

Reference Material

UNIT-3 HACKING INTO SYSTEM

What Is System Hacking in Ethical Hacking

In the popular imagination, the term “hacking” is synonymous with system hacking, a growing concern in cybersecurity. While malicious actors try to break into a computer system, their ethical hacker counterparts work with companies to stop these attackers in their tracks. This article will discuss everything you need to know, including the definition of system hacking, the various steps of system hacking, and the role of system hacking in [ethical hacking](#). Learn ethical hacking with a [ethical hacking course](#).

System Hacking : Explained in Brief

System hacking refers to using technical skills and knowledge to gain access to a computer system or network. Hackers employ many methods to get into a system by exploiting its vulnerabilities and concealing their activities to avoid detection.

Most people imagine system hacking as the work of so-called “black hat” or “gray hat” hackers who haven’t obtained the owner’s permission to enter the system. However, system hacking is also done by [ethical hackers](#) who received authorization beforehand to test the system’s security and improve any weaknesses.

The purpose of system hacking depends on the motivations of those who perform it. Malicious actors seek to exploit their discoveries after hacking into the system, usually for financial or political gain. Ethical hackers, however, are hired by companies as security consultants to help identify and fix vulnerabilities before these same malicious actors can exploit them.

How Malicious Actors Carry Out System Hacking

Malicious actors make use of multiple system hacking tools and techniques. System hacking software such as Nmap, Metasploit, Wireshark, and Acunetix help attackers detect and capitalize on vulnerabilities in the target system. Attackers may also use dedicated tools such as a phone hacking system for mobile devices.

Perhaps the best operating system for hacking is Kali Linux, a distribution of Debian Linux. Kali Linux has a wide range of security and penetration tools and is highly customizable, making it likely the best OS for hacking. Specific use

cases such as Kali Linux wifi hacking can be executed through pre-installed tools such as Aircrack-ng.

The System Hacking Steps / Types:

System hackers generally follow a well-worn set of steps to gain and maintain access to a system. Below, we'll discuss each of the four system hacking steps in detail.

First and foremost, system hackers must be able to access a system. This can be accomplished in multiple ways:

- **Password attack:** In perhaps the most basic technique, attackers can attempt to enter a system by entering the login credentials of a legitimate user. So-called “brute force” attacks try to guess a user’s password by testing all possible combinations until the correct one is discovered.
- **Stolen credentials:** System hackers may already have a user’s credentials, making it easy to access the system. For example, the user may have been tricked by a phishing email into divulging their password. Attackers also use databases of usernames and passwords exposed after a data breach, assuming that users reuse the same password for multiple systems.
- **Vulnerability exploitation:** New vulnerabilities are constantly being discovered in computer systems, while old ones may still be unpatched. Technically sophisticated attackers can exploit the vulnerabilities they discover through techniques like [SQL injection](#), [cross-site scripting](#), and [buffer overflows](#).

Password Cracking

Password cracking is the most enjoyable hacks for bad guys. It increases the sense of exploration and useful in figuring out the password. The password cracking may not have a burning desire to hack the password of everyone. The actual password of the user is not stored in the well-designed password-based authentication system. Due to this, the hacker can easily access to user's account on the system. Instead of a password, a password hash is stored by the authentication system. The hash function is a one-way design. It means it is difficult for a hacker to find the input that produces a given output. The comparison of the real password and the comparison of two password hash are almost good. The hash function compares the stored password and the hash

password provided by the user. In the password cracking process, we extract the password from an associated passwords hash.



Using the following ways, we can accomplish it:

1.Dictionary attack: Most of the users use common and weak passwords. A hacker can quickly learn about a lot of passwords if we add a few punctuations like substitute \$ for S and take a list of words.

2.Brute-force guessing attack: A given length has so many potential passwords. If you use a brute-force attack, it will guarantee that a hacker will eventually crack the password.

3.Hybrid Attack: It is a combination of Dictionary attack and Brute force attack techniques. This attack firstly tries to crack the password using the dictionary attack. If it is unsuccessful in cracking the password, it will use the brute-force attack.

4.Malware. Similar to phishing, using malware is another method of gaining unauthored access to passwords without the use of a password cracking tool. Malware such as [keyloggers](#), which track keystrokes, or screen [scrapers](#), which take screenshots, are used instead.

5.Rainbow attack. This approach involves using different words from the original password in order to generate other possible passwords. Malicious actors can keep a list called a [rainbow table](#) with them. This list contains leaked

and previously cracked passwords, which will make the overall password cracking method more effective.

6.Guessing. An attacker may be able to guess a password without the use of tools. If the threat actor has enough information about the victim or the victim is using a common enough password, they may be able to come up with the correct characters.

Default password database:

The term “attack” is used here to denote performing a variety of hacks, including brute force and social engineering, that require access to the target’s computer system or network. Here are some terms and processes related to this skill boot camp:

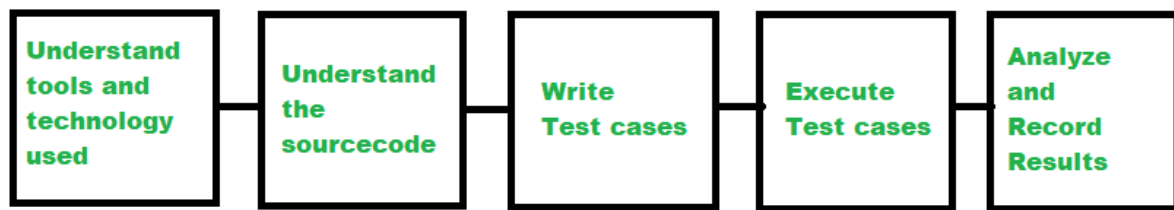
- Brute Forcing
- Password Hashing
- Capture The Flag (CTF)
- Phishing

1.Brute Forcing:

[Brute forcing](#) is the process of attempting password guesses against a computer system in order to gain unauthorized access to it. Brute forcing a password is a common practice among hackers, even though it is not used by most penetration testers, who instead prefer to employ [social engineering](#) tactics and exploits. To perform brute forcing, a hacker attempts combinations of words or numbers in the hope of eventually finding one that works on the target computer or network. It’s a popular technique because some people use weak passwords.

