PsLogList, RootkitRevealer and Sysmon. More utilities can be found on <https://docs.microsoft.com/en-us/sysinternals/downloads/security-utilities>

### **2.7.4 The ps Utility**

The ps utility is available in Linux operating systems and displays all the applications which are running in the computer system. This utility can be used to look for applications which have strange names and can then be removed.

## 2.8 PROTECTING AGAINST MALWARE

In order to protect a computer system against malware, the following steps can be adopted:

1. Avoid downloading free utilities from untrustworthy sources. These free utilities of unknown origin contain malwares such as adware, viruses and spyware which will infect the computer system.
2. Always have an updated antivirus utility. Antivirus is the main and basic protection software for a computer system. It scans for malicious code or malware in the computer system and it either quarantines the malicious software or deletes the malware from the computer system. If it is possible, use different antivirus from different vendors and other security tools such as a firewall and content filtering tools, to increase efficiency.
3. Always use strong passwords to protect your files and computer system. In case the computer system is compromised, the files will withstand password cracking software.
4. Always use a secure connection when transferring confidential information.
5. Always make regular backup of the files in the computer system.
6. Update the computer system with latest security patches.
7. Before running a software in a connected computer system network, always test and analyse the software for any suspicious behaviour in a stand-alone computer.
8. Make use of a firewall in a computer network system to prevent attacks from outside the network.
9. Ensure that email server removes emails that contain attachment such as .bat, .exe, .scr.
10. Train the staff in the organisation on security best practices.
11. Always scan external media for malwares before accessing the content in the drive.
12. Turn off services which are not frequently used since they are usually backdoors for malwares and hackers. For example, default operating system setting that install services such as FTP and Telnet can be switched off.

