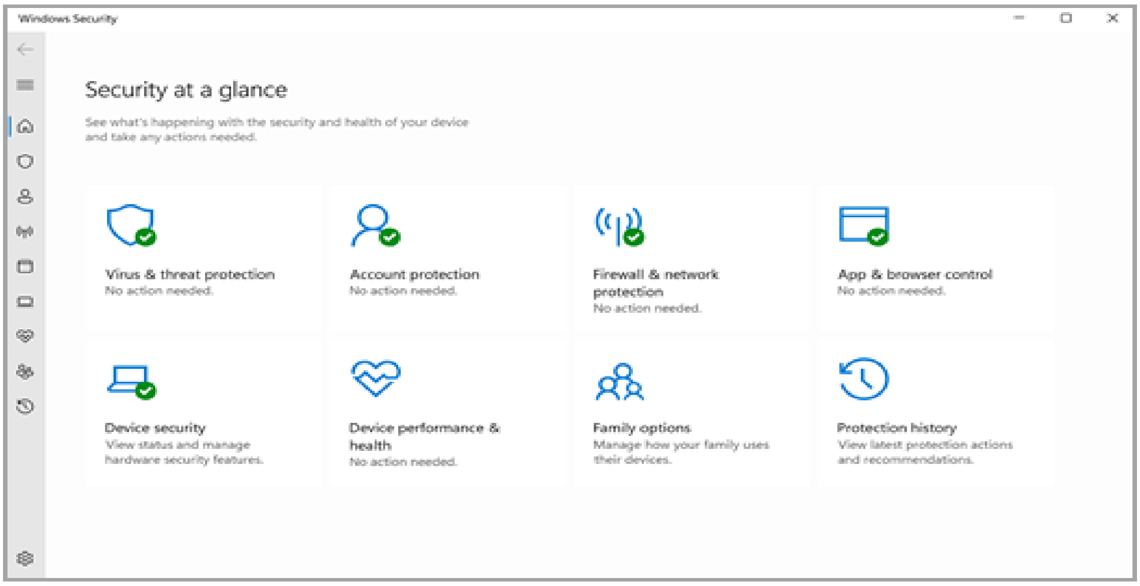
WEEK4: DAY-1

WINDOWS SECURITY: Windows Security is your home to manage the tools that protect your device and your data.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
View status and manage hardware security features.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.

Protection history
View latest protection actions and recommendations.

Important Of SECURITY Windows Security is built-in to Windows and includes an antivirus program called Microsoft Defender Antivirus. (In early versions of Windows 10, Windows Security is called Windows Defender Security Centre).

If you have another antivirus app installed and turned on, Microsoft Defender Antivirus will turn off automatically. If you uninstall the other app, Microsoft Defender Antivirus will turn back on automatically.If you're having problems receiving Windows Security updates, see Fix Windows Update errors and the Windows Update FAQ. To change your user account to an admin account, see Create a local user or administrator account in Windows.

WINDOWS SECURITY INFRASTRUCTURE

What Is Infrastructure Security?

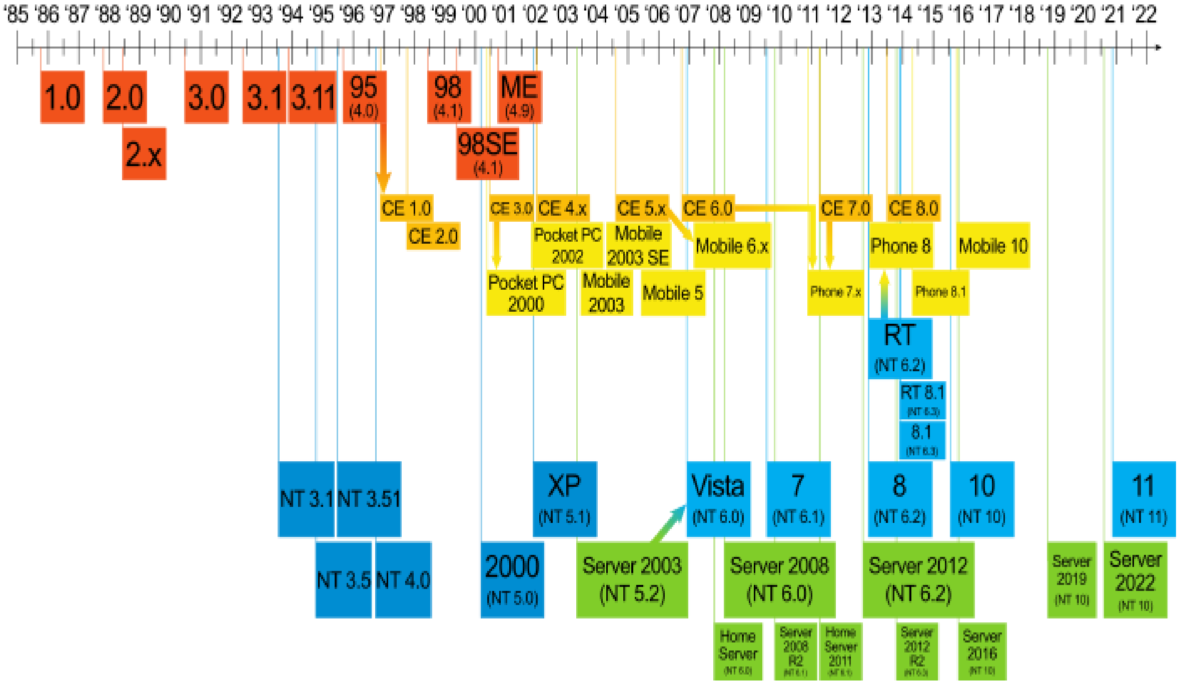
Infrastructure security is the practice of protecting critical systems and assets against physical and cyber threats. From an IT standpoint, this typically includes hardware and software assets such as end-user devices, data centre resources, networking systems, and could resources.

Benefits of infrastructure security

Enterprises depend on their technology assets to maintain operations, so protecting technology infrastructure is protecting the organization itself. Proprietary data and intellectual property (IP) provide many companies significant competitive advantages in the market, and any loss of or disruption of access to this information can have profound negative impacts to a company's profitability.

WINDOWS FAMILY PRODUCTS

Windows is a group of several proprietary graphical operating system families developed and marketed by Microsoft. Each family caters to a certain sector of the computing industry, for example Windows NT for consumers, Windows Server for servers, and Windows IoT for embedded systems.



WINDOWS WORKGROUPS AND ACCOUNTS

Workgroup accounts are the default account for Windows 10 computers and belong to the most basic of network infrastructures. This means that unless you join a domain (or a homegroup), your account will remain in a workgroup.

Windows Active Directory: Active Directory (AD) is a database and set of services that connect users with the network resources they need to get their work done. The database (or directory) contains critical information about your environment, including what users and computers there are and who's allowed to do what.

How Dose Active Directory work?

