Cyber Security in Context to Organisations

Do you how much is lost in cybercrime annually? It is estimated that at least $600, 000, 000, 000 is drained out of the global economy annually only through Cybercrime. And do you how much it costs an attacker to conduct a cyber heist.? In this article, we will be looking at what cybersecurity for an organization means and what actions they take to protect themselves from cyber-attacks.

CyberSecurity in Organizations

Computer security or cybersecurity is protecting oneself or an organization from malicious attacks for monetary or other indirect gains. With a lot of knowledge and resources available at hand on demand (on the Internet), it's become quite common that even someone who has a basic idea of how to google can cause a ruckus. An individual or organization needs to be secure digitally as they are physically. Organizations tend to maintain their security teams or hire a trusted third party that is capable of.

Cybersecurity teams have become an integral part of most organizations. When we consider cybersecurity teams, in general, they focus towards the centralized issues that are on the organizations' priority list, like data, applications, cloud, network services, etc. Companies usually have an infrastructure team, a threat management team and Identity and access management (IAM) team. Not all the organizations need to have the same structure or the same names, this is just an overview of how they work. The infrastructure is a very important asset of an organization and so it must be protected. The infrastructure security team are responsible for managing the audits, risks, disaster recovery programs and compliance of the infrastructure with market standards. Most common security standards are ISO 27001 and PCI-DSS.

The threat team is responsible for testing an application for vulnerabilities and report them for avoiding any exploits. The SOC team, which most of the times come under threat management team, is responsible for blocking and monitoring real-time attacks. You might have seen this many times in movie or some other places, the place where there will be a lot of huge screens are put displaying things (Yes, they do exist and many large organizations do this to keep an eye over their network. While all these teams seem familiar the IAM team is not known by many, this team is responsible for identifying a user and manage access to the resources as required. Interestingly the market for IAM tools is gaining as IAM is at the endpoint of security, i.e., the users(employees in the organization). Tools like cyberark, Sailpoint, okta, BeyondTrust and oracle identity management are the top tools used by most organizations to tighten their security while not causing and dent in their workflow.

CurrentStateofSecurity:

So from the structure of the security teams, we can see that organizations have started considering every aspect of the environment to protect themselves from cyber-attacks. Attacking on an organization (small to large) can cost somewhere around $112, 000 to anywhere up to $3.8 million and over, depending on the type of attack and what their intentions are.

Statistics say that margin between the cost of attack and the gain from attacks have started to reduce (Obviously leaving aside the social aspects of an attacker) as more and more organizations have invested in cybersecurity as the value of the information they hold is also risen dramatically.

Types of Hackers

A Hacker is a person who is intensely interested in the mysterious workings of any computer operating system. Hackers are most often programmers. They gather advanced knowledge of operating systems and programming languages and discover loopholes within systems and the reasons for such loopholes.

generally 10-types of Hackers, they are:

- **White Hat Hackers:** White hat hackers are the one who is authorized or the certified hackers who work for the government and organizations by performing penetration testing and identifying loopholes in their cybersecurity. They also ensure the protection from the malicious cyber crimes. They work under the rules and regulations provided by the government, that's why they are called *Ethical hackers* or *Cybersecurity experts*.
- **Black Hat Hackers:** They are often called *Crackers*. Black Hat Hackers can gain the unauthorized access of your system and destroy your vital data. The method of attacking they use common hacking practices they have learned earlier. They are considered to be as criminals and can be easily identified because of their malicious actions.
- **Gray Hat Hackers:** Gray hat hackers fall somewhere in the category between white hat and black hat hackers. They are not legally authorized hackers. They work with both good and bad intentions; they can use their skills for personal gain. It all depends upon the hacker. If a gray hat hacker uses his skill for his personal gains, he/she is considered as black hat hackers.
- **Script Kiddies:** They are the most dangerous people in terms of hackers. A Script kiddie is an unskilled person who uses scripts or downloads tools available for hacking provided by other hackers. They attempt to attack computer systems and networks and deface websites. Their main purpose is to impress their friends and society. Generally, Script Kiddies are juveniles who are unskilled about hacking.
- **Green Hat Hackers:** They are also amateurs in the world of hacking but they are bit different from script kiddies. They care about hacking and strive to become full-blown hackers. They are inspired by the hackers and ask them few questions about. While hackers are answering their question they will listen to its novelty.
- **Blue Hat Hackers:** They are much like the white hat hackers; they work for companies for security testing of their software right before the product launch. Blue hat hackers are outsourced by the company unlike white hat hackers which are employed by the (part of the) company.
- **Red Hat Hackers:** They are also known as the eagle-eyed hackers. Like white hat hackers, red hat hackers also aims to halt the black hat hackers. There is a major difference in the way they operate. They become ruthless while dealing with malware actions of the black hat hackers. Red hat hacker will keep on attacking the hacker aggressively that the hacker may know it as well have to replace the whole system.
- **State/Nation Sponsored Hackers:** State or Nation sponsored hackers are those who are appointed by the government to provide them cybersecurity and to gain confidential information from other countries to stay at the top or to avoid any kind of danger to the country. They are highly paid government workers.
- **Hacktivist:** These are also called the online versions of the activists. Hacktivist is a hacker or a group of anonymous hackers who gain unauthorized access to government's computer files and networks for further social or political ends.
- **Malicious Insider or Whistleblower:** A malicious insider or a whistleblower could be an employee of a company or a government agency with a grudge or a strategic employee who becomes aware of any illegal activities happening within the organization and can blackmail the organization for his/her personal gain.

Types of Hackers

Hackers can be classified into three different categories:

1. Black Hat Hacker
2. White Hat Hacker
3. Grey Hat Hacker

Black Hat Hacker

Black-hat Hackers are also known as an **Unethical Hacker or a Security Cracker**. These people hack the system illegally to steal money or to achieve their own illegal goals. They find banks or other companies with weak security and steal money or credit card information. They can also modify or destroy the data as well. Black hat hacking is illegal.

