Virus-Scanning Techniques

In general, there are five ways a virus scanner might scan for virus infections. Some of these were mentioned in the previous section, but they are outlined and defined here:

■ Email and attachment scanning: Since the primary propagation method for a virus is email, email and attachment scanning is the most important function of any virus scanner. Some virus scanners actually examine your email on the email server before downloading it to your machine. Other virus scanners work by scanning your emails and attachments on your computer before passing it to your email program. In either case, the email and its attachments should be scanned prior to your having any chance to open them and release the virus on your system.

■ Download scanning: Anytime you download anything from the Internet, either via a web link or through some FTP program, there is a chance you might download an infected file. Download scanning works much like email and attachment scanning but does so on files you select for downloading.

■ File scanning: This is the type of scanning in which files on your system are checked to see whether they match any known virus. This sort of scanning is generally done on an on-demand basis instead of an on-going basis. It is a good idea to schedule your virus scanner to do a complete scan of the system periodically. I recommend a weekly scan, preferably at a time when no one is likely to be using the computer.

■ Heuristic scanning: This was briefly mentioned in the previous section. Perhaps the most advanced form of virus scanning, this uses rules to determine whether a file or program is behaving like a virus and is one of the best ways to find a virus that is not a known virus. A new virus will not be on a virus definition list, so you must examine its behaviour to determine. whether it is a virus. However, this process is not fool proof. Some actual virus infections will be missed, and some nonvirus files might be suspected of being a virus.

■ Sandbox: Another approach is the sandbox approach. This basically means that you have a separate area, isolated from the operating system, in which a download or attachment is run. Then if it is infected, it won’t infect the operating system

Firewall Types and Components

There are numerous types of firewalls and variations on those types. But most firewalls can be grouped

into one of the following three families of firewalls.

■ Packet inspection

■ Stateful packet inspection

■ Application

Packet Filtering

-A packet filtering firewall is the most basic type of firewall. It acts like a management program that monitors network traffic and filters incoming packets based on configured security rules.
-These firewalls are designed to block network traffic IP protocols, an IP address, and a port number if a data packet does not match the established rule-set.
-While packet-filtering firewalls can be considered a fast solution without many resource requirements, they also have some limitations.
-Because these types of firewalls do not prevent web-based attacks, they are not the safest.

Application-level Gateways (Proxy Firewalls)

- Proxy firewalls operate at the application layer as an intermediate device to filter incoming traffic between two end systems (e.g., network and traffic systems). That is why these firewalls are called 'Application-level Gateways'.
- Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server.
- This protects the client's identity and other suspicious information, keeping the network safe from potential attacks.
- Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client.
- This approach creates an additional layer of security between the client and many different sources on the network.

Stateful Packet Inspection

- The Malwarebytes firewall will examine each packet, denying or permitting access based not only on the examination of the current packet, but also on data derived from previous packets in the conversation.
- This means that the firewall is aware of the context in which a specific packet was sent. This makes these firewalls far less susceptible to ping floods and SYN floods, as well as less susceptible to spoofing.
- The SPI firewall can also look at the actual contents of the packet, which allows for some very advanced filtering capabilities

Anti-Spyware

- Anti-spyware software detects spyware through rules-based methods or based on downloaded definition files that identify common spyware programs.
- Anti-spyware software can be used to find and remove spyware that has already been installed on the user's computer, or it can act much like an anti-virus program by providing real-time protection and preventing spyware from being downloaded in the first place.
- Spyware is a type of malware that is installed on a computer without the user's knowledge in order to collect information about them.
- This can pose a security risk to the user, but more frequently spyware degrades system performance by taking up processing power, installing additional software, or redirecting users' browser activity.

- Some of the most popular anti-spyware tools are:

Windows Defender. This program is pre-installed in contemporary versions of Windows and maintains a protection shield for the system, updating itself from time to time to keep up with threats.

HiJack This. A simple and effective program to check the computerized system for backdoors and other forms of dangerous malware. In addition, it generates a very complete report of your tasks, which makes it extremely practical.

Malwarebiytes Anti-Malware. To combat any type of malware, this program is one of the best known, since it operates independently of the antivirus, doubling the protection, and has a great capacity to detect harmful software.

Authentication

When a user logs on to a system, the system needs to authenticate her (and sometimes the user needs to authenticate the system). There are many authentication protocols. A few of the more common are briefly described here:

■ PAP: Password Authentication Protocol is the simplest form of authentication and the least secure. Usernames and passwords are sent unencrypted, in plain text. This is obviously a very old method that is not used anymore. However, in the early days of computing, there were no widely available packet sniffers, and security was far less of a concern.

