13/08/2024

Vidyalekhan

DATE
PAGE

Security Hardening

Defn: SAM File - store the hash of windows/OS's credentials.
Ways to reset your password?
Computer Mangement → Groups & Policies.
↳ Application, OS, Network.

Defn: Security hardening - process of strengthening a system or network against attacks. This includes implementing security measures to reduce vulnerabilities & protect sensitive data.

Tools: RootKit, Hiren Boot.

Imp: Reduced risk, Compliance, Enhanced security posture, improved reliability.

Identifying security vulnerability.

1) Vulnerability Scanning - automated tools scan systems & networks
2) Penetration Testing - EHs simulate real world attacks to exploit
3) Security Audits - manual assesments.

Securing Network Configurations.

1) Firewalls - windows defender.
2) IDS/IPS
3) VPNs
4) Network Segmentation
DMZ? Static & Dynamic Scans.
Taxonomy of a Malware

Vidyalekhan

DATE
PAGE

04/08/2024

Monitoring & logging.

1) Security Information & Event Management (SIEM)
2) Security Monitoring Tools (Wazoo) ↑
3) Log Analysis
   → Argus - linux based tool (AI/ML based).

Applying security patches & updates.

- Remote Access Trojan (Application Hardening)
  → Understand Android Architecture.
  → Windows Xp payload vulnerability (backdoor)
  → Sandbox environment.
- Dynamic & Advanced dynamic analysis
  → for Malwares.
- Exodus - crypto wallet
- NMAP??

- Open filtered
- Close filtered
- Open unfiltered
- Filtered.

Common Vulnerabilities in Systems.

1) Default password
2) Unpatched software
3) Misconfigurations
4) Hardcoded credentials.

16/08/2024

* Video on Google cloud security.

File & File Systems
→ long term information storage
→ file naming.
→ Gary Kasleer Database for file systems
→ Structure of a file - How does your file look like?
→ Magic Number.
→ File Attributes Table
→ File operations. (11)
→ An example program using file system calls.
→ File system implementation.
→ MS-Dos file system
→ File Allocation ~~System~~ Table (FAT) → file system
→ Master file table : Windows forensics (MFT & MFT mirror)
→ NTFS partition. (Defragmentation)
→ MFT record hexadecimal notation.

→ Memory Allocation in files (contiguous / Non-contiguous)
→ Structure?
→ Metadata.

→ Encryption : Stream cipher, Block cipher (combination?)
→ Assymetric Key Algorithm (3-way handshake?)
→ Myshark - Transport layer Security (TLS)
→ Hashing (not in syllabus)
→ Identification, Authentication, Authorization (MAC, DAC, RBAC)
→ How DNS works?
→ DNS records.
→ PS: Get-DnsClientCache. Cmd: ipconfig → Display Dns.
→ Hopping

18/08/2024

Security Hardening - Notes

Defn: SAM File - SAM stands for Sequence Alignment/Map format. It is a TAB delimited text format consisting of a header section, which is optional, an an alignment section.

Defn: SAM File in Windows security - The Security Accounts Manager (SAM) is a database file in windows that stores user account information, including usernames & hashed passwords. The SAM is managed by the local security Authority (LSA) and validates user logins by comparing passwords in the database. The SAMs main purpose is to make the system more secure & protect from data breaches.
C:\Windows\system32\config

Defn: Security Hardening - Security Hardening is a strategy that aims to improve the security of a system or network by reducing vulnerabilities & potential risks.

→ Ways to Identify Vulnerabilities:

- Vulnerability Scanning - The process of identifying security weaknesses & flaws in systems & software running on them.
- Penetration Testing - a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system.
- Security Audits - a systematic evaluation of a company's security & information system by measuring how well in conforms to an established set of criteria.

→ Securing Network Configurations.

- Firewalls – a network security device that monitors incoming & outgoing network traffic & decides whether to allow or block specific traffic based on a defined set of security rules.
- Intrusion Detection System (IDS) – a network security tool that monitors network traffic & devices for known malicious activity, suspicious activity or security policy validations.
- Intrusion Prevention System (IPS) – monitors real-time network traffic for a deeper examination & identification for possible security concerns.
- Virtual Private Networks (VPNs) – establishes a connection between your computer & a remote server owned by a VPN provider
- Network Segmentation – the process of dividing a computer network into smaller sections or subnets to improve network performance & security.
- Demilitarized Zone (DMZ) Network – a perimeter network that protects & adds an extra layer of security to an organization's internal local area network from untrusted traffic.
- Static & Dynamic Scans – static code analysis is a form of white-box testing that can help identify security issues in source code. Dynamic code analysis is a form of black-box vulnerability scanning that scans running applications to identify vulnerabilities.

→ Taxonomy of Malware – sirar.com

→ Monitoring & Logging

- Security Information & Event Management (SIEM) – collect data from various sources & analyze that data to help organizations detect & respond to security threats.
- Security Monitoring Tools – Wazuh is a free & open source security platform that unifies XDR & SIEM protection.
- Log Analysis – process of reviewing & interpreting logs generated by computer systems, networks, & applications to gain insight into their performance & health.

