Operating System Basics

1) The Windows OS :-

1.1 Windows History :-

⇒ Disk OS :

* First storage methods → punch cards, paper tapes, magnetic tape, even audio cassets

* Disk OS → an operating system that the computer uses to enable these data storage devices to read and write files

→ It provides a file system which organizes the files in a specific way on disk.

* MS-DOS → as command line as interface for people to create programs and manipulate data files.

→ with this, computer had a basic working knowledge of how to access the disk drive and load the OS files directly from disk as part of boot process.

=> OS vulnerabilities:

* It is some flaw or weakness that can be exploited by an attacker to reduce the viability of computer's information.

1.2 Windows Architecture and Operations:-

=> Hardware abstraction layers:

* HAL is software that handles all of the communication between the hardware and the kernel. The kernel is the core of OS and has control over entire computer.

=> User mode & kernel mode:

* Installed apps run in user mode
* OS codes runs in kernel mode
*

⇒ Windows file systems:

* exFAT → simple file system, supported by many OSs.

* Hierarchical FS+ → used on MAC OS X and allows much longer filenames, sizes.
→ not supported by windows without special software

* Extended FS → used with linux
→ not supported by windows

* New technology FS → commonly used in windows when installing.

⇒ Alternate data stream:

* NTFS stores files as series of attributes.
* The data in the file is stored in data stream.

⇒ Windows startup:

* two important items to registry:
  - HKEY_LOCAL_MACHINE
  - HKEY_CURRENT_USER

=> The Windows Registry:

* Windows stores all of information about hardware, apps, users, system settings in a large database known as registry.

* It's a hierarchical database where the highest level is known as a hive, below - key, followed by sub keys.

1.3 Windows configuration and Monitoring:

=> CLI and Powershell:

* Used to run programs, navigate file system and manage files and folders.

* types of commands from Powershell:

- cmdlets - These commands perform an action and return an output or object to the next command that'll be executed.
- powershell scripts - files with a .ps1 extension
- Powershell functions - pieces of codes that can referenced in a script.

⇒ Windows Management Instrumentation:

* Used to manage remote computers.

* Can retrieve information abt computers, components, hardware and software statistics...

⇒ Task Manager and resource monitor

* These are two important and useful tools.

* Provides insight into the performance of computer.

* useful, when investigating a malware problem.

1.4 Windows Security:-

⇒ The netstat command:

* It can be used to look for inbound or outbound connections that are not authorized.

* When used on its own, it shows all of the active TCP connections.

⇒ Event viewer:

* It logs the history of application, security and system events.

* It is a valuable trouble shooting tool because they provide information necessary to identify a problem.

* Two categories - windows logs
- Application and service logs

⇒ Windows updates Management:

* Patches - They are code updates that manufacturers provide to prevent a newly discovered virus or worm from making a successful attack.

⇒ windows Defender:

* Malware - viruses, worms, Trojan horses, keyloggers, spyware, adware.

⇒ windows Defender firewall :

* Firewall - A firewall selectively denies traffic to a computer.
  - They generally works by opening, and closing the ports used by various applications.

2) Linux Overview :

2.1 Linux Basics :-

* Linux - An OS that was created in 1991, open source, fast, reliable, small.
  - requires very little hardware resources to run
  - highly customizable

* Advantages - An open source
  - Its CLI is very powerful
  - User can have more control over OS
  - Allows better network communication tool

* PenTesting tools - packet generators, port scanners, proof-of-concept exploits
  - Its the process of looking for vulnerabilities in a network by attacking it.

2.2. Working in Linux shell :-

* User communicates with OS by CLI, GUI.

* GUI → default

  → hides CLI from user

* Basic Linux commands → programs created to perform a specific task.

* Command-line-based text editors

  → They allow for text file editing from remote computers

* Importance of text files

  → Everything is treated as files.

  → includes memory, disks, monitor, directories.

* Graphical text editors → includes a feature set designed to support a specific work scenario.

  → convinient and easy to use

2.3 Linux servers and clients :-

* Ports - a reserved network resource used by a service

  - a computer can be the server for multiple services by ports.

* Clients - programs or apps designed to communicate with specific type of server.

  - uses a well defined protocol to communicate with server.

* Nmap - a port scanner and network mapping tool to detect open ports.

  - an open source utility used for network discovery and security auditing.

* Telnet - a simple remote shell application.

  - considered insecure coz it doesn't provide encryption.

2.4. Basic Server Administration :-

* Service configuration files → services are managed by this

* Hardening Devices → involves implementing proven methods of securing device and protecting its administrative access.

→ Methods involves like password maintaings, configuring enhanced remote login features, implementing secure login with SSH.

* Monitoring service logs → Log files are records that a computer stores to keep track of important events.

→ catagorised as application, event, service and system logs.

* daemon → a bg process that runs without the need for use interaction.

2.5. The Linux file system :-

* Hard link - a file that points to same location as orginal file.
  - If one file is changed, then the other also will be changed

* symbolic link - applying changes to symbolic will also change original file.

* Mounting - mounting a filesystem is the process of linking the physical partition on block device to a directory, through which the entire filesystem can be accessed.

2.6. Working with Linux GUI :-

* GUI in Linux - based on X window system.
* X window - a windowing system designed to provide the basic frame work for a GUI.

2.7. Working on a Linux Host :-

* Package managers - Pacman (arch linux)

~~- dpkg (Debian package)~~

- dpkg / apt (Debian and Ubuntu linux)

* Processes - a running instance of a computer program.

* forking - a method that the kernel uses to allow a process to create a copy of it self.

* Rootkit check - a type of malware, designed to increase an unauthorised user's privileges or grant access to portions of software that should not normally allowed.

- to secure backdoor to a compromised computer

* Piping commands - many commands combined to perform more complex tasks by this technique.