White Hat Hacker

White hat Hackers are also known as **Ethical Hackers or a Penetration Tester**. White hat hackers are the good guys of the hacker world.

These people use the same technique used by the black hat hackers. They also hack the system, but they can only hack the system that they have permission to hack in order to test the security of the system. They focus on security and protecting IT system. White hat hacking is legal.

Gray Hat Hacker

Gray hat Hackers are Hybrid between Black hat Hackers and White hat hackers. They can hack any system even if they don't have permission to test the security of the system but they will never steal money or damage the system.

In most cases, they tell the administrator of that system. But they are also illegal because they test the security of the system that they do not have permission to test. Grey hat hacking is sometimes acted legally and sometimes not.

What is Vulnerability in Cyber Security?

A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for lurking cybercrimes and are open to exploitation through the points of vulnerability.

These hackers are able to gain illegal access to the systems and cause severe damage to data privacy. Therefore, cybersecurity vulnerabilities are extremely important to monitor for the overall security posture as gaps in a network can result in a full-scale breach of systems in an organization.

Examples of Vulnerabilities

Below are some examples of vulnerability:

- A weakness in a firewall that can lead to malicious hackers getting into a computer network
- Lack of security cameras
- Unlocked doors at businesses

All of these are weaknesses that can be used by others to hurt a business or its assets.

How is vulnerability different from a cyber security threat and risk?

Vulnerabilities are not introduced to a system; rather they are there from the beginning. There are not many cases involving cybercrime activities that lead to vulnerabilities. They are typically a result of operating system flaws or network misconfigurations. Cyber security threats, on the other hand, are introduced to a system like a virus download or a social engineering attack.

Cyber security risks are generally classified as vulnerabilities, which can lead to confusion as they are not one and the same. Risks are actually the probability and impact of a vulnerability being exploited. If these two factors are low, then the risk is low. It is directly proportional, in which case, the inverse is also true; high probability and impact of vulnerabilities lead to high risks.

The impact of cyberattacks is, generally, tied to the CIA triad of the resource. Some common vulnerabilities pose no risk when the vulnerability has not much value to an organization.

When does a vulnerability become exploitable?

A vulnerability, which has at least one definite attack vector is an exploitable vulnerability. Attackers will, for obvious reasons, want to target weaknesses in the system or network that are exploitable. Of course, vulnerability is not something that anyone will want to have, but what you should be more worried about is it being exploitable.

There are cases when something that is vulnerable is not really exploitable. The reasons could be:

1. Insufficient public information for exploitation by attackers.
2. Prior authentication or local system access that the attacker may not have
3. Existing security controls

Strong security practices can prevent many vulnerabilities from becoming exploitable.

What causes the vulnerability?

There are many causes of Vulnerabilities like:

1. **Complex Systems –** Complex systems increase the probability of misconfigurations, flaws, or unintended access.
2. **Familiarity –** Attackers may be familiar with common code, operating systems, hardware, and software that lead to known vulnerabilities.
3. **Connectivity –** Connected devices are more prone to have vulnerabilities.
4. **Poor Password Management –** Weak and reused passwords can lead from one data breach to several.
5. **OS Flaws –** Operating systems can have flaws too. Unsecured operating systems by default can give users full access and become a target for viruses and malware.

1. **Internet –** The internet is full of spyware and adware that can be installed automatically on computers.
2. **Software Bugs –** Programmers can sometimes accidentally, leave an exploitable bug in the software.
3. **Unchecked user input –** If software or a website assumes that all input is safe, it may run unintended SQL injection.

4. **People** – Social engineering is the biggest threat to the majority of organizations. So, humans can be one of the biggest causes of vulnerability.

Types of Vulnerabilities

Below are some of the most common types of cybersecurity vulnerabilities:

System Misconfigurations

Network assets that have disparate security controls or vulnerable settings can result in system misconfigurations. Cybercriminals commonly probe networks for system misconfigurations and gaps that look exploitable. Due to the rapid digital transformation, network misconfigurations are on the rise. Therefore, it is important to work with experienced security experts during the implementation of new technologies.

Out-of-date or Unpatched Software

Similar to system misconfigurations, hackers tend to probe networks for unpatched systems that are easy targets. These unpatched vulnerabilities can be exploited by attackers to steal sensitive information. To minimize these kinds of risks, it is essential to establish a patch management schedule so that all the latest system patches are implemented as soon as they are released.

Missing or Weak Authorization Credentials

A common tactic that attackers use is to gain access to systems and networks through brute force like guessing employee credentials. That is why it is crucial that employees be educated on the best practices of cybersecurity so that their login credentials are not easily exploited.

Malicious Insider Threats

Whether it’s with malicious intent or unintentionally, employees with access to critical systems sometimes end up sharing information that helps cyber criminals breach the network. Insider threats can be really difficult to trace as all actions will appear legitimate. To help fight against these types of threats, one should invest in network access control solutions, and segment the network according to employee seniority and expertise.

Missing or Poor Data Encryption

It’s easier for attackers to intercept communication between systems and breach a network if it has poor or missing encryption. When there is poor or unencrypted information, cyber adversaries can extract critical information and inject false information onto a server. This can seriously undermine an organization’s efforts toward cyber security compliance and lead to fines from regulatory bodies.

Zero-day Vulnerabilities

Zero-day vulnerabilities are specific software vulnerabilities that the attackers have caught wind of but have not yet been discovered by an organization or user.

In these cases, there are no available fixes or solutions since the vulnerability is not yet detected or notified by the system vendor. These are especially dangerous as there is no defense against such vulnerabilities until after the attack has happened. Hence, it is important to remain cautious and continuously monitor systems for vulnerabilities to minimize zero-day attacks.

What is Vulnerability Management?

Vulnerability management is the cyclical practice consisting of identification, classification, remediation, and mitigation of security vulnerabilities. There are three essential elements of vulnerability management viz. vulnerability detection, vulnerability assessment, and remediation.