→ Applying Security Patches & Updates.

- Remote Access Trojan (Application Hardening) – giving attackers control over infected systems.
- Windows Xp Payload Vulnerability (Backdoor) – a piece of code that is executed after a system has been exploited by an exploit.
- Sandbox Environment – a secure virtual space that allows users to test code or experiments without affecting the network, applications or hardware.
- NMAP – Network Mapper. It is an open-source Linux command line tool that is used to scan IP addresses & ports in a network & to detect installed applications.

Port scanning States

- Open – actively accepting TCP, UDP, SCTP associations
- Closed – accessible but no application listening on it
- Filtered – cannot determine if port is open due to pkt filtering
- Unfiltered – accessible but nmap cannot determine if open or closed
- Open|filtered – unable to determine if open or filtered
- Closed|filtered – unable to determine if closed or filtered

Vidyalekhan
DATE
PAGE

File & File Systems – Notes

Defn: Long Term Information Storage – preservation of data for extended periods of time.

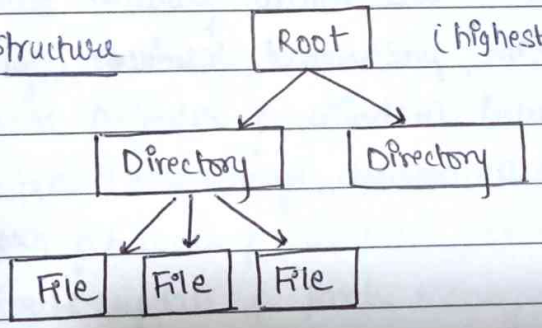
Defn: File Naming – a framework for naming your files in a way that describes what they contain & how they relate to other files. (extensions)

Defn: Gary Kessler's Database (GCKs) for file systems – data used to identify or verify the type of file. Such signatures are known as magic numbers or magic bytes. (first bits of a file which uniquely identify the type of file)

→ Magic Numbers.

→ Structure of a File – How does your file look like?
The file system structure defines how information in key directories & files are organized & how they are stored in an operating system.

Tree Structure



(highest level directory (\))

(FHS – Filesystem Hierarchy Standard)

Byte structure

Types of File Systems

→ File Allocation Table (FAT) – MS DOS File System
FAT is a file system used by computers & other digital devices to manage & organize data stored on storage devices. It keeps track of the location of each file on the device by using a table that maps file names to their physical location on the disk.

Hard drive architecture

Fragmented/Defragmented Disk

Vidyalekhan
DATE
PAGE

20/08

Difference b/w FAT & NTFS

→ New Technology File System (NTFS)
A process that the Windows New Technology operating system uses for storing, organizing & finding files on a hard disk efficiently.

1. A hard disk is formatted.
2. A file gets divided into partitions within the hard disk. (Defragmentation)
3. Within each partition the OS tracks every file stored in a specific operating system.
4. Each file is distributed & stored in one or more clusters or disk spaces of a predefined uniform size.
5. The size of each cluster will range from 512 bytes to 64 kilobytes.

Defn: Master File Table ($MFT) – It keeps records of all files in a volume, the files' location in the directory, the physical location of the files on the drive & file metadata.

* File Attributes – protection, password, creator, owner, read-only
* File Operations – create, delete, open, seek, append, get, set.

20/08/2024

→ How is data stored & retrieved in a hard drive?
→ Physical architecture of a hard drive.
→ Architecture of a SSD. (process flow)
→ Disk Scheduling Algorithms. (FCFS, LOOK, SSTF, SCAN, C-SCAN, C-LOOK)
→ Seek Time, Rotational Latency, Transfer Time, Disk Access Time, Disk Response Time, Starvation.
→ Non-Volatile Memory (NVM) Scheduling (FCFS)
→ Master Boot Record (MBR) (Root block, Super block, Inode list, block list).
→ RAID servers - ADMB Dynamic Data Manager Server Edition.

* Introduction to Windows OS security:
→ Windows security architecture - multilayer defense, integrated security, continual updates.
→ Windows Defender & Windows Defender Antivirus - real time protection, cloud based security, automatic updates.
→ Windows firewall & advanced security
→ Windows update & patch management.
→ User Account Control (UAC) & priviledge management

21/08/24

- Windows encryption & Bitlocker - full disk encryption, multi factor authentication.
- Windows audit & event logging
- Event logs - system events, security events, application events, custom logs.
- Accessing Event Viewer
- * Splunk

TA-1 : Windows OS Security (unit 1) 25 marks.

22/08/24

- Process State
- Deadlock in operating system
- Process Manager.
- Understanding system processes - process dfn, types, states, dependencies
- Monitoring & Managing processes - listing, details, controls
- Identifying & Terminating Malicious Processes
- Optimizing system performance
- Process Hacker
- Real-time system monitoring

29/08/24

Cyber Warfare

- Installing Autopsy (Tool)
- Cyberware – politically motivated hacking conducted by nations or state-sponsored groups.