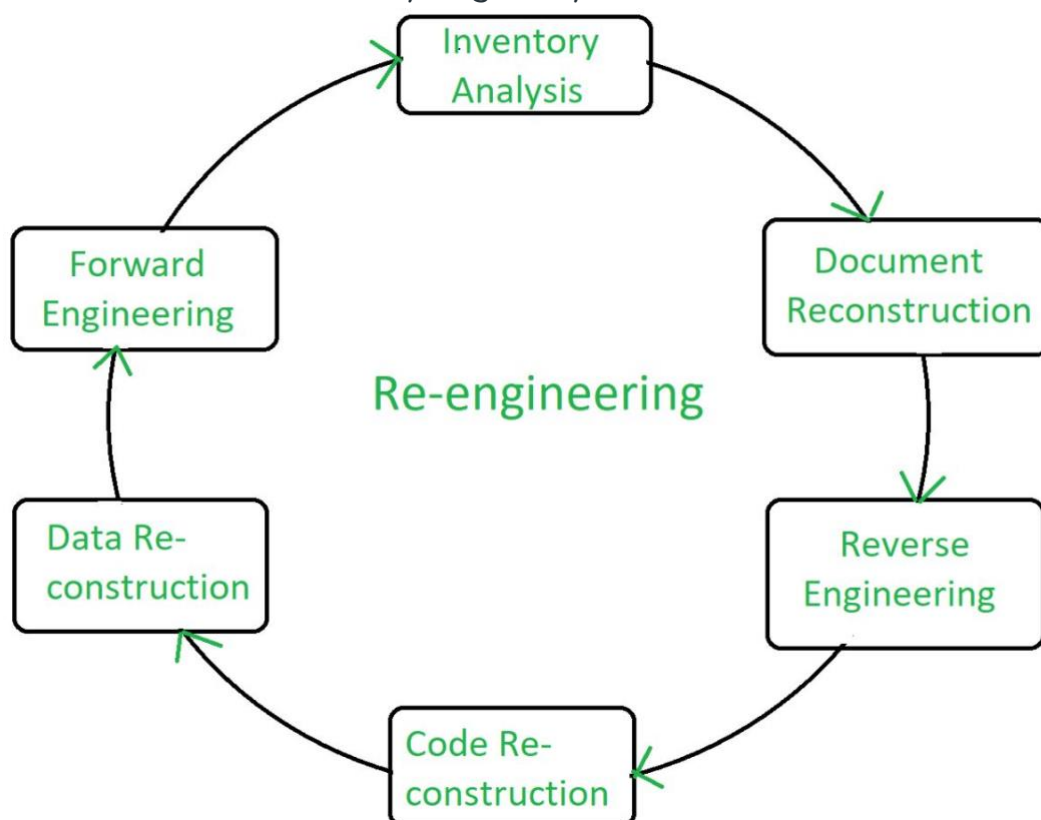
Password Hashing

[2.A Password Hashing System](#) (PHS) is a method of storing passwords securely, making them difficult for an unauthorized person to crack through brute force or dictionary attacks. A PHS is often referred to as a one-way hash function because the password is not reverse engineered after input, but rather the result is always the same (the hashed password). When entered into a target computer or network, all PHS’s return the same “hash value” which typically cannot be changed using traditional attack methods such as brute force and dictionary attacks.



3.Capture The Flag:

[Capture the Flag \(CTF\)](#) is a computer security competition in which teams compete to obtain as many flags as possible from a selected set of computers, and return them to their own base before time runs out. Typically, the goal is to infiltrate a secure computer system or network and retrieve data that can be used for further analysis or exploitation. CTF is generally used for training forensic technicians, penetration testers, and security engineers in several key areas including [reverse engineering](#), social engineering, assessments, and exploits. Once the flags are captured, teams are scored based on how many flags they obtained.



4. Phishing:

Phishing is a form of attack in which an attacker sends e-mails and malicious websites to entice a victim to reveal confidential information such as passwords, credit card numbers, and bank account information. The attacker then uses that information to compromise the target computer network or system. The term originates from “fishing”, as in using a fishing line to catch a fish. It is an unauthorized attempt to acquire the sensitive information of the victim by sending them a malicious or suspicious link.

MANUAL & AUTOMATED PASSWORD CRACKING:

We have passwords for emails, databases, computer systems, servers, bank accounts, and virtually everything that we want to protect. Passwords are in general the keys to get access into a system or an account.

In general, people tend to set passwords that are easy to remember, such as their date of birth, names of family members, mobile numbers, etc. This is what makes the passwords weak and prone to easy hacking.

One should always take care to have a strong password to defend their accounts from potential hackers. A strong password has the following attributes –

- Contains at least 8 characters.
- A mix of letters, numbers, and special characters.
- A combination of small and capital letters.

Key Points:

- Brute force attack is the most commonly used attack method for hacking.
- Password Hashing System is widely used on all platforms.
- Capture the Flag can be performed by multiple users simultaneously, which motivates hackers to improve their skills more.

Role of Attackers:

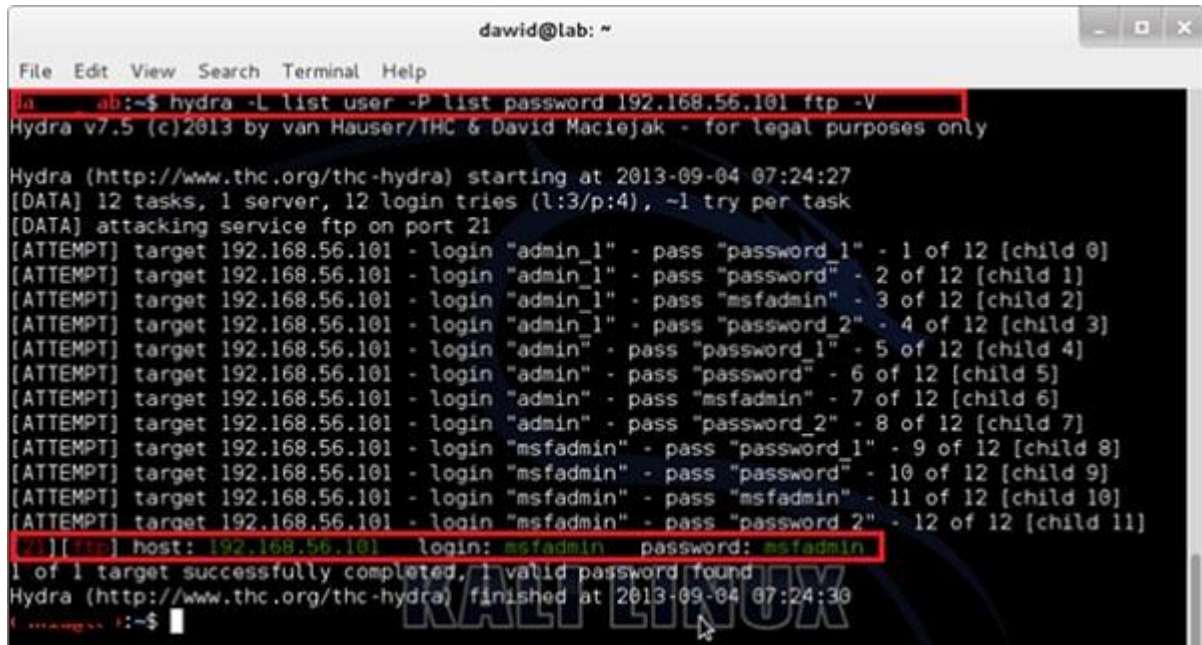
A penetration tester or ethical hacker seeks to gain unauthorized access to a shared network or system through the use of tools and methods that are related to physical security, network security, and social engineering. The attacker may test a system via one of several routes, such as via default accounts, operating systems and applications, services/ports, and open services/ports.