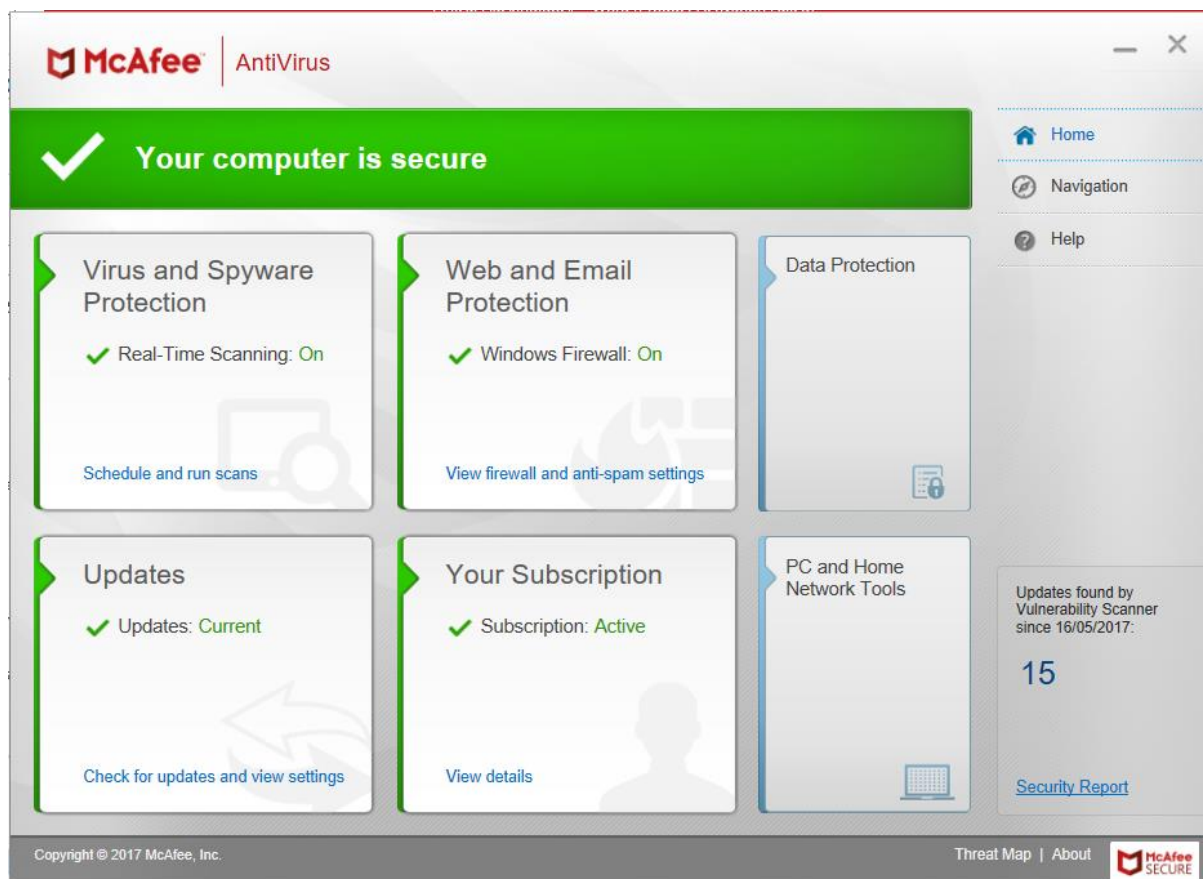


## 2.9 ANTIVIRUS

Antivirus are software utilised to avoid, detect and remove malware. Antivirus employs a diverse range of strategies to detect malware. One such strategy is the Signature-based detection: in this strategy, the antivirus searches for known patterns associated with a malware in executable code. The antivirus uses a virus definition which contains the signature of known malware. Once a malware has been detected, the antivirus tries to remove the malware. If the antivirus cannot remove the malware, it quarantines the file to prevent the malware to spread. Thus it is important to have an updated antivirus with the latest virus definition to protect the computer system from malware.

Example of known antiviruses are Norton Antivirus, McAfee and Avast.

Figure 5.8 shows a snapshot of McAfee Antivirus: It provides virus and spyware protection, Web and Email protection, updates of virus definition among others.



**Figure 5.8: Antivirus Utility**

## 3. NETWORK SECURITY ATTACKS

### 3.1 Introduction

There are different forms of attacks which happen to a computer system and network. Understanding these forms of attacks will help provide appropriate countermeasures and therefore provide better protection. Attacks can be categorised as either passive or active attacks.

In passive attacks, data are monitored without alternation whereas with active attacks, data are monitored with the intention to destroy, alter or corrupt the information in view to cause damage. Those types of attacks happen principally in a computer network environment where different computer systems are connected to each other.

### 3.2 Information Security

Information security has evolved over time in which the use of computer system and network are intensively being used. Computer systems are used to store information and the network is used to send/transmit information across the Internet. This has led to the concept of computer security and network security. Hence, *“Computer security is a collection of tools designed to protect data and thwart hackers and network security are measures to protect data during their transmission”*(Hussein Al-Bahadili, 2012).

Owing to the interconnected nature of computer systems, network security is becoming a significant aspect of information security. Most of the attacks performed nowadays are geared towards computer networks.

### 3.3 Network Security

Network security aims to provide a secure protocol in each layer of the TCP/IP stack protocol so that the complete network is secured, and not only the communication channel between the computer systems. However hackers try to attack the communication channel to monitor, capture, destroy, amend and replay the data contained in the packets. Therefore, network security aims to achieve **confidentiality** and **integrity properties**.

- Confidentiality: preventing an unauthenticated node from examining the information.

- Integrity: the data sent by the sender is the same when the receiver receives it. There has not been a change, modification, and alteration of the data after the sender has sent the information to the receiver.

### **3.4 Types of Attacks**

Attacks to network can be classified either as passive or active attacks.

#### **3.4.1 Passive Attacks**

Passive attacks are attacks which aim at learning about an information by monitoring the data travelling between the sender and receiver or analysing the data traffic flows without affecting the data and system resources. In passive attacks, confidentiality of the data is violated without affecting its state.

Examples of passive attacks are eavesdropping, traffic analysis and replay attacks.

- Eavesdropping: Eavesdropping involves capturing confidential information such as a password or secret data or public-private key by monitoring the data traffic flows. To safeguard against such attacks, encryption mechanism should be employed.
- Traffic Analysis: In traffic analysis, the network intruder monitors the data traffic between the sender and receiver so as to learn the type and amount of traffic between the source and destination. In this type of attack, there is no modification of the data.
- Replay Attacks: In a replay attack, the network intruder intercepts the message and resends the data after some time. One way to counteract replay attacks is to use digital signatures with timestamps or the use of random session keys which are generated frequently.

#### **3.4.2 Active Attacks**

Active attacks are attacks which aim at intercepting the data, and alter/modify or delete the information contained in the packets and then reintroduce the data in the network. In active attacks, both confidentiality and integrity of the data have been violated.