Example – Pegasus Whatsapp Virus, Prajval

- Types of Cyberwarfare attacks – Espionage, Sabotage, DoS Attacks.
- CERT IN.
- Cyberwarfare Examples – Stuxnet Virus, Sony Pictures Hack, Bronze Soldier Attack.
- Combating Cyberwarfare – cyber wargames, layered defense

- Data leakage case – Assignment (Autopsy)

30/08/24

- Three classes of OS – Client OS, Server OS, Embedded OS
- Raspberry pie
- Service Pack & Email Security
- Windows automatic update & patch installation.
- Windows Backup & Restore Point
- Importance of securing client devices.
- Server Security Considerations.
- TCP connection scan – Principles & Usage.
- TCP SYN Scan
- OS fingerprinting.

Vidyalekhan
DATE
PAGE

Microsoft Windows Hardening
THM Room

Windows Editions.

Windows XP → Windows Vista (short lived) → Windows 7 → Window 8.x (short lived)
Windows 10 (Server 2019)
↓
Windows 11

File System.

- The file system used in modern versions of windows is the New Technology File System (NTFS).
- Before NTFS, there was FAT16/ FAT32 & HPFS (High Performance File System).
- NTFS is known as a journaling file system. In case of a failure, the file system can automatically repair the files/folders on the disk using information stored on a log file, unlike FAT.
- Features of NTFS - supports files larger than 4GB, specific permissions, folder & file compression, encryption (EFS).
- NTFS permissions - Full control, modify, read & execute, list folder contents, read, write.
- Alternate Data Streams (ADS) - Every file has atleast one data stream ($DATA) and ADS allows files to contain more than one stream of data.
- Environment Variables - store information about the OS environment. This information includes details such as OS path, no. of processors used by OS, location of temp. folders.

The system environment variable for windows directory is '%windir%'.

User Accounts, Profiles & Permissions.

- Types of user accounts - administrator & standard
- Local User & Group Management - usrmgr.msc
- Each group has permissions set to it & users are assigned or added to groups by the administrator. When a user is assigned to a group, the user inherits permissions of that group. A user can be assigned to multiple groups.

User Access Control.

- How does UAC work? - when a user with account type of administrator logs into a system, the current session doesn't run with elevated permissions. When an operation requiring higher-level priviledges needs to execute, the user will be prompted to confirm if they permit the operation to run.
- Task Manager - provides information about the applications & processes currently running on the system, CPU/RAM Utilization etc.

General Concepts.

- Windows Services - create & manage critical functions such as network connectivity, storage, memory, sound, user creds, data backup. Categories - Local, Network, System.
- Windows Registry - Unified container database that stores config. settings, essential keys & shared preferences for windows & third party applications.
- Event Viewer - shows log details about all events occurring on your comp.
- Telemetry - data collection sys to identify sec issues in software

Identity & Access Management.

- Administrator - software installation, accessing registry editor, service panel etc.
- Standard - access to regular applications, browser etc.

Vidyalekhan
DATE
PAGE

MIDSEM EXAMINATION

NOTES

Linux Security Hardening (A Comprehensive Guide)

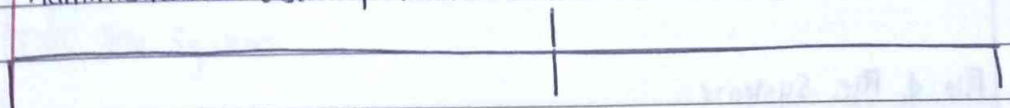
- Securing boot processes & startup services –
  1) Secure Boot – BIOS/UEFI
  2) Systemd – tmpfiles – systemd init system
  3) Startup services – reduce attack surface.
- Secure Package Management & Updates –
  1) Trusted Repositories – verifying signatures
  2) Regular Updates – patch management
  3) Package Management Tools – apt, yum, dnf
- Kernel Security Configurations –
  1) Kernel Modules – reduce attack surface.
  2) Security Enhancements – StackGuard, PAX, RELRO.
  3) Kernel Parameters – system settings.
  4) Hardened Kernel – hardened versions of Ubuntu & CentOS.
- Firewall & Port Control –
  1) Firewall Rules – inbound / outbound
  2) Port Scanning – nmap
  3) Firewall Configuration – ufw, iptables.
- Restricting Network Services –
  1) Disable Unnecessary Services – fsh, telnet, ftp.
  2) Use Secure Protocols – SSH ← Telnet, HTTPS ← HTTP
  3) Network Segmentation – isolate critical systems.

- Logging & Monitoring –
  1) syslog (centralized) – collect logs from various sources.
  2) auditd (security audit) – track sys changes & identify issues.
  3) rsyslog (flexible) – adv. log filtering, routing, analysis.
- Intrusion Detection & Alerting –
  1) Firewall Rules – intrusion detection rules.
  2) IDS – scan & analyze network traffic.
  3) SIEM – centralize security logs.
  4) Alerting – notify admins real-time.
- Hardening SSH & Remote Access – Use strong passwords, use key-based authentication, disable password logins, port 22 security.
- Best Practices & ongoing maintainance – regular security audits, training, updates.