Active Directory offers a set of services for administrators to manage their IT networks. These services are deployed on a Windows server called a domain controller. Active Directory Domain Services (AD DS) is the most widely used Active Directory service. It authenticates Active Directory objects and authorizes access to network resources. AD DS also stores and organizes data in a logical, hierarchical structure and can be managed from anywhere in the network. Other important AD services include Active Directory Federation Services (AD FS), Active Directory Certification Services (AD CS), Active Directory Lightweight Directory Services (AD LDS), and Active Directory Rights Management Services (AD RMS).

GRUP POLICY

Group Policy is a hierarchical infrastructure that allows a network administrator in charge of Microsoft's Active Directory to implement specific configurations for users and computers. Group Policy is primarily a security tool, and can be used to apply security settings to users and computers.

Example of Group Policy

Examples of group policies include configuring operating system security, adding firewall rules, or managing applications like Microsoft Office or a browser. Group Policies also install software and run startup and login scripts.

WINDOWS AS **SERVICE**

Windows as a service is the approach Microsoft introduced with Windows 10 to deploy, update and service the operating System. Examples: web browsers, document editing software and PDF readers.

END-OF-SUPPORT

End-of-support refers to a situation in which a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for previous versions.

End-of-support is also known as an end-of-support policy.

SERVICING CHANNEL

Offers organizations some flexibility to choose when and how often their devices are updated to the latest build of Windows 10. There are three main Servicing Channels which give IT administrator’s choice, including Windows Insider, Semi-Annual Channel (Targeted), and Semi-Annual Channel.

Windows Update: Windows Update is a free Microsoft service that's used to provide updates like service packs and patches for the Windows operating system and other Microsoft software. It can also be used to update drivers for popular hardware devices.

Patches and other security updates are routinely released through Windows Update on the second Tuesday of every month—it's called Patch Tuesday. However, Microsoft releases updates on other days as well, like for urgent fixes.

Windows update used for

Windows Update is used to keep Microsoft Windows and several other Microsoft programs updated. Updates often include feature enhancements and security updates to protect Windows from malware and malicious attacks. You can also use Windows Update to access the update history that shows all the updates that have been installed to the computer through the Windows Update service.

WINDOWS UPDATE AVAILABILITY

All modern Windows operating systems use Windows Update, like Windows 11 and Windows 10, but also the other versions through Windows XP. However, this service doesn't update most of your other, non-Microsoft software. You'll need to update those programs yourself or use a free software updater program to do it for you.

WINDOWS SERVER UPDATE SERVER (WSUS)

Windows Server Update Services (WSUS) is a Windows server role that can plan, manage and deploy updates, patches and hotfixes for Windows servers, client operating systems (OSes) and other Microsoft software. It allows system administrators to control when and how systems install updates and provides a central point for clients to get the updates. It is designed for small to medium-sized business (SMB) use. There is typically no additional cost to add WSUS to a Windows network.

WINDOWS AUTOPILOT

Windows autopilot is a collection of technologies used to set up and pre configure new devices, getting them ready for productive use.

WINDOWS VIRTUAL DESKTOP (WVD)

Windows Virtual Desktop (WVD) is an Azure service that, combined with appropriate licenses, services, and resources, delivers a complete virtualized multi-user Windows 10 (or a single-user Windows 7) experience together with Office 365 Proplus. WVD includes centralized management and monitoring; system administrators can quickly deploy and manage desktops, apps, and Windows servers in the Azure Cloud.

THIRD PARTY PATCH MANAGEMENT

The process of installing patches to third party applications that are installed on your company's endpoints, to address bugs in the software.

WINDOWS AS **SERVICE**

Windows as a service is the approach Microsoft introduced with Windows 10 to deploy, update and service the operating System. Examples: web browsers, document editing software and PDF readers.

END-OF-SUPPORT

End-of-support refers to a situation in which a company ceases support for a product or service. This is typically applied to hardware and software products when a company releases a new version and ends support for previous versions. End-of-support is also known as an end-of-support policy.

WINDOWS ACCESS CONTROLS

Access control refers to security features that control who can access resources in the operating system. Applications call access control functions to set who can access specific resources or control access to resources provided by the application.

What Are the 4 Type of Access Control?

- Mandatory Access Control (MAC)
- Role-Based Access Control (RBAC)
- Discretionary Access Control (DAC)
- Rule-Based Access Control (RBAC or RB-RBAC)

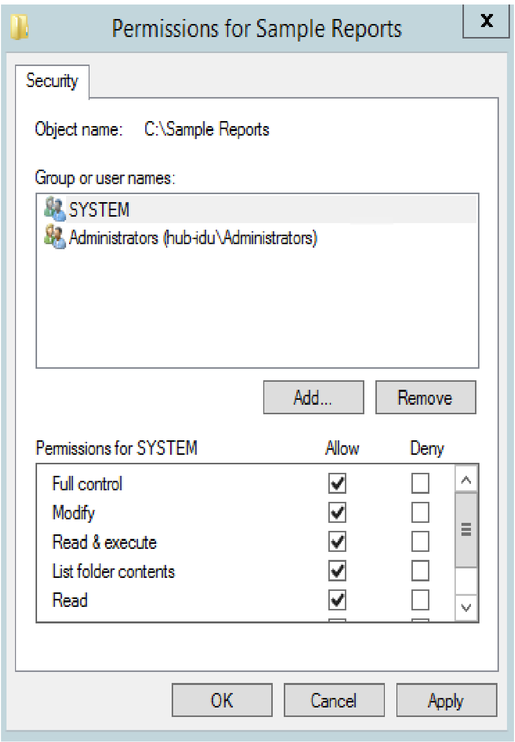
Video Surveillance
Door Security
Man Traps
Paper Access Logs

Why Is Access Control Important?

The goal of access control is to minimize the security risk of unauthorized access to physical and logical systems. Access control is a fundamental component of security compliance programs that ensures security technology and access control policies are in place to protect confidential information, such as customer data. Most organizations have infrastructure and procedures that limit access to networks, computer systems, applications, files and sensitive data, such as personally identifiable information and intellectual property.

NTFS PERMISSIONS

NTFS permissions are used to manage access to the files and folders that are stored in NTFS file systems. NTFS (NT File System) permissions are available to drives formatted with NTFS. The advantage with NTFS permissions is that they affect local users as well as network users and they are based on the permission granted to each individual user at the Windows logon, regardless of where the user is connecting.



Object name: C:\Sample Reports

Group or user names:

- SYSTEM
- Administrators (hub-idu\Administrators)

Permissions for SYSTEM	Allow	Deny
Full control	☑	□
Modify	☑	□
Read & execute	☑	□
List folder contents	☑	□
Read	☑	□

Who Can Apply Or Set NTFS Permissions:

While any administrator knows how to set or change NTFS permission levels, the tricky part is how to manage them consistently and efficiently for hundreds or thousands of different users.

1. In Windows Explorer, right-click a file, folder or volume and choose Properties from the context menu. The Properties dialog box appears.
2. Click the Security tab.
3. Under Group or user names, select or add a group or user.
4. At the bottom, allow or deny one of the available permissions.

