End-System Security

Host Security

Any device with an IP address connected to the network is considered a host. A host is an important and integral part of any network in the organization. Host security plays a vital role in securing organization network activities since the host can be the major conduit. If the host is compromised, all devices and services risk being compromised as well. Host security refers to the protection of hardware, software, information stored, and services running on these computers from any kind of theft or damage.

The organization should ensure the confidentiality, availability, and integrity of the host and its data. An unsecure configuration of a host can put the entire network at risk. Even though proper host security measures are taken into consideration while installing the host in the network, the host can still be unsecure through its use. Over time, the hardware and software installed on the host become outdated and are prone to various types of threats inherent to poor patch management methodologies. Thus, it is important to address and ensure the security of the host during its lifecycle.

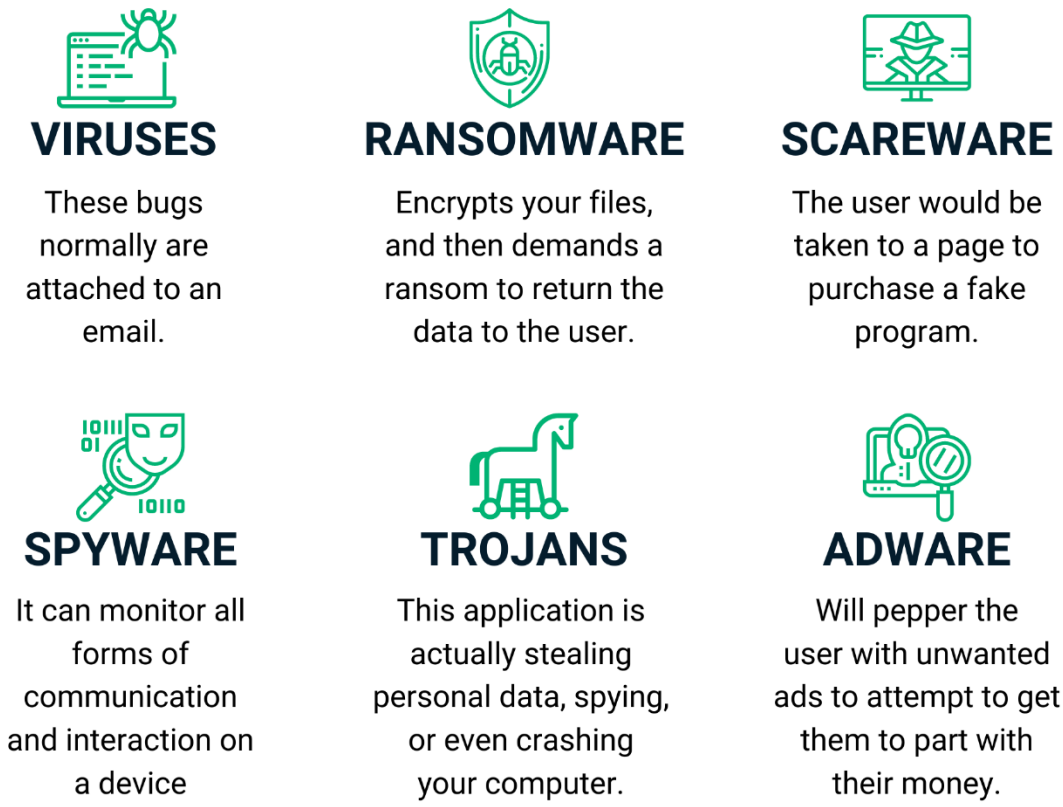
The organization needs to systematically monitor the hosts in order to understand the probability of attacks and to identify the various possibilities of attacks on the hosts. Understanding the areas of compromise can help the administrators come up with solutions to prevent those attacks. They can put forward various policies and regulations to strengthen the security of the hosts, thereby providing negligible (or no) impact to the organization's business. Appropriate training and awareness can help administrators maintain the security of the host in an organization.

Common Threats Specific to Host Security

Hosts can be at risk of both internal and external threats. The internal threats mainly occur within an organization and the damage caused by these threats can lead to a great loss of assets for an organization. These threats include malware attacks,

information theft, unauthorized access, illegal use of corporate resources, etc. Any sort of attack on the host internally can affect the end users and the business of an organization. Administrators should evaluate their host against possible internal and external threats. To ensure host security, you should be aware of different threats to which the host is vulnerable. The host can be at risk of being exploited by the following major threats.

Malware Attack



Viruses: Viruses are programs that replicate by reproducing itself to infect the host system. These make changes in the host by deleting files, reformatting the hard drive, etc. A virus-infected system cannot operate again as before.

Worms: They are viruses that repeat itself without much human interaction. They have the ability to spread and infect systems as they travel through the network or the Internet.

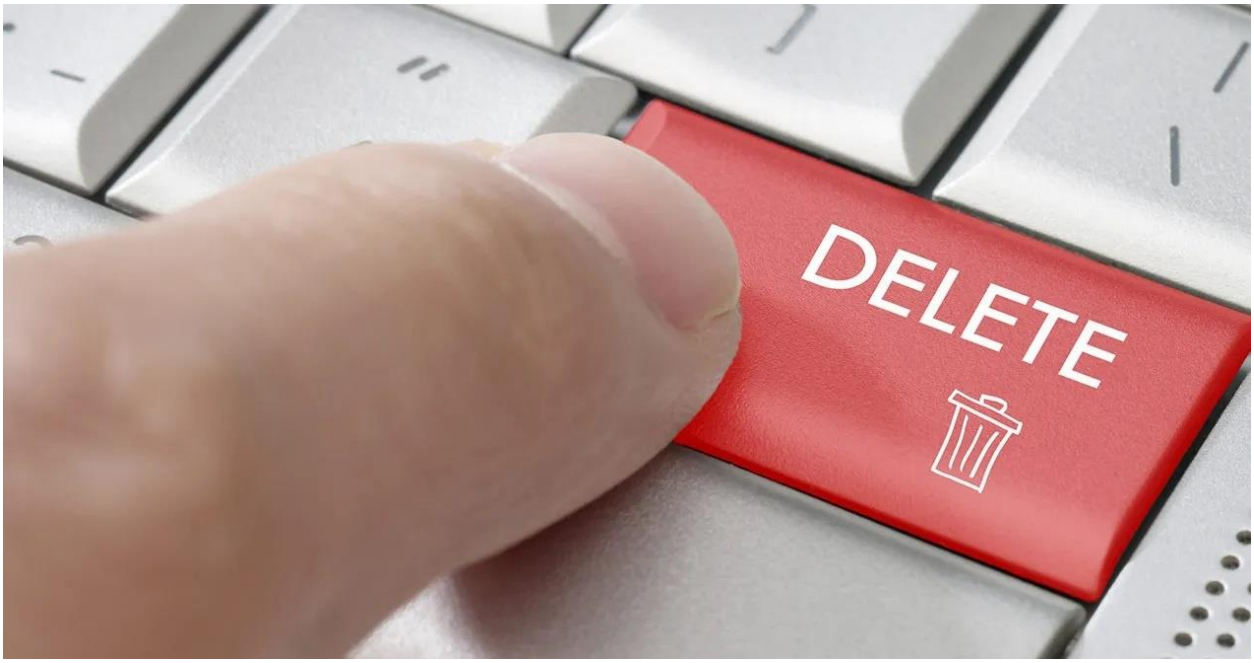
Trojans: A Trojan is considered one of the most complex threats and it creates damage to the host. They hide the payload part of the data packet while travelling through the network, thereby allowing file corruption, remote access, interrupting firewalls, and antivirus. Another impact of a Trojan is its ability to steal data. This makes it easier for the attackers to gather sensitive information.

Spyware: Spyware is a malware that is used for spying on the actions performed by a user and gathers the information of all activities performed by them on the system. For example, a keylogger is a type of spyware that is used to capture keystrokes.

Backdoor: A backdoor is planted to skip all the authentication steps required and gain unauthorized access to remote computers.

Accidental or intentional deletion of data

Users can sometimes delete any confidential data (intentionally or accidentally) that affects the security of the host.



The deletion or removal of data can affect the host security:

- A person gaining access to the host can perform intentional or unintentional deletion or modification of data present in the system.
- Acquire the information present in the system.
- Compromise the availability, confidentiality, and integrity of the stored data.

Unauthorized Access

Unauthorized access refers to gaining unauthorized access to restricted files, data, operation, and services running on a host. An attacker, if successful in gaining unauthorized access to the system, can perform any malicious action, which will affect the security of the hosts in the network. The unauthorized access can result in stealing, accessing sensitive files, and installing a virus in the system.

An attacker can take advantage of various vulnerabilities in order to compromise a specific host. Threats of exploiting vulnerabilities on a host can take various ways to get into the system and infect it. The lack of sufficient knowledge, skills, and unsecure configurations in host security opens up the network to different types of the security threats:

- **Unpatched Computers**: The majority of attacks on a host are due to the lack of proper patching or the use of outdated software installed on the host. An unpatched computer can create security loopholes and gives attackers a path to compromise it.
- **E-mail**: Host system security can be compromised through sending unsolicited emails such as phishing, malicious attachments, spam emails, etc.
- **Network File Sharing**: Network file sharing permits the users to share files between their individual systems over the Internet. Even though it makes things easier for users to share files, it paves the way for many threats such as malware infections, exposure of sensitive or important information, etc.
- **Internet Downloads**: Internet downloads from untrusted sources can lead users to download malware onto their systems.
- **Social Engineering**: Attackers use social engineering techniques to gain sensitive information, which may help them further to gain unauthorized access, infect a system with malware, etc.
- **Blended Threats**: An attacker uses a combination of multiple techniques to attack or infect the system.

Host Assessment

Before configuring host security, identify the purpose of each host, which can be:

- Category of information stored and processed by the host
- Security requirements needed for information
- Network services provided by the host
- Security requirements needed for network services
- User groups that have access to the host
- Trust relationships between hosts

Host Security Baselining

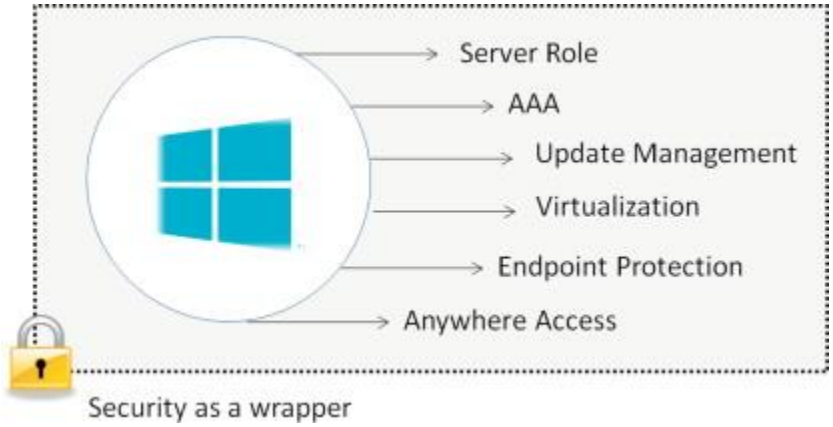
Host security baselining plays an important role in enhancing the host security of organizations. Administrators must define and establish a security baseline for hosts in the network depending upon their purpose, criticality, etc. The establishing of a security baselines depends on the needs of the organization. Defining any security baseline requires active involvement of management and various departments of an organization to include their preferences. Host security baselines help you easily identify the hosts with configurations that do not match as stated in the baseline. A host security baseline sets a security objective (standards, guidelines, checklists, etc.) that must be met to attain a high level of host security for an organization. It specifies the reference points for installation, hardening, placing of new hosts in the network, and all activities performed on the host. Baselining facilitates more protection for the host and helps in determining the actions taken for further security. The baselines should be regularly updated and monitored.

The baselines help you to determine:

- The way the host performs in the network.
- The type of data the host uses to communicate across the network.
- Identify the services and resources associated with each host.
- The type of connectivity required for each host.
- A clear picture regarding the working of each host

OS Security

Operating system security refers to securing three components: OS integrity, confidentiality, and availability. Each host in the network has a specific OS installed and running. Typical functions of an OS are managing security, system, communication, input/output, and hardware and software services for the host on which it is installed. OS security has a direct impact on host security. OS-level protection is required to attain host security.



Each OS provides a number of built-in security features. The security features help administrators in hardening the security of the host if configured appropriately based on the OS security baseline established by the organization. The OS security puts forth certain steps to protect the hosts from malware or hacker invasions.

As the operating systems are large and complex, it may come across many security issues. The chances of a virus or a worm invading the system are greater when there are not adequate security policies. In addition, the operating system provides many services that are critical to the functioning of the operating system. The OS security features must include measures that can take control of these services running on the OS.

Baselining Operating System Security

The organization establishes OS security baselines to implement a standard for installing and configuring the operating system. Setting up a baseline varies from one organization to another. The administrators should take care while creating the baseline for an operating system and confirm that it meets the company requirements. The baseline for the OS needs to include the configuration of various operation system settings as well as recording each step (this helps future configurations). The baseline for the OS should also include the actions performed on the system.

The OS security baseline should address the following security configurations at minimum:

- **Non-essential Services**: Only essential services should be enabled on the OS. Enabling unnecessary services on an OS can give a path to an attacker to compromise the host through OS security flaws. For example, if a host is not functioning as a webserver or a mail server, it should be disabled immediately.
- **Patch Management**: The operating system should undergo patch management regularly in order to ensure that the OS is updated with all the latest updates and fixes.
- **Password Management**: Operating systems need to persuade the users to use complex and strong passwords based on the organization's policy. Password management should also urge the users to change the password after a certain period of time and implement user lockout after a fixed number of attempts.
- **Unnecessary Accounts**: Organizations need to monitor the account details of the users. They may remove or delete all unwanted and guest user accounts.
- **File and Directory Protection**: Organizations should control the file and directory permissions using access control lists.
- **File and File System Encryption**: Encryption of files and folders, as well as the formatting of disk partitions, in a file system with the help of encryption features provided by the OS.
- **Enable Logging**: Tracking all log activities of an operating system. File Sharing: Disabling unwanted file sharing applications running on the operating system.

Windows Security Baseline

Microsoft announces the security baseline settings for their desktop and server OS products periodically. With each release, Microsoft reevaluates older settings to determine whether they address contemporary threats or not, and then adds updated baseline settings to address newly discovered vulnerabilities and misconfigurations. It generally includes guidelines and checklists for:

- Installing software.
- Disabling unnecessary services.
- Applying Windows OS security updates and patches.
- Applying local security policy settings.
- Configuring automatic update settings
- Managing user accounts.
- Managing passwords.

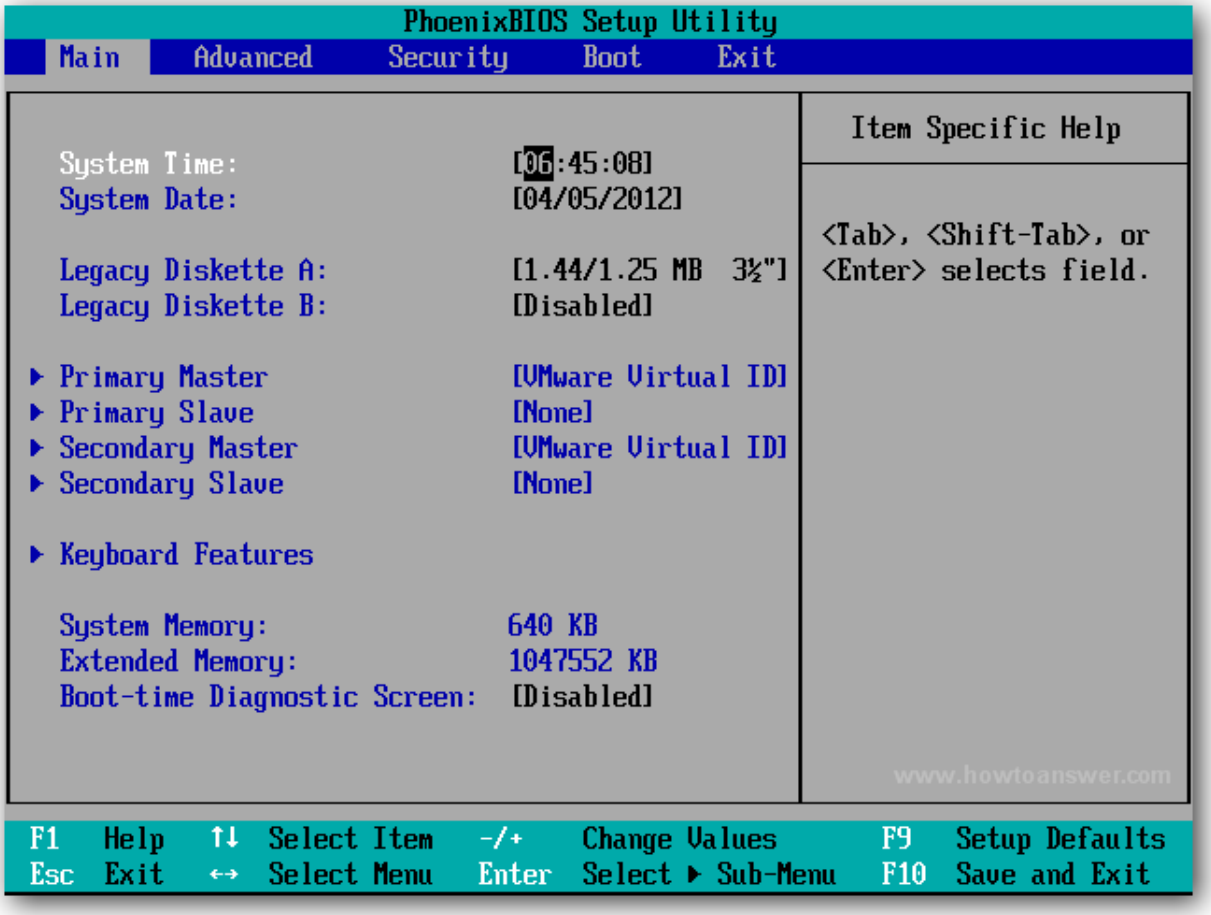
The Windows security baseline defines the steps for identifying the security updates and configuration changes required. The baselines compare and measure the scheduling, construction methods, management, and results in the operating system.