■ SPAP: Shiva Password Authentication Protocol is an extension to PAP that does encrypt the username and password that is sent over the Internet.

■ CHAP: Challenge Handshake Authentication Protocol calculates a hash after the user has logged in. Then it shares that hash with the client system. Periodically the server will ask the client to provide that hash. (This is the challenge part.) If the client cannot, then it is clear that the communications have been compromised. MS-CHAP is a Microsoft-specific extension to CHAP.

■ EAP: A framework frequently used in wireless networks and point-to-point connections. It was originally defined in RFC 3748 but updated since then. It handles the transport of keys and related parameters. There are several versions of EAP. It has many variations, including these:

- ■ LEAP: Lightweight Extensible Authentication protocol was developed by Cisco and has been used extensively in wireless communications. LEAP is supported by many Microsoft operating systems including Windows 7 and later versions. LEAP uses a modified version of MS-CHAP.
- ■ Extensible Authentication Protocol—Transport Layer Security : This utilizes TLS in order to secure the authentication process. Most implementations of EAP-TLS utilize X.509 digital certificates to authenticate the users.
- ■ Protected Extensible Authentication Protocol (PEAP): This encrypts the authentication process with an authenticated TLS tunnel. PEAP was developed by a consortium including Cisco, Microsoft, and RSA Security. It was first included in Microsoft Windows XP.

■ Kerberos: Kerberos is used widely, particularly with Microsoft operating systems. It was invented at MIT and derives its name from the mythical three-headed dog The system is a bit complex, but the basic process is as follows :

When a user logs in, the authentication server verifies the user's identity and then contacts the ticket-granting server. (These are often on the same machine.) The ticket-granting server sends an encrypted "ticket" to the user's machine. That ticket identifies the user as being logged in. Later when the user needs to access some resource on the network, the user's machine uses that ticket-granting ticket to get access to the target machine. There is a great deal of verification for the tickets, and these tickets expire in a relatively short time.

concept of publishing an obscene information in IT act 2000

The main objective of this act is to carry lawful and trustworthy electronic, digital and online transactions and alleviate or reduce cybercrimes. The IT Act has 13 chapters and 90 sections. The last four sections that starts from 'section 91 – section 94', deals with the revisions to the Indian Penal Code 1860.

The IT Act, 2000 has two schedules:

First Schedule –

Deals with documents to which the Act shall not apply.

Second Schedule –

Deals with electronic signature or electronic authentication method.

The offences and the punishments in IT Act 2000 :

1. Tampering with the computer source documents.
2. Directions of Controller to a subscriber to extend facilities to decrypt information.
3. Publishing of information which is obscene in electronic form.
4. Penalty for breach of confidentiality and privacy.
5. Hacking for malicious purposes.
6. Penalty for publishing Digital Signature Certificate false in certain particulars.
7. Penalty for misrepresentation.
8. Confiscation.
9. Power to investigate offences.
10. Protected System.
11. Penalties for confiscation not to interfere with other punishments.
12. Act to apply for offence or contravention committed outside India.
13. Publication for fraud purposes.
14. Power of Controller to give directions.

SECTION	PUNISHMENT
Section 43	This section of IT Act, 2000 states that any act of destroying, altering or stealing computer system/network or deleting data with malicious intentions without authorization from owner of the computer is liable for the payment to be made to owner as compensation for damages.
Section 43A	any corporate body dealing with sensitive information that fails to implement reasonable security practices causing loss of other person will also liable as convict for compensation to the affected party.
Section 66	Hacking of a Computer System with malicious intentions like fraud will be punished with 3 years imprisonment or the fine of Rs.5,00,000 or both.
Section 66 B, C, D	Fraud or dishonesty using or transmitting information or identity theft is punishable with 3 years imprisonment or Rs. 1,00,000 fine or both.
Section 66 E	This Section is for Violation of privacy by transmitting image or private area is punishable with 3 years imprisonment or 2,00,000 fine or both.
Section 66 F	This Section is on Cyber Terrorism affecting unity, integrity, security, sovereignty of India through digital medium is liable for life imprisonment.
Section 67	This section states publishing obscene information or pornography or transmission of obscene content in public is liable for imprisonment up to 5 years or fine or Rs. 10,00,000 or both.

Mobile Forensics

- Mobile forensics, a subtype of digital forensics, is concerned with retrieving data from an electronic source. The recovery of evidence from mobile devices such as smartphones and tablets is the focus of mobile forensics.
- Because individuals rely on mobile devices for so much of their data sending, receiving, and searching, it is reasonable to assume that these devices hold a significant quantity of evidence that investigators may utilize.
-Mobile devices may store a wide range of information, including phone records and text messages, as well as online search history and location data.
-We frequently associate mobile forensics with law enforcement, but they are not the only ones who may depend on evidence obtained from a mobile device.