How Do Remove NTFS Permissions

1. Select the folders from which permissions are to be removed.
2. Select the user account and / or groups for whom permissions should be changed.
3. Click the permissions drop down list choose the permissions set to be removed.
4. Finally choose the type of permission allow or deny.

SHARED FOLDER PERMISSION

Share permissions allow you to control who accesses folders over the network.

Shared permissions Type

- Full Control: Allows users to create, read, update and delete files and folders in a directory, as well as NTFS files and folders. By default, the “Administrators” group is granted “Full Control” permissions.

- Change: Allows users to read files, as well as add, edit and delete files and folders. “Change” permissions are not assigned by default.
- Read: Allows users to read content in files and folders, as well as execute programs. The “Everyone” group is assigned “Read” permissions by default.

Configure Permission in The Windows Registry

1. Open the Windows Registry Editor: Click Start, and select Run. ...
2. Navigate to the following folder: HKEY_USERS\S-1-5-20.
3. Right-click the S-1-5-20 folder, and select Permissions. ...
4. To add the domain user, click Add.
5. For the Full Control option, select the Allow check box.
6. Click OK.

ACTIVE DIRECTORY PERMISSIONS

Permissions in Active Directory are access privileges that you grant to users and groups that permit them to interact with objects.

Assigning permissions to active directory:

1. Go to the security tab of the OU (An organizational unit) you want to give permissions to.
2. Right-click the relevant OU and click Properties.
3. Go to the security tab and click Advanced.
4. Click Add and browse to your user account. As stated above you need to add the user account to the OU.
5. Select This object and all descendant objects and select the following permissions:
6. Create Computer Objects

7. Delete Computer
8. Click OK

PRIVILEGES

Privilege is defined as the delegation of authority to perform security-relevant functions on a computer system. A privilege allows a user to perform an action with security consequences. Examples of various privileges include the ability to create a new user, install software, or change kernel functions.

BITLOCKER DRIVE ENCRYPTION

What Is Bitlocker?

BitLocker Drive Encryption, or BitLocker, is a Microsoft Windows security and encryption feature that is included with certain newer versions of Windows. BitLocker enables users to encrypt everything on the drive Windows is installed on, protecting that data from theft or unauthorized access.

How Dose BitLocker Use?

BitLocker uses a specialized chip called a Trusted Platform Module (TPM). The TPM stores Rivest-Shamir-Adleman encryption keys specific to the host system for hardware authentication. The TPM is installed by the original computer manufacturer and works with BitLocker to protect user data.

Security policy Enforcement

For security policies to work, they must be enforced. Enforcement capabilities for password protection may include requiring the use of a password, controlling the minimum and maximum length of passwords, mandating special characters or numerals in passwords, governing the frequency with which passwords are changed, and controlling if or when passwords can be reused.

Enforcement of permissible applications policy can involve either warnings or actions if a user is found to have application not authorized by the enterprise or to have authorized applications missing. Apply a Security Template

Click Start, click Run, type mmc, and then click OK. On the File menu, click Add/Remove Snap-in. Click Add. In the Available Stand Alone Snap-ins list, click Security Configuration and Analysis, click Add, click Close, and then click OK.

How do I create a security template?

Right-click %System Root%\Security\Templates, and then click New Template. In the Template name box, type a name for the new template. If you want, you can type a description in the Description box, and then click OK. The new security template appears in the list of security templates.

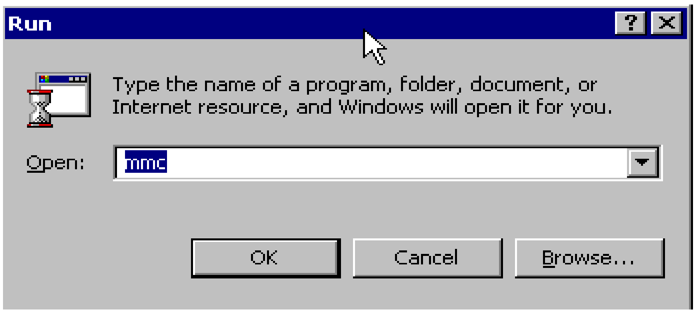
Employing the Security configuration and analysis snap

The Security Configuration and Analysis is a stand-alone snap-in tool that users can use to import one or more saved configurations to a private security database.

How to use the Security Configuration and Analysis tool?

Windows 2000 includes a tool called "Security Configuration and Analysis" that can help you check your security settings. Unfortunately, this tool is well hidden in a default installation of Windows 2000. This document shows you how to use this tool.

1.) Click on the "Start" menu, and choose "Run".

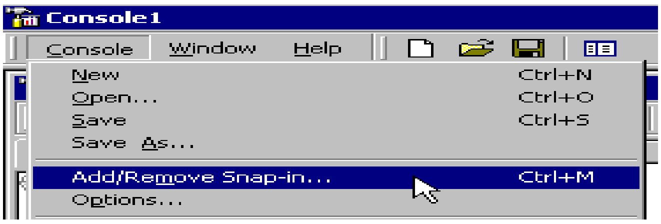


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

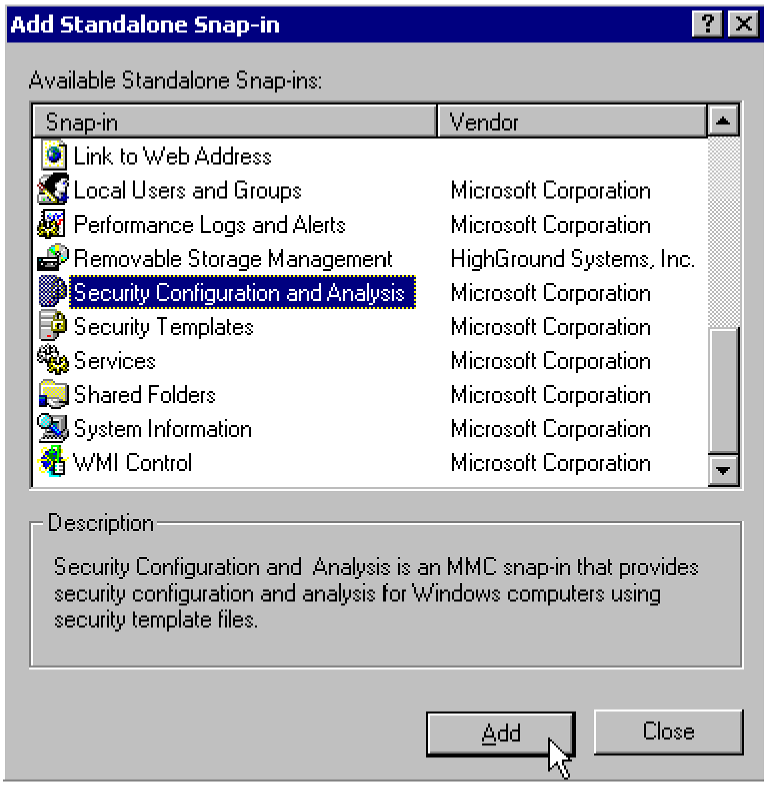
Open: mmc

2.) Type "mmc" into the run dialog, and press Return.