Microsoft Baseline Security Analyzer (MBSA)

The Microsoft Baseline Security Analyzer (MBSA) lets administrators scan local and remote systems for missing security updates as well as common security misconfigurations. The MBSA is used to analyze the security standards for the organization by identifying the updates required by the organization and rectifying the weaker settings of Microsoft Windows. MBSA helps small and medium-sized business organizations analyze the security status and standards and check whether it is compatible with the Microsoft security recommendations. All the scan results produced by MBSA check for critical issues, non-critical issues, and the best methods that describe the remedies that can be taken for securing the operating system.

Setting up a BIOS Password

Setting up a BIOS password is the first protection layer of the computer. It helps you maintain OS security at a low level.



Steps:

- Enter the BIOS Setup Utility interface
- Select Security and set Supervisor Password. It will control the access to the setup utility.
- Now, set User Password.

Setting up a BIOS password helps you in controlling the access of the system from external users. The BIOS of an operating system provides the feature of setting up a password that, in turn, prevents other users from:

- Accessing the system.
- Booting the computer.
- Booting from removable devices.
- Changing BIOS settings.

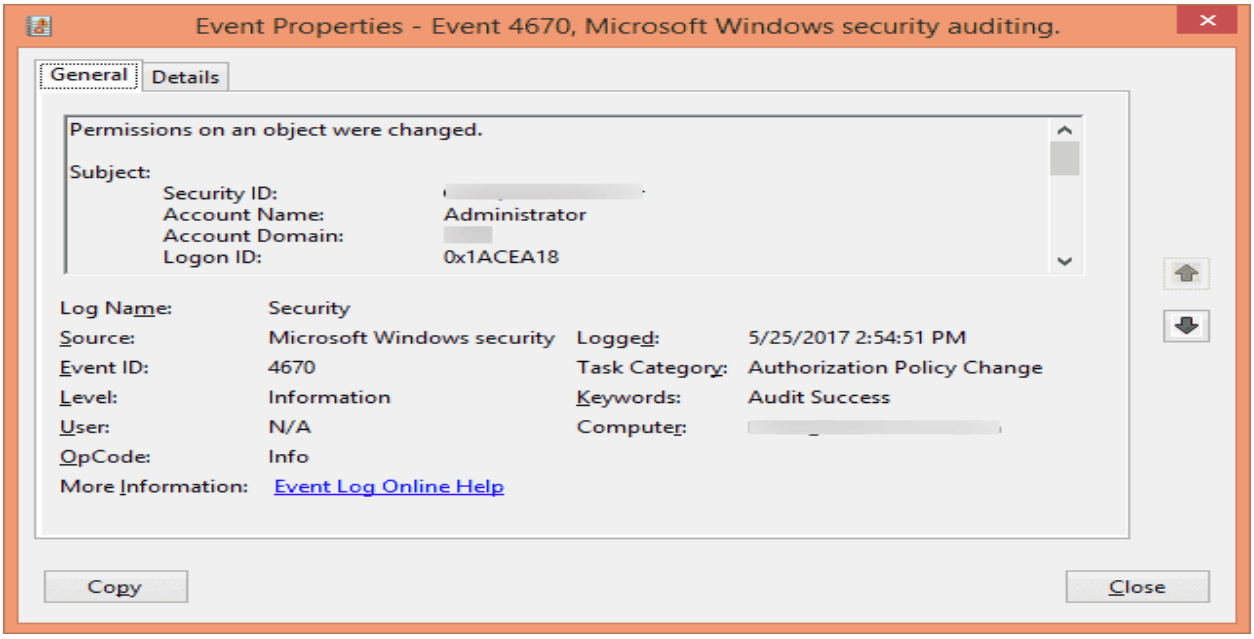
BIOS passwords are most suitable for systems in public places or a workplace that disables other users from installing another operating system over an existing one. A BIOS setup program can be used for setting a BIOS password. This is easily done by clicking any key before the booting of the operating system. Clicking on the “Press F2 to

enter set up" message helps the user to go the BIOS settings page. Every computer has documentation available that helps with setting up the BIOS password.

The BIOS provides an extra layer of security by starting even before the operating system and other hardware. This allows the user to enter the password and prevents many password-cracking applications to run. It is a complex task to retain the BIOS password when compared to operating the password. Hence, users need to remember the BIOS password because if the user is unable to remember the BIOS password, then the user will be locked out. The users can always try resetting the BIOS password, but most of the time all the attempts are in vain, as it requires more time and provides only less chances of changing it.

Auditing Windows Registry

The Windows registry, otherwise known as registry, is a database of all the configurational settings of Microsoft Windows. Windows registry stores details like settings for software programs, hardware devices, user preferences, OS configurations, etc. At a glance, Windows registry consists of all details regarding the operating system. Accessing Windows registry requires the user to execute the regedit command in the command prompt.



The registry keys are as follows:

- **HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT:** Here, HKEY_LOCAL_MACHINE is the registry hive; Software and Microsoft groups are under this registry hive. Whereas Microsoft falls under the Software registry key.
- **HKEY_CURRENT_ CONFIG:** This registry key contains information regarding the currently used hardware profile.
- **HKEY_CURRENT_USER**: This registry gives all details regarding the users that are currently present on the computer. The user details include desktop settings,

network connections, printers, application preferences, and personal program groups. A new HKEY_CURRENT_USER sub-key is created every time a user logs in.

- **HKEY_CLASSES_ROOT**: This key contains the file name extensions and COM class registration information.

Process Monitor Tool

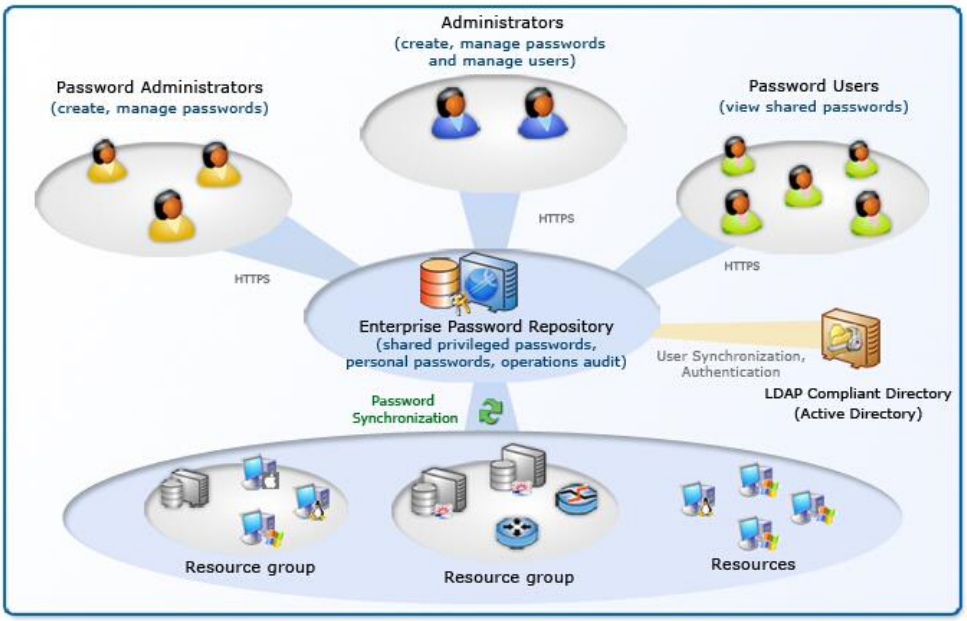
The Process monitor (Procmon) tool is one of the monitoring tools that help administrators monitor and audit the registry, file system, and network. It captures specific types of input/output operations, which might occur through the registry, file system, or network. It combines the features of Filemon and Regmon; thus, it provides real-time results related to the file system and registry.

Some of the features of the Process Monitor include:

- Captures input and output data.
- Allows setting up filters as per the user requirement reducing the loss of data.
- Gathers accurate information of process details.
- Relationship among the processes can be traced.
- Native log format stores all data in one location.

User and Password Management

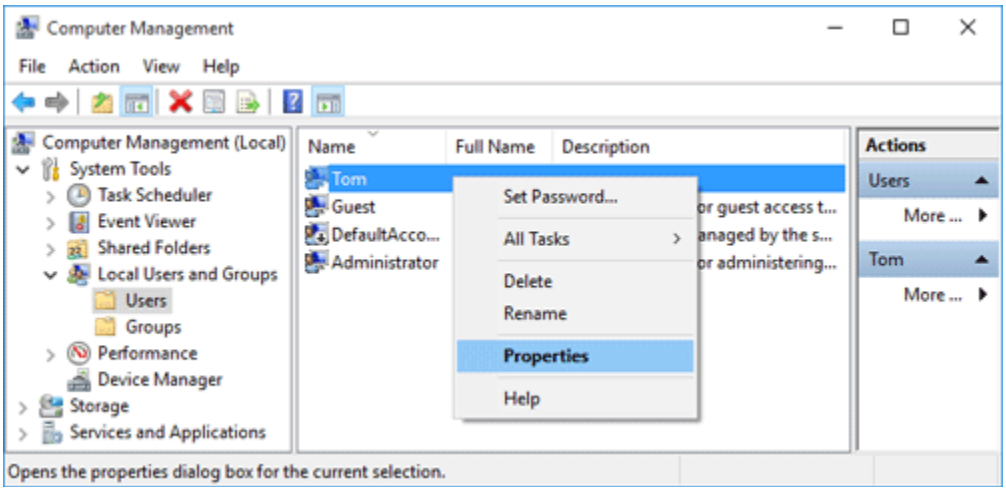
The Windows operating system has a different view in managing the user accounts and passwords. User management in Windows helps administrators identify and control the users logged in the system. This management includes identifying people logged into the network, as well as managing the user login and logout times.



User management provides a better authentication and authorizations of users accessing the network. Monitor user permissions before granting permission to access the network and analyze the logging details. The administrators have the benefit of analyzing the user details and activities. They can filter the user details by IP address or by user, thereby enabling easy management for the users. The whole concept of user management is based on the user logging in and logging out of the system. A user trying to access the system is first authenticated and allowed access to the system. There are certain policies for user management that define particular rules for managing the user accounts. A user can have multiple accounts or a single account. Multiple accounts on a single computer allow multiple users to store data and files in the same system, apply background themes according to each user's preference, etc. Users can create three types of accounts in Windows:

- **Administrator Account**: These account users have the complete privilege of performing any action on the system. These users can install and uninstall programs, make configurational changes to the system, add or remove other user accounts in the system, etc.
- **Standard Account**: Standard account users are users that have limited access to the system. They can access only those files and folders saved in their user account. They do not have the permission to change or delete any configurations of other users.
- **Guest Account**: These types of users do not have access to any of the files and folders on the system. These users can only check their email on the system.

The password management in Windows proceeds with the authentication of the user trying to access the system. In other words, all user accounts should be efficiently secured with passwords. An organization should have a well-defined and effective password policy that helps in minimizing the risks of password compromise during authentication. The policies created need to ensure the availability, confidentiality, and integrity of the passwords allowing access to only authorized users and preventing unauthorized access. Several access controls assist in maintaining the integrity and availability of passwords; whereas, maintaining the confidentiality of the passwords always remains a challenge for the organization. Maintaining the confidentiality of the password includes several security controls and decisions.



Some of the guidelines for creating strong and complex passwords are:

- Ensure that the password created does not include the username.
- Construct it using a combination of uppercase characters, lowercase characters, digits, and special characters.
- Avoid using a password used previously.
- Change the passwords periodically.
- The passwords need to be a minimum of eight characters in length.
- The password should not be a word from a dictionary.
- Always set a length for the passwords.
- Avoid storing the passwords at any location. If you need to store it, do so in an encrypted form.
- Do not share the password.

Best practices for using passwords in a better way are:

- Train users on the best ways to protect the passwords.
- Make them aware of the various forms of attacks on passwords.
- Use encryption techniques in order to securely store the password.
- Properly define the password security policies followed throughout the organization.

Disabling Unnecessary User Accounts

Administrators should disable unwanted accounts by deactivating them. Deleting a user account is entirely different from disabling an account. Disabled user accounts can be restored, whereas deleted user accounts cannot be restored. Here are the steps for disabling a user account in Windows:

- Go to Control Panel and press Enter.
- Select the option Administrative Tools.
- Click on Local Security Policy.

- Click on Local Policies option on the left side of the pane and click on Security Options under it. Find the option User Account Control from the list of options in the results pane. Disable the user account option.

An alternative method for the above-mentioned step is as follows:

1. Go to Control Panel -> User Accounts -> Manage Accounts

2. Turn Off the Guest Account if it is On.

Configuring User Authentication

Authentication validates and identifies the users accessing the application. It defines whether the user trying to access the system has user permissions to access and to perform actions.

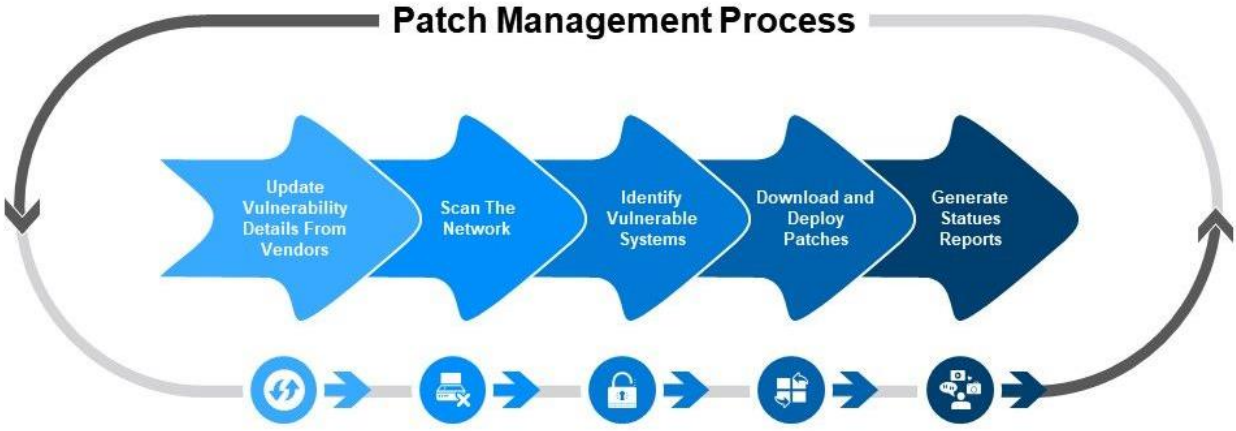
- **Change names and passwords for default accounts**: Systems that have multiple accounts should maintain different usernames and passwords.
- **Disable inactive accounts:** If an employee leaves the company, it is the role of the administrator to disable/delete all the accounts of the employee. Timely action can save the resources of the system from intrusion.
- **Assign rights to groups not individual users**: Administrators should deploy and implement a group policy in the organization. Group policies allow the administrators to assign rights to specific users. Implementation of group policies makes it easy for administrators to monitor the user activities.
- **Do not permit shared accounts**: Avoid shared accounts in a network. Accounts shared by users act as an open invitation to intruders.
- **Enforce appropriate strong password policy**: Administrators should encourage users to create strong passwords for their accounts. Easy passwords are more vulnerable to threats.