Examples of active attacks are Denial of Service (DoS), Sinkhole, Spoofing, Session Hijacking and web defacement attacks

##### **3.4.2.1 Denial of Service Attacks**

In a Denial of Service (DoS) attack, the attacker's aim is to prevent legitimate users from accessing data or services provided by the computer network. This attack is performed by sending a large amount of data packets to the computer systems and its network such that

both the computer system and the network cannot respond to legitimate requests of users. By keeping the receiver busy with illegitimate request, the receiver will not be able to respond to other requests, thus denying a service to other users. Besides, DoS attacks also aim at slowing down the network by flooding the network with a large amount of data such that the bandwidth is consumed by the attacker's request instead of user request. Such attacks are conducted against a single computer system or an entire organisation network.

DoS attacks are perpetrated against websites, email services, online banking systems and other services. The attacker aims to prevent legitimate users from accessing these services by stopping the website from loading the content, and preventing the system from getting access to the Internet. This is performed by "flooding" the network with information that it cannot handle.

DoS attacks can be categorised as follows:

- Simple DoS attacks: where attacks are being launched by a single computer system towards a single target in a network.
- Distributed Denial of Service attacks (DDoS): where attacks are being launched by a group of computer systems known as BOTs, BOTNETs or zombies towards a single target.

#### 3.4.2.1.1 DDoS Attacks Explained

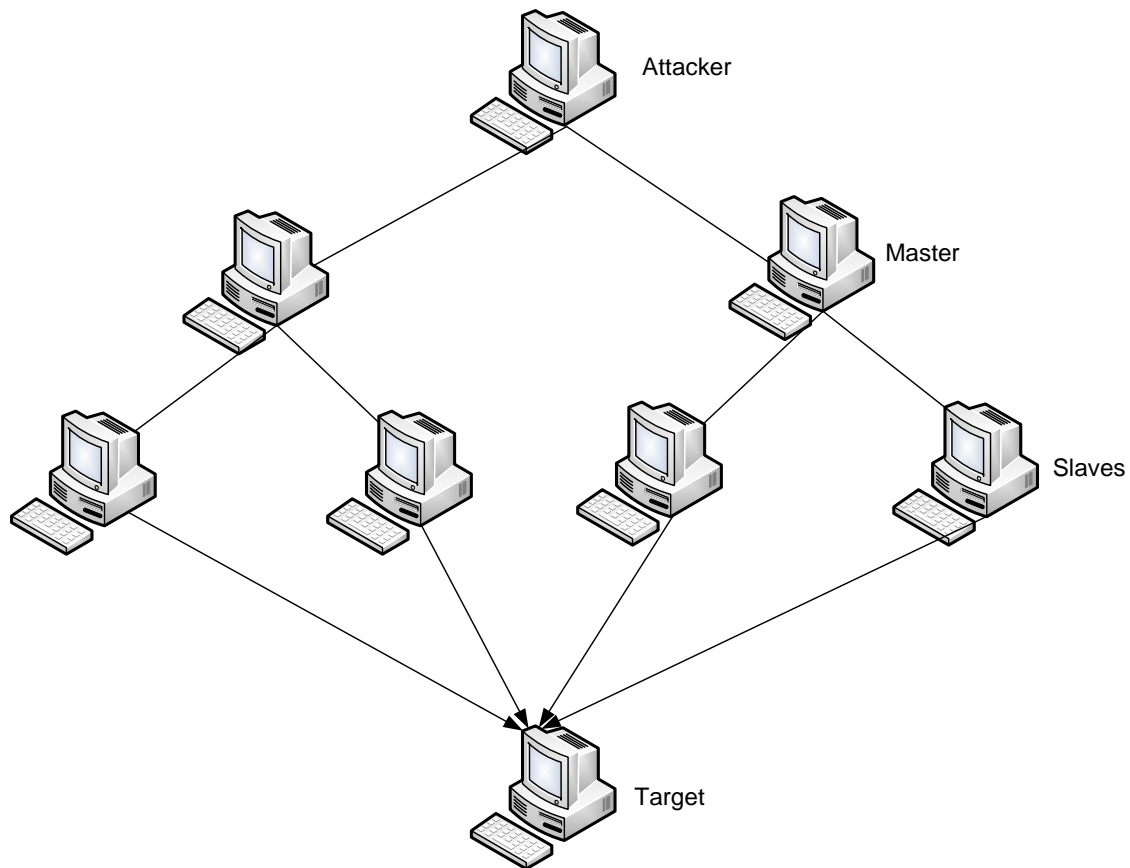
This section will provide a brief explanation on how Distributed Denial of Service (DDoS) attacks happen. As stated earlier DDoS attacks are launched by a group of computer systems which have been hacked to send a large number of packets to a single target such that the latter cannot handle legitimate requests from users.