Uses of Mobile Forensics:
The military uses mobile devices to gather intelligence when planning military operations or terrorist attacks. A corporation may use mobile evidence if it fears its intellectual property is being stolen or an employee is committing fraud.

Process of Mobile Device Forensics:

- **Seizure and Isolation:** According to digital forensics, evidence should always be adequately kept, analysed, and accepted in a court of law. Mobile device seizures are followed by a slew of legal difficulties. The two main risks linked with this step of the mobile forensic method are lock activation and network / cellular connectivity.
- **Identification:** The identification purpose is to retrieve information from the mobile device. With the appropriate PIN, password, pattern, or biometrics, a locked screen may be opened. Passcodes are protected, but fingerprints are not. Apps, photos, SMSs, and messengers may all have comparable lock features. Encryption, on the other hand, provides security that is difficult to defeat on software and/or hardware level.
- **Acquisition:** Controlling data on mobile devices is difficult since the data itself is movable. Once messages or data are transmitted from a smartphone, control is gone. Despite the fact that various devices are capable of storing vast amounts of data, the data itself may be stored elsewhere. For example, data synchronization across devices and apps may be done either directly or via the cloud. Users of mobile devices commonly utilize services such as Apple's iCloud and Microsoft's One Drive, which exposes the possibility of data harvesting. As a result, investigators should be on the lookout for any signs that data may be able to transcend the mobile device from a physical object, as this might have an impact on the data collecting and even preservation process.
- **Examination and analysis:** Because data on mobile devices is transportable, it's tough to keep track of it. When messages or data from a smartphone are moved, control is lost. Despite the fact that numerous devices can hold vast amounts of data, the data itself may be stored elsewhere.
- **Reporting:** The document or paper trail that shows the seizure, custody, control, transfer, analysis, and disposition of physical and electronic evidence is referred to as forensic reporting. It is the process of verifying how any type of evidence was collected, tracked, and safeguarded.

Finding Evidence in System Logs

- Regardless of what operating system you are using, the operating system has logs. Those logs can be critical in any forensic investigation, and you should retrieve them.
Windows Logs
Let's start with Windows 7/8/10. With all of these versions of Windows, you find the logs by clicking on the Start button in the lower-left corner of the desktop and then clicking the Control Panel. You then click on Administrative Tools and the Event Viewer. Here are the logs you would check for. (Note that not all appear in every version of Windows.)
Note: With all of these, you have to turn the logging on; otherwise, there will be nothing in these logs.
■ Security log: This is probably the most important log from a forensics point of view. It has both successful and unsuccessful login events.
■ Application log: This log contains various events logged by applications or programs. Many

applications will record their errors here in the application log.
■ System log: The System log contains events logged by Windows system components. This includes events like driver failures. This particular log is not as interesting from a forensics perspective as the other logs are.
■ ForwardedEvents log: The ForwardedEvents log is used to store events collected from remote computers. This will only have data in it if event forwarding has been configured.
■ Applications and Services logs: This log is used to store events from a single application or component rather than events that might have systemwide impact .

Linux Logs

Obviously , Linux also has logs you can check. Depending on your Linux distribution and what services you have running on it (like MySQL), some of these logs may not be present on a particular machine:

■ /var/log/faillog: This log file contains failed user logins. This can be very important when tracking attempts to crack into the system.

■ /var/log/kern.log: This log file is used for messages from the operating system's kernel. This is not likely to be pertinent to most computer crime investigations.

■ /var/log/lpr.log: This is the printer log and can give you a record of any items that have been printed from this machine. That can be useful in corporate espionage cases.

■ /var/log/mail.*: This is the mail server log and can be very useful in any computer crime investigation. Emails can be a component in any computer crime and even in some noncomputer crimes such as fraud.

■ /var/log/mysql.*: This log records activities related to the MySQL database server and will usually be of less interest to a computer crime investigation.

■ /var/log/apache2/*: If this machine is running the Apache web server, then this log will show related activity. This can be very useful in tracking attempts to hack into the web server.

■ /var/log/lighttpd/*: If this machine is running the Lighttpd web server, then this log will show related activity. This can be very useful in tracking attempts to hack into the web server.

■ /var/log/apport.log: This records application crashes. Sometimes these can reveal attempts to compromise the system or the presence of a virus or spyware.

■ /var/log/user.log: These contain user activity logs and can be very important to a criminal investigation.