Patch Management

Patch management is an integral part of OS security. Patch management enhances the security of the system with regular updates. In an IT infrastructure, patch management needs to be efficient in order to maintain the security of the system. Patch management involves applying patches, service packs, or upgrading the OS to a newer version. Patch management facilitates a consistent configured environment that is secure against the vulnerabilities and threats on an operating system.

Patch Management Process:

- **Detect**: Install tools that can automatically detect updates and initiate the patch management process.
- **Assess**: Identify the severity of the vulnerabilities and the amount of patch required to remove the error.
- **Acquire**: Take the patch for testing if proper security measures are not taken for the detected vulnerabilities.
- **Test**: Install a patch on a test system, so that the complications of the update can be verified against the product configuration
- **Deploy**: Deployment of all the patches to other systems.
- **Maintain**: Maintain all other systems by sending notifications regarding the detected vulnerabilities.



The patch management process can be implemented in two ways on the user machines:

- Distribute a written process among the employees that can be implemented on their host machines.

- Implement an auto patch management system that allows the administrators to control the deployment of the patches on host machines.

Patch Management Processes:

Written Process: In this process, the organization trusts their employees by allowing them to install patches and keep their system updated. In such scenarios, organizations randomly check the systems of the users to make sure employees adhere to the patch management policy. However, following this process in an organization is not safe and can easily expose the IT infrastructure to intrusions.

Automated Process: Automated process is more reliable in terms of keeping the security of the organization. Once the vendors release the security updates, it becomes the responsibility of the administrators to apply those patches in time. These updates can fix the security vulnerabilities in the system or network. Installation of security patches reduces the risk of data loss.

Patch Management Principles:

- Every patch management strategy should have a service pack.
- Product lifecycle can be a key element in the patch management strategy.
- Perform risk assessment.
- Use mitigating factors for determining applicability and priority.
- Use only workarounds for deployment.
- Use only methods available for the detection and deployment.

Administrators should be aware of the security requirements of their organization and ensure that patch management is based on those requirements. They can also inform other users regarding the security patch and updates. Scheduling and prioritizing is required in performing patch management in Windows. Every patch management needs to have a patch cycle that provides a standard application for the patches and updates.

Configuring an Update Method for Installing Patches

The Windows OS provides users the option of automated updates. Turning on the Windows automatic updates in the control panel enables Windows to download and install all the updates. The process can take place automatically without much interaction from the user. However, the user must respond on time to the alerts that occur during the update process. Missing any alert can actually stop important updates.

Shavlik Patch

With Shavlik Patch you leverage a single Configuration Manager workflow for publishing updates for both Microsoft and non-Microsoft products.

Kaseya

Kaseya provides the tools and infrastructure to enforce policies and to easily address the complexities of software and security patch deployment and simultaneously deploys all required patches across machines.

LabTech's App-Care

The App-Care patch management solution extends LabTech's Microsoft update patching to third-party applications with seamless integration to close security holes and guard against attacks. It automatically downloads third-party patches from the manufacturer and pushes them to computer to close security gaps in third party applications.

Lumension

Lumension patch management software helps IT professionals uncover security vulnerabilities and deploys security patches across an entire network to eliminate them. This patch management software can be used on Windows, Mac OS X, UNIX, and Linux platforms as well as third-party applications and infrastructure devices.

Methods to Secure Host System (Windows)

Disabling Unused System Services

Unnecessary services run in the background on the systems the user is not aware of. Leaving these services enabled can give a path to the attacker to compromise the system, as some of them can be vulnerable to different types of attacks. Administrators can find unnecessary services running on the system based on an organization policy. The policy statement may include lists of necessary services that should be allowed to run on the system and unnecessary services that should be not allowed to run. An administrator can create, pause, stop, and restart a service as per the system and user requirements. On the user machine, administrators can disable a service that is not required. Disabling unnecessary services is important because it reduces the chances of system exploitation. Services like IIS, FTP, SQL Server, Proxy services, and Telnet are usually not required by the users. Administrator privileges are required to enable and disable services on a particular host.

Go to Control Panel -> Administrative Tools -> Services

Disable the following service on any machine other than a server:

- IIS
- FTP
- SQL server
- Proxy services
- Telnet
- Universal Plug And Play on any machine

Set Appropriate Local Security Policy Settings

Local policy settings allow the enforcement of many systems, users, and security-related settings in Microsoft Windows. These policy settings include Password Policy, Audit Policy, and User Permissions. There are default policy settings available; however, the administrator needs to configure more policies in order to confirm security. An administrator should define and set the policies as per the organization's security policies

1. Go to Control Panel

2. Click Administrative Tools -> Local Security Policy

3. In the security settings, perform one of the following actions:

    a. Click Account Policies in order to edit the password policy and account lockout policy

    b. Click Local Policies in order to edit audit policy, user rights assignment, and security options

4. Double-click on the policies in order to modify or edit the policies

5. Click OK after performing the desired action

Every organization should enforce a policy that their employees change their password after a specified time of interval. This necessitates policies that outline the requirements for setting a password. The changes in password policy affect only the local computer. However, the configuration of the policies depends on the policies for each organization.

For instance, an organization can edit or configure the local password policies as follows:

- Click on Account Policies
- Password Policy in the left pane
- Double-click on Enforce password history in the right pane
- **Maximum password age**: Determines the time period for using a password. Default value is 42.
- **Minimum password age**: Determines the minimum number of days the user needs to use the password.
- **Minimum password length**: Determines the length of the passwords. Usually the minimum value is "8."
- **Password must meet complexity requirements**: Determines the criteria for creating a password. This option is enabled and includes uppercase and lowercase letters, numbers, and special characters.
- **Store passwords using reversible encryption:** Always "Disabled," as it allows the attacker to crack the password easily.

Configuring Windows Firewall

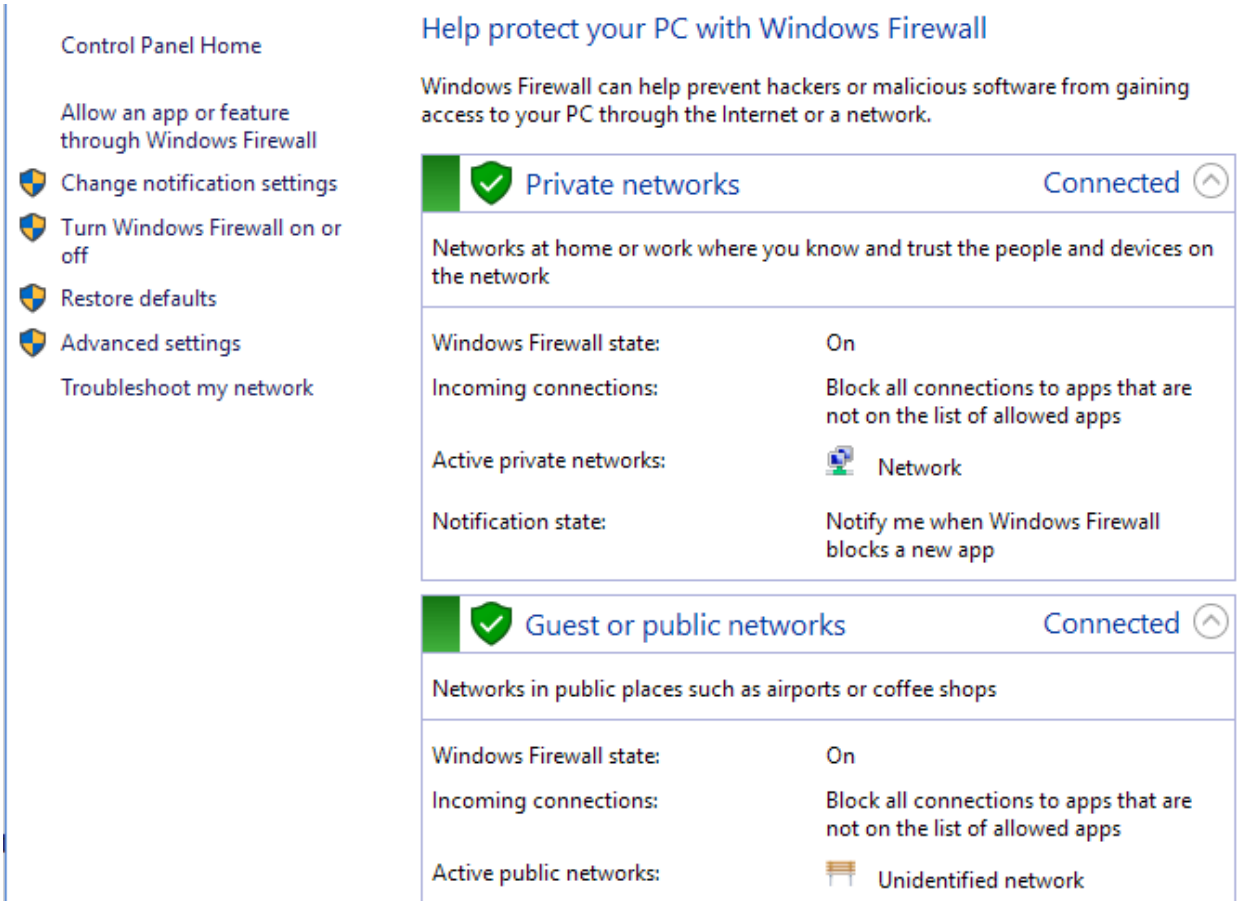
Go to Control Panel

Windows Firewall and click Turn Windows Firewall on or off.

Windows Firewall is a built-in feature that governs the security of Windows. It helps in preventing intrusions (internally or externally). Windows Firewall has the ability to monitor the incoming and outgoing traffic. Rules and exceptions in the Windows firewall maintain the logs of the traffic. Administrators can apply rules and exceptions based on the type of network and location of the machine. Turning the Firewall ON filters communication passing through it. Administrator privileges are required to turn ON the Windows firewall feature. The following steps define how to turn ON the Firewall:

1. Start -> Control Panel -> Windows Firewall

2. Click Turn Windows Firewall ON or OFF



Beside traffic filtering and blocking, the Windows Firewall also maintains additional information such as:

1. **Windows Firewall state**: Informs if the firewall is ON or OFF.

2. **Incoming connections**: Notifies the action the firewall will take for incoming connections.

3. **Active private network:** Displays the name of the active private network.

4. **Notification state**: Notifies the action taken by the firewall for applications.

Configuration of Windows Firewall is done through the option, Advanced Security. Windows Firewall with Advanced Security displays the detailed functioning of the firewall. It helps in the implementation of rules and exceptions for the firewall. The snap-in displays the rules and exceptions for inbound and outbound traffic.

Inbound Rules: They apply to traffic that is coming from the network or the Internet to your Windows computer or device. For example, if you are downloading a file through Bit Torrent, the download of that file is filtered through an inbound rule.

Outbound Rules: These rules apply to traffic that is originating from your computer and going to the network and the Internet. For example, your request to load a website in your web browser that is outbound traffic and is filtered through an outbound rule.

Connection security rules: Less common rules that are used to secure the traffic between two specific computers while it crosses the network. This type of rule is used in very controlled environments with special security requirements. Unlike inbound and outbound rules that are applied only to your computer or device, connection security rules require both computers involved in the communication to have the same rules applied.

All the rules can be configured so that they are specific to certain computers, user accounts, programs, apps, services, ports, protocols, or network adapters. You can display the rules of a certain type by selecting the appropriate category in the column on the left.

Creating an Inbound/Outbound Rule:

1. Go to Outbound Rule → In the Actions pane, click New Rule
2. Select the Type of Rule you want to create → Next
3. Type the pathname of the program → Next
4. Select the Action you want to take → Next
5. Select the Network Location for implementing the rule → Next
6. Enter the Name of the rule and Description if necessary → Finish
7. The new rule will appear in the Actions pane

Install Antivirus Software

Protecting the system from viruses is an important task for host security; it should be a primary focus for administrators and the users working on the system. By installing updated antivirus software, you can protect your system from virus-infected files, system crash, unwanted pop-ups, and damage to the operating system caused by a malware infection. Administrators can also use various third-party antivirus solutions for better protection. Windows has a built-in antivirus solution (called Windows Defender) to protect the system from virus infection. Windows Defender runs in the background and notifies you when you need to take specific action. However, you can use it anytime to scan for malware if your computer isn't working properly or if you clicked a suspicious link online or in an email message. Windows Defender is malware protection software used in order to detect and mitigate viruses and other malicious programs.

Windows Defender scan process:

1. Search for Windows Defender in the search bar

2. Open Windows Defender

3. Select the Type of Scan of choice:

I. **Quick scan**: Scans only those areas of the computer that are more prone to virus attacks.

II. **Full Scan**: Scans all files and folders present in the system. This process may be a time-consuming process.

III. **Custom Scan**: Scans only those files or folders as provided by the user.

4. Click Scan Now

Third-Party Antivirus Software

Below is the list of some third-party antivirus software that can be used to protect your host from malware infections.

AVG Antivirus

AVG Antivirus helps stop, remove, and prevent the spreading of viruses, worms, and Trojans. It protects your PC from malware on and helps stop anything that's infected.

Symantec Norton Security with Backup

Norton Security Scan determines if your system has been infected with viruses, malware, spyware, or other threats. It checks for suspicious or dangerous cookies and removes those that raise a concern.

Avast Pro Antivirus

Avast Pro Antivirus scans for all the files being downloaded through torrents, servers, or flash drives. The files are first tested before being saved in the system. The software can secure the DNS settings, preventing the hijacking of the DNS, fake-password attacks, etc. The antivirus pre-determines the malicious packet/data travelling toward the user's router device or network and dumps it before exploitation.

McAfee

The McAfee antivirus software tool scans the core components of the system and ensures it is up to date. The software installs the updates in the background without affecting the productivity of the system. The tool can diagnose whether malware, worms, or Trojans are hiding in the backend of the processes and modules. McAfee has a feature to maintain schedule scans on the host machine.

Avira

Avira antivirus tool protects the system from viruses, worms, and Trojans. It scans unknown files in real time for malware and exploits, blocks harmful websites before they load, and identifies potentially unwanted applications hidden within legitimate software.

Quick Heal

Quick Heal is antivirus software used to protect your system from viruses, worms, Trojans, spyware, and other such threats.

Kaspersky

Kaspersky antivirus delivers essential protection against all types of malware. It safeguards you from the latest viruses, spyware, worms, and more.

Panda

Panda provides real-time protection against the latest malware. It protects PC, Mac, or Android devices against all types of threats.

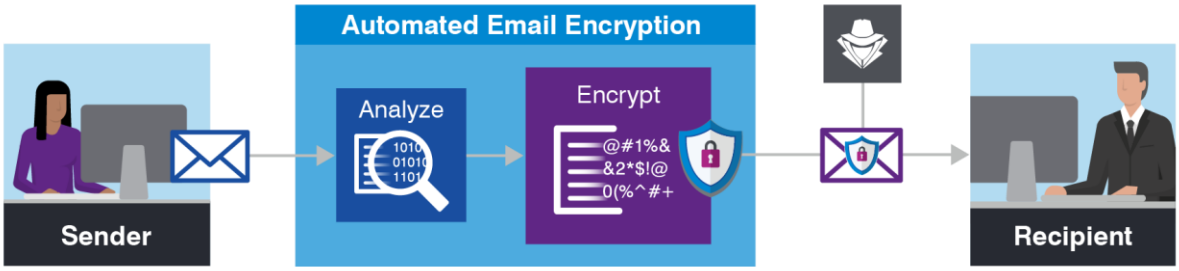
GData

GData has a feature that proactively detects malware in the system. It scans SSL-encrypted emails for malicious attachments and suspicious content. Trend Micro's Maximum Security Trend Micro's Maximum Security helps you to prevent identity theft by blocking phishing emails. It scans privacy settings on social media accounts and provides a secure browser for safe online banking.