To start a DDoS attacks, the hackers need to compromise a group of computer systems instead of a single computer system (DoS) in order to send coordinated packets to a single host. The group of compromised computer systems are also referred to as BOTs, BOTNETS or zombies and are then used to launch coordinated attacks to a victim system. DDoS attacks can become difficult to track since the attacks come from separate destinations with different IP addresses. Hence it is difficult to trace the actual originator of the attack.

DDoS systems can be broken down in four categories:

- i. Attacker/Hacker: The hacker will compromised a group of system to be under his control
- ii. Master: The master start the attacks
- iii. Zombie/BOT/BOTNET: A group of computer systems compromised by and managed by the master
- iv. Victim/Target: The computer system to be attacked by the zombies, BOT or BOTNET

Figure 5.9 illustrates the DDoS attacks.



**Figure 5.9 – DDoS Attack**

From Figure 5.9, an attacker/hacker needs to identify vulnerable computer systems and install DDoS tools into them in order to turn them into a Master computer system. Once we have master computer systems, the masters will search for other weak computer systems in order to turn them into zombies/BOT/BOTNETs and install DDoS tools. Example of DDoS tools used are Trinoo, WinTrinoo, Tribal Flood Network, DAVOSET, HULK (HTTP Unbearable Load King), Low Orbit Ion Cannon (LOIC), and hping.

The phase in which the attacker searches and identifies the masters and zombies in the computer system is known as the *intrusion phase*.

Then there is the DDoS attack phase in which the target system is being attacked by the zombies.

#### 3.4.2.1.2 Symptoms of a DoS or DDoS attacks

It should be mentioned that not all disruptions to a service are the product of a DoS attacks. However the following symptoms are an indication of a probably DoS or DDoS attacks:

- Abnormal slow network performance

- Inaccessibility of website
- An increase of spam emails

### 3.4.2.1.3 DoS & DDoS Prevention

Below are some security measures which can be utilised to counteract DoS and DDoS attacks:

- **Router Throttling:** The main aim is to control the flow of traffic leading towards a server or a potential target which is under attack. This is a proactive process in which the traffic is being regulated to avoid overloading a server or a potential target.
- **Network Filtering:** Filter packets before allowing them to enter the network. Filtering spoofed packets and discarding suspicious packets will decrease the chance of a DoS/DDoS attacks. Through the filtering mechanism, we can prevent an attacker from trying to take control of vulnerable computer systems. The use of firewall, intrusion detection system and enabling filtering in routers will help mitigate the attacks.
- **Honeypots:** Honeypots are included in a network in order to intercept malicious attackers. Normally honeypots are installed in well-defined places in the network. However it is recommended from time to time to vary the location of the honeypots to continuously monitor and trap malicious activities.
- **Push-back:** DDoS attacks generate a large amount of packets which often create congestion at the routers (e.g. filling up the router queue or resources) before coming to the target/victim system. As a result, routers can beforehand drop packets which are creating the congestion. The use of a Push back daemon is required which will analyse and decide which packets to drop.

Other migration approaches available are Divide and Conquer, Self-Cleansing Intrusion Tolerance and Moving Target Defence (Deka, 2017).

### **3.4.2.2 Sinkhole**

Sinkhole is a service attack that stops a node from receiving the complete and correct information. In this attack, the malicious node supplies wrong information to the client nodes such that the latter sends all its requests to that malicious node. In this attack, modification and dropping of packets are performed.

### **3.4.2.3 Spoofing**

A spoof attack is when a malicious node impersonates another node in the network in order to start attacks, intercept data and modify data against the nodes in the network. There are different categories of spoofing such as Internet Protocol (IP) address spoofing, Address Resolution Protocol (ARP) spoofing and Domain Name Server (DNS) spoofing. For example in DNS spoofing attacks, the attackers corrupt the DNS information found in the DNS resolver's cache and thus the DNS will provide an erroneous IP address for a particular domain name.

### 3.4.2.4 Session Hijacking

Session hijacking occurs when an attacker successfully takes control of a user session after the user has been properly identified with the server. In session hijacking, the hacker finds out the correct session ID or sequence number for the current undergoing client/server communication and then takes control of the client's session by generating the sequence number. Session hijacking principally targets applications which use Transport Control Protocol (TCP) and occurs in three phases:

- i. **Identification of a user session:** The hacker will monitor and track a user session after the latter has successfully been authenticated by a server. The hacker will also predict the next sequence to be used by the user.
- ii. **Resynchronisation of the connection between the attacker and user:** After the hacker has identified which sequence number is to be used, the hacker resynchronises the connection between the server and the user by either resetting the connection or terminating the connection between the server and the user.
- iii. **Inserting data by the hacker:** Once the connection has been resynchronised, the hacker will use the anticipated sequence number and send a packet to the server. The server will accept the packet thinking that the packet is coming from the authenticated user.