3.) The "Microsoft Management Console" (mmc) appears. Click on the "Console" menu, and choose "Add/Remove Snap-in..."



4.) Scroll down and click on the "Security Configuration and Analysis" snap-in, and click on the "Add" button.



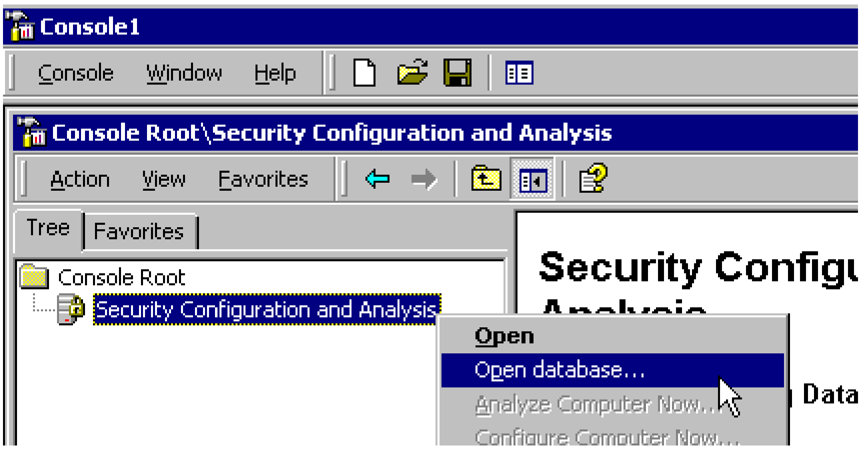
Snap-in	Vendor
Link to Web Address	
Local Users and Groups	Microsoft Corporation
Performance Logs and Alerts	Microsoft Corporation
Removable Storage Management	HighGround Systems, Inc.
Security Configuration and Analysis	Microsoft Corporation
Security Templates	Microsoft Corporation
Services	Microsoft Corporation
Shared Folders	Microsoft Corporation
System Information	Microsoft Corporation
WMI Control	Microsoft Corporation

Description

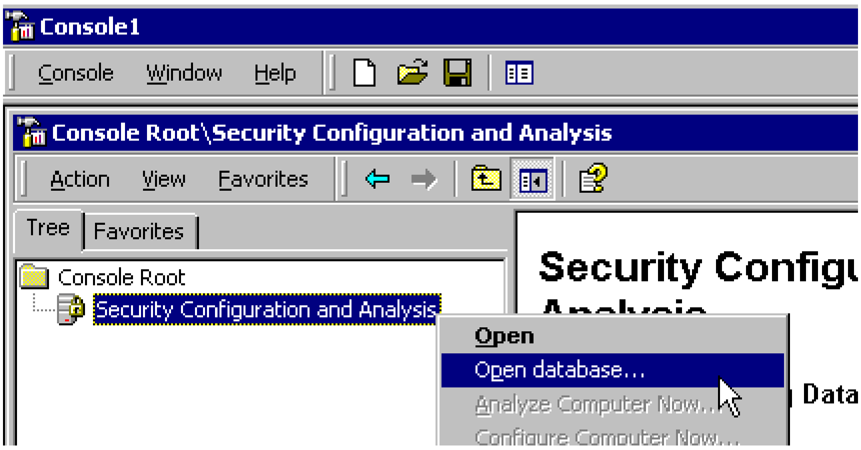
Security Configuration and Analysis is an MMC snap-in that provides security configuration and analysis for Windows computers using security template files.

5.) Click on the "Close" button, and then click on the "OK" button.

6.) Right click on the "Security and Configuration Analysis" node, and choose "Open Database..."

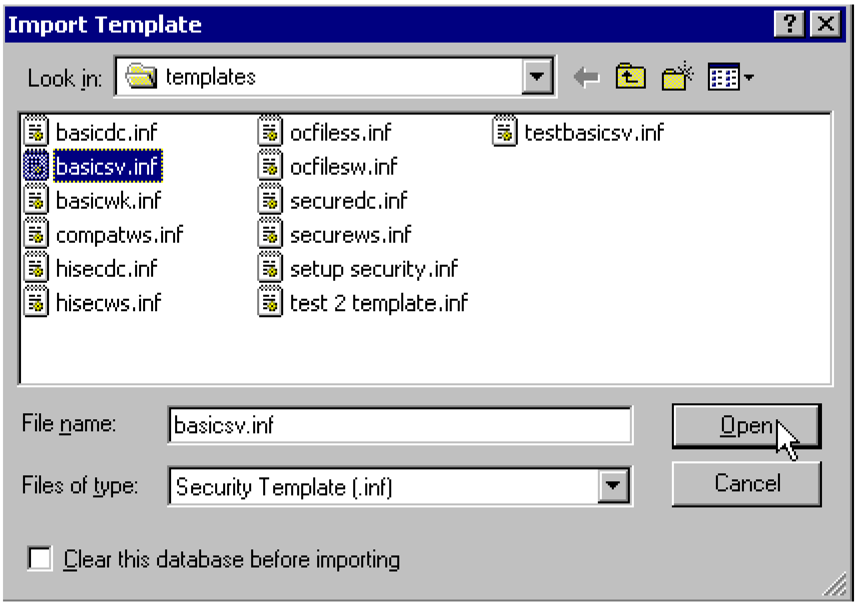


7.) Type in any name for the security database. The security database is just temporary storage for this program. In the figure below, the user has entered the name "security Test" for the database. Click on the "Open" button.



8.) Choose a template to import. Note that you can also make your own template using the "Security Templates" MMC Snap-in

Choose the Security Template that is appropriate for your situation (basicsv.inf is a good place to start). Click on the "Open" button.



Look in: templates

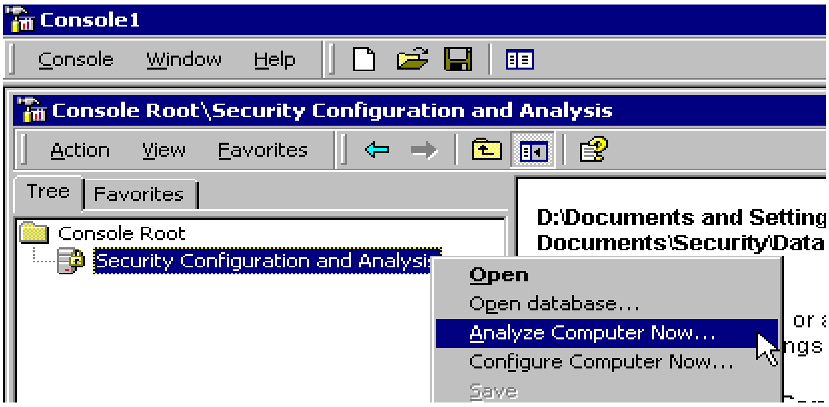
basicdc.inf
basicsv.inf
basicwk.inf
compatws.inf
hisecdc.inf
hisecws.inf
ocfiless.inf
ocfilesw.inf
securedc.inf
securews.inf
setup security.inf
test 2 template.inf
testbasicsv.inf