Windows Security Template – A Comprehensive Guide.

- Employing Security Configuration & Analysis Snapin
  Template Selection → Analysis Snap-in → Implementation → Monitoring. ←
- Local Group Policy Objects (GPOs) –
  1) Policy Hierarchy – user rights, software restrictions, file access.
  2) Security Settings – computer configuration
  3) User Configuration – privileges, restrictions.
  4) Policy Scope – remote systems only.

- Domain Group Policy Objects (GPOs) -
  1) Centralized management - entire domain.
  2) Policy Hierarchy - site, domain, OU
  3) Policy Inheritance - higher level → lower levels.
- Administrative Users & Permissions



Administrator

modify security settings
install software
manage other users.

Power User

DO	DONT
install software	modify sec. policies
config. sys settings	manage domain users.
manage certain UA	

Standard User

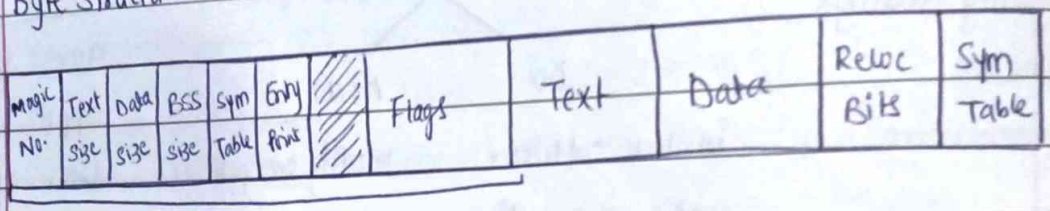
access to common applications & user specific files only.

- Applocker for application control -
  1) Rule based control - allowed / blocked
  2) Enhanced Security - viruses, worms, trojans.
  3) Application whitelisting - allowed apps.
  4) Policy Enforcement - local / ~~group~~ domain GPOs.
- User Account Control (UAC) Settings -
  1) Privilege Elevation - prompts users.
  2) Security Threshold - level of security
  3) Application Control - blacklisting
  4) User Experience - disruptive / balance.
- Recommended Password Policy Settings - length, complexity, history, expiration.

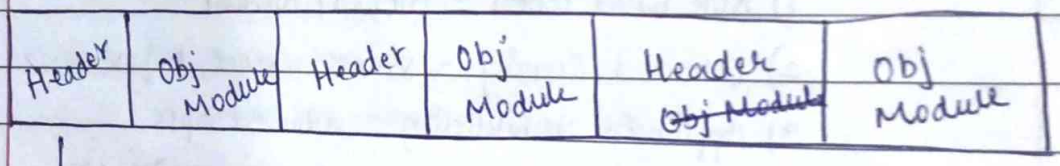
- Account lockout Policy settings - threshold, duration, reset.
- Rec. Security Options & Admin Templates -
  1) Network Security
  2) System Access
  3) User Authentication.

File & File Systems.

1) Byte structure.

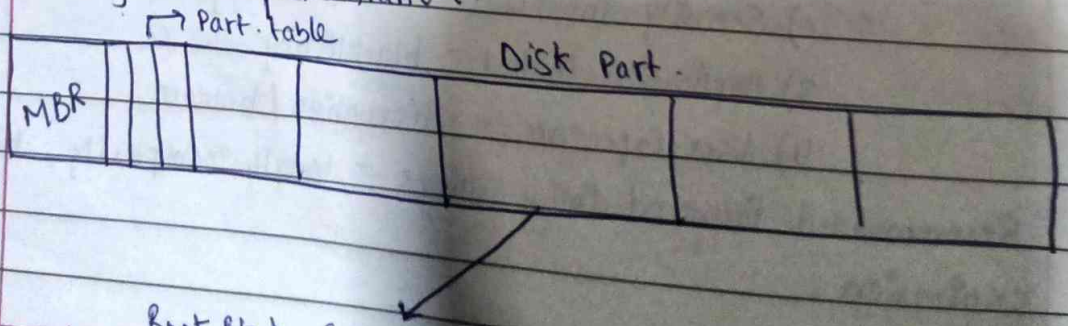


2) Record structure.



↳ Module Name, Date, Owner, Protection, Size

3) File System Implementation.



Boot Block, Super block, Free Sp. Mgmt, Inodes, Root, Files

4) MS-DOS File System.

8	3	1	10	2	2	2	4
Name	Ext.	ATT	//// Res. ////	Time	Date	First Block no.	Size

5) FAT File System.

Boot Sector	File Allocation Table	Root Dir	Directory	Clusters.

6) NTFS.

MBR	MFT Res | Unres	File System Data	MFT copy

Common Cyberattacks & Countermeasures.