Email Security

Email threats have rapidly evolved as one of the major concerns for cyber users. Spamming is one such threat to email security. Spamming involves sending unsolicited bulk email (UBE), junk mail, or unsolicited commercial email (UCE) frequently to individual users or group of users. These spam emails typically cost users money. Spam

mail sent via virus-infected networks can install a backdoor that allows the spammer to access the computer and use it for malicious purposes.



Anti-Spammers

Anti-spam is a method of denying spam emails in the user's email. Generally, anti-spam methods scan the computer's IP address, email signatures, and data. This can minimize users from receiving spam emails. There are many types of anti-spam systems used together with many email systems and internet service providers (ISPs).

There are various benefits for using email security:

- Provides complete security from any kind of cyber-attack through email by preventing unwanted bulk emails and viruses.
- Identify unknown malware and other malicious links in the emails.
- Helps in reacting to the detected spam emails.

Spam-Filtering Software

Below is a list of anti-spammer tools for email security.

MX Guarddog

MX Guarddog offers complete email security, with no software to install and no changes to your email clients. The tool protects user emails against, viruses, malware, phishing emails, DoS attacks, etc.

FireEye Email Security

FireEye Email Security products detonate and analyze suspicious email attachments and embedded URLs, as well as block malicious activity, to enhance email security. With these capabilities, organizations can prevent, detect, and respond to email-based cyber-attacks. AV and anti-spam protection are available to handle casual attacks and nuisance traffic. Customers can select Email Threat Prevention cloud (ETP) for a complete, off-premise email security solution with no hardware or software to install.

Symantec Email Security Symantec Email Security effectively blocks unwanted email. It is a capable of blocking spear-phishing and targeted attack malicious URLs with Real Time Link. It analyzes the email body, subject, and headers, as well as text within document attachments, to identify and prevent loss of confidential data.

SpamFighter

SpamFighter protects all the email accounts on your PC. It protects against phishing, identity theft, and other email fraud. It blacklists and block emails and domains. Avast

Avast Internet Security has anti-spam features that allow you to stay safe from phishing and do not have to waste your time with junk emails.

K9

K9 is an email-filtering application that works in conjunction with the regular POP3 email program. It automatically classifies incoming emails as spam (junk email) or non-spam without the need for maintaining dozens of rules or constant updates to be downloaded. It uses intelligent statistical analysis that can result in extremely high accuracy over time. K9 is for standard POP3 email accounts only. It does not support IMAP, nor does it support Hotmail, AOL, or any other kind of webmail-type systems. It does not natively support SSL or secure authentication.

Spamihilator

Spamihilator works between the email client and the Internet and examines every incoming message. It filters the spam and non-spam mails. The Spamihilator uses a number of filters in order to identify spam present on the user network. The program works with almost every email client, such as Outlook, Mozilla Thunderbird, Eudora, IncrediMail, Pegasus Mail, Phoenix Mail, Opera, etc.

G-Lock SpamCombat

SpamCombat removes the spam, virus, and junk emails from your inbox. It eliminates all unwanted messages at the server level without receiving them with the email client. G-Lock SpamCombat uses filters like Complex filter, Whitelist, Blacklist, HTML Validator, DNSBL filter, and the Bayesian filter in order to avoid spam in the inbox.

Cyberoam Anti-spam

Cyberoam Anti-Spam provides real-time spam protection over SMTP, POP3, and IMAP protocols. It protects organizations from zero-hour threats and blended attacks that involve spam, malware, botnets, phishing, and Trojans. AVG Antivirus AVG antivirus is a cloud-based email security service that delivers comprehensive protection against spam, viruses, phishing attacks, and other email-borne threats. It performs an automatic update and identifies the spam before it affects the user's network.

Enabling Pop-Up Blockers

A pop-up blocker is a feature that automatically prevents websites from opening windows that aren't the main browser window. Pop-up blockers allow you to control what happens as you travel the web and prevent sites from filling your desktop with pop-up windows you do not want or need. All modern browsers have pop-up blockers. It prevents the unnecessary storage of webpages and their pop-ups in the system. Usually, sites add pop-ups so that users can get extra information about their search.

However, it is advisable to turn on the pop-up blocker to avoid any intrusion on the system.

Follow the below steps to enable the pop-up blocker feature to prevent unwanted windows from opening:

Internet Explorer:

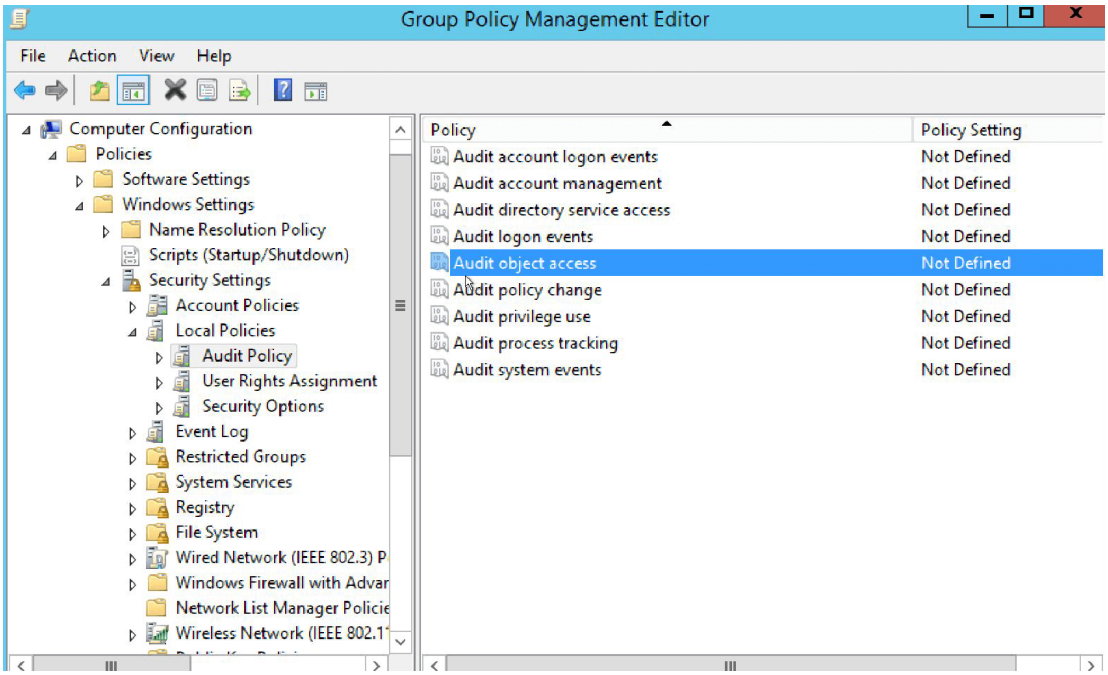
1. Click on Start -. Control Panel
2. Select Internet Options -> Privacy tab
3. To enable the pop-up blocker, check on the box “turn on pop-up blocker”
4. Click on Settings option to provide exceptions to the websites
5. Enter the name of the websites in the textbox “Address of website to allow” -> Allow
6. Select the “Blocking Level” as per the requirement
7. Close -> Apply -> OK

Mozilla Firefox:

1. In Mozilla Firefox, click -> Options
2. Go to Content -> Check the box “Block pop-up windows”
3. Exceptions tab will allow adding the URL to exclude from pop-up block rule
4. Click OK

Windows Log Review and Audit

Conduct peer log review and audit periodically to look for any suspicious activity and respond to the security incidents. You need to have administrative access privileges to conduct a log review and audit. Event Viewer provides a quick overview of when, where, and how an event occurred. Navigate to Control Panel, go to Administrative Tools, and then double-click Event Viewer.



Check Windows Event Log for various types of logs:

- System log
- Security logs
- Setup logs
- Application logs

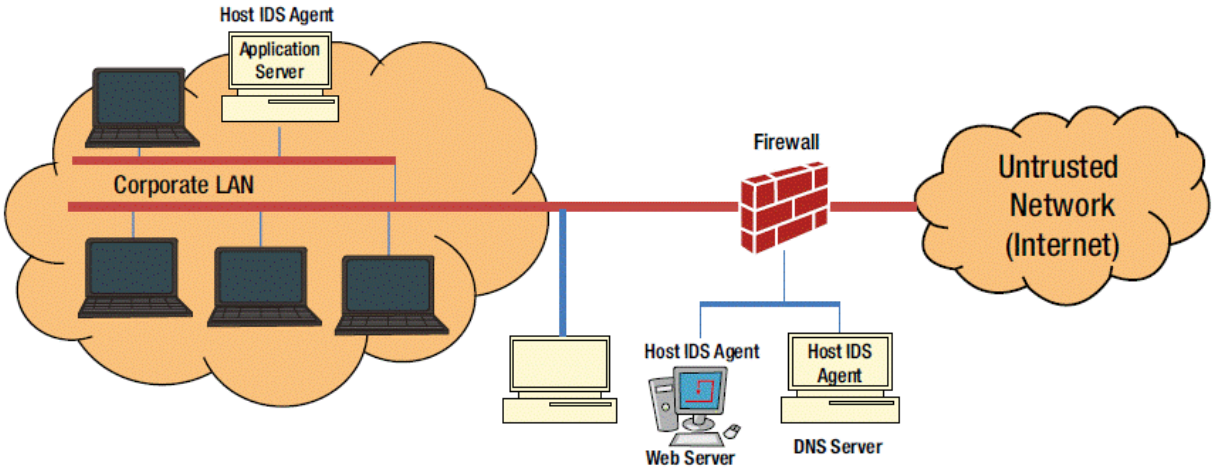
Typical log entries contain the following types of information about the events:

- **Level**: It defines the severity of event. Various types of severity levels are Information, Warning, Error, Critical, and Component.
- **Keywords**: It defines the type of event that occurred. Various types of events are AuditFailure, AuditSuccess, Classic, Correlation Hint, Response Time, SQM, WDI Context, and WDI Diag.
- **Date and Time**: It defines the date when events occurred.
- **Source**: It defines the source of the event.
- **Event ID:** An unique event ID is assigned for each type of event.
- **Task Category**: It defines task categories

A Windows log review and audit involves monitoring and analyzing the log entries for suspicious behavior. Administrators find the log review and audit helpful in troubleshooting problems with Windows and other programs as well as detecting signs of malicious activities or attempts such as unauthorized login attempts made on the computer. All user activities on a Windows computer is recorded and stored in a file called the Windows Event Log. Administrators can view these log entries with the help of Event Viewer. Event Viewer tracks information in several different logs.

Configuring Host-Based IDS/IPS

The host-based IDS analyzes and identifies the presence of any malicious activity in a computer system on which the IDS works. It analyzes all the parts of the computer system, especially the resources used by each application, the current state of the system, the storage information (that includes RAM, log files, file system, and checks) for any changes in the application.



The host-based IDS detects:

- System compromise.
- Unwanted or unused applications.
- Any kind of modification in the critical configuration files (like registry settings).
- Malware.
- Rootkits.
- Rogue processes.
- Any important services that are paused during a process.
- User access to systems and applications.

The host-based IDS analyzes the internal and external of a computer system and checks whether all applications and programs in the computing system follow the security policies. The host-based IDS can work in combination with a NIDS, which means that the host-based IDS can detect any malfunction missed by a network-based IDS. The administrator can compare the analysis done by the host-based IDS and the network-based IDS in order to confirm the presence of any changes in the system performed by the intruders. However, the network administrator should consider implementing both a network-based IDS and a host-based IDS to secure their network.

Host-based IDS	Network-based ID
Analyze the log files and contains all information regarding the status of the system	Analyze the network traffic
Protects even when the LAN is off	Protects only when the LAN is ON
More Versatile	Less Versatile

More affordable	Cheaper to implement and needs less administration

Advantages of a host-based IDS:

- **Very low false positives**: The host-based IDS perform analysis directly on the host, thereby analyzing all the log files. This reduces the number of false positives.
- **Narrow operating system focus**: A host-based IDS functions only on certain operating systems, which, in turn, minimizes the number of drawbacks.
- **Non-network-based attacks**: Identifies the attacks on the physical machine as well.

Host-Based IDS: OSSEC

OSSEC is a platform to monitor and control your systems. It mixes all the aspects of HIDS (host-based intrusion detection), log monitoring, and Security Incident Management (SIM)/Security Information and Event Management (SIEM). It runs on most operating systems, including Linux, OpenBSD, FreeBSD, Mac OS X, Solaris, and Windows.

Key Features:

- **File Integrity Checking**: The goal of file integrity checking (or FIM file integrity monitoring) is to detect these changes and alert you when they happen. It can be an attack, a misuse by an employee, or even a typo by an admin; you will be alerted of a change to any file, directory, or registry.
- **Log Monitoring**: Every operating system, application, and device on your network generates logs (events) to let you know what is happening. OSSEC collects, analyzes, and correlates these logs to let you know if something suspicious is happening (attack, misuse, errors, etc.).
- **Rootkit Detection**: Criminal hackers want to hide their actions; but when using rootkit detection, you can be notified when the system is modified in a way common to rootkits.
- **Active Response**: Active response allows OSSEC to take immediate action when specified alerts are triggered. This may prevent an incident from spreading before an administrator can take action.

Host-Based IDS: AlienVault Unified Security Management (USM)

AlienVault's Unified Security ManagementTM (USMTM) platform accelerates and simplifies threat detection, incident response, and compliance management for IT teams with limited resources. With essential built-in security controls and integrated threat intelligence, AlienVault USM presents complete security visibility of threats affecting your network and how to mitigate them quickly. Its intrusion detection capability includes:

- Network IDS
- Host IDS
- File Integrity Monitoring (FIM)

USM detects intrusions such as:

- System compromises
- Rootkits
- Unwanted applications
- Critical services that have been stopped
- Malware
- Modification of critical configuration files (e.g., registry settings, password, etc.)
- Rogue processes
- User access to systems and applications
- Privilege escalations

Host-Based IDS: Tripwire

Tripwire software can help to ensure the integrity of critical system files and directories by identifying all changes made to them. Tripwire configuration options include the ability to receive alerts via email if particular files are altered and automated integrity checking via a cron job. Using Tripwire for intrusion detection and damage assessment helps you keep track of system changes and can speed the recovery from a break-in by reducing the number of files you must restore to repair the system. Tripwire compares files and directories against a baseline database of file locations, dates modified, and other data. It generates the baseline by taking a snapshot of specified files and directories in a known secure state. (For maximum security, Tripwire should be installed and the baseline created before the system is at risk from intrusion.) After creating the baseline database, Tripwire compares the current system to the baseline and reports any modifications, additions, or deletions.

File System Security

Setting Access Controls and Permission

Access controls can provide the authority to users, groups, and computers to access files and folders on the computer. When a user or an application requests access to the operating system resources, they need to submit their credentials to the operating system. The credentials are access tokens created every time a user or an application tries to log in. The operating system verifies whether the access token created has the permission to access the objects before permitting the user or the application to access the objects. Here, the OS compares the details contained in the access tokens with the Access Control Entries (ACE) for verification. The ACEs can block or permit the services depending on the type of the object. For example, the ACEs available for a printer are Print, Manage Printing, and Manage Documents. The ACLs contain a combination of the ACEs of an object.

Access Control Principles:

- Least amount of access of objects to users or user groups, thereby allowing them to perform only needed functions.
- The owner of an object is the one who created that object.

- Proper permissions are set up for files and folders while installing the operating system. Upgrade the level of permissions from least privilege to the desired level during installation itself.
- The files and other documents included in a folder can inherit the permitted privileges assigned to that folder.

Appropriate tools can help in managing the permissions of any folders.

Event Viewer helps in viewing the security logs associated with any object.

Access Control Entries: An ACL can have zero or more ACEs, wherein each ACE has the access to an object. Overall, there are six types of ACEs, out of which securable objects support three (Generic types); the other three are directory service objects (Object-specified types).

The three generic types of ACEs are:

Access-denied ACE: Used in the discretionary access control list in order to prevent access to any user.

Access-allowed ACE: Used in the discretionary access control list in order to allow access to any user.

System Audit ACE: Used in the system-access control list in order to create an audit log for each attempt by a user while accessing the objects.

The three types of object-specified types are:

Access denied, object specific: Used in the discretionary access control list to block access to a property or property set. It can even stop the inheritance level of a specified type of child object.

Access allowed, object specific: Used in the discretionary access control list to permit access to a property or property set. It can even stop the inheritance level of a specified type of child object.

System audit, object specific: Used in the system-access control list in order to create an audit log when a user attempts to access the child object.

The object-specific types and generic types differ only in the design of the inheritance level.