File name: basicsv.inf

Files of type: Security Template (.inf)

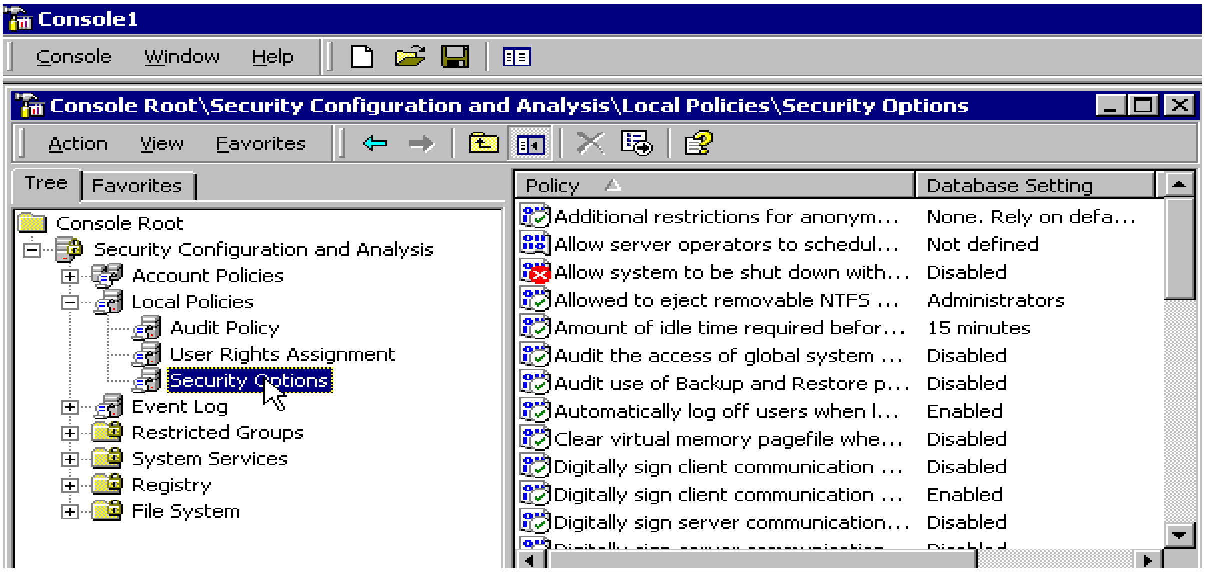
☐ Clear this database before importing

9.) Right click on the "Security Analysis and Configuration" node in the left pane, and choose "Analyze Computer Now".



10.) The tool then compares your computer's settings to those that are recommended by the template.

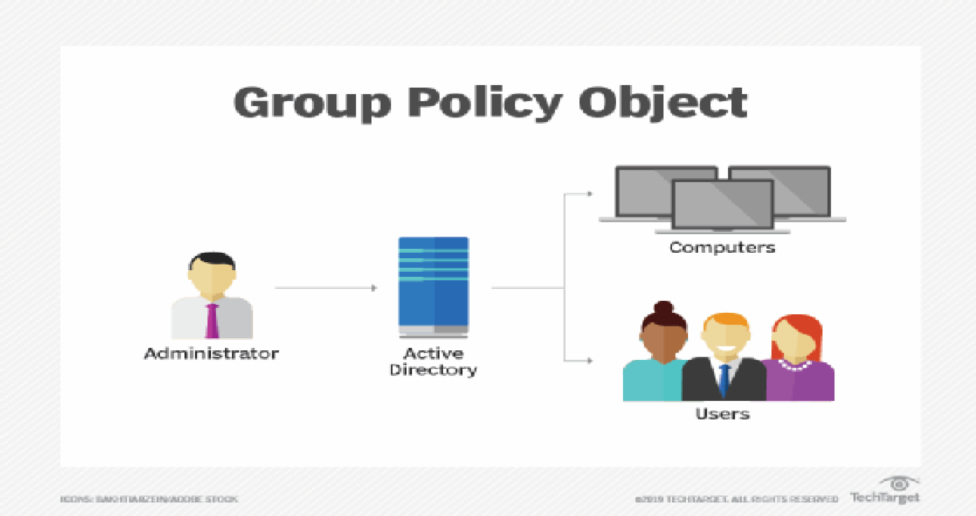
11.) When the analysis is complete, navigate through all the items in the left pane. A read "X" will appear in the right pane for any settings the template recommends you change.



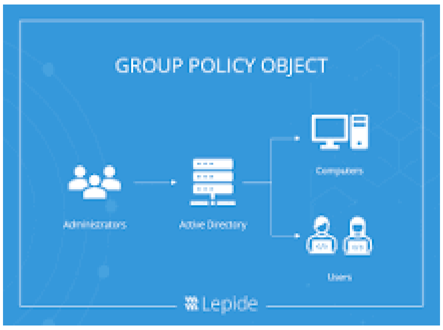
Policy	Database Setting
Additional restrictions for anonym...	None. Rely on defa...
Allow server operators to schedul...	Not defined
Allow system to be shut down with...	Disabled
Allowed to eject removable NTFS ...	Administrators
Amount of idle time required befor...	15 minutes
Audit the access of global system ...	Disabled
Audit use of Backup and Restore p...	Disabled
Automatically log off users when l...	Enabled
Clear virtual memory pagefile whe...	Disabled
Digitally sign client communication ...	Disabled
Digitally sign client communication ...	Enabled
Digitally sign server communication...	Disabled

Local Group Policy Objects

- A local Group Policy Object refers to the collection of group policy settings that only the local computer and to the users who log on to that computer.



Domain group policy objects



A Group Policy Object (GPO) is **a group of settings that are created using the Microsoft Management Console (MMC) Group Policy Editor**. GPOs can be associated with a single or numerous Active Directory containers, including sites, domains, or organizational units (OUs).

Administrative user: Administrative users are responsible for implementing and maintaining security services, such as adding users, building profiles, or managing general site administration.

Privileged account management: Privileged account management is a part of identity and access management (IAM) that deals exclusively with the protection of privileged accounts in an enterprise, including those of operating systems, databases, servers, applications, virtual machines, and networking devices.

Administrative Privileges: Administrative privileges are the ability to make major changes to a system, typically an operating system. It can also mean large software programs such as a database management system.

How to reduction of administrative privileges

The correct approach to restricting administrative privileges is to:

- identify tasks which require administrative privileges to be performed
- validate which staff members are required and authorized to carry out those tasks as part of their duties
- create separate attributable accounts for staff members with administrative privileges, ensuring that their accounts have the least amount of privileges needed to undertake their duties
- Revalidate staff members’ requirements to have a privileged account on a frequent and regular basis, or when they change duties, leave the organization or are involved in a cyber-security incident.