Dictionary Attack

In a dictionary attack, the hacker uses a predefined list of words from a dictionary to try and guess the password. If the set password is weak, then a dictionary attack can decode it quite fast.

PASSWORD CRACKING TOOLS

Hydra is a popular tool that is widely used for dictionary attacks. Take a look at the following screenshot and observe how we have used Hydra to find out the password of an FTP service.

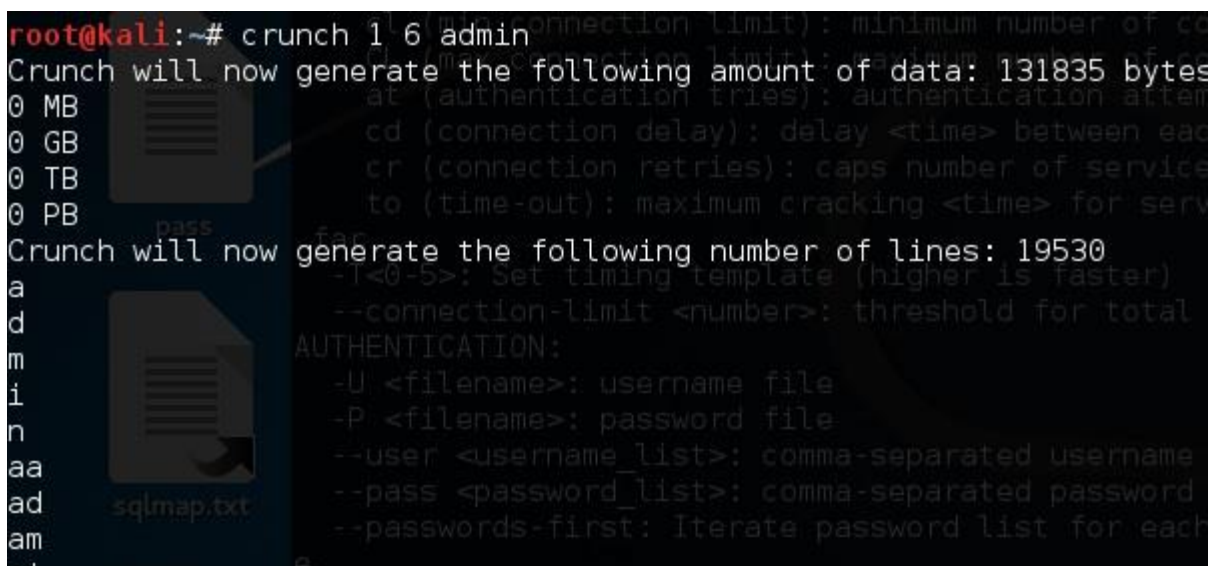


```
dawid@lab: ~  
File Edit View Search Terminal Help  
da ab:~$ hydra -L list user -P list password 192.168.56.101 ftp -V  
Hydra v7.5 (c)2013 by van Hauser/THC & David Maciejak - for legal purposes only  
  
Hydra (http://www.thc.org/thc-hydra) starting at 2013-09-04 07:24:27  
[DATA] 12 tasks, 1 server, 12 login tries (l:3/p:4), ~1 try per task  
[DATA] attacking service ftp on port 21  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_1" - 1 of 12 [child 0]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password" - 2 of 12 [child 1]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "msfadmin" - 3 of 12 [child 2]  
[ATTEMPT] target 192.168.56.101 - login "admin_1" - pass "password_2" - 4 of 12 [child 3]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_1" - 5 of 12 [child 4]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password" - 6 of 12 [child 5]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "msfadmin" - 7 of 12 [child 6]  
[ATTEMPT] target 192.168.56.101 - login "admin" - pass "password_2" - 8 of 12 [child 7]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_1" - 9 of 12 [child 8]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password" - 10 of 12 [child 9]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "msfadmin" - 11 of 12 [child 10]  
[ATTEMPT] target 192.168.56.101 - login "msfadmin" - pass "password_2" - 12 of 12 [child 11]  
[*][*][*] host: 192.168.56.101 login: msfadmin password: msfadmin  
1 of 1 target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2013-09-04 07:24:30  
da ab:~$
```

Hybrid Dictionary Attack

Hybrid dictionary attack uses a set of dictionary words combined with extensions. For example, we have the word “admin” and combine it with number extensions such as “admin123”, “admin147”, etc.

Crunch is a wordlist generator where you can specify a standard character set or a character set. **Crunch** can generate all possible combinations and permutations. This tool comes bundled with the Kali distribution of Linux.

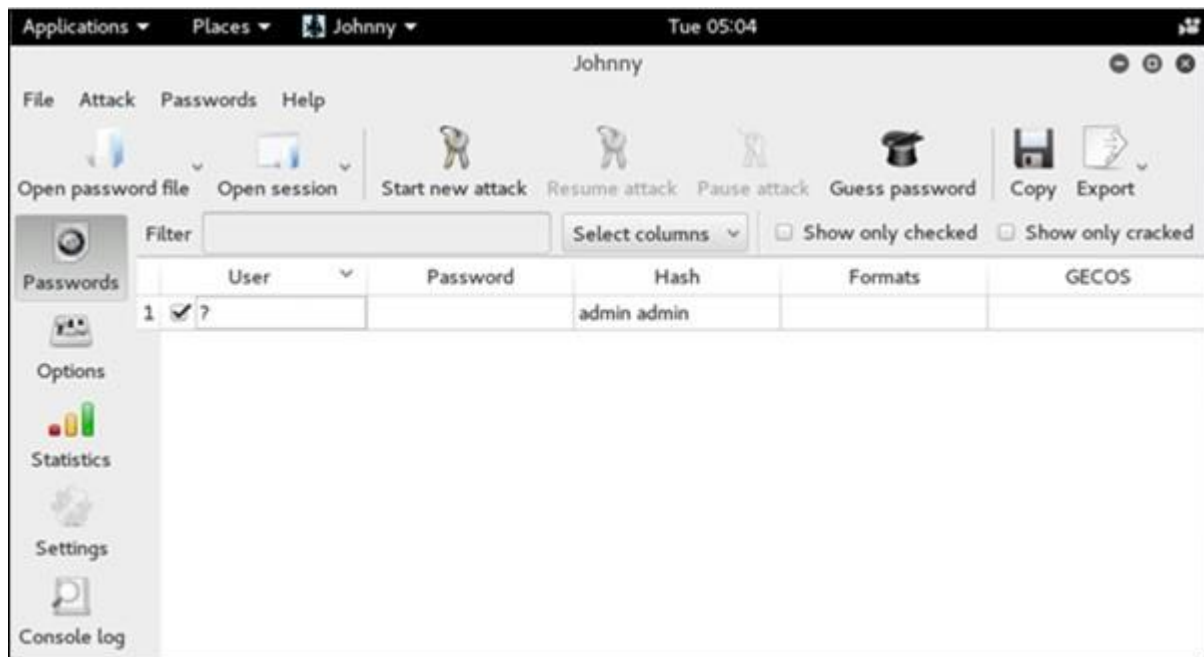


```
root@kali:~# crunch 1 6 admin  
Crunch will now generate the following amount of data: 131835 bytes  
0 MB  
0 GB  
0 TB  
0 PB  
Crunch will now generate the following number of lines: 19530  
a  
d  
m  
i  
n  
aa  
ad  
am  
ai  
-l <0-5>: Set timing template (higher is faster)  
--connection-limit <number>: threshold for total  
AUTHENTICATION:  
-U <filename>: username file  
-P <filename>: password file  
--user <username_list>: comma-separated username  
--pass <password_list>: comma-separated password  
--passwords-first: Iterate password list for each
```