Access Control Lists: An access control list is a table that provides a detailed description of the access rights of the users toward accessing objects. Every object has an access control list that contains the details of the user rights and privileges for accessing that object. Each OS system has specific ACLs. The ACLs have one or more ACEs that contain the details of the users.

Permissions: Each container or object has a security descriptor attached to itself. This security descriptor contains a detailed description regarding the user access rights. The security descriptor is created along with the container or object. An ACE represents the

permission to users or user groups and the whole list or set of permissions is contained in an access control list (ACL). There are two types of permissions:

Explicit permission: Permissions that set by default upon creation.

Inherited permission: These are permissions achieved from the parent object to the child object.

Setting Access Controls and Permission to Files and Folders

Applying NTFS permissions to Files and Folders

Setting access controls to files and folders can specify which users and user groups can have the access permissions. NTFS files and folder permissions allow users to access files stored on the local computer and access files stored in a shared folder over the network. NTFS also allow sharing permissions on shared folders in accordance with file and folder permissions.

NTFS permissions for file:

Full Control: Specifies whether a user has all permissions to files. Users having full control have complete access rights to any file, even if he/she is denied permission.

- **Modify**: This allows the user to read, write, execute, and traverse.
- **Read and Execute**: Allows the users to go through each directory and read all files.
- **Read**: This allows the users to list folders, read files, read attributes, and read permissions.
- **Write**: Allows users to create files, write data, create folders, and set attributes.

NTFS permissions for the folder:

- **Full Control**: Specifies whether the user has complete access to folders.
- **Modify**: This allows the user to read, write, execute, and traverse.
- **Read & Execute**: This allows the users to list folders, read files, read attributes, and read permissions.
- **List Folder Contents**: Specifies if the user can access the included folders and sub-folders.

- **Read**: This allows the users to list folders, read files, read attributes, and read permissions.
- **Write**: Allows users to create files, write data, create folders, and set attributes.

Creating and Securing a Windows File Share

The Windows environment puts forward the concept of shared folders that allows all the users to access the resources contained in that particular shared folder. A shared folder enables every user to view and access the contents of the folder without any restriction. However, the organization needs to employ certain restrictions or permissions that can protect the contents in the shared folder.

A shared folder can contain applications, personal data, or any other data. The permissions set on the data depend on the type of content included in the shared folder. Certain features of a shared folder are:

- The shared folder permissions apply only to folders, not files.
- The shared permissions do not apply evenly to the files and folders contained in the shared folder.
- The permission to access the folder applies to all users who gain access to connect to the folder.
- Resources using FAT use shared folder permissions for protection.
- Permission applied to a group includes permission for each user in that particular group

There are certain best practices followed while providing shared folder permissions:

Assign folder permissions to group accounts, not user accounts: Assigning permission to group accounts is much easier than applying it to user accounts. A user in a user account can be a part of different shared folders; and each folder can have different share folder permissions. This leads to a combination of user and group folder permissions. In the case of group permissions, it is just a matter of addition or removal of users from the group and there is no need to reassign the permission to the users.

Assign certain restrictions on the permissions applied to the users in such way that the users can still perform their task.

Consolidate all the applications and other resources in one location.

Do not explicitly deny permission to a shared resource: If there are any denied shared folder permissions to a user, then that user cannot have that permission even if they are allowed permission to another group.

Set NTFS file system permissions for users logging locally: Shared folder permissions apply to those resources that are shared through the network and not locally. In addition, shared folder permissions apply to those files and folders in the FAT volume.

Ensure that the copied or moved shared folder possesses the shared folder permissions.

These steps will show how to create and secure a Windows file share.

1. Click on Start Menu and type “Computer Management” in the search box

2. Click System tools → Share Folders

3. Right click Shares → New Shares

4. Create a Shared Folder Wizard will launch → Next

5. In “Folder path” textbox, enter the path of the folder to be shared → Next

6. In “Share name” enter the name of the folder to be shared → Next

7. As per the requirement administrators can select the option from set the kind of permissions

8. Finish

Data and File System Encryption

Data encryption is used to prevent intercepting and altering (or misuse) the data. The Windows operating system provides a built-in encryption mechanism (such as EFS and BitLocker) to encrypt a specific file, folder, or the entire drive. EFS (Encryption File System) EFS (Encryption File System) is a built-in mechanism in the Windows operating system. EFS uses the standard DESX algorithm, which depends on a 128-bit encryption key.

EFS Features:

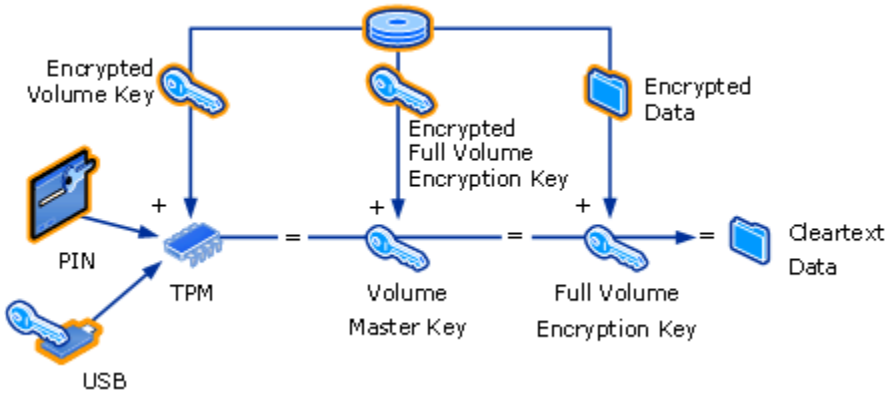
- Enabling encryption is an easy task.
- Helps in deciding the users that can access files and folders.
- Enables easy opening and closing of encrypted files.
- Easy to disable the encryption applied to a folder.

EFS Limitations:

- It works only for the NTFS file system.
- Lose encryptions when encrypted data copies to a non-NTFS system.
- Risk of data loss.

BitLocker

BitLocker extends the level of protection to the disk level. All the sensitive and important documents on the drive can be easily protected using BitLocker. It prevents the attackers from accessing the system password or documents even after removing the hard drive and placing it on another PC. The main feature of BitLocker is that it encrypts any new file added to the drive. However, copying files to another drive or PC keeps the files in the decrypted form.



BitLocker finds its application in encrypting:

- The operating system drive
- The internal hard drives
- The external hard drives

BitLocker checks for any security changes when the system starts. If it finds any kind of change in the BIOS, it locks the operating system and prevents it from performing further actions. BitLocker uses TPM (Trusted Platform Module), a microchip built into the computer that helps in storing the encryption keys. The TPM assists BitLocker to protect the system from attacks and theft.

Benefits of Bitlocker:

- Provides protection by encrypting the hard disk; thus, providing protection to the information stored in a physically damaged and irreversible hard drive.
- Since BitLocker offers boot-time inspection, it prevents the chances of any unauthorized changes.
- It helps protect data even in the case of a system theft since the attacker cannot access the encrypted files
- Provides better offline protection for files and other sensitive documents. While online, the user needs to configure NTFS permission or use EFS.

Data Encryption Recommendations

The organization should consider encrypting important and sensitive data related to business information or “secrets” (intellectual property). It may include messages, financial reports, legal docs, patents, product releases, research and development data, etc. Data is protected from prying eyes even if the computer is stolen. You should consider encrypting sensitive information stored in following locations:

- C:\HOME directory.
- My Documents under C:\Documents and Settings.
- Local Settings under C:\Documents and Settings.

Data Encryption Recommendations:

- Utilize full-disk encryption on the drive to protect all your data.

- Encrypt a folder instead of individual files.
- Encrypt a folder that contains sensitive information.
- Use a strong password for encryption.
- Use third-party encryption tools to encrypt your sensitive data (if required)

Third-Party Data Encryption Tools

VeraCrypt

VeraCrypt is used for on-the-fly encryption (OTFE). It can create a virtual encrypted disk within a file or encrypt a partition. 7Zip 7-Zip is open-source software that performs encryption with high compression.

Cryptainer LE

Cryptainer LE can encrypt every kind of file format, whether it is textual, tabular, graphical, organized in a database, audio, or video. It also allows users to password-protect files and folders on CD ROMs, DVDs, etc.

AxCrypt

AxCrypt integrates seamlessly with Windows to compress, encrypt, decrypt, store, send, and work with individual files. Password-protect any number of files using strong encryption.

KeePass

KeePass supports the Advanced Encryption Standard (AES, Rijndael) and the Twofish algorithm to encrypt its password databases.

Steghide

Steghide is a steganography program, which hides bits of a data file in some of the least significant bits of another file in such a way that the existence of the data file is not visible and cannot be proven.

OpenPuff

OpenPuff securely encrypts and hides files inside of other files. It supports many file formats like images (BMP, JPG, PCX, PNG, TGA), audio support (AIFF, MP3, NEXT/SUN, WAV), video support (3GP, MP4, MPG, VOB), ad Flash-Adobe support (FLV, SWF, PDF).

Cryptoforge

CryptoForge is file encryption software for personal and professional data security. It allows protecting the privacy of sensitive files, folders, or email messages. After encrypting the information, one can store it on unsecure media or transmit it on an unsecure network—like the Internet—and still keep it secret. Later, it decrypts the information into its original form. Later, the information can be decrypted into its original form.

AutoKrypt

AutoKrypt is data encryption software designed for automation. It automatically encrypts or decrypts files and folders on a schedule.

EncryptOnClick

EncryptOnClick helps to encrypt and protect sensitive files.

Features:

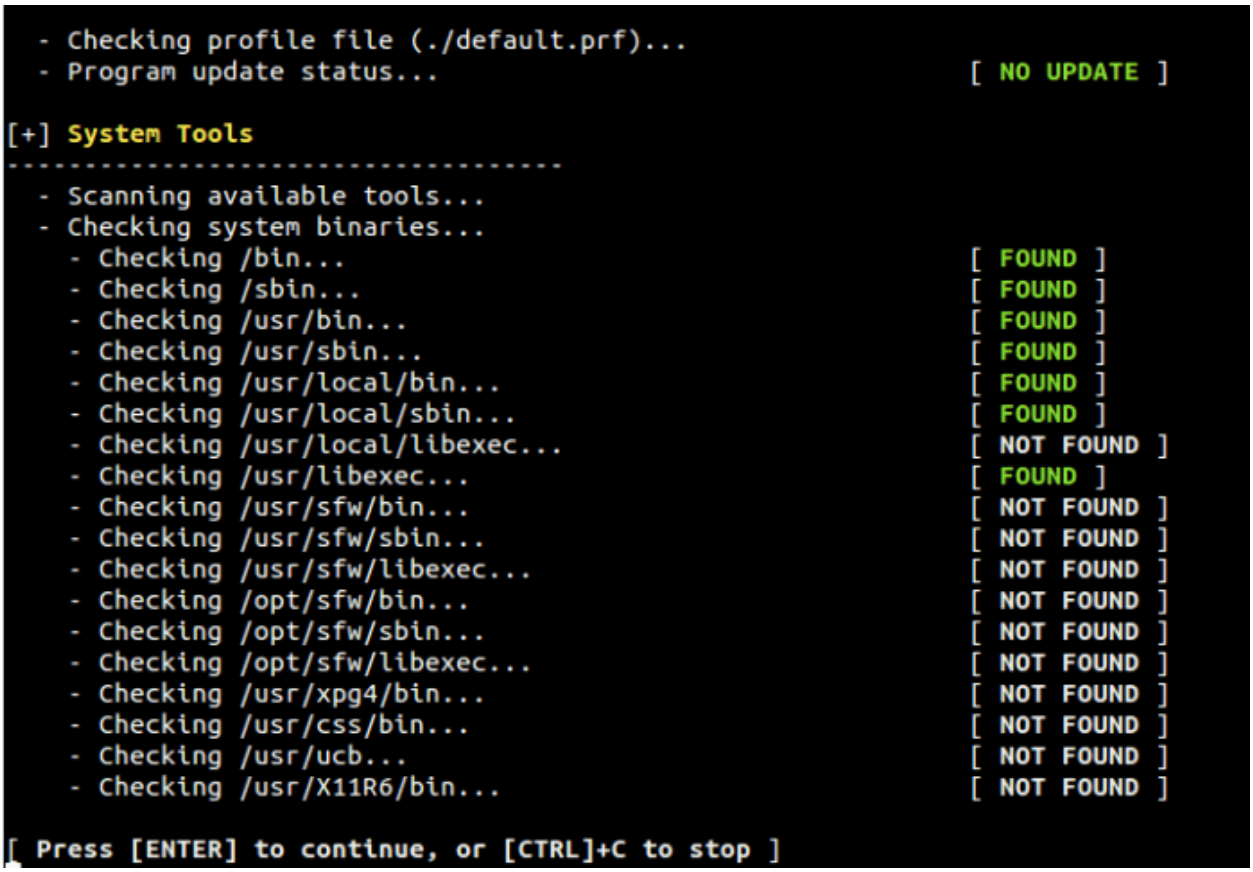
- Secure encryption and decryption method is used (256-bit AES encryption).
- Files are both compressed and encrypted, which results in a smaller file.
- Password protected.
- Encrypt single files or all files in a folder.
- Unicode-enabled so filenames in any language can be encrypted.
- Encrypt, decrypt, compress, and un-compress files, which can also be opened and decrypted using third-party programs like WinZip 9 (provided the correct password is used).

Linux Security

Linux Baseline Security Checker: Buck-Security

Buck-security allows you to get a quick overview of the security status of your system. It conducts a security check against the baseline

- Searching for world-writeable files
- Searching for world-writeable directories
- Searching for programs where the setuid is set
- Searching for programs where the setgid is set
- Checking your umask
- Checking if the sticky-bit is set for /tmp
- Searching for superusers
- Checking firewall policies
- Checking if sshd is secured
- Searching for listening services
- Creating and checking checksums of system programs
- Searching for installed attack tool packages



Buck-security is a security scanner for Debian and Ubuntu Linux. It runs a couple of important checks and helps you harden your Linux system. This enables you to quickly overview the security status of your Linux system. As a system administrator, you often get into situations where you have to take care of a server that has been maintained by other people. In this situation, it is useful to get an idea of the security status of the system immediately. Buck-security was designed exactly for this. It runs a few important checks and returns the results. It was designed to be extremely easy to install, use, and configure.

Password Management

The /etc/login.defs file defines the site-specific configuration for password management in Linux. The users in an organization need to ensure that the default password policy matches the organization's password policy. The "root" account is the most privileged account in Linux. The root account gives access to administrators to add accounts, change user passwords, audit and monitor log files, etc. The root account does not have any security features imposed on it. Administrators can easily perform their tasks with a root account. If an administrator wants to change the password on behalf of a user, they have to log into the root account. The user and group accounts can change their own passwords using the commands below:

An individual user can change their password using the command: **$ passwd**. This prompts the user to change the password by asking for the current and the new password.

An administrator can change the password for an individual user from his end using the command: **# passwd user name**. This prompts the admin to provide the new password.

The administrator can change the password of any group accounts by the command**: # passwd g group name.**

Change password for a user account

$ passwd

Output

- Changing the password
- (current) UNIX password:
- Enter new UNIX password:
- Retype new UNIX password:
- passwd: password updated successful

Change Group Password

When the -g option is used, the password for the named group is changed. **#passwd g marketing**

Using the above command will change the password of the users in the Marketing group.

With the help of /etc/login.defs, you can set common best practices for password management in Linux such as:

- Use strong “root” passwords
- Avoid using old passwords
- Always set a minimum password length
- Provide complex passwords
- Set an expiration period

Disabling Unnecessary Services

The user needs to be completely sure about the services running on their Linux system and they should be based on the organizational policy. Normally, installing an operating system installs many services and packages automatically. These packages will automatically be installed without the user’s knowledge. The installation of many unnecessary services creates security threats to hosts. The unnecessary services are not required or go against the organization security policy; as such, they should be disabled. Administrators should check if their Linux system is running unnecessary services and disable them periodically. The administrator can use the command # ps ax in order to view all the services running in a particular Linux system. This command

lists the active services running in the system along with their product ID (PID). They can then compare the services running on a host with an organization's policy and disable any unwanted services.

Killing Unnecessary Processes

The kill command is usually used in order to terminate any services in Linux. This allows the service to run without a reboot after killing a service. There are many ways to execute the kill command. The kill command is generally represented using:

 # kill [signal or option] PID (s)

It is mandatory to know the PID before running the kill command. Type the command **# ps A** in order to know the PIDs for all the processes running in the system. After knowing the PID for a particular service, type the command for killing a service.