AppLocker:

AppLocker advances the app control features and functionality of Software Restriction Policies.

examples of scenarios in which AppLocker can be used:

- Your organization's security policy dictates the use of only licensed software, so you need to prevent users from running unlicensed software and also restrict the use of licensed software to authorized users.
- An app is no longer supported by your organization, so you need to prevent it from being used by everyone.

User Account Control

User Account Control (UAC) helps prevent malware from damaging a PC and helps organizations deploy a better-managed desktop. With UAC, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system. UAC can block the automatic installation of unauthorized apps and prevent inadvertent changes to system settings.

UAC allows all users to log on to their computers using a standard user account. Processes launched using a standard user token may perform tasks using access rights granted to a standard user. For instance, Windows Explorer automatically inherits standard user level permissions. Additionally, any apps that are started using Windows Explorer (for example, by double-clicking a shortcut) also run with the standard set of user permissions.

Windows Firewall (officially called **Windows Defender Firewall** in Windows 10), is a firewall component of Microsoft Windows. It was first included in Window3 XP and Windows Server 2003. Prior to the release of Windows XP Service Pack 2 in 2004, it was known as **Internet Connection Firewall**. With the release of Windows 10 version 1709 in September 2017, it was renamed Windows Defender Firewall.

Microsoft decided to significantly improve both the functionality and the interface of Windows XP's built-in firewall, rebrand it as Windows Firewall, and switched it on by default since Windows XP SP2.

Data encryption and authentication -IPsec

IPsec is defined by the IPsec working group of the IETF. It provides authentication, integrity, and data privacy between any two IP entities. Management of cryptographic keys and Security Associations can be either manual or dynamic using an IETF-defined key management protocol called Internet Key Exchange (IKE). The main advantage of using IPsec for data encryption and authentication is that IPsec is implemented at the IP layer.

LINUX SECURITY

Security-Enhanced Linux (SELinux) is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC).

Why Linux security is important?

Linux security is important because Linux is so popular with web servers, attackers write custom scripts targeting the operating system to scan for known vulnerabilities and exploit them.

LINUX FUNDAMENTAL

This course is the first of a series that aims to prepare you for a role working as an information technology professional.

What are the fundamental linux:

- The Linux Filesystem.
- Understanding the filesystem.
- Working with file links.
- Searching for files.
- Working with users and groups.
- Working with file permissions.
- Working with text files.
- Working with VIM text editor.

OPERATING SYSTEM COMPARISON

comparison of operating systems, of computer devices, as listing general and technical information for a number of widely used and currently available PC or handheld (including smartphone and tablet computer) operating systems. The article "Usage share of operating systems" provides a broader, and more general, comparison of operating systems that includes servers, mainframes and supercomputers.

Because of the large number and variety of available Linux distributions, they are all grouped under a single entry; see comparison of Linux distributions for a detailed comparison. There is also a variety of BSD and DOS operating systems, covered in comparison of BSD operating systems and comparison of DOS operating systems.

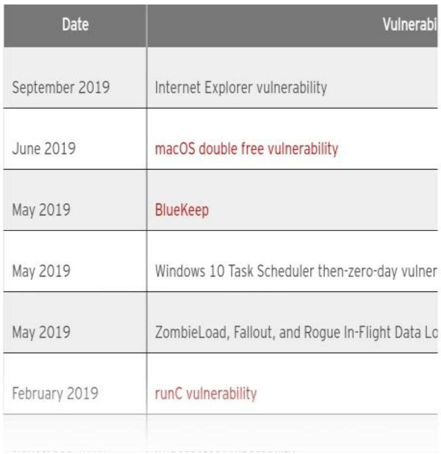
How do you compare different operating systems?

Single-user operating systems have only one user but may allow multiple programs to run at the same time. A multi-tasking operating system allows more than one program to be running at the same time, from the point of view of human time scales. A single-tasking system has only one running program.

LINUX VULNERABILITIES

Vulnerability is a weakness or error in a system or device's code that, when exploited, cacompromise the confidentiality, availability, and integrity of data stored in them through unauthorized access, elevation of privileges, or denial of service.

Here are some of the recent, notable vulnerabilities.



Date	Vulnerabi
September 2019	Internet Explorer vulnerability
June 2019	macOS double free vulnerability
May 2019	BlueKeep
May 2019	Windows 10 Task Scheduler then-zero-day vulner
May 2019	ZombieLoad, Fallout, and Rogue In-Flight Data Lo
February 2019	runC vulnerability

LINUX OPEARTING SYSTEM

What is Linux?

Linux is a Unix-like, open source and community-developed operating system (OS) for Computers, servers, mainframes, mobile devices and embedded devices. It is supported on almost every major computer platform, including x86, ARM and SPARC, making it one of the most widely supported operating systems.

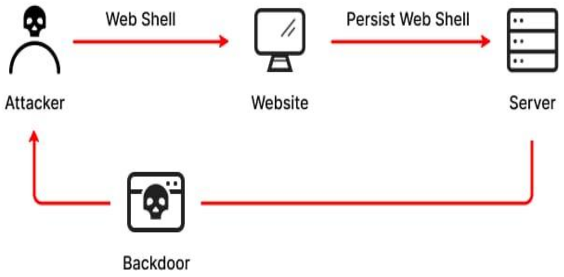
How is the Linux operating systems used?

Every version of the Linux OS manages hardware resources, launches and handles applications, and provides some form of user interface. The enormous community for developers and wide range of distributions means that a Linux version is available for almost any task, and Linux has penetrated many areas of computing.

For example, Linux has emerged as a popular OS for web servers such as Apache, as well as for network operations, scientific computing tasks that require huge compute clusters, running databases, desktop and endpoint computing, and running mobile devices with OS versions like Android.

SHELL

Web shells are malicious scripts that enable threat actors to compromise web servers and launch additional attacks. Threat actors first penetrate a system or network and then install a web shell. From this point onwards, they use it as a permanent backdoor into the targeted web applications and any connected systems.



KERNAL

Kernal is central component of an operating system that manages operations of computer and hardware. It basically manages operations of memory and CPU time. It is core component of an operating system. Kernel acts as a bridge between applications and data processing performed at hardware level using inter-process communication and system calls.

Types of kernal

● Monolithic Kernel – It is one of types of kernel where all operating system services operate in kernel space.

● Micro Kernel – It is kernel types which has minimalist approach.

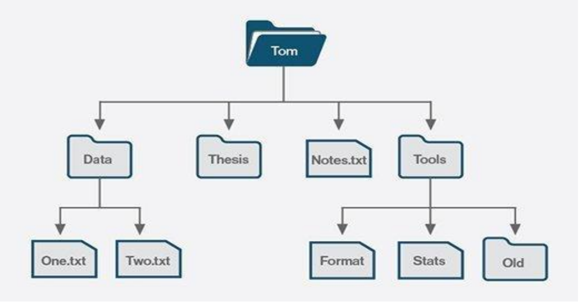
● Hybrid Kernel – It is the combination of both monolithic kernel and microkernel. ...