Brute-Force Attack

In a brute-force attack, the hacker uses all possible combinations of letters, numbers, special characters, and small and capital letters to break the password. This type of attack has a high probability of success, but it requires an enormous amount of time to process all the combinations. A brute-force attack is slow and the hacker might require a system with high processing power to perform all those permutations and combinations faster.

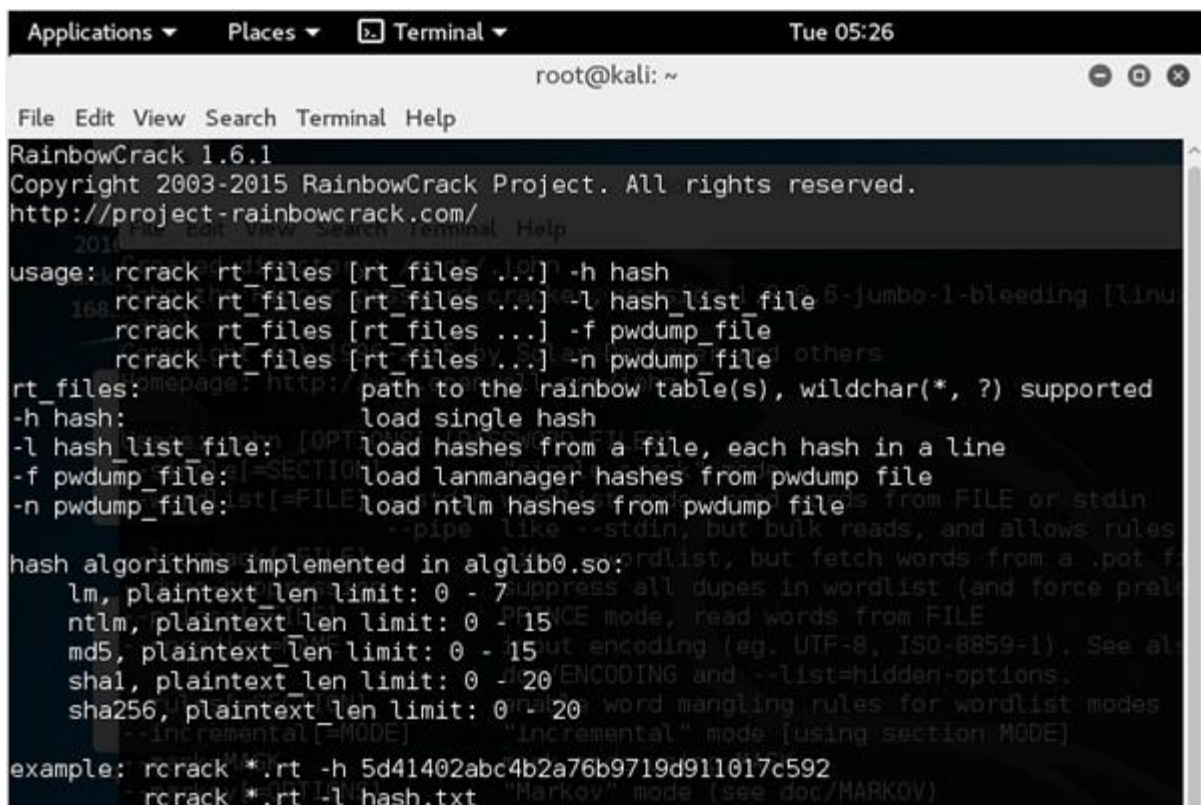
John the Ripper or **Johnny** is one of the powerful tools to set a brute-force attack and it comes bundled with the Kali distribution of Linux.



Rainbow Tables

A rainbow table contains a set of predefined passwords that are hashed. It is a lookup table used especially in recovering plain passwords from a cipher text. During the process of password recovery, it just looks at the pre-calculated hash table to crack the password. The tables can be downloaded from <http://project-rainbowcrack.com/table.htm>

RainbowCrack 1.6.1 is the tool to use the rainbow tables. It is available again in Kali distribution.

A screenshot of a terminal window on a Kali Linux system. The window title is 'root@kali: ~' and the date/time is 'Tue 05:26'. The terminal shows the output of the 'rccrack' command with the '-h' flag, displaying the help text for RainbowCrack 1.6.1. The help text includes copyright information, a website link, and a detailed list of command-line options and their functions. The options include '-h hash', '-l hash_list file', '-f pwdump_file', and '-n pwdump_file'. It also lists implemented hash algorithms (lm, ntlm, md5, sha1, sha256) and their plaintext length limits. The terminal text is as follows:

```
RainbowCrack 1.6.1
Copyright 2003-2015 RainbowCrack Project. All rights reserved.
http://project-rainbowcrack.com/

usage: rccrack rt_files [rt_files ...] -h hash
       rccrack rt_files [rt_files ...] -l hash_list file
       rccrack rt_files [rt_files ...] -f pwdump_file
       rccrack rt_files [rt_files ...] -n pwdump_file

rt_files: path to the rainbow table(s), wildchar(*, ?) supported
-h hash:  load single hash
-l hash_list file: load hashes from a file, each hash in a line
-f pwdump_file:  load lanmanager hashes from pwdump file
-n pwdump_file:  load ntlm hashes from pwdump file

hash algorithms implemented in alglib0.so:
lm, plaintext_len limit: 0 - 7
ntlm, plaintext_len limit: 0 - 15
md5, plaintext_len limit: 0 - 15
sha1, plaintext_len limit: 0 - 20
sha256, plaintext_len limit: 0 - 20

example: rccrack *.rt -h 5d41402abc4b2a76b9719d911017c592
         rccrack *.rt -l hash.txt
```

PROCESS OF System Hacking

Malicious actors make use of multiple system hacking tools and techniques. System hacking software such as Nmap, Metasploit, Wireshark, and Acunetix help attackers detect and capitalize on vulnerabilities in the target system. Attackers may also use dedicated tools such as a phone hacking system for mobile devices.