Vulnerability Detection

Vulnerability detection includes the following three methods:

- Vulnerability scanning
- Penetration testing
- Google hacking

Cyber Security Vulnerability Scan

As the name suggests, the scan is done to find vulnerabilities in computers, applications, or networks. For this purpose, a scanner (software) is used, which can discover and identify vulnerabilities that arise from misconfiguration and flawed programming within a network.

Some popular vulnerability scanning tools are SolarWinds Network Configuration Manager (NCM), ManageEngine Vulnerability Manager Plus, Rapid7 Nexpose, Acunetix, Probely, TripWire IP 360, etc.

Penetration Testing

Penetration testing or pen testing is the practice of testing an IT asset for security vulnerabilities that an attacker could potentially exploit. Penetration testing can be automated or manual. It can also test security policies, employee security awareness, the ability to identify and respond to security incidents, and adherence to compliance requirements.

Google Hacking

Google hacking is the use of a search engine to locate security vulnerabilities. This is achieved through advanced search operators in queries that can locate hard-to-find information or data that has been accidentally exposed due to the misconfiguration of cloud services. Mostly these targeted queries are used to locate sensitive information that is not intended for public exposure.

Cyber Security Vulnerability Assessment

Once a vulnerability is detected, it goes through the vulnerability assessment process. What is a vulnerability assessment? It is a process of systematically reviewing security weaknesses in an information system. It highlights whenever a system is prone to any known vulnerabilities as well as classifies the severity levels, and recommends appropriate remediation or mitigation if required.

The assessment process includes:

- **Identify vulnerabilities:** Analyzing network scans, firewall logs, pen test results, and vulnerability scan results to find anomalies that might highlight vulnerabilities prone to cyber-attacks.
- **Verify vulnerabilities:** Decide whether an identified vulnerability could be exploited and classify its severity to understand the level of risk
- **Mitigate vulnerabilities:** Come up with appropriate countermeasures and measure their effectiveness if a patch is not available.
- **Remediate vulnerabilities:** Update affected software or hardware wherever possible.

There are several types of vulnerability assessments:

- **Network-based assessment:** This type of assessment is used to identify potential issues in network security and detect systems that are vulnerable on both wired and wireless networks.
- **Host-based assessment:** Host-based assessment can help locate and identify vulnerabilities in servers, workstations, and other network hosts. It generally assesses open ports and services and makes the configuration settings and the patch management of scanned systems more visible.
- **Wireless network assessment:** It involves the scanning of Wi-Fi networks and attack vectors in the infrastructure of a wireless network. It helps validate that a network is securely configured to avoid unauthorized access and can also detect rogue access points.
- **Application assessment:** It is the identification of security vulnerabilities in web applications and their source code. This is achieved by implementing automated

vulnerability scanning tools on the front-end or analyzing the source code statically or dynamically.

- **Database assessment:** The assessment of databases or big data systems for vulnerabilities and misconfiguration, identifying rogue databases or insecure dev/test environments, and classifying sensitive data to improve data security.

Vulnerability management becomes a continuous and repetitive practice because cyber attacks are constantly evolving.

Vulnerability Remediation

To always be one step ahead of malicious attacks, security professionals need to have a process in place for monitoring and managing the known vulnerabilities. Once a time-consuming and tedious manual job, now it is possible to continuously keep track of an organization's software inventory with the help of automated tools, and match them against the various security advisories, issue trackers, or databases.

If the tracking results show that the services and products are relying on risky code, the vulnerable component needs to be located and mitigated effectively and efficiently.

The following remediation steps may seem simple, but without them, organizations may find themselves in a bit of difficulty when fighting against hackers.

Step 1: Know Your Code – Knowing what you're working with is crucial and the first step of vulnerability remediation. Continuously monitoring software inventory to be aware of which software components are being used and what needs immediate attention will significantly prevent malicious attacks.

Step 2: Prioritize Your Vulnerabilities – Organizations need to have prioritization policies in place. The risk of the vulnerabilities needs to be evaluated first by going through the system configuration, the likelihood of an occurrence, its impact, and the security measures that are in place.

Step 3: Fix – Once the security vulnerabilities that require immediate attention are known, it is time to map out a timeline and work plan for the fix.

Hackers and Crackers

Hackers are good people who hack devices and systems with good intentions. They might hack a system for a specified purpose or for obtaining more knowledge out of it. Crackers are people who hack a system by breaking into it and violating it with some bad intentions.

Difference between Hackers and Crackers

For so many years, there is a debate between hackers and crackers. Both terms are linked with one subject which is Hacking. **Hacking** may be defined as the technique or planning which is done to get access to unauthorized systems. Simply we can say gaining access to a network or a computer for illegal purposes. The person who does that is very intelligent and skilled in computers. The person who is skilled in Hacking are divided into 2 categories:

1. **Hackers:** Hackers are kind of good people who do hacking for a good purpose and to obtain more knowledge from it. They generally find loopholes in the system and help them to cover the loopholes. Hackers are generally programmers who obtain advanced knowledge about operating systems and programming languages. These people never damage or harm any kind of data.
2. **Crackers:** Crackers are kind of bad people who break or violate the system or a computer remotely with bad intentions to harm the data and steal it. Crackers destroy data by gaining unauthorized access to the network. Their works are always hidden as they are doing illegal stuff. Bypasses passwords of computers and social media websites, can steal your bank details and transfer money from the bank.

The Difference between Hackers and Crackers:

Hacker	Cracker
The good people who hack for knowledge purposes.	The evil person who breaks into a system for benefits.
They are skilled and have advanced knowledge of computers OS and programming languages.	They may or may not be skilled, some crackers just know a few tricks to steal data.
They work in an organization to help protect their data and give them expertise in internet security.	These are the person from which hackers protect organizations.
Hackers share the knowledge and never damages the data.	If they found any loophole they just delete the data or damages the data.
Hackers are the ethical professionals.	Crackers are unethical and want to benefit themselves from illegal tasks.
Hackers program or hacks to check the integrity and vulnerability strength of a network.	Crackers do not make new tools but use someone else tools for their cause and harm the network.

