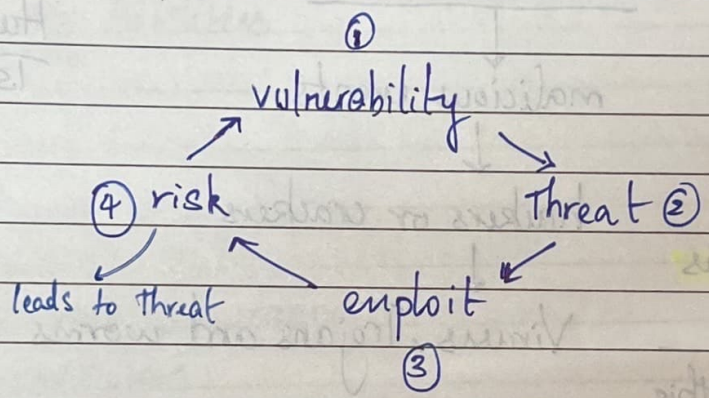
M T W T F S S
Page No.: YOUVA
Date:

Module-1 Introduction to Cyber Security Tools & Cyber Attacks

05/09/2022 W1

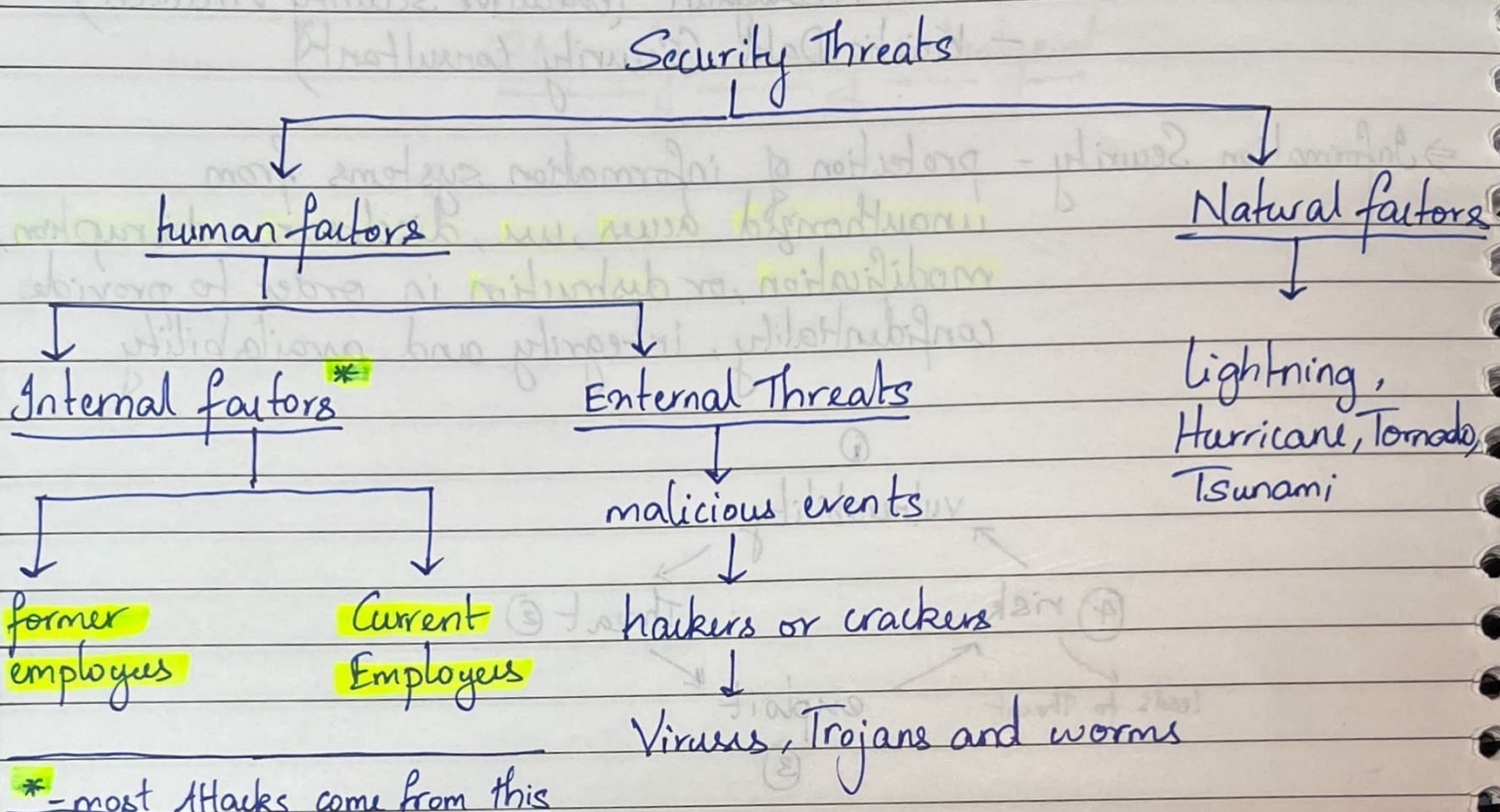
Notable instructors' names – Kennuth Gonzalez (pen tester)
– John Mclaughlin (executive Security Architect)
– Kristin Dahl (Security Consultant)

⇒ Information Security – protection of information systems from unauthorized acess, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity and availability.