● Exo Kernel – It is the type of kernel which follows end-to-end principle.

● Nano Kernel –It is the type of kernel that offers hardware abstraction but without system services.

FILE SYSTEM

A file system stores and organizes data and can be thought of as a type of index for all the data contained in a storage device. These devices can include hard drives, optical drives and flash drives.

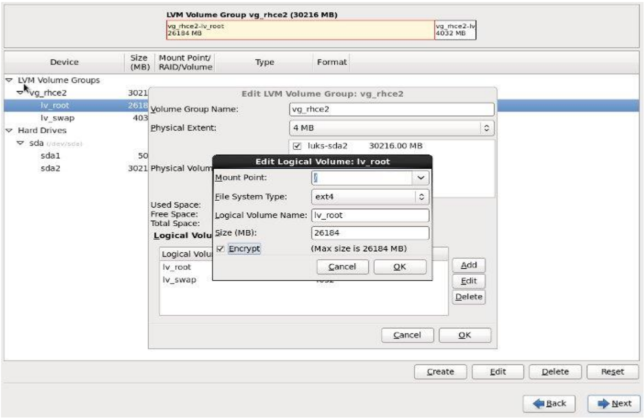


Types of file system:

- Disk file systems.
- Flash file systems.
- Tape file systems.
- Database file systems.
- Transactional file systems.
- Network file systems.
- Shared disk file systems.
- Special file systems.

LINUX UNIFIED KEY SETUP

Linux Unified Key Setup (LUKS) is a specification for block device encryption. It establishes an on-disk format for the data, as well as a passphrase/key management policy.



LVM Volume Group vg_rhce2 (30216 MB)

vg_rhce2-lv_root 26184 MB | vg_rhce2-lv 4032 MB

Edit LVM Volume Group: vg_rhce2

Volume Group Name: vg_rhce2

Physical Extent: 4 MB

☑ luks-sda2 30216.00 MB

Edit Logical Volume: lv_root

Mount Point: /

File System Type: ext4

Logical Volume Name: lv_root

Size (MB): 26184

☑ Encrypt (Max size is 26184 MB)

LINUX SECURITY PERMISSION

Linux security permissions, attributes, and ownership control the access level that the system processes and users have to files. This ensures that only authorized users and processes can access specific files and directories.

Permissions Type

- read – The Read permission refers to a user’s capability to read the contents of the file.
- write – The Write permissions refer to a user’s capability to write or modify a file or directory.
- execute – The Execute permission affects a user’s capability to execute a file or view the contents of a directory.

LINUX USER ACCOUTS

User is an entity, in a Linux operating system, that can manipulate files and perform several other operations. Each user is assigned an ID that is unique for each user in the operating system.

How to add a user in a linux:

- Log in as root.
- Use the command user add "name of the user" (for example, user add roman)
- Use plus the name of the user you just added to log on.
- "Exit" will log you out.

PLUGGABLE AUTHENTICATION MODULES

pluggable authentication module (PAM) is a mechanism to integrate multiple low-level authentication schemes into a high-level application programming interface (API).

Advantage of PAM

- a common authentication scheme that can be used with a wide variety of applications.
- significant flexibility and control over authentication for both system administrators and application developers.
- a single, fully-documented library which allows developers to write programs without having to create their own authentication schemes.

How do PAM module work

Linux-PAM separates the tasks of authentication into four independent management groups: account modules check that the specified account is a valid authentication target under current conditions. This may include conditions like account expiration, time of day, and that the user has access to the requested service.

COMMOND -LINE

Throughout this book, the term command line is used to refer to all of the various non-GUI executables installed with an operating system, along with, and especially, the built-in, keywords, and scripting capabilities available from the shell—its command-line interface.

WHY BASH?

For scripting purposes, we choose the bash shell and command language. The bash shell has been around for decades, is available in nearly every version of Linux, and has even permeated the Windows operating system.

Command line illustration:

This book makes heavy use of the command line through numerous examples. A single-line command illustration will appear as follows:

```
Is-l
```

If the single-line command illustration also displays output, it will appear as follows:

```
$ls-l
-rw-rw-r-- 1 dave dave 15 Jun 29 13:49 hashfilea.txt
-rwxrw-r-- 1 dave dave 627 Jun 29 13:50 hashsearch.sh
```

Note the use of the $ character in the illustration that includes output. The leading $ character is not part of the command, but is meant to represent the simple prompt of the shell command line.

SERVICE HARDENING

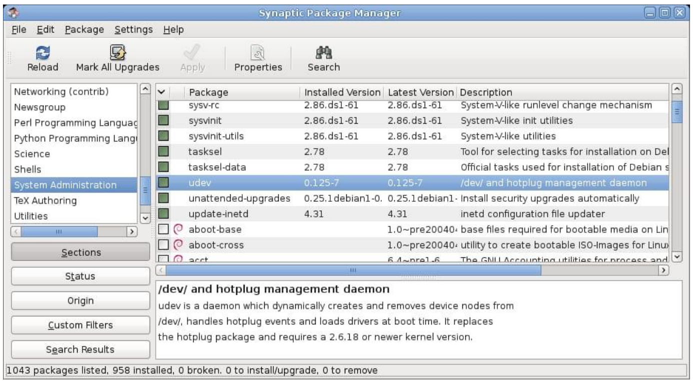
Systems hardening is a collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas.

Example of Hardening

Examples of application hardening include, but are not limited to: Patching standard and third-party applications automatically. Using firewalls. Using antivirus, malware, and spyware protection applications.

PACKAGE MANAGEMENT

A package manager or package-management system is a collection of software tools that automates the process of installing, upgrading, configuring, and removing computer programs or a computer in a consistent manner.



	Package	Installed Version	Latest Version	Description
🟩	sysv-rc	2.86.ds1-61	2.86.ds1-61	System-V-like runlevel change mechanism
🟩	sysvinit	2.86.ds1-61	2.86.ds1-61	System-V-like init utilities
🟩	sysvinit-utils	2.86.ds1-61	2.86.ds1-61	System-V-like utilities
🟩	tasksel	2.78	2.78	Tool for selecting tasks for installation on Del
🟩	tasksel-data	2.78	2.78	Official tasks used for installation of Debian s
🟩	udev	0.125-7	0.125-7	/dev/ and hotplug management daemon
🟩	unattended-upgrades	0.25.1debian1-0.	0.25.1debian1-	Install security upgrades automatically
🟩	update-inetd	4.31	4.31	inetd configuration file updater
□	aboot-base		1.0~pre20040	base files required for bootable media on Lin
□	aboot-cross		1.0~pre20040	utility to create bootable ISO-Images for Linux
□	acct		6.4~pre1-6	The GNU Accounting utilities for process and

/dev/ and hotplug management daemon

udev is a daemon which dynamically creates and removes device nodes from /dev/, handles hotplug events and loads drivers at boot time. It replaces the hotplug package and requires a 2.6.18 or newer kernel version.