1) Phishing - Email Spoofing, URL Manipulation, Social Engg
2) ARP Poisoning - attackers send forged ARP messages to associate their own MAC address with a legitimate IP addr on the network. Static ARP table, ARP inspection, Secure n/w protocols.
3) MAC Flooding - attacker sends frames, switch overwhelmed, network disrupted.
4) Denial of Service - SYN flood, Ping of death (ICMP), Smurf (ICMP echo). [Firewall, Rate Limiting, IDS]
5) DDoS - Botnets
6) Social Engg - Baiting, Pretexting, Scare Tactics, Impersonation.

Introduction to Logging & Monitoring.

Logs : system events, user actions, error messages

Monitoring : continuously observing system metrics

- Configuring logs -
  1) log levels - debug, info, critical, warning, error
  2) log rotation - size & age of logs
  3) log destination - database, SLS
  4) log format - JSON, Apache CLF
- Logging with Syslog -
  1) Syslog protocol - centralized logging
  2) Syslog daemon - UDP port 514
  3) Syslog configuration - filter log messages
- Alternatives to Syslog -
  1) Centralized logging - Graylog, ELK, Splunk
  2) Cloud-based logging - AWS, Azure, Google Cloud
  3) Application logging - Java's log 4j, Python
  4) Event streaming services - Apache Kafka, Apache Pulsar
- Parsing logs with grep - regular expr, pattern matching, output options.
- Filtering logs -
  1) Sed - stream editor for non-int. text
  2) awk - programming lang.
  3) cut - sections of lines
- Monitoring logs with auditd - audit configuration, securing monitoring & alerting, log collection & analysis.

Accounting with auditd - user activity tracking, security audit, resource management & utilization, Reporting & analysis
Best practices for log management - centralized logging, log format log rotation, security considerations

= IP Tables
powerful firewall tool for Linux (host-based firewall)
default - filter table
chains - sequences of rules
RETURN - sends it back to the ~~prev~~. chain for processing.
~~Allow~~ Append (new rule)
Accept | Drop | Return -s: source -p: port -i: Interface
iptables -save - manual
iptables - persistent - automatic /etc/iptables/rules.v4
Common issues - installation errors, persistence failures, table initialization error, command syntax issues
Additional Security Measures:
1) OpenVPN - secure point-to-point connection
2) Fail2Ban - scans log files & bans IP
3) UFW - firewall

#N/w ing layers & OSI

Vidyalekhan
DATE
PAGE

Introduction to threats & vulnerabilities in comp. networks.

1) Attack Surface - area exposed (potential entry point).
2) Attack Vector - method / technique.

- Exploiting attack surface - identify attack surface, choose attack vector, execute the attack.
- Practical examples - WAS, SQLI, exploitation.
- Techniques for identifying attack surface - VAPT, log analysis, TI

BB WB GB

- Mitigating Attacks - Patch mgmt, n/w seg, PoLP, MFA.
- IDS, SIEM

Introduction to Windows Operating System Architecture. (mentioned).

Process Hacker.

- open-source / free tool to manage & monitor processes on your computer.
- Understanding sys. process - defn, dependency, types, states.
- Monitoring & Managing processes - listing, details, control.
- Optimizing system performance - resource monitoring, process prioritization, termination, system tuning.
- Troubleshooting Application Issues - process analysis, dependency check, resource conflicts, error logging

Zenmap : A Comprehensive Network Scanner.

- Open source network scanner that allows you to explore & map computer networks. (port scanning, vulnerability scanning, service detection, operating system fingerprinting).

Ping Scan (nmap -sn <dest>) - identifying active hosts on a networ non-intrusive (does not establish a connection), can be blocked by firewalls, ICMP "echo request" packets.

TCP connection scan - establish a full TCP connection with the target host. SYN, ACK → ACK/RST to identify if the port is open or closed respectively. (nmap -sT <target>) [Connect Scan]

TCP SYN Scan (nmap -sS <target>) [Half-Open Scan] - SYN → SYN+ACK/ RST to identify if a port is open or closed respe

OS Fingerprinting - identifying the OS running on the target host bas on its responses to network requests.

↓ 1) TCP/IP stack characteristics 2) Timing Patterns
ISS/ISN 3) Service Detection.

DNS Reconnaissance - gathering information about a target domain's DNS records.

1) Domain name 2) IP address 3) MX records.

Netcat - (nc) versatile network utility used to establish connecti and transfer data. (port listening, remote connection, data transfe

ICMP Debugging - Tools like 'ping' and 'traceroute' use ICMP pkt to test network connectivity.