Hacker	Cracker
Hackers have legal certificates with them e.g CEH certificates.	Crackers may or may not have certificates, as their motive is to stay anonymous.
They are known as White hats or saviors.	They are known as Black hats or evildoers.

Cyber Attack

A cyber attack is **an assault launched by cybercriminals using one or more computers against a single or multiple computers or networks**. A cyber attack can maliciously disable computers, steal data, or use a breached computer as a launch point for other attacks. Cybercriminals use a variety of methods to launch a cyber attack, including malware, phishing, ransomware, denial of service, among other methods.

malware threats

Malware is malicious software that enables the attacker to have full or limited control over the target system. Malware can damage, modify, and/or steal information from the system. There are various types of malware such as **viruses, Trojans, worms, rootkits, spyware, and ransomware**

What Are the Most Common Types of Malware Attacks?

- Adware.
- Fileless Malware.
- Viruses.
- Worms.
- Trojans.
- Bots.
- Ransomware.
- Spyware.

Vulnerabilities:

Vulnerabilities are weaknesses in a system that gives threats the opportunity to compromise assets. All systems have vulnerabilities. Even though the technologies are improving but the number of vulnerabilities are increasing such as tens of millions of lines of code, many developers, human weaknesses, etc. Vulnerabilities mostly happened because of Hardware, Software, Network and Procedural vulnerabilities.

1. Hardware Vulnerability:

A hardware vulnerability is a weakness which can used to attack the system hardware through physically or remotely.

For examples:

1. Old version of systems or devices
2. Unprotected storage
3. Unencrypted devices, etc.

2. Software Vulnerability:

A software error happen in development or configuration such as the execution of it can violate the security policy. For examples:

1. Lack of input validation
2. Unverified uploads
3. Cross-site scripting

4. Unencrypted data, etc.

3. Network Vulnerability:

A weakness happen in network which can be hardware or software.
For examples:

1. Unprotected communication
2. Malware or malicious software (e.g.:Viruses, Keyloggers, Worms, etc)
3. Social engineering attacks
4. Misconfigured firewalls

4. Procedural Vulnerability:

A weakness happen in an organization operational methods.
For examples:

1. Password procedure – Password should follow the standard password policy.
2. Training procedure – Employees must know which actions should be taken and what to do to handle the security. Employees must never be asked for user credentials online. Make the employees know social engineering and phishing threats.

Malware and its types

Malware is a program designed to gain access to computer systems, normally for the benefit of some third party, without the user's permission. Malware includes computer viruses, worms, Trojan horses, ransomware, spyware and other malicious programs.

Types of Malware:

- **Viruses –**
  A Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data. Opening a file can trigger a virus. Once a program virus is active, it will infect other programs on the computer.

- **Worms –**
  Worms replicate themselves on the system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas. Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects a host, it is able to spread very quickly over the network.

  - **Spyware –**
    Its purpose is to steal private information from a computer system for a third party. Spyware collects information and sends it to the hacker.

  - **Trojan horse –**
    A Trojan horse is malware that carries out malicious operations under the appearance of a desired operation such as playing an online game. A Trojan horse varies from a virus because the Trojan binds itself to non-executable files, such as image files, audio files.

- **Logic Bombs –**
  A logic bomb is a malicious program that uses a trigger to activate the malicious code. The logic bomb remains non-functioning until that trigger event happens. Once triggered, a logic bomb implements a malicious code that causes harm to a computer. Cybersecurity specialists recently discovered logic bombs that attack and destroy the

hardware components in a workstation or server including the cooling fans, hard drives, and power supplies. The logic bomb overdrives these devices until they overheat or fail.

- **Ransomware –**
  Ransomware grasps a computer system or the data it contains until the victim makes a payment. Ransomware encrypts data in the computer with a key which is unknown to the user. The user has to pay a ransom (price) to the criminals to retrieve data. Once the amount is paid the victim can resume using his/her system.

- **Backdoors –**
  A backdoor bypasses the usual authentication used to access a system. The purpose of the backdoor is to grant the cyber criminals future access to the system even if the organization fixes the original vulnerability used to attack the system.

- **Rootkits –**
  A rootkit modifies the OS to make a backdoor. Attackers then use the backdoor to access the computer distantly. Most rootkits take advantage of software vulnerabilities to modify system files.

- **Keyloggers –**
  Keylogger records everything the user types on his/her computer system to obtain passwords and other sensitive information and send them to the source of the keylogging program.

Sniffing

Sniffing is a process of monitoring and capturing all data packets passing through given network. Sniffers are used by network/system administrator to monitor and troubleshoot network traffic. Attackers use sniffers to capture data packets containing sensitive information such as password, account information etc.

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

There is so much possibility that if a set of enterprise switch ports is open, then one of their employees can sniff the whole traffic of the network. Anyone in the same physical location can plug into the network using Ethernet cable or connect wirelessly to that network and sniff the total traffic.

In other words, Sniffing allows you to see all sorts of traffic, both protected and unprotected. In the right conditions and with the right protocols in place, an attacking party may be able to gather information that can be used for further attacks or to cause other issues for the network or system owner.

What can be sniffed?

One can sniff the following sensitive information from a network −

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the promiscuous mode so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.

A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing

Sniffing can be either Active or Passive in nature.