In session hijacking both the confidentiality and integrity of the data are compromised since the data can be modified/ altered by the hacker.

For an in-depth coverage of session hijacking, you can refer to SANS Institute White Paper: <https://www.sans.org/reading-room/whitepapers/windows/session-hijacking-windows-networks-2124>

#### 3.4.2.4.1 Session hijacking tools

There are several tools available to perform session hijacking. This section will enumerate a few of those tools.

- Juggernaut (Beyond Security, 1999) is a network sniffer tool used to hijack TCP session and operates on Linux. Juggernaut can be used to monitor all network traffic on the local area network or can be configured to listen for a special character known as a token. For example, Juggernaut can be used to monitor a login session, record all the traffic for that login session and identify the password for that session or simply hijack that session after the user has been authenticated.
- Hunt (Packet Storm, 2018) is a Linux- based program for monitoring and hijacking user sessions. Hunt mainly sniffs TCP connection, tracks it and resets the connection. The main features which Hunt offers
  - Connection Management - tracking a connection and detecting an ongoing connection,
  - Normal active hijacking with the detection of the ACK storm,
  - Address Resolution Protocol Spoofing,
  - Synchronization of the valid client with the server after hijacking,
  - Restarting a connection.
- T-Sight (En Garde Systems, 2018) is a Windows based program which is used to select active user session, predicts sequence number and hijack an active user session. T-Sight is a licensed software offered by En Garde Systems.

- IP Watcher is another software licensed by En Garde Systems (En Garde Systems, 2018). IP Watcher is a network security tool used to control unencrypted login session on the local area network. It is used mainly for “*investigating suspicious activity, obtaining evidence of misuse, and even stopping malicious users before they do any damage*”.
- Achilles is a hijacking tool for intercepting principally HTTP session data (web connection). This tool will capture data between the user and server connection and will modify the data so as to hijack the web session.

#### **3.4.2.4.2 Preventing Session Hijacking**

Below are some security measures which can be utilised to counteract Session Hijacking:

- IPsec: IPsec is an encryption mechanism employed at the network level. The packets which carry the data are encrypted. As a result, a hacker will not be able to monitor an ongoing connection since the packet is encrypted. Thus the hacker will not be able to hijack the connection since the attacker will not be able to decrypt the data. As a result, the hacker will not be able to predict the sequence number which is an important step to hijack a connection.
- Secure Sockets Layers (SSL): SSL protects data being sent over a web connection and is available in most browsers. An example is the HTTPS which means that the web connection is secure and data is encrypted during the browsing session.
- Secure Shell (SSH): SSH protects the local area network from IP spoofing which is the usual starting methods to hijack a connection. Therefore protecting the IP address reduces the risk of session hijacking.
- Session Timeout: This allows a connection to timeout after some time of inactivity. Allowing a session to remain active indefinitely will facilitate the task of the hacker to monitor and sniff the connection to determine the sequence number.

Other measures that can be employed to limit session hijacking are the use of robust authentication, use of strong username and password, and use of firewall.

#### **3.4.2.5 Web Attacks**

Websites are continuously under attacks. They are primarily the interface between the client (user/web application) and the server (service to be rendered). If a website is hacked, then both the client and the server are under threat. For example, online banking involves a web application for the user to be able to perform a financial transaction and the processing is performed at the web server. The web server will host the database which stores the user’s banking details. The web application will enable the user to access the database over the Internet. If the web application and the web server are compromised, then the confidentiality and integrity of the data are at risk. It is important to secure the web application, communication between the web application and web server, and the web server.



### 3.4.2.5.1 Hypertext Transfer Protocol

For communicating between a web application and a web server, the Hypertext Transfer Protocol (HTTP) is used. The HTTP will allow a web client to exchange information with the web server. For example, to login to Facebook website, a user will use the browser (which acts as a web client or web application) and will type in the address bar of the browser the following url: <http://www.facebook.com>. The browser will use the HTTP protocol to connect with the Facebook web server. Once connected with the server, data can be exchanged. All the data (pictures and videos) reside in the web server. The data will be transferred to the user's browser to view the pictures. Therefore, understanding how the web application and server work will enable to secure it from hackers and attackers.