1) Packet Loss 2) Unreachable Hosts 3) Network Congestion

Windows Security Infrastructure

- Classes / Types of Operating Systems -
  1) Client 2) Server 3) Embedded
- Service Pack - collection of updates & patches
- Email Security - protecting against malware, phishing attacks & spam.
- Windows Updates (Types) & Patch Installation -
  1) Automatic 2) Scheduled 3) Manual.
- Windows Backup - copy of data / sys. settings
- Windows Restore Points - copy of state at a specific point in time.
- Securing Client Devices - strong pwds, antivirus, firewall, regular updates
- Server Security Considerations -
  1) Physical (room) 2) Network (fw; IDS) 3) Data (encryption) 4) UAC. (PoLP)
- Security Challenges with Embedded Systems -
  1) Limited Resources 2) Inc. Nw Connectivity (attack surface) 3) Vulnerabilities 4) Security Measures
- Keeping software up-to-date with service packs.
  1) Improved Security 2) Enhanced Performance 3) New features 4) Compatability.
- Secure Email Practices.
  1) Strong pwds 2) Links / attachments 3) Spam Filter 4) Encryption.

Windows Event logging & Management

Logs: provide a detailed record of system activity & potential problems (error messages).

- Types of Event logs. — eventvwr.msc
  1) System events - startup, shutdown, driver, sys config
  2) Security events - logins, access permission, modification
  3) Application events - error, warning, performance
  4) Custom events - tracking a specific task.
- Configuring event log settings —
  1) log levels 2) log size 3) log Rotation
- Monitoring event logs —
  1) Real-time (event viewer) 2) Scheduled 3) Alerts (critical levels)
- Analyzing / Filtering event log data —

Event ID	Source	Event Level	Description

- Automating event log mgmt -
  1) Scheduled tasks - log analysis, alert, cleanup
  2) Scripting - PowerShell, VBScript
  3) Monitoring Tools - third party
  4) log Management Sol^{n}s - integrate with centralized sol^{n}s.
- Securing event log data - access control, network security, data encryption.
- Event log Issues - log overflow, corrupted logs, missing events, performance issues.

Windows Operating System Security (overview)

- System Security Features.
  1) Secure Boot - prevents malware during bootstrapping
  2) Trusted Boot - verifying integrity of OS components.
  3) Measured Boot - verify integrity against a secure log
  4) Device Health Attestation - health of firmware & boot process
- Virus & Threat Protection.
  1) Microsoft Defender Antivirus
  2) Attack Surface Reduction
  3) Controlled Folder Access
- Network Security Enhancements.
  1) Transport Layer Security (Windows 11 TLS 1.3)
  2) DNS Security (HTTPS (DoH))
  3) Firewall
- Encryption & Data Protection.
  1) Bitlocker mgmt
  2) Personal Data Enc.
  3) Email Enc. (S/MIME) (Secure/ Multipurpose Internet Mail Extensions)

Windows Hardening (Detailed checklist for Windows Server & Windows 10)

Defn: Windows Hardening - improving the security of the OS by reducing attack surface & vulnerabilities.

Defn: Windows Security Baselines (Baseline Security Analyzer) - pre configured security settings provided by microsoft, ensures compliance, configuring new installations, mitigating vulnerabilities

- Checklist -
  1) User Config (UAC)
  2) Network Config (IDS, DNS, FW)
  3) Service Config (PoLP)
  4) logs & NTP (Syslog)

DATE
PAGE

- Windows Defender Advanced Threat Protection - antimalware, exploit, automa attack surface reduction.
- Microsoft Smart Screen - scans downloads & blocks malicious payloads
- Windows Sandbox - run untrusted apps in isolated env.

→ Process of System Hardening

Discovery → Assessment → Remediation (implementation) → Monitoring

Understanding DNS Records

DNS records - translates human-readable domain names into machine-readable IP addresses. (mapping)

hostname (Name) → IPv4 (Data), static/dynamic, fwd lookup zones

hostname → IPv6

IP → hostname, rev. DNS lookups

hostname → hostname

specify mail server on behalf of a domain

specify servers authoritative for a domain, start of authority for a DNS

service discovery

store arb. text data.

Info :

Passive AV Exploits	Active AV Exploits
- Phishing	- Malware
- Typosquatting	- Unauth. access
- Social Engg.	- Ransomware

DATE
PAGE

Type of OS
Service pack
email security
Patch installation
Backups

Unit 1

→ Three classes of an Operating System:
Operating System - An operating system [illegible] between the computer software & user operated [illegible] point users to operate devices effectively.

Client OS - A client OS is designed for individual users.
Can connect an individual user at a time.
Are less secure
Use for client-based tasks.
Windows 10, Windows 11

Server OS - A server OS is used for enhanced network connectivity & resource sharing.
It can connect several clients simultaneously
It is more secure
It is designed for servers
Windows Server 2019, Windows Server 2022

Embedded OS - An embedded OS is designed for specialized systems.
It is a secure OS
It is complex
It is used in specialize devices (eg. ATMs)
Windows Embedded Compact, Windows IoT Core, Red Hat Enterprise

→ Service Pack

Defn A collection of services, patches & updates that improves the security, performance & stability of the operating system.