Passive Sniffing

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting address resolution packets (ARP) into a target network to flood on the switch content addressable memory (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques −

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Spoofing Attacks
- ARP Poisoning

Protocols which are affected

Protocols such as the tried and true TCP/IP were never designed with security in mind and therefore do not offer much resistance to potential intruders. Several rules lend themselves to easy sniffing −

- HTTP − It is used to send information in the clear text without any encryption and thus a real target.
- SMTP (Simple Mail Transfer Protocol) − SMTP is basically utilized in the transfer of emails. This protocol is efficient, but it does not include any protection against sniffing.
- NNTP (Network News Transfer Protocol)− It is used for all types of communications, but its main drawback is that data and even passwords are sent over the network as clear text.
- POP (Post Office Protocol) − POP is strictly used to receive emails from the servers. This protocol does not include protection against sniffing because it can be trapped.
- FTP (File Transfer Protocol) − FTP is used to send and receive files, but it does not offer any security features. All the data is sent as clear text that can be easily sniffed.
- IMAP (Internet Message Access Protocol) − IMAP is same as SMTP in its functions, but it is highly vulnerable to sniffing.
- Telnet − Telnet sends everything (usernames, passwords, keystrokes) over the network as clear text and hence, it can be easily sniffed.

Sniffers are not the dumb utilities that allow you to view only live traffic. If you really want to analyze each packet, save the capture and review it whenever time allows.

Gaining Access:

In this phase, the hacker designs the blueprint of the network of the target with the help of data collected during Phase 1 and Phase 2. The hacker has finished enumerating and

scanning the network and now decides that they have some options to gain access to the network.
For example, say a hacker chooses a Phishing Attack. The hacker decides to play it safe and use a simple phishing attack to gain access. The hacker decides to infiltrate the IT department. They see that there have been some recent hires and they are likely not up to speed on the procedures yet. A phishing email will be sent using the CTO's actual email address using a program and sent out to the techs. The email contains a phishing website that will collect their login and passwords. Using any number of options (phone app, website email spoofing, Zmail, etc) the hacker sends an email asking the users to log in to a new Google portal with their credentials. They already have the Social Engineering Toolkit running and have sent an email with the server address to the users masking it with a bitly or tinyurl.
Other options include creating a reverse TCP/IP shell in a PDF using Metasploit (may be caught by spam filter). Looking at the event calendar they can set up an Evil Twin router and try to Man in the Middle attack users to gain access. A variant of Denial of Service attack, stack-based buffer overflows, and session hijacking may also prove to be great.

Escalating Privileges

Privilege escalation in cybersecurity is a malicious attempt to abuse an app or OS bug or error of configuration in order to gain unauthorized access to sensitive information

Privilege escalation attacks exploit weaknesses and security vulnerabilities with the goal of elevating access to a network, applications, and mission-critical systems. There are two types of privilege escalation attacks including vertical and horizontal. Vertical attacks are when an attacker gains access to an account with the intent to perform actions as that user. Horizontal attacks gain access to account(s) with limited permissions requiring an escalation of privileges, such as to an administor role, to perform the desired actions.

Privilege escalation is an attack vector that many businesses face due to loss of focus on permission levels. As a result, security controls are not sufficient to prevent a privilege escalation.

Privilege escalation attacks occur when a threat actor gains access to an employee's account, bypasses the proper authorization channel, and successfully grants themselves access to data they are not supposed to have. When deploying these attacks threat actors are typically attempting to exfiltrate data, disrupt business functions, or create backdoors.

All of these actions can have a major impact on business continuity and should be considered when drafting a business continuity plan.

When encounter a privilege escalation attack, how you respond is critical. Here are a few questions to consider:

- What did the attacker have permission and access to?
- How are business services currently being impacted?
- What other activities were performed on this account during the duration of the attack?

What Are The Types Of Privilege Escalation Attacks?

Not every attack will provide threat actors with full access to the targeted system. In these cases, a privilege escalation is required to achieve the desired outcome. There are two types of privilege escalation attacks including vertical and horizontal.

Vertical Privilege Escalation

Vertical privilege escalation occurs when an attacker gains access directly to an account with the intent to perform actions as that person. This type of attack is easier to pull off since there is no desire to elevate permissions. The goal here is to access an account to further spread an attack or access data the user has permissions to.

Day in and day out I analyze numerous phishing emails that attempt to perform this attack. Whether it's a "bank", "Amazon", or any other countless number of ecommerce sites, the attack is the same. "*Your account will be deactivated due to inactivity. Please click this link and login to keep your account active."* This is, however, one example of many cookie-cutter phishing templates seen in "the wild".

Horizontal Privilege Escalation

Horizontal privilege escalation is a bit tricky to pull off as it requires the attacker to gain access to the account credentials as well as elevating the permissions. This type of attack tends to require a deep understanding of the vulnerabilities that affect certain operating systems or the use of hacking tools.

Phishing campaigns have been used to perform the first part of the attack to gain access to the account. When it comes to elevating permissions, the attacker has a few options to choose from. One option is to exploit vulnerabilities in the operating system to gain system or root-level access. The next option would be to use hacking tools, like Metasploit, to make the job a bit easier.

Examples Of Privilege Escalation Attacks

Now that you have a better understanding of what a privilege escalation attack is, I'm going to show you 5 real-world examples including:

1. Windows Sticky Keys
2. Windows Sysinternals
3. Process Injection
4. Linux Passwd User Enumeration
5. Android Metasploit

Executing Applications

Intruder executes malicious applications after gaining administrative privileges so they can run malicious programs remotely, to capture all sensitive data, crack passwords, capture screenshots or to install a backdoor.

Tool: RemoteExec, PDQ Deploy, DameWare NT Utilities

Keylogger

keystroke loggers are programs or hardware devices that monitor each keystroke a user types on a keyboard, logs onto a file, or transmits them to a remote location.

keyloggers are placed between the keyboard hardware and the OS

A key logger can

- Record each keystroke
- capture screenshots at regular intervals of time showing user activity such as when he or she types a character or click a mouse button
- Track the activities of users by logging window titles, names of launched applications and other information
- monitor online activity of users by recording addresses of the websites that they are have visited and with the keywords entered by them
- record all the login names, bank and credit card numbers and passwords including hidden passwords or data that are in asterisk or blank spaces
- record online chat conversion

Types of Keylogger

- Hardware Keylogger
- Software Keylogger

Spyware

Spyware is stealthy computer monitoring software that allows you to secretly record all activities of a computer user.