For example, in order to achieve the PID for the service cupsd, type the command:

#ps ax | grep cupsd

Linux Patch Management

In Linux, the patch updates are applied to software components such as a kernel or services. The patches help you remove any existing vulnerabilities, look into security problems, and include the latest features. Administrators are required to test the patches before installing them on a host machine. Testing the upgraded software helps verify the upgraded software is correct.

Some Linux distributions can be configured to warn you when patches for installed software are available. Security fixes are the most important patches that resolve system security issues. Once the security threat is revealed, Linux distributes its security patches in hours. Administrators should keep themselves up to date while handling Linux security issues. An easy way to receive all the updates is to constantly subscribe for updates from the vendors. The updates should be for kernels, inetd, and for certain services.

- Linux systems can have a command-line or a graphic software tool.
- Most of the updates can be located on the distribution's website.
- The admin can download and install updates using third-party applications.

The Red Hat Linux distribution provides a patch management system solution through two tools:

1. **Red Hat Network (RHN)**: To get the benefits of patches available in RHN, organizations are required to purchase its license. The web resource can be configured on host machines. It provides information on the current available patches for Linux. Users can have custom or free services from the online resource. For routine awareness of patch releases, administrators are advised to setup a Java-based program called the RHN Alert Notification Tool. When a new update is released, it notifies the administrator through a change in its icon.

2. **RPM Package Manager**: The functioning of RPM is similar to RHN; however, it does not provide detailed information about every patch available. RPM provides a list of available patches through a user interface. The functioning of RPM is operated by the command rpm. When an important patch is set to necessary, RPM downloads the patch on the system.

Understanding and Checking Linux File Permissions

Access control through file permissions is useful to control unauthorized access to system resources. An individual user, group of users, or all the users of the system can have access to certain directories and files if they have the permissions to access them.

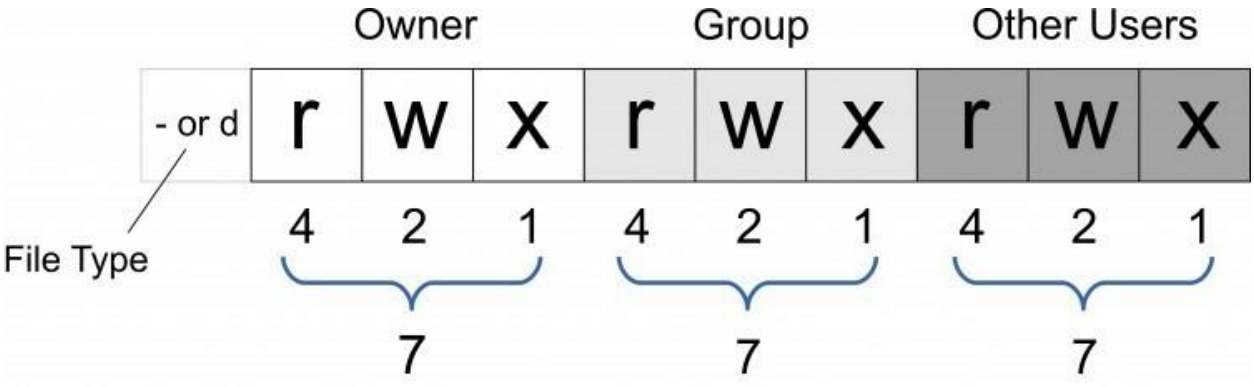
Each file and directory has three user-based permission groups:

- **Owner**: Applies only to the owner of the files or directories.
- **Group**: Applies to the group using the files and directories.
- **All users**: Applies to all the users in the system.

Permission Types

Each file or directory has three types of basic permissions:

- **Read**: Users can only read the contents of the files or directories.
- **Write**: Users can only write or modify the changes of the files or directories.
- **Execute**: Users can execute the files or directories to view its contents. The execute permission affects a user's capability to execute a file or view the contents of a directory.



User Rights/Permissions

The permission in the command line can be written as: _rwxrwxrwx

1 owner:group 1. The first three characters (rwx) are for the Owner permissions.

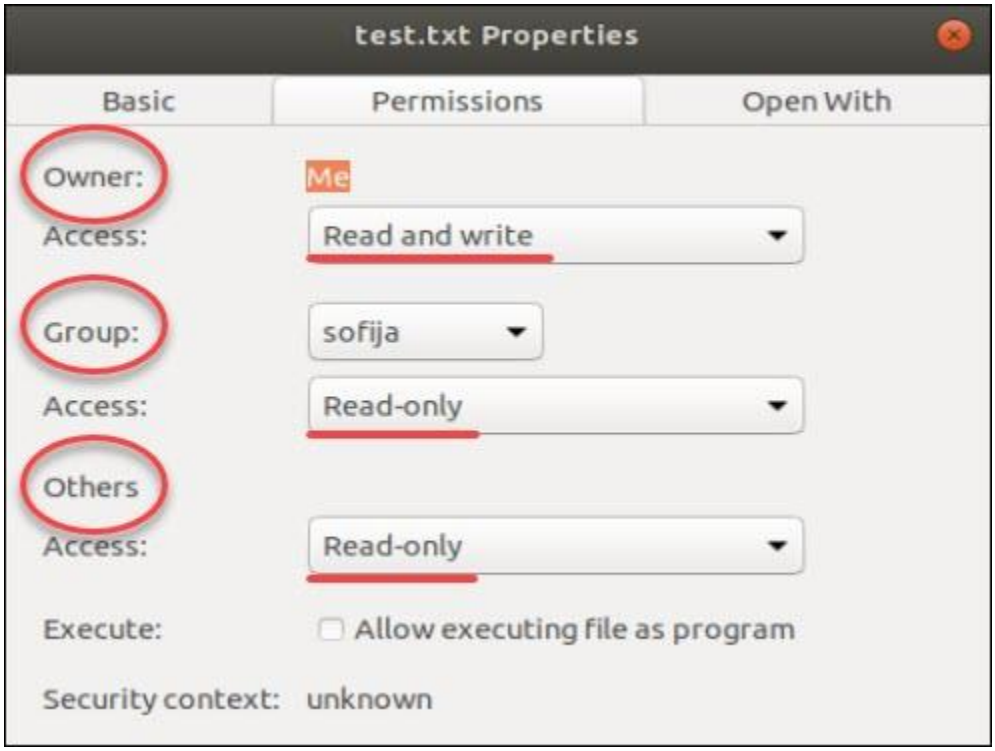
2. The next three characters (rwx) are for the Group permissions.

3. The next three characters (rwx) are for the All Users permissions.

4. The number in the command represents the hard links of the file.

5. The Owner and Group assignment formatted as Owner: Group

Check and Verify Permissions for Sensitive Files and Directories



Host-Based Firewall Protection with IPtables

IPtables are command-line firewall utilities that can allow or deny traffic. IPtables are preinstalled in a Linux system. In order to update or install IPtables, the user needs to regain the IPtables package using the command: **sudo apt-get install iptables**

Every packet traversing through the filter system is assigned to an appropriate table depending on the tasks performed by the packet. The table contains chains that display the details of the destination of the packet. The tables can be used to create rules and the user has the ability to create their own chains and link them from the built-in chains. This facilitates the ability to create complex rules. However, the user needs to be extra alert while using the IPtables commands as any small error in the command can lock the system and would require the user to fix the error manually.

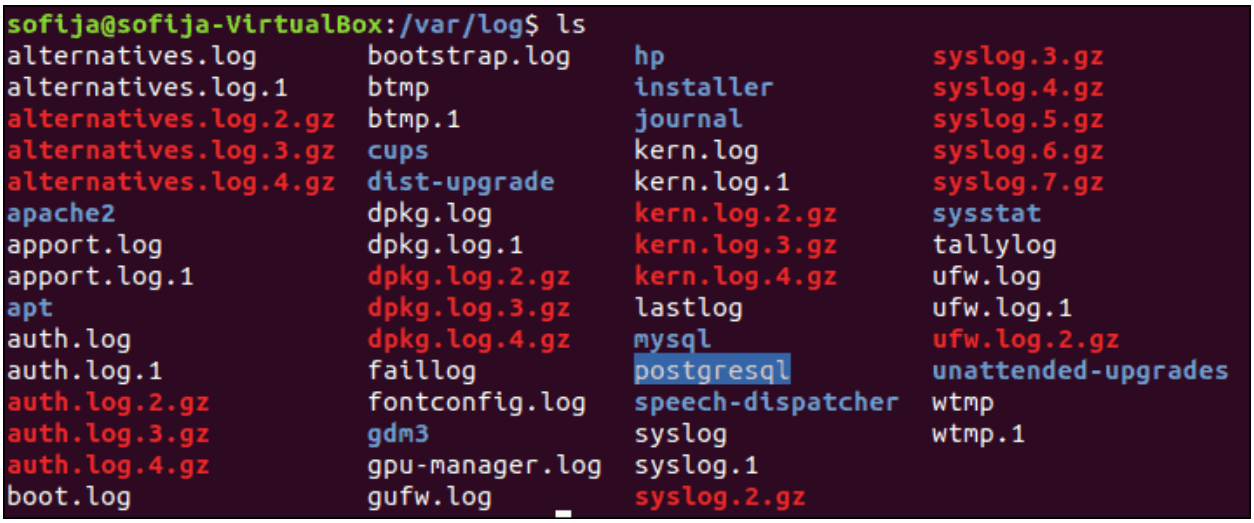
There are three different types of chains:

- **Input**: The input chain verifies the incoming connections and its behavior. The IPtables compares the IP address and port of the incoming connection to a rule in the chain.
- **Forward**: The forward chain mainly forwards the incoming connections to its destination. The command iptables L v verifies whether an incoming connection needs a forward chain

- **Output**: The output chain is used for output connections, wherein the chain checks for the output chain and decides whether to allow or deny the output request.

Log Review and Audit

Various types of Linux OS and core applications logs are stored under /var/log directory.



Few things to be considered while conducting a log review and audit

- Find the log sources and tools required for performing an audit.
- Keep log records at a single location for easy access.
- Verify whether the user can safely rely on the time stamps due to different time zones.
- Analyze all system changes, updates, and errors occurring in the system.
- Check all incidents in a system.
- Comparison of logs provide an overall picture of the status of the system.
- Get all details regarding a log (like the reason for that system event).

System Log Viewer

Most log files are in plain-text format. You can view these log files using any text editor. However, some log files are not readable in a human format when opening with a text editor.

The System Log Viewer is a graphical, menu-driven viewer that facilitates the viewing and monitoring of the system logs. It comes with a few functions that can help you manage your logs, including a log monitor and log statistics display. It allows you to view system log files in an interactive, real-time application.

Log File Viewer is useful if you are new to system administration because it provides an easier, more user-friendly display of your logs than a text display of the log file. It is also useful for more experienced administrators, as it contains a monitor to enable you to continuously monitor crucial logs.

Note: Log File Viewer is useful only to those who have access to the system log files, which generally requires root access.

Hardening Servers

Server hardening refers to the increased level of security provided in order for the servers to operate in a more secured environment. Hardening a server involves applying all the system security measures with some server-specific security measures depending upon the type of service it provides.

Before Hardening Servers

Administrators should consider the following points before hardening the servers:

1. Identify the network service that a server is providing.
2. Identify the network service software installed.
3. Identify its users.
4. Determine the user privileges required.
5. Plan for server authentication and authorization.
6. Determine the access control strategies and measures for the server.

Administrators use various methods and tools for hardening the server. Hardening involves securing the key components of the IT architecture to reduce the risks of attack

The three main components that require hardening are:

1. **Operating System**: The hardening of an operating system involves securing the system so it is configured to limit the possibilities of internal or external attacks. The methods for hardening may vary depending on the operating system used.

2. **Network**: Administrators can perform network-hardening activities by using security protocol standards. Administrators can customize and maintain the network policies as per the organization's requirement. Administrators should regularly review the network logs and audit them. Network devices that are not operational should be removed from the network.

3. **Applications**: Every application and service installed on the network should undergo the hardening process. This ensures that any loopholes present in the applications and services are protected against attacks. A number of common operating system-based services are installed by default and need to be reviewed.

Hardening a Webserver

The webserver is a client-server architecture that enables service requests through the HTTP protocol. Proper authentication and firewall techniques enhance the security features for sites that do not require public or external access. The Secure Sockets Layer ensures security for web-based transactions. Proper analysis of the webserver logs ensures it is secure and checks for any unusual behavior. Any attempts to access suspicious webpages have the potential to exploit the security of the webserver. Administrators should ensure that webservers are updated with the latest patches

Hardening of Webservers Can Reduce

- Attacks into your own network
- Attacks into some other network

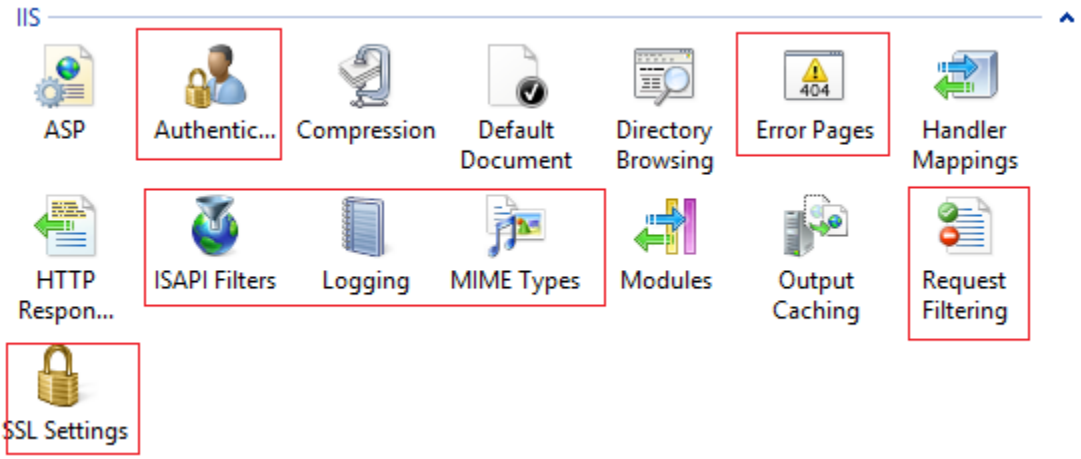
General Guidelines for Webserver Security

- Install servers securely
- Configure appropriate access controls
- Properly organize the webserver software and webserver host OS
- Secure all webserver content
- Uphold the reliability of the webserver
- Configure authentication and encryption
- Use file integrity checkers
- Enable logging
- Develop a backup plan for the webserver
- Establish a secure network for a webserver

Webserver Hardening Techniques

- Place the webserver at an isolated location: This is because any external access to the webservers could enable them to access internal hosts allowing them to capture and monitor the traffic between the internal hosts. In addition, it facilitates better management of the servers to prevent attacks.

- Place the supporting servers on other isolated subnets: This allows for the passage of allowed traffic only between the webserver and that particular server. For example, only the SQL protocol is permitted between a SQL server and the webserver.
- Disable source routing and IP forwarding on the router: Enabling source routing and IP forwarding can lead to MITM attacks and IP spoofing on a webserver.
- Place firewalls with the servers.



Use appropriate access control: Controls the access to the webserver software. Access controls should be applied to:

- Sever log files
- System configuration and software files
- Application software and configuration files
- Password files

Recognize the level of protection required: Only authorized administrators can read or write webserver log files. Some temporary files are restricted and are stored in subdirectories. Only those services that created the file have the permission to access those subdirectories and files.

Enable logging: Proper logging of the webserver files helps locate any irregular activities in the server. The following types of logging help monitor webserver logs:

- Transfer logging
- Error logging
- Agent logging
- Referrer logging

Proper authentication and encryption mechanisms: Find methods to overcome the use of address-based authentication and HTTP basic authentication.

Keep a copy of the website content on a secure host: Create strategies for transferring website content to a secure location as a backup. In addition, it helps increase the security mechanisms for this content.

Hardening an Email Server: Recommendations

An organization requires electronic mail (email) systems (Email Server) for business or simple exchange of information between people. These email servers, if not configured properly, can be compromised and used for a malicious purpose. An important thing about the hardening of an email server is to disable the unwanted configuration options in the server software. A perfect method to increase the security of the server is to allow only authorized users access to the email.