- Software manager releases it as a single downloadable package or an installation disc.
- Provide users with an easy & convinient way to update software
- They are free updates
- They are typically numbered – SP1, SP2, SP3 etc.
- Stability, Security, Functionality, User Experience, Risk Reduction

Examples Microsoft SharePoint Designer 2013 SP1
Microsoft office Proofing Tools 2013 SP1

→ Windows Updates & Patch Management.

- Patches are usually smaller in size and quicker to install as they only address specific problems. Updates can be larger & may take longer to install.
- Patches are typically released as required whenever a specific issue is identified and needs to be addressed urgently. Updates are usually released regularly to provide a cumulative set of improvements & changes to the software.

— Security, Stability, Functionality
— Fix vulnerabilities
— Address compatibility issues

* Patch Compliance – level of adherence to an organization or system's patching policies & requirements.

→ Windows Backup

Defⁿ: Creates a copy of your data & system settings, allowing you to restore them in case of data loss or failure.

1) Restore Points - capture state of your system at a specific point in time
2) Regular Backups.

→ Importance of Securing Client Devices

1) Using strong pwds 2) Antivirus 3) Firewalls 4) Regular Updates

→ Server Security Considerations

1) Physical → Phy. access
2) Network → Firewall/IDS
3) Data → Enc., DLP
4) User Access Control → Limit user access

→ Embedded Systems & Security Challenges

1) Limited Resources 2) Connectivity 3) Vulnerabilities 4) Sec. Measures

→ Keeping Software Up-to-Date with Service Packs

1) Improved Security 2) Enhanced performance 3) New features 4) Compatibility

→ ~~Insecure~~ & Implementing Secure Email Practices

1) Using pwds 2) Link Attachments 3) Anti-Spam filters 4) Encrypt.

→ Process Hacker.

- free, open source
- manage & monitor processes

→ Understanding system processes.

1) Process definition 2) Types 3) States 4) Dependencies

→ Monitoring & Managing processes

1) Process listing 2) Process Details 3) Process control

→ Identifying & terminating malicious processes.

1) Suspicious process 2) Process Termination 3) Malware Detection

→ Optimizing System Performance.

1) Resource Monitoring 2) Process Prioritization 3) Process Termination
4) System Tuning

→ Troubleshooting Application Issues

1) Process Analysis 2) Dependency check 3) Resource Conflicts
4) Error Logging 5) Troubleshooting

→ Advanced features & customization

1) Modules 2) Plugins 3) Customization 4) Scripting.

→ Handle & file Mgmt

Thread & Module Information

1) Handle exploration 2) Handle closure 3) Process Prioritization

→ Network Connection Monitoring

1) Active Connections 2) N/w Analysis 3) Troubleshooting N/w issues
4) Security Monitoring

→ Disk Activity Analysis

1) Disk Activity Monitoring 2) Performance Optimization

→ Thread Stack Traces

1) Debugging 2) Performance Analysis 3) Crash Analysis

→ Service Management

1) Service Control 2) Service mgmt 3) Service Config 4) Driver Control

→ GPU Usage Monitoring

1) GPU Utilization 2) Performance Analysis 3) Troubleshooting
4) Resource Allocation

WSUS
System Restore
WAC
Bitlocker
Device Driver Rollback
Enforcing

→ Architechure (features)

1) 2) Integrated Security 3) Continual Updates

→ Windows Defender Antivirus

1) Real time protection 2) Cloud based intelligence 3) Automatic Updates

→ Windows Firewall

1) Network protection 2) Customizable rules 3) Advanced configuration

→ Windows Update & Patch Mgmt.

1) Automatic updates 2) Manual control 3) Centralized Mgmt (WSUS)

→ User Account Control

1) Priviledge seperation 2) Elevation prompts 3) least priviledge

4) Granular control

Centralized mgmt
- Group Policy

→ Windows Encryption (Bitlocker)

1) Full disk encryption 2) MFA 3) Enterprise management

→ Windows Audit & Event Logging

1) Security logging 2) Centralized monitoring 3) Advanced filtering

→ Windows Security Policy & Group Policy

1) Centralized mgmt 2) Granular control 3) Inheritance & delegation

→ Securing Remote Access (VPN)

1) Secure Remote Access 2) VPN encryption 3) MFA.

→ NTFS Permissions.

- Set of rules that govern access to files & folders on windows drives.
- Basic access levels – read, read & execute, write, modify, list, full
- Adv permissions, inheritance, viewing permission, changing permission.

→ Shared folder Permissions.

- Who can access a folder & what they can do with it
- Full control, Change, Read
- They will not apply to users accessing locally.

→ Registry Key Permissions.

- Set of access control entries that define what and how an account can access a registry key.
- binary nos. seperated by spaces
- Delete, Read_control, Write_DAC, Write_Owner.

→ Active Directory Permissions.