Perhaps the best operating system for hacking is Kali Linux, a distribution of Debian Linux. Kali Linux has a wide range of security and penetration tools and is highly customizable, making it likely the best OS for hacking. Specific use cases such as Kali Linux wifi hacking can be executed through pre-installed tools such as Aircrack-ng.

The System Hacking Steps

System hackers generally follow a well-worn set of steps to gain and maintain access to a system. Below, we'll discuss each of the four system hacking steps in detail.

1. Gaining Access

First and foremost, system hackers must be able to access a system. This can be accomplished in multiple ways:

- **Password attack:** In perhaps the most basic technique, attackers can attempt to enter a system by entering the login credentials of a legitimate user. So-called “brute force” attacks try to guess a user’s password by testing all possible combinations until the correct one is discovered.
- **Stolen credentials:** System hackers may already have a user’s credentials, making it easy to access the system. For example, the user may have been tricked by a phishing email into divulging their password. Attackers also use databases of usernames and passwords exposed after a data breach, assuming that users reuse the same password for multiple systems.
- **Vulnerability exploitation:** New vulnerabilities are constantly being discovered in computer systems, while old ones may still be unpatched. Technically sophisticated attackers can exploit the vulnerabilities they discover through techniques like [SQL injection](#), [cross-site scripting](#), and [buffer overflows](#).

2. Escalating Privileges

Once inside the computer or network, a system hacker may not be able to carry out the entire plan of attack right away. Instead, the hacker needs to exploit bugs or flaws in the system to gain additional privileges beyond those authorized initially. This process is known as privilege escalation.

There are two main types of privilege escalation: horizontal and vertical.

- In **horizontal privilege escalation**, the attacker initially gains access to a standard user’s account before spreading throughout the network to other user accounts. These other accounts may have files, applications, and emails that will be useful in the attack.
- In **vertical privilege escalation**, the attacker seeks to possess a higher-level user account, such as one with administrator or root access. This access makes it much easier for hackers to continue their attacks undetected and launch more diverse attacks.

3. Maintaining Access

Even after gaining access to the system, hackers must work to maintain this access so that the attack isn't interrupted—or if it's interrupted, it can continue later.

For instance, the attackers may install keyloggers or spyware on a system to record the user's activities and keystrokes. By secretly capturing user credentials, attackers can re-enter the system later, even if the password is changed.

Another technique to maintain access is installing a backdoor: a hidden “portal” that allows hackers to bypass normal security controls and directly enter the system. This can be done through malware such as Trojan horses that appear innocuous and remain hidden for a long time.

4. Clearing Logs

Finally, system hackers must cover their tracks to prevent or delay their target from discovering the attack. One common practice is to clear the system logs, which can provide crucial evidence that an attacker has gained unauthorized entry. Hackers may use tools such as Meterpreter to erase the proof of their movements throughout the network.

An additional essential step involves hackers deleting the history of the commands they've executed in shell programs such as Bash (for Linux) or the Windows shell. Without deleting these commands, victims could examine their shell history to reconstruct the attacker's actions precisely.

Using keyLoggers in Ethical Hacking:

Keyloggers are many hackers and script kiddie's favorite tools. Keylogging is a method that was first imagined back in the year 1983. Around then, the utilization of this product was uncommon and just the top examination organizations and spies could get their hands on it, yet today, it is a typical element offered by most government operative applications like TheOneSpy. Individuals use it as an opportunity to guarantee the assurance of their families, organizations, and the ones they care about.

Keylogger is a software that records each and every keystroke you enter, including mouse clicks. Hardware keyloggers are also available which will be inserted between keyboard and CPU. It provides the following features:

1. It takes a minute to install this software/hardware in the victim's system, from the next second onwards attacker will get every activity going on in the victim computer.
2. Each and every activity happening in the victim's system with screenshots will be recorded. This activity will be saved in the victim's system or it can be mailed to the attacker email or can be uploaded to the FTP server.
3. Keylogging highlight of spy applications is adept at recording each and every keystroke made by utilizing a console, regardless of whether it is an on-screen console.
4. It likewise takes a screen capture of the screen when the client is composing (Usually this screen capture is taken when a click on the mouse is clicked).
5. It works watchfully, escaped the client's view, for example, the focused on the client could never discover that all his keystrokes are being recorded.
6. Keyloggers recorder can record writings, email, and any information you compose at whatever point using your support.
7. The log record made by the keyloggers would then have the option to be sent to a predefined gatherer.
8. Some keyloggers tasks will likewise record any email that tends to your use and Web website URLs you visit.

Some software keyloggers code can capture additional information without requiring any keyboard key presses as input. They include:

1. **Clipboard logging:** Anything duplicated to the clipboard is caught.
2. **Screen logging:** Randomly coordinated screen captures of your PC are logged.
3. **Control text capture:** The Windows API allows for programs to request the text value of some controls, it means a password can still be captured albeit it is behind a password mask.
4. **Activity tracking:** Recording of which programs, folders, and windows are opened and also the screenshots of every.
5. Recording of program queries, instant message conversations, FTP downloads alongside the other internet activities.

Types Of Keylogger: There are basically two types of Keyloggers:

1. **Hardware Keylogger:** This is a thumb-size device. It records all the keystrokes you enter from the keyboard then saves it in its memory. Later this data will be analyzed. The drawback of this device is, It

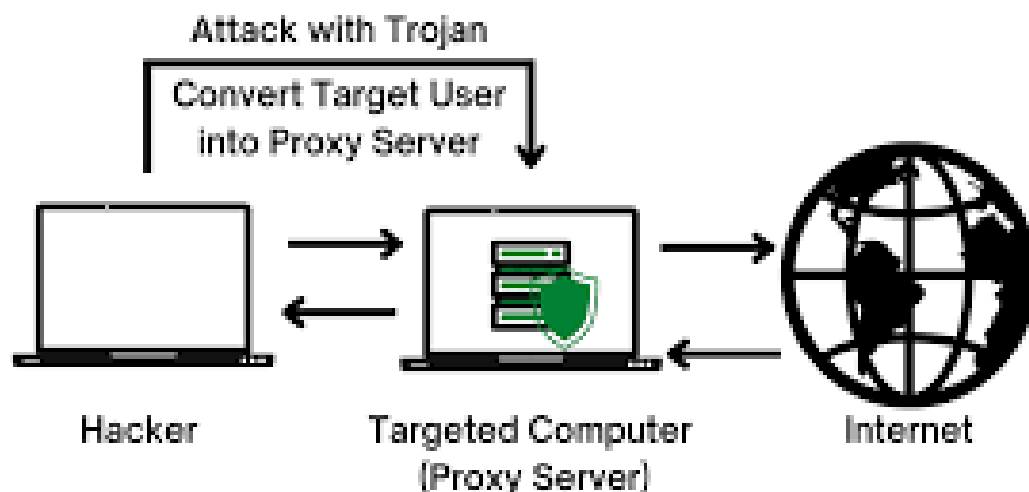
can't record mouse clicks, can't take screenshots, and even can't email, more importantly, It requires physical access to the machine. Hardware Keylogger is advantageous because it's not hooked into any software nor can it's detected by any software.