### 3.4.2.5.2 Web Server Weaknesses

- **Default Web Server Configuration:** There are different web server programs available, for example, Apache, Microsoft Internet Information Server (IIS) and Nginx to be able to communicate with the web application. However, while configuration the web server, the default parameters are maintained which make the web server vulnerable to hackers. Therefore it is important to ensure that proper permission and restrictions are configured for each user (web application) according to his/her status. If default setting is maintained for any user, a hacker will be able to get access to the server and to the data.
- **Software Flaws:** Web servers are software programs which can carry flaws and are installed on top of other software such as Operating Systems. Therefore it is important that the flaws are found and rectified. Updating the software either by upgrading to a newer version or by applying patches is important to ensure loopholes do not exist.
- **Buffer Overflow:** A web server can be victim of buffer overflow where too many data are sent to the web server so that it cannot handle them. Therefore it is important that enough resources are provided to be able to handle the data and also to differentiate between legitimate data and a DoS attack.

Other potential web server weaknesses are as follows: intercepting privileges permissions for the owner of the web server, using DNS spoofing to reroute a user to another web server, using SQL injection to get access to the database in case both the database and web server are on the same system, altering the URL of the website to redirect user to another web server.

### 3.4.2.5.3 Securing the Web Server

It is important to secure a web server so that hackers do not exploit its vulnerabilities. Below are some ways which will help increase the security of the web server:

- Do not use default settings and ensure that the correct permissions and privileges are given to everyone using the webserver. In some cases, revoke permissions and privileges for suspecting users.
- Disable default application such as FTP (file transfer protocol) or Telnet or SSH which are on the same computer systems as that of the web server. This will prevent hackers from connecting to the web server.
- Restrict the number of software to be installed on the web server to only a bare minimum to avoid being exploited due to software flaws.
- Prevent users from browsing the web server configuration file.
- Always upgrade and apply patches.

- Apply bounds checking to avoid buffer overflow.
- Ensure that a firewall is active between the web server and the Internet.
- Disable ports which will not be utilised.

#### 3.4.2.5.4 Web Application Weaknesses and associated solutions

The web application is a program which will enable the user to get access to the information stored in the web server. The web application will display the information for the user. Usually a web application will be a website implemented using HTML, JavaScript or VB Script and CSS programming language. A browser will render the codes of the web application for the user. Furthermore, the web application will also provide other functionalities such as access to database, email and forum.

Below are some weakness associated with the web application and suggested solutions:

- **Cross-Site Scripting (XSS) or Script Injection:** XSS is the ability to inject scripts in the web application to be run on to the web server. XSS is the ability to execute web server commands by the values input from user onto the web application. Without proper validation of user input, server commands can be executed. There are different types of XSS namely Stored, Reflected and DOM (Document Object Model). One way to limit this flaw is to validate form fields, cookies and query fields.
- **SQL Injection:** SQL injection enables an attacker to take control of the query to be sent by the web application to the web server. Therefore by modifying the query, an attacker can create, update and modify records or transactions of the database found at the webserver. One measure to counteract this flaw is to introduce common SQL delimiter in the query such as single quote ‘.
- **Session hijacking:** Once the user has been authenticated by the server, the session can be hijacked. Using the measures as described in 3.4.2.4.2 will limit this flaw.
- **Cookie Poisoning:** Cookies is an important part of the HTTP protocol. Cookies are used by the web server which sends data to the web application and the latter will store and resend it to the web server. Cookies are sent to the web server each time the web application sends a request. Cookies contains sensitive information such as the user identification and session state. Therefore intercepting the cookie will put at risk both the web application and web server. Hence it is important that the cookie are authenticated.
- **Bruteforce:** Almost all web applications make use of a login functionality which requests the username and password of the user. This is basically the first step in hacking into someone’s account by trying to guess the username and password. Bruteforce attacks try all combinations of username and password in order to get access to the account. Automated tools are available in order to guess the credential. For example, Burp Intruder (Portswigger, 2018) is an automated tools to attack web applications. To guess password, the dictionary attack can be used, that is try all the word found in a dictionary as password. To avoid bruteforce attacks, make use of strong username and password.
- **Buffer Overflow:** Web application needs to store information input by the user as well as information obtained from the web server. Overloading the memory of the web application with too much data will cause buffer overflow. To avoid such problem, perform user input validation and bound checking validation.