Email Sever Security Guidelines:

- Configure the mail relay format properly to prevent attackers from using the mail server as a gateway.
- Configure the SMTP authentication method. This requires users to access the SMTP server and provide username and password credentials before sending an email.
- Restrict the number of users that can access the SMTP server. This minimizes the chances of any DoS attacks on the network.
- Enable DNS lookup to verify the existence of the sender's email domain. This helps restrict any mail from unknown senders.
- Enable the Sender Policy Framework in order to restrict spoofed sender addresses.
- Activate SURBL (Spam URI Real-Time Block Lists) in order to identify any unwanted links and messages in an email.
- Keep track of the spammers who always send spam emails. This can limit unwanted Internet connections on the email system. Use POP3 and IMAP for authentication purposes.

Hardening FTP Servers: Recommendations

Administrators should implement the following security measures while configuring the FTP service:

Inactivate unidentified FTP accounts: Installing FTP services automatically enables anonymous access to FTP servers by any user. The users do not need any authentication to use the account. Disabling this anonymous access will minimize unauthorized users accessing the FTP server and placing illegal and dangerous files on your sites. This enables only authorized users to access the FTP server.

Enable logging for your FTP site: Keeping track of the FTP logs can help in identifying the users accessing the site and the IP addresses they use. Logs provide a detailed description on the status of the site and validates if there are any attacks or threats.

Configure access controls on authenticated FTP accounts with the help of ACLs: Access control lists limit unauthorized access to the FTP directory using NTFS permissions. However, users permitted to the FTP directory should not include everyone

in one group, as it changes the configuration for those users who are limited to accessing FTP accounts.

Restrict access by IP or domain name: Limiting access to FTP to only a certain number of users reduces attacks from unauthorized users.

Restrict logon attempts and time: Users access the FTP site within a specified logon time. FTP denies permission to any user attempting to access the FTP site after the logon time has expired. With this restriction, only those users who are authorized for a specific time period have access.

Configure filtering rules for your FTP service: The filtering rules check for each FTP request. If it matches the filtering rules, that particular request is allowed; or if it doesn't match a filtering rule, it is declined.

Use SSL/FTPS for authenticated FTP accounts: This represents the SSL settings for the FTP service. Increasing the security of the FTP service can allow only authorized users to access the FTP accounts.

Hardening Routers: Recommendations

The following are recommended best practices for enhancing the security of a router:

- **Changing the default password**: Most users do not change the default password of the router after installation. This is the same thing as giving a key to attackers so they can easily log into your router.
- **Deactivate IP-directed broadcasts**: Enabling IP-directed broadcasts will allow attackers to send ICMP ECHO requests to another user broadcast address (using a spoofed address). The broadcast network responds to the ECHO request, thereby affecting the working of all hosts in the network.
- **Deactivate the HTTP configuration**: Enabling the HTTP protocol for routers sends clear-text traffic.
- **Restrict ICMP Ping requests**: Accepting PING requests enables attackers to guess the active hosts and scan the network without the original user's knowledge.
- **Disable IP source routing**: Enabling this routing feature allows attackers to identify the path taken by the packet. These give users the ability to sniff packets from the network.
- **Identify the need for packet filtering**: Filtering of packets depends on the needs of the organization. The filtering mechanism helps identify whether to permit or block traffic.
- **Creating ingress and egress address filtering policies**: Creating policies for verifying the inbound and outbound traffic based on an IP address increases the security of the router.
- **Physical security of the router**: It is mandatory to maintain physical security of the router because inappropriate placement of routers allow attackers to sniff and have direct access to the appliance.
- **Review the security logs**: Appropriate review of the security logs will provide detailed information regarding what attacks, if any, have been launched against

the router. It also provides a detailed description of the router. Reviewing the logs of the router provides an overall idea regarding the status of the network, too.

In addition to the above recommendations, implement the following best practices to harden your router security:

- Disable unnecessary router interfaces.
- Disable unnecessary services.
- Disable unnecessary management protocols.
- Disable ARP and proxy ARP.

Hardening Switches

The best way to confirm switch security is by using port-level security. Port-level security limits the number of MAC addresses connected to a device. The three different methods of connecting MAC addresses to a port are as follows:

- **Statically**: Allows only a single MAC address to be connected to a port.
- **Dynamically**: These are present by default in the content-addressable memory.
- **Sticky**: A MAC address given to a specific port. This MAC address can be lost if not saved during reboot.

Additional switch security best practices:

- Create a strong password.
- Create time-out sessions and user access rights.
- Disable auto-trunking on ports and activate port security for MAC addresses in order to control access.
- Deactivate all ports that are not in use and assign them an unused VLAN number.
- Control the number of VLANs that can pass over a trunk.
- Maximize the use of access control lists.
- Review all security logs of the switch
- Implement AAA for local and remote access to the switch.
- Keep the switch configuration file offline and control access to it.

Logs Review and Audit: Syslog

Syslog enables network devices to record event messages to the logging server or the syslog server. It is possible to log many events and the syslog protocol can handle many different devices. Normally, Windows-based servers do not support syslog. However, there are many third-party tools available that can actually gather the Windows server log information and then forward it to the syslog server.

Database: Syslog servers create a database in order to store log data from large networks.

Management and Filtering Software: The management and filtering software helps filter data from the database. At times, network administrators find it difficult to find

the log details from the database. The use of this software can actually enable the administrators to filter the required data.

Syslog Messages: Syslog messages include all the information like the IP address, timestamp, and the actual log message. The syslog uses a method called facility that identifies the source of message on any machine. The syslog message also has a severity level field that determines the severity level. A severity level of '0' signifies that the message is an emergency. The severity level of '1' signifies that the messages need immediate action. The syslog messages severity can go up in range.

Limitations of a syslog server:

- The syslog protocol actually does not provide any specific method for formatting messages, which causes issues concerning the consistency of the messages.
- Syslog uses UDP as a protocol for the transport of messages. As UDP is connectionless oriented, there are chances for a syslog server to lose packets.
- There is no method for authenticating the syslog messages. It can actually provide access to another machine and send fake log events.

Application Security Recommendations

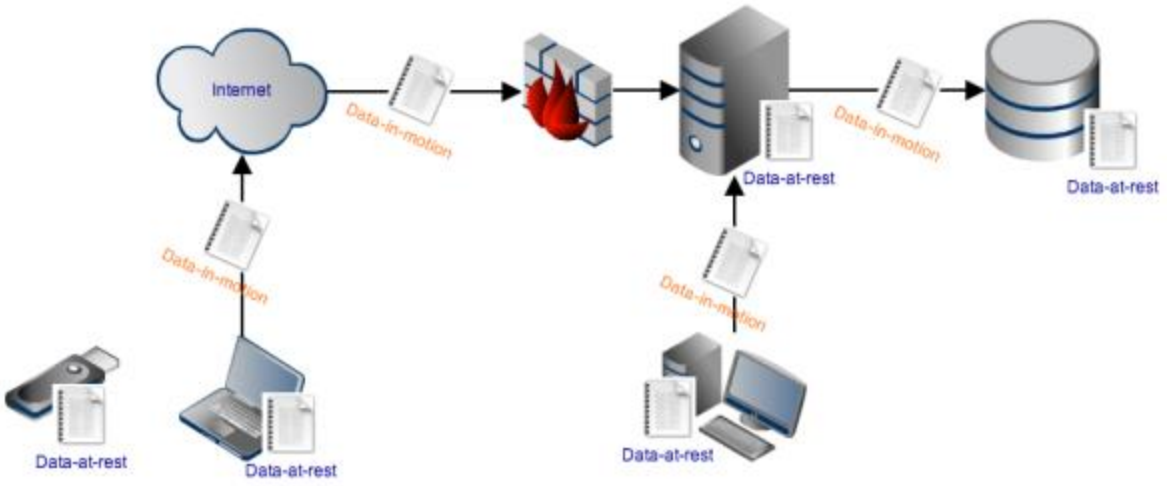
- Assess security features of software before purchasing any software
- Use centralized management of critical software
- Monitor software use
- Ensure only authorized personnel can install software on the system
- Train staff on software use and security policies

Data Security

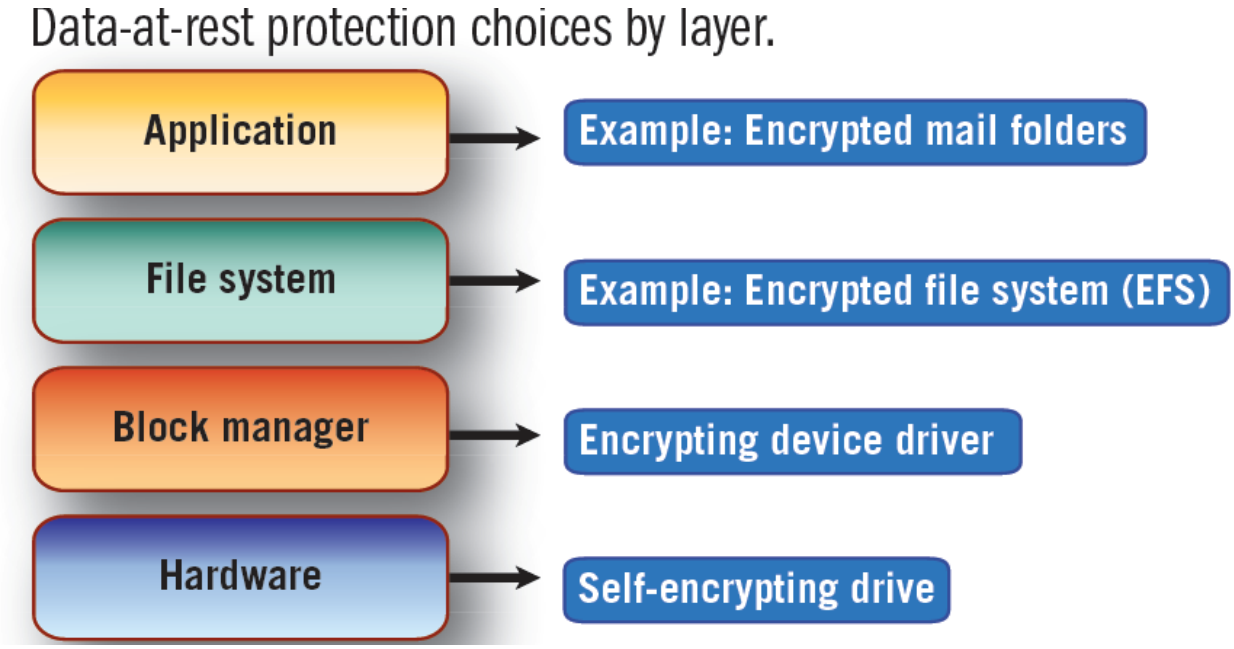
Data security is the main concern for many organizations, regardless of their size. Data security ensures protective measures are applied to computers, databases, and websites. A few examples of data security are hardware/software encryption, data backup, and data masking. Organizations should ensure various levels of business data security.

Data Security at Rest

Data at rest refers to inactive data stored in digital form at a physical location. It includes archived or reference data that never changes. It does not include data moving through the network. Data at rest encryption protects the data using encryption. The process of encryption preserves or protects the data stored in a particular location.

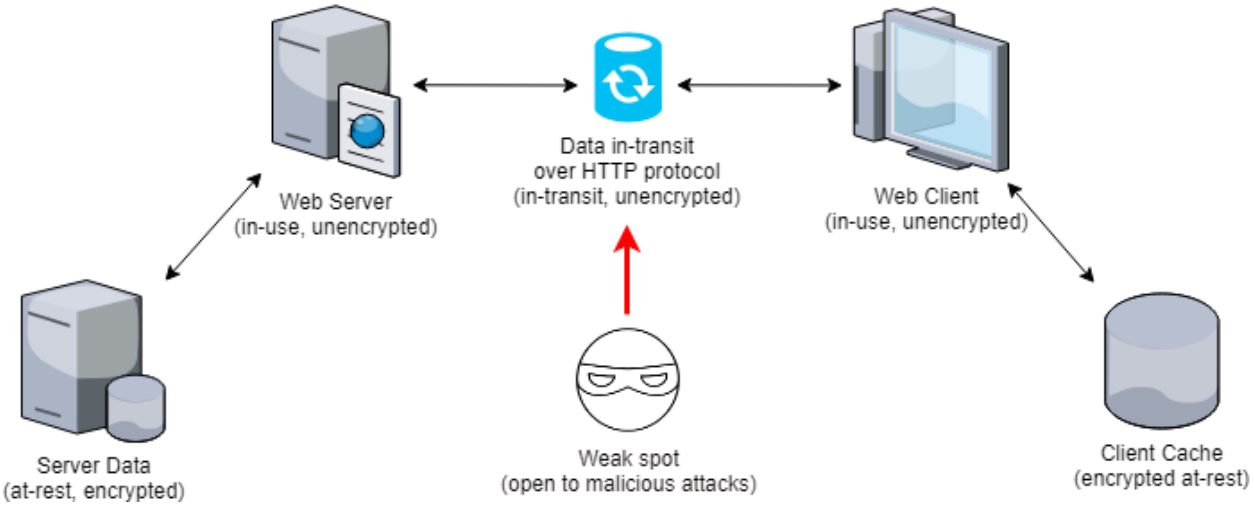


Organizations can completely depend on an encryption process for their data security. The process of encryption applies to both structured and unstructured data. Network administrators need to constantly check the encryption mechanisms used for protecting data. The encryption of data at rest includes encryption methods such as AES and RSA. The data needs to be encrypted even if access controls fail. Keep the encryption keys at a separate location and make sure the keys are updated constantly. A data federation is another method used for protecting data at rest from unauthorized access.



Data Security in Transit

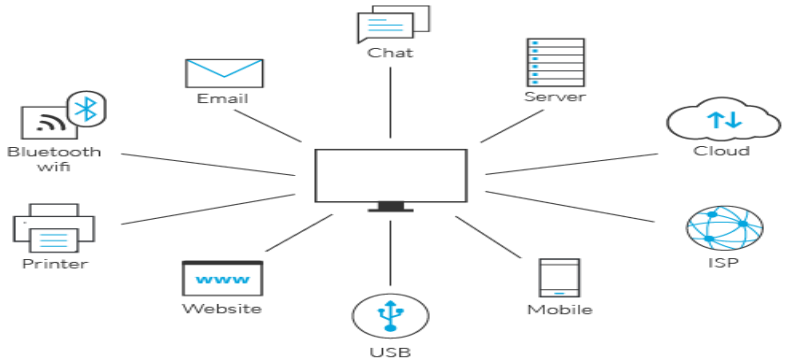
Data in transit can traverse the network and this gives attackers additional access opportunities to the data. Organizations can protect their confidential data using two types of encryption mechanisms: SSL and TLS.



SSH replaces TELNET and SFTP replaces FTP. Any protocols using SSL/TLS use certificates to exchange public keys and public keys to exchange private keys. Similarly, a session key uses asymmetric encryption and a certificate for exchange. Symmetric encryption uses the same session key for secure, fast encryption and decryption. Network traffic authentication requires encryption for data in transit. Encryption is not a mandatory mechanism for a public-facing website. However, encryption can play a role if the organization wants users to logon before accessing their webpages. This protects the privacy and data of the user.

Data Loss Prevention (DLP)

To confirm users do not send or use sensitive data outside the organization, enable DLP. DLP controls what data users can send through the network. DLP uses different rules to classify what data is critical and sensitive in an organization.

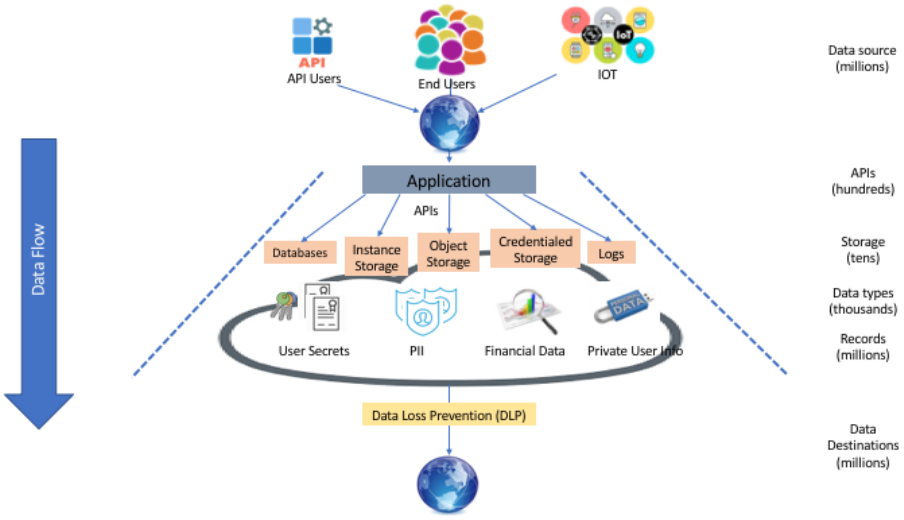


Data loss prevention (DLP) does not allow users to send confidential corporate data outside the organization. The term is used to describe software products that help a network administrator control what data end users can transfer. DLP rules block the transfer of any confidential information across external networks. This controls any unauthorized access to company information and prevents anyone from sending malicious programs to the organization.