2. **Software Keylogger:** Software Keylogger can be installed in the victim's system even if they use updated Antivirus. There are lots of software available in market which make a Keylogger undetectable by latest antivirus, we are going to study about them too in upcoming chapters. There are many keyloggers available in market with various features.

TROJANS & BACKDOORS:

TROJANS:

Trojan Horse is a type of malware. Malicious software of this type masquerades as legitimate software to hack computers. Trojan prefers to operate discreetly and establishes security backdoors via which other infections can enter the system. The trojan is designed to gain unauthorized distant access to a computer. A hacker can use Trojans to edit and delete the files present on a victim system, or to observe the activities of the victim. Trojans can steal all your financial data like bank accounts, transaction details, PayPal related information, etc. These are called Trojan-Banker.



WORKING OF TROJAN :

Backdoor Trojans are malicious software programs that provide unauthorized access to a computer in order to launch a remote attack. Remote attackers can use a hacked machine to send commands or gain complete control.

Backdoor malware and viruses circumvent authentication protocols in order to gain access to systems and avoid detection. Once a Trojan has gained a footing in a system, it adds itself to the starting routine of the computer, preventing harmful programs from being permanently terminated by rebooting the machine.

Backdoor malware is commonly referred to as a Trojan. A Trojan horse is a malicious computer software that masquerades as something it isn't in order to spread malware, steal data, or open a backdoor on your system. Computer Trojans, like the Trojan horse from Greek mythology, usually come with a terrible surprise.

1. Trojans are a highly adaptable tool in the arsenal of cybercriminals. They can disguise themselves as an email attachment or a file download, and they can convey a variety of malware threats.
2. Backdoor Trojans may masquerade as legitimate software in order to deceive users into executing them. They can also be disseminated via spam email attachments or malicious URLs.
3. Using a backdoor, a Trojan allows an attacker to get remote access to a computer and take control of it. This gives the bad actor complete control over the device, allowing them to delete files, reset the machine, steal data, and install malware.
4. As a gateway, backdoor trojans have the potential to either install malware on your system or, at the absolute least, expose your machine to attack.
5. Backdoors are routinely used to build botnets. Without your knowledge, your system becomes a part of a zombie network that is used for attacks.
6. Backdoors may also be used to monitor your Internet behavior and run code and instructions on your device.

Infection techniques

How Does a Backdoor Trojan infection techniques **OR** Affect a System?

To effectively install a backdoor virus on your computer, thieves must first identify a weak spot (system vulnerabilities) or a hacked program.

Here is a list of some of the most prevalent system flaws –

- Software that has not been patched

- Ports on the network should be open
- Passwords that are easy to guess
- Firewalls that are ineffective
- A piece of malware, such as trojans, can also generate vulnerabilities. Backdoors are created by hackers using trojans that already present on a device.

A backdoor trojan, once triggered, allows hackers to take control of the infected device remotely. They may steal, receive, and delete files, reset the device, and install malware, among other hazardous behaviours.

Hackers will want to make sure they can rapidly re-enter your computer after gaining access through a backdoor infection so they can steal your data, install crypto mining software, hijack your device, or harm your business. And hackers are well aware that re-hacking a device may be tough, especially if the vulnerability is patched.

- Remote File Inclusion (RFI), an attack vector that targets weaknesses inside programs that dynamically reference external scripts, is the most common backdoor installation method. The reference function is fooled into downloading a backdoor virus from a remote host in an RFI situation.
- Scanners are commonly used by perpetrators to find websites with unpatched or obsolete components that allow for file injection. After that, a successful scanner exploits the flaw to install the backdoor on the underlying server. It can be accessible at any moment after it has been installed, even if the vulnerability that allows it to be injected has been patched. That is why, they install a backdoor on the target device, so that even if the vulnerability is addressed, the backdoor will still allow them to access the device.
- To get around security regulations prohibiting the upload of files larger than a particular size, backdoor trojan injection is frequently done in two steps.
 - 1.The first step is to install a **dropper**, which is a tiny program whose primary purpose is to retrieve a larger file from a remote site.
 - 2.The second phase begins with the backdoor script being downloaded and installed on the server.

LIFECYCLE & CLASSIFICATION OF VIRUS:

The life cycle of a computer virus can be divided into four phases:

Dormant phase

The virus is idle in the dormant phase. It has accessed the target device but does not take any action.

Note: Not all viruses have the dormant phase.

Propagation phase

In the propagation phase, the virus starts propagating by replicating itself. The virus places a copy of itself into other programs or accomplishes certain system areas on the disk. Each infected program will contain a clone of the virus, which will enter its own propagation phase as well.

Triggering phase

The triggering phase starts when the dormant virus is activated. It will perform the actions it is supposed to accomplish. This phase can be caused by various system events like the count of the times the virus has cloned or after a set time interval has elapsed.

Execution phase

In the execution phase, the payload will be released. It can harm deleting files, crashing the system, and so on. It can be harmless too and pop some humorous messages on screen.

CLASSIFICATION OF VIRUS:

A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually a trojan horse) inserts the virus into the system.

For more details, refer to [this](#).