- Who can access the resource & the level of access they have.
- Read, Write, Full control

→ MBSA

- free tool that helped professionals assess the security of their windows computers.
- checks, recommendations, scans, CLI

Unit 2

→ Employing the security Configuration Analysis Snap-in
1) Template Selection 2) Analysis & Comparison 3) Implementation
4) Monitoring & Auditing

→ Understanding Local Group Policy Objects
1) Policy Hierarchy 2) Security Settings 3) User Config. 4) Policy Scope

→ Understanding Domain Group Policy Objects
1) Centralized Mgmt 2) Policy Hierarchy 3) Inheritance

→ Users & Permissions
1) Administrator (full control) 2) Power User (limited access) 3) Standard User (Restricted access)

→ Applocker for application control
1) Rule based control 2) Enhanced Security 3) App Whitelisting 4) Policy enf.

→ User Acc. Control Setting
1) Priviledge elevation 2) Security threshold 3) App Control 4) User experience

→ Recc. Pwd Policy Settings
1) Length 2) Complexity 3) History 4) Expiration

→ Recc Acc Lockout Policy Settings
1) Threshold 2) Duration 3) Reset

→ Recc. Security Options
1) N/w security 2) Sys access 3) User auth.

Vidyalekhan

DATE
PAGE

Unit 3

→ Securing boot processes & startup services.

1) Secure Boot 2) Systemd - tmpfiles 3) Startup Services

→ Secure package mgmt & updates

1) Trusted Repositories 2) Regular updates 3) Pkg Mgmt Tools

→ Kernel Security Configurations

1) Kernel modules 2) Security Enhancements 3) Kernel parameters
4) Hardened Kernel

→ Firewall & Port Control

1) Firewall rules 2) Port Scanning 3) Firewall configuration

→ Restricting Network Services

1) Disable unnecessary services 2) Secure N/w protocols 3) N/w segmentation

→ Logging & Monitoring

1) Syslog 2) auditd 3) rsyslog

→ Intrusion Detection & Alerting

1) Firewall Rules 2) IDS 3) SIEM 4) Alerting Systems

→ Hardening SSH & Remote Access

1) Strong pwds 2) Key Based auth
3) Disable pwd logins 4) Port 22 security

→ Best Practices

1) Audits 2) Training
3) Staying Updated

Cyber power - ability to use digital tech to protect/promote interests in cyberspace

Cyber Strategy - plan that protect org's data from cyber threats

Unit 4

Defn: Cyber warfare - politically motivated hacking conducted by nations or state-sponsored groups to disrupt the activities of another nation.

→ Types of cyberwarfare attacks.

1) Espionage 2) Sabotage 3) DOS.

→ Cyber Warfare Examples

1) Stuxnet Virus 2) Sony Pictures Hack 3) Bronze Soldier Attack.

→ Combating Cyber warfare.

1) Cyber wargames 2) Layered defense approach 3) Securing pvt. sector

→ Imperva's Cyber Warfare Protection

1) Application security 2) Data security & DDoS Protection.

→ Operational reasons for cyber warfare.

1) Info dominance 2) Critical Infra disruption 3) Asymm. Adv.

→ Advanced Persistent Threats.

1) Sophisticated 2) Patient 3) State-sponsored

→ International Cooperation in Cyber Defense.

1) Global collab 2) Multilateral frameworks 3) Public Pvt Partnership

Unit 5

→ Understanding Information Assurance
1) Protecting Data 2) Cybersecurity measures 3) Compliance & Regulations

→ Principles of N/w centric operations
1) Shared Awareness 2) Rapid decision making 3) Distributed capabilities

→ Psychological Operations (Foundations)
1) Influencing perceptions 2) Shaping narrative 3) Cognitive dominance
4) Audience focussed

→ Integrating Info. Assurance
1) VA 2) RM 3) IRM

→ N/w centric warfare capabilities
1) Satellite intelligence 2) Unmanned systems 3) Cyber capabilities
4) N/w communication

→ Psychological Ops Training
1) Strategic msg 2) Deception 3) Cultural awareness 4) Psych warfare

→ Defensive info ops
1) Threat identification 2) Vulnerability mitigation 3) IRM
4) Resilience & redundancy

→ Offensive info ops
1) Disruption 2) Destruction 3) Deception

SE Tools :
1) American Registry for Internet Numbers
2) Freedom of Information Act requests
3) Maltego 3
4) Social Engineering Toolkit
5) Twitscoop, Tweep3
6) Trendistic
7) Twittermap
8) PicFrog
9) TinyURL
10) Edgar
11) Spokeo, Telesprut.com

→ Info. Superiority
1) Access to info 2) Info sharing

→ Role of info in modern warfare
1) Situational awareness 2) logistics

→ PSYOPS Techniques
1) Propaganda 2) Rumor 3) Psych warfare 4) Perception mgmt

→ Decephon & Disinfo. campaigns
Methods Countermeasures

→ Building cognitive dominance.
1) Understand enemy 2) Perceptions 3) Narrative

→ Leveraging social media & big data.
1) SM influence 2) BDA 3) SM monitoring

→ Countering info manipulation
1) Media literacy 2) Fact check 3) CS.

→ Developing info. superiority strategies.
1) Identify obj 2) Target audience 3) Lev. resources
4) assess effectiveness.