Implement DLP software according to the organizational rules set by management. This prevents accidental/malicious data leaks and loss. If an employee tries to forward or

even upload company data on cloud storage (or even on a blog), the action will be denied by the system. Management adopts a DLP policy when internal threats to a company are detected. Data loss prevention is a policy to ensure that none of its employees sends sensitive information outside the organization.

New emerging DLP tools not only prevent the loss of data, but also monitor and control irregular activities from occurring on the system.



There are DLP products available that help administrators determine what data users transfer. DLP products are also known as data leak prevention, information loss prevention, or extrusion prevention products. DLP is a strategy used by organizations to:

- Discover sources of data leaks
- Monitor those data leakage sources
- Protect organization assets and resources
- Prevent accidental disclosure of information to unintended parties
- Manage resources with business rules, security policies, and software

Data Loss Prevention Best Practices

Data loss prevention best practices are:

- Identify the business need for implementing a DLP solution in an organization.
- Ensure the DLP solution supports various data formats.
- Determine the type of DLP required based on the type of data protection needed.
- Always pay close attention while deploying a DLP, as any small mistake in the implementation will affect data protection.
- DLP should be able to mitigate any false positives.
- Perform regular risk profile updates, as an organization needs to ensure DLP incidents are documented.

- Provide security policy training to employees.

DLP Solution Vendors Symantec

Symantec DLP keeps track, secures your confidential data, and ensures its safety, wherever it lives in the cloud, on premises, or on mobile devices. It helps you keep data safe on Windows and Mac endpoints by performing local scanning and real-time monitoring. It monitors confidential data that is being downloaded, copied, or transmitted to or from laptops and desktops (through email or cloud storage). It uses a single web-based console to define data loss policies, review and remediate incidents, and perform system administration across all of your endpoints, mobile devices, cloud-based services, and on-premise network and storage systems.

Websense

Websense Data Security Suite contains three modules: Data Security Gateway, Data Discover, and Data Endpoint. It provides a single intuitive, web-based interface for management and reporting of Websense web, email, and data security solutions.

Trustwave

Trustwave Data Loss Prevention helps enterprises discover, monitor, and secure data at rest, in motion, and in use to prevent exfiltration and ensure regulatory compliance. It analyzes all web-based communication and attachments, including email, instant messenger, P2P file sharing, blogs, social media, FTP, and Telnet for violations of an organization's governance, compliance, and acceptable use policies. Automatically blocks HTTP, HTTPS, and FTP traffic violating compliance policies. It can investigate data at rest to find and protect sensitive information residing in the stored data. Discovery of sensitive data allows security teams to focus their initiatives on specific users and systems, and then implement the appropriate measures to meet compliance requirements.

Blue Coat

Blue Coat Data Loss Prevention (DLP) enables you to detect and block potential data leaks quickly and accurately, all while achieving industry and regulatory compliance. With Blue Coat DLP, you can leverage powerful discovery capabilities to prevent sensitive, unsecured data from traveling across the network and winding up in the wrong hands.

Code Green Network's TrueDLP

Code Green Networks' TrueDLPTM solution is comprised of Network DLP, Discovery DLP, and Cloud DLP and locates sensitive data resting on databases and network servers, including data in the cloud.

McAfee

McAfee Total Protection for Data Loss Prevention (DLP) safeguards intellectual property and ensures compliance by protecting sensitive data wherever it lives on premises, in the cloud, or at the endpoints. McAfee Total Protection for DLP is delivered through

physical or virtual low-maintenance appliances and the McAfee ePolicy Orchestrator platform for streamlined deployment, management, updates, and reports. Palisade Systems Palisade DLP provides a simple, all-in-one, cost-effective approach to data loss prevention (DLP), which enables organizations to: Monitor: Palisade monitors all traffic and data leaving the network, making you aware of what is happening with your most critical data.

- **Analyze**: Palisade inspects and analyzes documents for protected/confidential data to discover where sensitive data resides in use, in motion, or at rest.
- **Prevent**: Palisade prevents data loss using DLP enforcement, protocol management, web filtering, and enforcing data protection policies to ensure secure treatment of data and proper adherence to company protocols.

Digital Guardian DLP

Digital Guardian DLP provides visibility and audit reporting of potentially unsecured data. It uses patent-pending Database Record MatchingTM detection to accurately locate and identify sensitive data at rest on endpoints and servers across your networks and cloud storage. Automatic, configurable scanning of local and network shares using discovery-specific inspection policies ensures sensitive content is discovered wherever it is located. Detailed audit logging and reports provide you with the information needed to demonstrate compliance, protect confidential information, and reduce data loss risk.

PixAlert

Data Leakage Prevention (DLP) programs will effectively secure critical and sensitive data by discovering & identifying data at rest that needs to be protected. It helps networks discover and manage where critical data is located, monitoring and protecting networks and employees against dissemination and leakage of unsecure data.

Safend

The Wave Data Protection Suite goes wherever your devices go, on or off your network, online or offline. Which means it protects your data from the full range of modern risks: device theft, emails, flash drives, portable hot spots, hardware keyloggers, etc.

Virtualization Terminologies The following are the virtualization technologies:

- **Host Operating System**: A Host Operating System is the OS installed physically on the computer hardware that seeks direct access to the hardware resources for computations. Resources it can access include processor, memory, storage media, etc.
- **Guest Operating System**: This is the operating system installed virtually on a host operating system. It is dependent on the host operating system for computations and resource allocations.
- **Hypervisor or Virtual Machine Manager (VMM):** An application or firmware allows multiple guest operating systems to share a host's hardware resources. It acts as middleware that allows the user to install a virtual operating system called 'Guest OS' on the 'Host OS.'

- **Execution Environments**: It is the logical entity environment (Software/Hardware) that enables execution of programming code/software. JVM (Java Virtual Machine) is the best example, which acts as an execution environment for JAVA programs.
- **Service Levels**: A service level is a signed contract between the cloud provider and the cloud customer that lists all the services offered by the cloud provider to the customer. It also includes the terms and conditions between the two parties.

Introduction to Virtualization

Virtualization offers computing, storage, and networking hardware. Virtualization refers to the separation of the services or requests from the physical processes. The mechanism of virtualization has enabled IT managers to group resources across the enterprise, providing better management of those resources.

Before Virtualization: The hardware infrastructure (host machine) runs a single operating system with all its applications.

Different types of virtualization techniques are:

1. **Full Virtualization**: The guest OS is not aware that it is running in a virtualized environment. It sends commands to the Virtual Machine Manager (VMM) to interact with the computer hardware. The VMM then translates the command to binary instructions and forwards it to the host OS. The resources are allocated to the guest OS through the VMM.

2. **OS-Assisted Virtualization or Para Virtualization**: In this type of virtualization, the guest OS is aware of the virtual environment in which it is running and communicates with the host machines by requesting for the resources. The commands are translated into binary code for the computer hardware. The VMM is not involved in the request and response operations.

3. **Hardware-Assisted Virtualization**: Modern microprocessor architecture has special instructions to aid the virtualization of hardware. These instructions allow the guest to execute privileged instructions directly on the processer. The operating system makes the system calls behave like a user program.

4. **Hybrid Virtualization**: In this type of virtualization, the guest OS uses the functionality of Para Virtualization and uses the Virtual Machine Manager (VMM) for binary translation to different types of hardware resources.

While designing a virtual environment, the levels involved in the application are:

- **Storage Device Virtualization:** This is the virtualization applied on storage devices such as data striping and data mirroring. RAID is a good example of storage virtualization.
- **File System Virtualization**: This type of virtualization provides complete virtualization to the data for sharing and protection within the software at this level. Virtualized data pools manipulate the files and the data based on user demand.

- **Server Virtualization**: Server-level virtualization enables management to partition or virtualize the server's operating system environment. Logical partitioning of the server's hard drive is involved in the server virtualization.
- **Fabric Virtualization**: This level of virtualization makes the virtual devices independent of the physical computer hardware. It creates a massive pool of storage areas for different virtual machines running on the hardware. Virtualization uses Storage Area Network (SAN) technology to perform fabric-level virtualization.

Characteristics of Virtualization

Virtualization has the following characteristics:

Partitioning: It is the ability to run multiple operating system instances with their applications on a single physical system by virtually partitioning the hardware resources; the resources are allocated to handle host and guest requests.

Isolation: Each virtual machine is isolated from its host physical system and other virtual machines. This characteristic of virtualization prevents the effects of actions performed by one virtual machine from affecting the other machines.

Encapsulation: A virtual machine represents a single file used for identification based on its services. Encapsulation protects a virtual machine from interference from the other virtual machines.

Benefits of Virtualization

Virtualization provides:

- **A cost-effective solution for the central data hub:** Replacing the physical hardware with virtual machines can actually cut down the cost of purchasing more hardware, increasing the space in the server room. Too many servers can emit a lot of heat, which could lead to a server crash.
- **A time-efficient option for the IT infrastructure**: The use of virtual machines can reduce the time it takes for installing computer components in an organization. The concept of virtualization enables the network administrator to perform tests on the software without consuming time and resources.
- **Back up the Servers**: Virtualization ensures the complete restoration of the network at a faster rate. The use of virtual machines reduces the time it takes the physical hardware to recover.

The virtualization process enables users in an organization to use different platforms in a single machine according to their needs. It provides continuous transition from one operating system to another in the same machine.

The following are the benefits of virtualization technology:

- Centralized storage in virtual machines prevents the loss of data.
- If the virtual machines are remote, then only one application present in one VM is attacked.

- The VM allows secure sharing of sensitive information.
- An attacked VM can be rolled back to a state prior to the attack.
- Virtualization improves the physical security due to the presence of a few physical devices and a few data centers.
- Provides better event incident handling

Common Virtualization Vendors

VMware

VMware virtualizes computing, from the data center to the cloud to mobile devices, to help customers be more agile, responsive, and profitable. It offers services such as:

- **VMware vCloud Suite**: vCloud Suite is a complete kit used for developing and managing a private cloud infrastructure effectively.
- **VMware vSphere**: VSphere virtualization enables the creation of a cloud infrastructure and virtually collaborates all the server-related resources.
- **Horizon View**: Horizon view is a virtual desktop service that offers remote access to different resources available to the users under a common platform.
- **VMware Fusion**: Fusion enables Mac users to run Windows-based applications without compatibility issues.
- **VMware Workstation**: Workstation enables the user to run multiple virtual machines from a single desktop.
- **VMware VCenter Operations Management Suite**: The operations management suite efficiently manages all the services for their user and ensures quality service.

Citrix

Citrix securely delivers Windows, Linux, web, and SaaS apps (plus full virtual desktops) to any device. Citrix solutions for applications and desktop virtualization can help your business increase productivity, enhance security, and reduce costs.

ORACLE

Oracle offers the virtualization, from desktop to the data center. Oracle virtualization enables you to virtualize and manage your full hardware and software stack. Oracle provides virtualization applications and tools for:

Server Virtualization: Server Virtualization enables the IT of an enterprise to effectively handle its server infrastructure such as memory, CPU, and storage devices. The server handles multiple client requests simultaneously by logically partitioning and isolating its resources.

Desktop Virtualization: Desktop virtualization uses hypervisors that run on a bare-metal server (i.e. physical hardware). It provides the flexibility to install several virtual machines and run them along with the host operating system.

Virtualization Security and Concerns

A virtualized environment facilitates the detection of new attack exposures, thereby forcing the user to take protective measures for both hosts and the virtual machines. In a non-virtualized environment, each host is separately held, consisting of separate services and webservers. The services run in their own spaces and they connect directly to the network. In a virtualized environment, several guest hosts are placed in a single host. Here, all the services are grouped together, thereby increasing the chances of vulnerabilities in the system. Virtualization Security Concerns There are different issues and challenges while implementing and using virtualization. Two major challenges are:

1. Traditional threats

2. New threats

Traditional threats to the virtual environment include:

- Malicious code in virtual machines and appliances.
- Errors while configuring virtual network and firewalls.
- Hypervisor configuration liabilities.
- Data leakage.

New threats to the VM environments are:

- Management console vulnerability allows the attacker to remotely control the virtual machines using the management consoles.
- A vulnerable hypervisor can act as a danger to both the host as well as virtual machines.
- Poor hypervisor design makes the whole system vulnerable to attacks.

Steps to encrypt a virtual machine:

- Step 1: Shut down your virtual machine
- Step 2: Go to configure from the virtual machine menu and a dialogue box appears
- Step 3: Click options and select security
- Step 4: In the security pane, click turn on and provide a password and click OK
- Step 5: The password provided in step 4 will be used for encrypting/decrypting the virtual machines

Secure Virtual Network Management

Approaches for secure virtual network management include:

- **Physical Network Security Device (PNSD):** This physical network security device resides outside the host machine and deploying it for every host machine may reduce performance. This approach does not provide security to VMs
- **Physical Network Security Device (PNSD) with VLANs**: Use physical network security devices (PNSD) with VLANs; it reduces the consumption of host resources.
- **Host Intrusion Prevention System (HIPS)**: It resides inside the virtual server, uses host machine resources, and offers server-level protection.

- **Virtualized Network Security System (VNSS):** It resides on a virtual LAN and consumes the host machine's resources. It monitors, partitions the virtual environments, and provides security to virtual network segments, VLANs, servers, and devices

Methods to secure virtual environments include:

- **Resource Limitation**: Apply resource usage limits to each virtual machine so that it minimizes the risk of using multiple shared hardware resources at one time, which can affect performance of the virtual machine.
- **Security Measures**: Install antivirus, spyware, and intrusion detection systems. Keep everything updated on each virtual machine to reduce security vulnerabilities.
- **Native remote management services**: Use native remote management services to reduce the risk of an attacker intrusion into a virtual machine.

Guidelines to secure virtual environments are:

- Authentication to the virtual devices.
- Restricted connectivity to all virtual resources.
- Segmenting the virtual infrastructure.
- Virtual resource reservation and limits.
- Apply standard infrastructure security measures into the virtual infrastructure.
- Use native remote management services (RMS) to communicate with virtual machines.
- A host-based IPS (HIPS) protects the virtual environment from security threats.

Best Practices for Virtual Environment Security

The following are additional best practices for virtualization security:

- Create virtualization security policies for OS, networks, kernel, traffic, backup, and deployment.
- Separate virtual networks into security or trust zones and provide high security at critical areas.
- Update the hypervisor environment regularly.
- Disable unnecessary hypervisor devices and all emulated hardware from the virtual environment.
- Secure virtual systems with antivirus software, IDSs, firewall, etc.
- Use security controls to limit unauthorized access and restrict access to unprivileged networks.
- Implement strong access controls for virtual environment management.
- Monitor configuration of host virtual machines and VMware infrastructure at regular intervals.
- Frequently audit event logs for suspicious and unexpected activity.
- Provide continuous training to improve an administrator's skillset on virtualization security trends and technologies.

- Implement regular updates for downloaded software and security patches on virtual machines.
- Protect the integrity of every guest operating system.
- Use strong passwords for BIOS, OS, and network configuration on both hosts and guest machines.
- Audit and control the administrative access to the hypervisor's accounts and credentials.
- Protect the host system with high security measures, as it provides direct access to VMs, networks, devices, applications, and hypervisors.
- Actively audit, monitor, and test virtual networks and network traffic from violations
- **Enforce the Least Privileges**: It is a core security principle that makes users operate with the least set of privileges that are necessary to finish the task/job.
- **Harden Access Controls**: Deploy controls to the hypervisor and virtual machines in a secure manner to avoid unauthorized access.
- **Monitor the Virtual Traffic:** There are various tools available to identify malicious traffic and defend the virtual machines from intrusions and attackers.
- **Record VM Migrations**: Migration between virtual machines must be recorded to monitor and diagnose machine failures.
- **Monitor VM Snapshots and Rollback:** Create a work environment to monitor virtual machines. If there any issues, rollback to a stable state using snapshots that are taken at particular intervals by the administrator.
- **Scan and Audit Virtual Machines:** Virtual machines are scanned at regular intervals to discover vulnerabilities and service failures