Hiding Files

Rootkits

Rootkits are programs that hackers use in order to evade detection while trying to gain unauthorized access to a computer. Rootkits when installing on a computer, are invisible to the user and also take steps to avoid being detected by security software.

A rootkit is a set of binaries, scripts and configuration files that allows someone to covertly maintain access to a computer so that he can issue commands and scavenge data without alerting the system's owner.

Depending on where they are installed there are various types of rootkits:

- Kernel Level Rootkits
- Hardware/Firmware Rootkits
- Hypervisor (Virtualized) Level Rootkits
- Boot loader Level (Bootkit) Rootkits

NTFS DATA Stream

Alternative Data Stream support was added to NTFS (Windows NT, Windows 2000 and Windows XP) to help support Macintosh Hierarchical File System (HFS) which uses resource forks to store icons and other information for a file. Using Alternative Data Streams a user can easily hide files that can go undetected unless close inspection.

Steganography

The art of hiding a data inside another data/medium is called steganography.

For eg: hiding data within an image file

The secret message is called overt file and the covering file is called covert file.

Types of Steganography

- Image Steganography
- Document Steganography
- Folder Steganography
- Video Steganography
- Audio Steganography
- White Space Steganography

Covering Tracks in cyber security

Covering tracks is **one of the most stage during system hacking**. during this stage, the attacker tries to cover and avoid being detected, or "traced out," by covering all track, or logs, generated while gaining access to the target networks or computer.

Covering Tracks

Once an attacker finishes his work, he wants to erase all tracks leading the investigators tracing back to him. This can be done using

1. Disable auditing.
2. Clearing logs.
3. Modifying logs, registry files.
4. Removing all files, folders created.

Worms

A computer worm is **a type of malware whose primary function is to self-replicate and infect other computers while remaining active on infected systems**. A computer worm duplicates itself to spread to uninfected computers.

Computer Worm

A worm is a harmful software (virus) that repeats itself as it moves from computer to computer, leaving copies of itself in each computer's memory. A worm finds a computer's vulnerability and spreads like an illness throughout its associated network, constantly looking for new holes. Worms, like viruses, are spread by email attachments from seemingly trustworthy senders. Worms then propagate through a user's email account and address book to contacts.

Some worms reproduce and then go dormant, while others inflict harm. The worm's code is referred to as payload in such circumstances.

How do they work?

Computer worms make use of network flaws to spread. The worm is hunting for an unobserved back door into the network. To spread computer worms for the first time, hackers usually send phishing emails or instant chats with malicious attachments. The worm is disguised by cyber thieves so that the recipient is willing to run it. For this aim, duplicate file extensions and a data name that appears harmless or urgent, such as "invoice," are utilized. When the user opens the attachment or clicks on the link, the malware (computer worm) will be downloaded into their system or lead to a harmful website.

As a result, the worm enters the user's system without their knowledge. After being terminated, the worm looks for a way to duplicate itself and infiltrate new computers. For example, the worm can send an email to all contacts on the infected machine, which contains worm replication. A payload is a feature that many worms currently have. The term "payload" refers to the "payload" and, in this example, an attachment that the worm carries. The worm can, for example, has ransomware, viruses, or other malware, all of which can harm afflicted computers. In the event of a blackmail assault, these can, for example, remove or encrypt files on the PC.

A computer worm can also create a back door that other malicious programs can use later. This flaw allows the worm's creator to take control of the infected computer. Meanwhile, malware operations frequently use a combination of several malware types. Take the

WannaCry ransomware or the Petya / Not-Petya ransomware, for example. These include a worm component, which allows the virus to replicate and spread through back doors in other network systems.

Because the worm or its programmer can use the infected system's computing capacity, they are frequently integrated into a botnet. Cyber thieves then employ these, for example, in DDoS assaults or crypto mining.

What are the types of computer worms?

Malicious computer worms come in a variety of forms −

Email worms

To spread, email worms create and send outbound messages to all addresses in a user's contact list. When the recipient opens the mail, it contains a malicious executable file that infects the new system.

Successful email worms typically use social engineering and phishing approaches to persuade users to open the linked file.

File-sharing worms

File-sharing worms are malicious programs that hide as media files.

Stuxnet, one of the most well-known computer worms of all time, comprises two parts: a worm that spreads malware via USB devices infected with the host file and malware that targets supervisory control and data acquisition systems. Industrial contexts, such as power utilities, water supply services, and sewage plants are frequently targeted by file-sharing worms.

Cryptoworms

Cryptoworms encrypt data on the victim's computer system. This worm can be used in ransomware attacks, in which the attackers contact the victim and seek payment in exchange for a key to decrypt their files.

Internet worms

Some computer worms are designed to attack prominent websites that have weak security. They can infect a computer viewing the website if they can infect the site. Internet worms then propagate to other devices connected to the infected PC via internet and private network connections.

Worms that spread via instant messaging

Instant messaging worms, like email worms, are disguised as attachments or links, which the worm uses to spread throughout the infected user's contact list. The only difference is that it comes as an instant message on a chat site rather than an email.

If the worm hasn't had time to replicate itself on the machine, it may usually be stopped by resetting the user's chat service account password.

Virus vs. computer worm

Because they behave similarly, some people mistakenly believe that a computer worm and a computer virus are the same things. They might even call it a "worm computer virus" or "worm virus malware." The truth is that the two threats are similar yet distinct.

The major distinction between a virus and a worm is that viruses require human action to activate, whereas worms replicate only in the presence of a host system. In other words,

unless you run a virus, your computer will not be harmed. A virus on a flash drive connected to your computer, for example, will not harm your system unless you activate it. A worm, as previously stated, does not require a host system or user input to spread.