1043 packages listed, 958 installed, 0 broken. 0 to install/upgrade, 0 to remove

LINUX SECURITY ENHANCEMENT AND INFRASTRUCTURE

SECURITY ENHANCED LINUX

Is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls. SEL inux is a set of kernel modifications and user-space tools that have been added to various Linux distributions.

AppArmor

Is a Linux kernel security module that allows the system administrator to restrict programs' capabilities with per-program profiles. Profiles can allow capabilities like network access, raw socket access, and the permission to read, write, or execute files on matching paths.

LINUX HARDENING

Operating system (OS) hardening, a type of system hardening, is the process of implementing security measures and patching for operating systems, such Windows, Linux, or Apple OS X, with the objective of protecting sensitive computing systems.

Address space layout randomization

ASLR) is a technique that is used to increase the difficulty of performing a buffer overflow attack that requires the attacker to know the location of an executable in memory.

Kernel module security

The kernel enforces security between applications and the system at the process level through standard Linux facilities, such as user and group IDs that are assigned to applications. By default, applications cannot interact with each other and applications have limited access to the Operating System.

SSHH HARDENING

Secure Shell is the popular protocol for doing system administration on Linux systems. It runs on most systems, often with its default configuration. As this service opens up a potential gateway into the system, it is one of the steps to hardening a Linux system.

Open scap

Open SCAP ecosystem provides multiple tools to assist administrators and auditors with assessment, measurement, and enforcement of security baselines. We maintain great flexibility and interoperability, reducing the costs of performing security audits.

CIS hardening Guidelines

Physical protection brings to mind video cameras, combination locks, and motion detectors, all designed to prevent intruders from breaching a facility. Likewise, IT and cyber security professionals rely on system hardening to reduce the number of "unlocked" doors that malicious actors can exploit.

- **CIS mission** :

Accessibility, clarity, and inclusivity underscore the CIS's system hardening efforts. Because it produces easily understandable and accessible cybersecurity bespractices, tools, and threat information, the CIS's impact spans the globe.

- **CIS Controls:**

Version 7.1 of the CIS benchmarks divides 20 control categories into three sections: basic controls, foundational controls, and organizational controls.

Critical CIS Controls for small business:

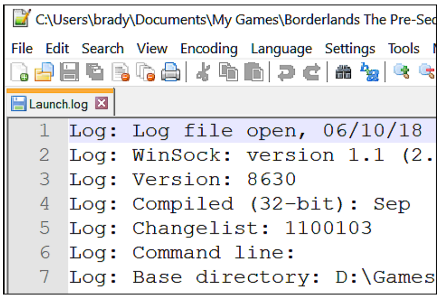
The CIS benchmarks provide a broad outlook of security implementation rather than Industry-specific standards. The breakdown of CIS controls into basic, foundational, and organizational categories helps smaller companies with fewer resources, and human resources still achieve an acceptable level of cyber security.

CIS Image Hardening:

The CIS guidelines cover a variety of topics, including image hardening. An image is like a backup copy of a server or virtual machine that can be duplicated or cloned. This duplicated version can then be used to set up another server or instance of a virtual machine.

Log Files

A log file is a computer-generated data file that contains information about usage patterns, activities, and operations within an operating system, application, server or another device, and is the primary data source for network observability.


C:\Users\brady\Documents\My Games\Borderlands The Pre-Seq
File Edit Search View Encoding Language Settings Tools
Launch.log

```
Log: Log file open, 06/10/18
Log: WinSock: version 1.1 (2.
Log: Version: 8630
Log: Compiled (32-bit): Sep
Log: Changelist: 1100103
Log: Command line:
Log: Base directory: D:\Games
```

KEY LOG FILES

The key log file is a text file generated by applications such as Firefox, Chrome and curl when the SSLKEYLOGFILE environment.

SYS LOG

Syslog is a protocol that computer systems use to send event data logs to a central location for storage. Logs can then be accessed by analysis and reporting software to perform audits, monitoring, troubleshooting, and other essential IT operational tasks.

There are three layers to syslog: content, application, and transport.

- The transport layer sends the message over a network.
- The application layer enables the message to be routed around, interpreted, and stored.
- The content layer is the actual data contained within the message, which contains several standardized informational elements, including facility codes and severity Levels.

SYSLOG SECURITY

Syslog stands for “System Logging Protocol,” Syslog used for system management and security auditing as well as general informational, analysis, and debugging messages.

LOG ROTATION

log rotation is an automated process used in system administration in which log files are compressed, moved (archived), renamed or deleted once they are too old or too big (there can be other metrics that can apply here). New incoming log data is directed into a new fresh file (at the same location).

CENTRALIZED

centralization (see spelling differences) is the process by which the activities of an organisation, particularly those regarding planning and decision-making, framing strategy and policies become concentrated within a particular geographical location group.

Why centralized system is important

The single greatest benefit of centralizing is eliminate redundancy, ensure accuracy of data and save time. A centralized database means that everyone in the company has one primary quote,contract or price list.

LOGGING

The logging and monitoring of security events are two elements of a single process that is critical to the upkeep of safe infrastructure. Every action in your environment is a security event,from emails to logins to firewall changes.

Types of security log

1. Security log:

Smart devices in a company's environment have become even more important to the business as enterprises move toward a cloud-first strategy.

2. Endpoint logs:

Attackers can access your network by successfully exploiting vulnerabilities in endpoint devices including laptops, mobile phones, and computer systems.

3. Iot logs:

The Internet of Things (IoT) is a network of physical objects that communicate with one another rthrough the internet.

4. server log:

Server logs may provide a wealth of information about your environment's current condition.

5. proxy log:

Proxy servers are critical components of an organization's network because they provide anonymity, control access, and save bandwidth.

6.SAN infrastructure log:

Let us imagine a situation, if a server-side transceiver on a fibre switch loses communication,the data on that server is no longer available.

7. Hypervisors:

By balancing workloads and utilizing resources more efficiently, hypervisors can help us IT professionals do our jobs better.

AUDIT ID

What is an audit is What?

A process also acquires its audit ID when the user logs in, and this audit ID is inherited by all child processes started by the user's initial process. The audit ID helps enforce accountability. Even after a user becomes root, the audit ID remains the same.

FIREWALL: NETWORK AND ENDPOINT

What is firewall?

Firewall is a network security device that monitors incoming and outgoing network trafficand decides whether to allow or block specific traffic based on a defined set of security rules.

- **what is a endpoint?**

The desktop firewall protects the integrity of endpoints by regulating inbound and
outbound traffic.

- **what is a network?**

Network firewalls are security devices used to stop or mitigate unauthorized access to private networks connected to the Internet, especially intranets.

ROOTKIT DETECTION

A rootkit scan is the best way to detect a rootkit infection, which your antivirus solution can initiate. If you suspect a rootkit virus, one way to detect the infection is to power down the computer and execute the scan from a known clean system. Behavioral analysis is another method of rootkit detection.