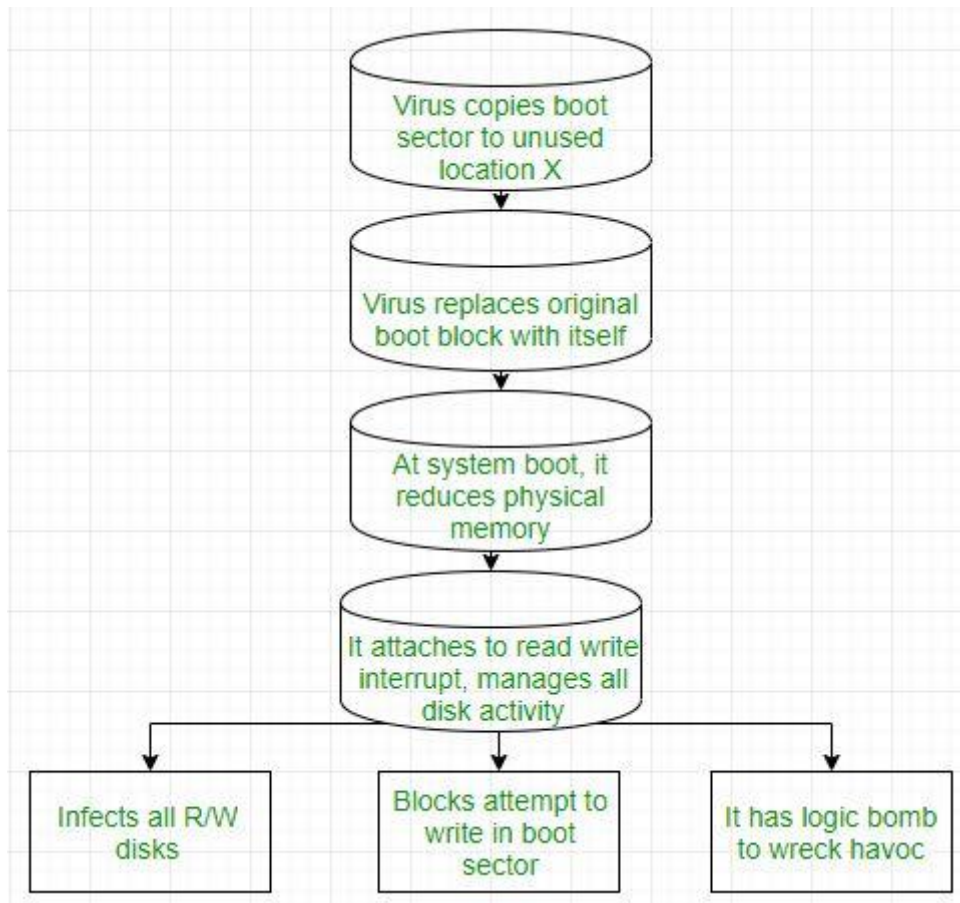
Various types of viruses:

- **File Virus:**

This type of virus infects the system by appending itself to the end of a file. It changes the start of a program so that the control jumps to its code. After the execution of its code, the control returns back to the main program. Its execution is not even noticed. It is also called a **Parasitic virus** because it leaves no file intact but also leaves the host functional.

- **Boot sector Virus:**

It infects the boot sector of the system, executing every time system is booted and before the operating system is loaded. It infects other bootable media like floppy disks. These are also known as **memory viruses** as they do not infect the file systems.



- **Macro Virus:**

Unlike most viruses which are written in a low-level language (like C or assembly language), these are written in a high-level language like Visual Basic. These viruses are triggered when a program capable of executing a macro is run. For example, the macro viruses can be contained in spreadsheet files.

- **Source code Virus:**

It looks for source code and modifies it to include virus and to help spread it.

- **Polymorphic Virus:**

A **virus signature** is a pattern that can identify a virus (a series of bytes that make up virus code). So in order to avoid detection by antivirus a polymorphic virus changes each time it is installed. The

functionality of the virus remains the same but its signature is changed.

- **Encrypted Virus:**

In order to avoid detection by antivirus, this type of virus exists in encrypted form. It carries a decryption algorithm along with it. So the virus first decrypts and then executes.

- **Stealth Virus:**

It is a very tricky virus as it changes the code that can be used to detect it. Hence, the detection of viruses becomes very difficult. For example, it can change the read system call such that whenever the user asks to read a code modified by a virus, the original form of code is shown rather than infected code.

- **Tunneling Virus:**

This virus attempts to bypass detection by antivirus scanner by installing itself in the interrupt handler chain. Interception programs, which remain in the background of an operating system and catch viruses, become disabled during the course of a tunneling virus. Similar viruses install themselves in device drivers.

- **Multipartite Virus:**

This type of virus is able to infect multiple parts of a system including the boot sector, memory, and files. This makes it difficult to detect and contain.

- **Armored Virus:**

An armored virus is coded to make it difficult for antivirus to unravel and understand. It uses a variety of techniques to do so like fooling antivirus to believe that it lies somewhere else than its real location or using compression to complicate its code.

- **Browser Hijacker:**

As the name suggests this virus is coded to target the user's browser and can alter the browser settings. It is also called the browser redirect virus because it redirects your browser to other malicious sites that can harm your computer system.

- **Memory Resident Virus:**

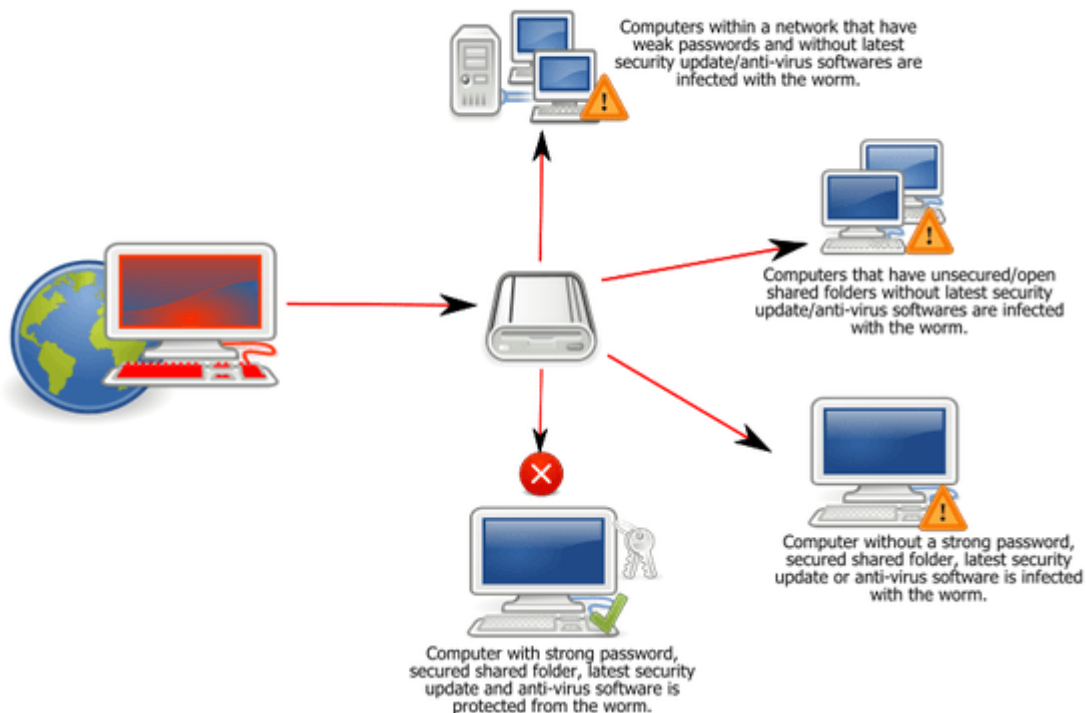
Resident viruses installation store for your RAM and meddle together along with your device operations. They behave in a very secret and dishonest way that they can even connect themselves for the anti-virus software program files.