What kind of harm may a computer worm do?

A worm may not do any harm at all: in the early days of computing, worms were often developed as pranks or demonstrations of concept to exploit security flaws. They did little more than reproducing themselves in the background on afflicted machines. When the worm made too many copies of itself on a single system and slowed down its activities, it was often the only way to notice something was wrong. Worms became a means to an end when OS security increased and building a worm that could breach it became more difficult and time-consuming.

Nowadays, worms almost always incorporate payload code that performs more than the worm's reproduction and propagation. There are numerous distinct forms of computer worms that cause various kinds of damage to their victims. Some transform computers into "zombies" or "bots" that launch DDoS attacks; others search their hosts for banking logins or other sensitive financial information, and still, others encrypt the victim's hard drive and demand a bitcoin ransom before restoring their data.

The infection vector is another approach to classify different types of worms. Email worms, instant messaging and IRC worms, file-sharing worms, and internet worms fall under this category, looking for any opportunity to propagate.

How to prevent worms?

Malicious software can take many forms, including computer worms. Take these measures to help protect your computer against worms and other internet threats.

- Because software vulnerabilities are a common source of infection for computer worms, make sure your computer's operating system and programs are up to date. Because updates frequently include patches for security problems, install them as soon as they become available.
- Another popular method for hackers to transmit worms is through phishing (and other types of malware). When opening unwanted emails, be particularly cautious, especially those from unknown senders that include attachments or questionable URLs.
- Make sure you have a good internet security software solution to help you block these dangers. Anti-phishing technologies, as well as defenses against viruses, spyware, ransomware, and other online threats, should be included in a solid solution.

Trojans

A Trojan, or Trojan horse, is **a type of malware that conceals its true content to fool a user into thinking it's a harmless file**. Like the wooden horse used to sack Troy, the "payload" carried by a Trojan is unknown to the user, but it can act as a delivery vehicle for a variety of threats.

Types of Trojan viruses

Some of the most common types of Trojan virus include:

- **Backdoor Trojans** - This type of Trojan allows hackers to remotely access and control a computer, often for the purpose of uploading, downloading, or executing files at will.

- **Exploit Trojans** -These Trojans inject a machine with code deliberately designed to take advantage of a weakness inherent to a specific piece of software.
- **Rootkit Trojans** -These Trojans are intended to prevent the discovery of malware already infecting a system so that it can affect maximum damage.
- **Banker Trojans** -This type of Trojan specifically targets personal information used for banking and other online transactions.
- **Distributed Denial of Service (DDoS) Trojans** - These are programmed to execute DDoS attacks, where a network or machine is disabled by a flood of requests originating from many different sources.
- **Downloader Trojans** -These are files written to download additional malware, often including more Trojans, onto a device.

How to recognize and detect a Trojan virus

Because Trojans are used as a delivery device for a number of different types of malware, if you suspect your device may have been breached by a Trojan, you should look for many of the same telltale signs of malicious software. These may include:

- Poor device performance- Is your computer or mobile device running slowly or crashing more frequently than normal?
- Strange device behavior- Are programs running you didn't initiate or are other unexplained processes being executed on your device?
- Pop-up and spam interruptions- Are you noticing an uptick in the number of interruptions from browser pop-ups or email spam?

If your device is exhibiting these symptoms, it's possible a Trojan virus has managed to sneak its payload onto your computer. Try searching your computer for any programs or applications you don't remember installing yourself. Enter any unrecognized file names or programs into a search engine to determine if they are recognized Trojans.

Finally, if you haven't already, scan your computer with antivirus software to see if it has uncovered a malicious file.

Examples of Trojans

- **Zeus** - Also known as Zbot, Zeus is a successful Trojan malware package with many variants used to carry out a number of different types of attack. It's perhaps most well-known for its successful hack of the U.S. Department of Transportation.
- **Wirenet** - Wirenet is a password-stealing Trojan notable for being among the first to target Linux and OSX users, many of whom were migrating from Windows operating systems based on perceived security flaws.
- **Mobile banking Trojans** - Webroot has documented a number of Trojans written to target mobile banking apps for the purpose of stealing login credentials or replacing legitimate apps with malicious ones.

Protect your computer from Trojan horse threats

As with protecting against most common cybersecurity threats, effective cybersecurity software should be your front line of protection. An effective internet security solution should run fast, frequent scans and alert you as soon as a Trojan virus is detected.

If you're reading this because it's already too late, see our page on removing malware infecting your computer. If you're reading this to stay safe from these types of attacks in the future, there are a few best practices in addition to installing cybersecurity software to help keep yourself safe:

- Never download or install software from a source you don't trust completely
- Never open an attachment or run a program sent to you in an email from someone you don't know.
- Keep all software on your computer up to date with the latest patches
- Make sure a Trojan antivirus is installed and running on your computer

Viruses

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.

Various types of viruses:

- **FileVirus:**
  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.

- **BootsectorVirus:**
  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.

- **MacroVirus:**
  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.

- **SourcecodeVirus:**
  It looks for source code and modifies it to include virus and to help spread it.

- **PolymorphicVirus:**
  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

ischanged.

- **EncryptedVirus:**
  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.

- **StealthVirus:**
  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.

- **TunnelingVirus:**
  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.

- **MultipartiteVirus:**
  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.

- **ArmoredVirus:**
  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.

- **BrowserHijacker:**
  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.

- **Overwrite virus:**

This type of virus deletes the information contained in the file that it infects, rendering them partially or totally is useless once they have been infected.

- **Directory Virus:**

This virus is also called called File System Virus or Cluster Virus. It infects the directory of the computer by modifying the path that is indicating the location of a file.

- **Companion Virus:**

This kind of virus usually use the similar file name and create a different extension of it. For example, if there's a file "Hello.exe", the virus will create another file named "Hello.com" and will hide in the new file

- **FAT Virus:**

The **File Allocation Table** is the part of the disk used to store all information about the location of files, available space , unusable space etc.
This virus affects the FAT section and may damage crucial information.

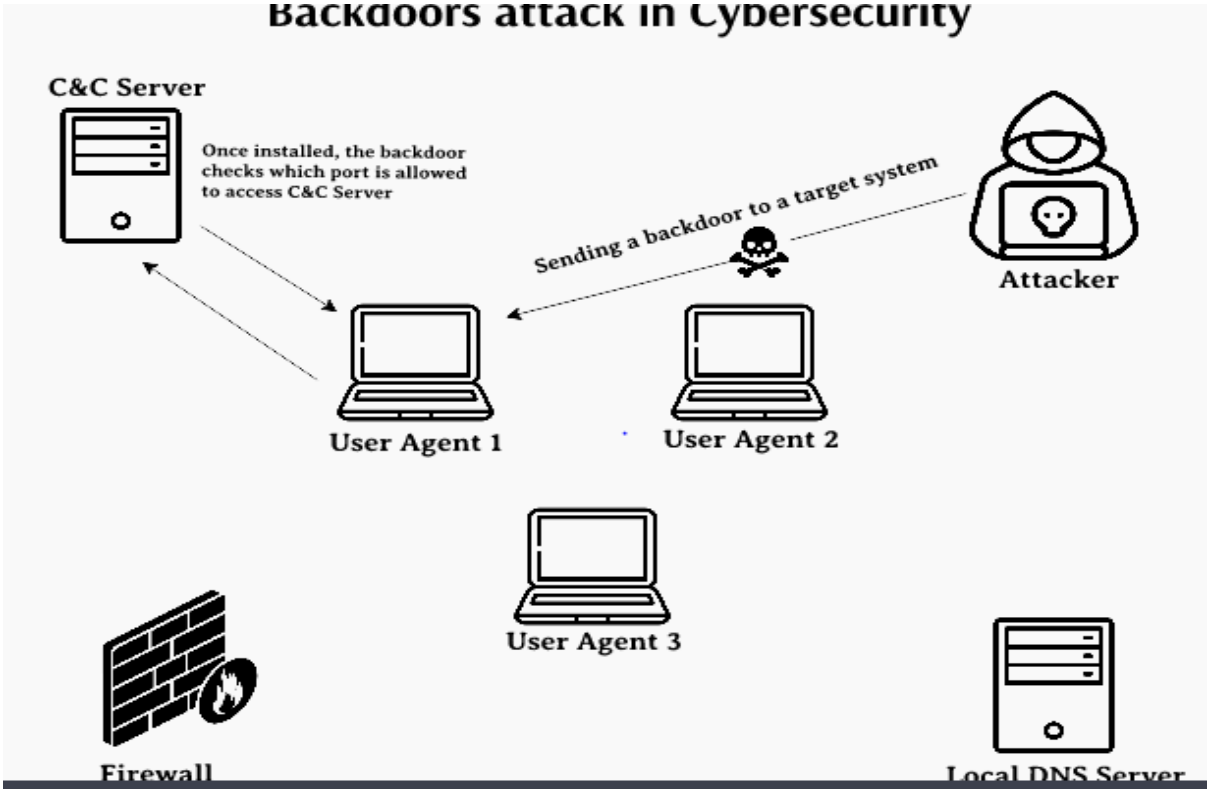
BackDoors

A backdoor attack is **a way to access a computer system or encrypted data that bypasses the system's customary security mechanisms**. A developer may create a backdoor so that an application, operating system (OS) or data can be accessed for troubleshooting or other purposes.

How to Prevent Backdoor Attacks?
Cyber security or security of the web deals with the security mechanism of the cyber world. Cyber security is extremely necessary as it is important that computer networks have strong cyber security mechanisms set up to prevent any form of attack that may lead to compromise of computer network security. Proper awareness about cyber attacks can help in preventing cyber attacks to a large extent.
Here, in this article, we will discuss backdoor attacks in detail including what is a backdoor attack, the aim behind backdoor attacks, the types of backdoor attacks, and the different ways to prevent backdoor attacks.

Aim:
The mechanism of a backdoor attack includes processes that breach the authentication security of the system. The security of the application is exploited by providing remote access to certain resources of the application. The cyber attackers then take advantage of using the remote part to execute malicious code into the system.

In a backdoor attack, the authenticated system of the computer network faces backlash as security is compromised and access to resources is forcefully taken access by cyber attackers.
The attackers are not allowed to access to make changes in the computer system and use it to their benefit for executing malicious code and viruses, including harmful malware. The remote access granted to the attacker unable them to perform security threat operations irrespective of the location from where they try to execute the attack. All the security policies are breached and attackers get administrator access to the system through this attack. A backdoor attack is a form of DDoS attack and serves as a gateway for malware to enter the computer network security.



Types of Backdoor Attack:

There are two different types of Backdoor attacks. They are as listed as follows –

1. Administrative Backdoor Attack: Software developers create backdoor pathways seldom in their program so if by chance any failure is recorded into the computer system then the developers will have access to the code and can help to involve the problem. Cyber attackers can take advantage of this backdoor pathway and can get into the system to access it in an unauthorized way and leading to backdoor attacks in computer network architecture.

2. Malicious Backdoor Attack: A malicious Backdoor Attack occurs when the program gets into the system through harmful malware.RAT (Remote Access Trojan) is used by cyber attackers for installing malicious backdoor programs.

Prevention of Backdoor Attack:

Listed are some ways to prevent Backdoor attacks from taking place:

- **Continuous Monitoring of Security System**: Monitoring the system network helps in checking loopholes that may turn into potential entry points for backdoor attacks.
- **Having Strong firewalls in Computer Network**: Firewall filters the traffic in a computer network and a strong firewall can prevent attackers from getting into the system.
- **Protection of computer networks through Strong Passwords**: Having a strong password helps in establishing the strong security of the system. Users should never stick to default passwords and should always have passwords that are difficult to crack.