Direct Action Virus:

The main perspective of this virus is to replicate and take action when it is executed. When a particular condition is met the virus will get into action and infect files in the directory that are specified in the AUTOEXEC.BAT file path.

WORMS:

Worm:Win32 Conficker



A worm is a malicious computer program that replicates itself usually over a computer network. An attacker may use a worm to accomplish the following tasks

- **Install backdoors on the victim's computers.** The created backdoor may be used to create zombie computers that are used to send spam

emails, perform distributed denial of service attacks, etc. the backdoors can also be exploited by other malware.

- Worms may also **slowdown the network by consuming the bandwidth** as they replicate.
- Install **harmful payload code** carried within the worm.

• Trojan, Virus, and Worm Differential Table

- Worms exploit vulnerabilities in the operating systems. Downloading

	Trojan	Virus	Worm
Definition	Malicious program used to control a victim's computer from a remote location.	Self replicating program that attaches itself to other programs and files	Illegitimate programs that replicate themselves usually over the network
Purpose	Steal sensitive data, spy on the victim's computer, etc.	Disrupt normal computer usage, corrupt user data, etc.	Install backdoors on victim's computer, slow down the user's network, etc.
Counter Measures	Use of anti-virus software, update patches for operating systems, security policy on usage of the internet and external storage media, etc. operating system updates can help reduce the infection and replication of worms.		
	<ul style="list-style-type: none"> • Worms can also be avoided by scanning, all email attachments before downloading them. 		

VIRUS CONSTRUCTION KIT:

Virus Construction Kits are programs, which enable persons with no or very limited programming skills to produce viruses according to specifications, or to produce variants of known viruses with different properties. As the name implies the Virus Construction Kits allow inexperienced programmers to produce viruses acting according to their wishes, assembled from a range of standard building bricks.

Virus Construction Kits are designed by various underground groups of virus writers, and distributed world-wide through Bulletin Board Systems or mailbox systems. The best known groups currently writing Virus Construction Kits are "NUKE" and "Phalcon/SKISM". Due to the widespread use of the Virus Construction Kits, it is unavoidable for staff tasked with responsibility for information security to include defensive measures against the kits in their range of virus countermeasures. A number of cases are known, in which Virus construction Kits freely circulated within corporate networks and were placed on corporate servers without the information security staff detecting or knowing anything about this, or even being able to detect the danger associated with this software. At least one case is known, in which a disgruntled employee produced a number of viruses using Virus Construction Kits, and subsequently used these to infect the computer systems of the corporation in question. Because of lacking knowledge of this particular threat the person responsible for information security was unable to apply a preventive method.

ENVIR

This was the first attempt to distribute a Virus Construction Kit as a kind of shareware and ask money for it. It is a first Generation Virus Construction Kit, which is menu driven. The program was coded by a French programmer and its functionality was limited (so-called "cripple-ware"). This way the programmer attempted to assure that the user paid the FF120 he demanded for the program. All menu choices in the program, allowing users to specify how they wanted their virus to look and behave, were fully functional, but when ask to compute the new virus, the program would stop and demand payment of the license fee. It is not known whether anybody ever paid the license fee and received a fully functional version. However, a partly functional hacked version circulated with an American electronic underground magazine for a while. The latest known version of GENVIR is 1.0.

1.VCL (The Virus Creation Lab)

VCL is a second Generation advanced Virus Construction Kit, which is menu-driven. It was programmed in 1992 by "Knowhere Man", a member of the underground group "NuKE". The VCL allows combination of chosen program code modules into a virus. It furthermore allows the user to generate a commented assembler source code listing, allowing manual modification and subsequent reassembly of the virus. The VCL generates fully functional and stable viruses. It is also capable of producing logical bombs and trojan horses. The latest known version of the VCL is 1.0.

2.PS-MPC (The Phalcon/SKISM Mass Produced Code Generator)

The PS-MPC is also a second Generation Virus Construction Kit, in this case programmed through an ASCII configuration file rather than through a menu-driven user interface. PS-MPC was programmed by "Dark Angel", a member of the virus-writing group "Phalcon-SKISM". PS-MPC is largely based on the Virus Creation Lab VCL and was distributed via mailbox systems in 1992. The complete source code for the kit in the C programming language was distributed together with the program, itself. The PS-MPC produces more compact and better assembler source code than the VCL. Also the assembler listings produced by this Virus Construction Kit are fully commented. Two versions of the PS-MPC are known: Version 0.9beta was published in the July 1992 issue of the electronic underground publication "40HEX", and version 0.91beta was published in August 1992. Version 0.91beta was extended with a few new functions, and some bugs in the 0.90beta versions were corrected. The PS-MPC produces by and large working and stable viruses. It is probably the most widely distributed Virus Construction Kit.

3.G 2 (G Squared)

G2 is a second Generation Virus Construction Kit. It was programmed in 1993 by "Dark Angel", the same virus writer, who one year earlier had written and published the PS-MPC. The "Phalcon/SKISM" group is very active, and still publishes its own underground publication, 40HEX. Also the G 2 Virus Construction Kit is controlled by means of an ASCII configuration file and produces a commented assembler listing for a virus. According to the documentation enclosed with the kit, this is not a rehash of the PS-MPC, but a completely new Virus Construction Kit programmed from scratch. G 2 mainly distinguishes itself from other Virus Construction Kits by being able to implement partly polymorphic program routines. G2 is completely capable of producing fully functional and stable computer viruses. The last known version of the G 2 Virus Construction Kit is version 0.70beta from January 1993.

4.IVP (Instant Virus Production Kit)

The IVP is a second Generation Virus Construction Kit. It was programmed by "Admiral Bailey" in 1992 and distributed via mailbox systems. "Admiral Bailey" is a member of the virus writer group "YAM Youngsters Against

McAfee". The IVP is written in Turbo Pascal 7.0 and requires an ASCII configuration table to produce viruses. The IVP is also able to produce Trojan horses and to encrypt viruses. Used as intended, the IVP is able to produce fully functional viruses, but depending on the contents of the ASCII configuration table the system can also be brought to produce non-functional program code, which either will not run, or crashes the computer. The latest known version of the IVP is version 1.0.

5.VCS (Virus Construction Set)

The VCS is a first Generation Virus Construction Kit, which was published in 1991 by a German virus writer group, "VDV Verband Deutscher Virenliebhaber". The VCS is a primitive Virus Construction Kit, which based on an ASCII text file with a maximum length of 512 bytes, produces simple viruses, which infect only COM files. After a certain number of infections and replications the virus displays a text on the computer display, and proceeds to delete the files AUTOEXEC.BAT and CONFIG.SYS. The VCS was originally published in a German language version, but an English hack emerged later. The latest known version is version 1.0.