① – A flaw, loophole, oversight or error that can be exploited to violate system privacy
② – event, natural or man-made, able to cause negative impact to an organization
③ – defined way to breach the security of an IT System through a vulnerability
④ – situation involving exposure to danger.

⇒ Security Threats



* - most Attacks come from this

⇒ Vulnerability Assessment - search for weaknesses/exposures in order to apply a patch or fix to prevent a compromise.

⇒ Roles in information Security

- CISO (chief information Security officer)
- Information Architect
- I.S Consultant
- I.S Analyst
- I.S Auditor
- Security Software Developer
- Pen tester / ethical hacker
- Vulnerability Assessor
- Digital forensic Analyst

Cyber Crime - $100 Billions (US)
Cyber Attacks - $400 Billions (yearly worldwide)
Data lost Cost - $2.1 Billions (2019)

→ Most frequently targeted industries (2022)
- Business
- Healthcare
- Banking/financial
- Government/military
- Education
- Energy/Utilities

→ (2018)
- finance and Insurance
- Transportation
- professional services
- Retail
- ~~Marketing~~
- Manufacturing
- Media
- Government
- healthcare
- Education
- Energy

→ Malicious Domain Categories
- 77% spam
- 8% Computer Crime + Hacking
- ~~8%~~
- 5% malware
- 5% phishing
- 4% Botnet C2 Server

⇒ How to start a cyber security program ?

- Security program (evaluate, create teams, baselines, identify and model threats, risk monitoring and control)
- Asset manage (classification, implementation steps, asset Control, documents)
- Admin Controls (policies, procedures, standards, user education, incident- respond, disaster recovery, physical security)
- Tech Controls (Network infra, endpoints, Servers, vulnerability management, monitoring and Logging)

⇒ Computer Security challenges
- Security not as simple as it seems ✓
- Solutions can be Attacked themselves ✓
- protection of enforcement structure can complicate solutions. ✓

M T W T F S S

Page No.: YOUVA

Date:

⇒ Critical thinking is controlled, purposeful thinking directed toward a goal.

⇒ Cybersecurity - The technical skills

- Intrusion detection ✓
- Reverse engineering ✓
- programming ✓
- Virtualization ✓
- Cryptography ✓
- Networking ✓
- Operating Systems ✓
- Database Modeling ✓

↳ Critical thinking - 5 key skills

⇒ Challenge Assumptions : systematically list and challenge
: Refine as you learn more

⇒ Consider Alternatives : Brainstorm full range of possibilities
: Break into Components
: 5 w questions and how?

⇒ Evaluate data : Crux of the scientific method
: Does the data fit your hypothesis?

⇒ Identify Key Drivers : What are the driving forces at play?
: this can help you identify the future

⇒ Understand Content : MOST IMPORTANT!
: put yourself in other's shoes - reframe problem

*

The art of war teaches us to rely not on the likelihood of the enemy's not coming, but on our readiness to receive him; not on the chance of his not attacking, but rather on the fact that we have made our position unassailable. (not predictable)

– The art of war. Sun Tzu

⇒ 4 types of actors

- Internal
- Hackers
- Hacktivists (political action and movements)
- Government

P.T.O

M T W T F S S
Page No.:
Date:
YOUVA

W2
06/09/2022

⇒ Government hackers
- The Tailor Access Operation (US)
- NSA (US)
- 61398 (Israel)
- Unit
  - Unit 8200 (China)

⇒ Tools and Attacks

- SeaDaddy and SeaDuke (Cyberbears US Election)
  - Generate backdoors into party committee to access mails, documents for 6 months
- BlackEnergy 3.0 (Russian Hackers)
  - Used to exploit vulnerabilities on SCADA*, PLCs** or ICS** Systems. (Used on power plants, nuclear or water plants)
- Shamoon (Iran Hackers)
- Dougu and Flame (Olympic Games US and Israel)
- DarkSeoul (Lazarous and North Korea)
- WannaCry (Lazarous and North Korea)

  - exploit infra and data ← from other businesses, personal information, etc

* enables automation of industrial processes by capturing operational technology. (Supervisory Control and data acquisition)

** programmable logic Controller - industrial computers used to control different elutro-mechanical processes for use in manufacturing, plants, or automation environments.

*** Industrial Control system - supports industrial processes.

⇒ Attack Classifications

- passive Attacks
  - eavesdropping styles of Attacks
  - traffic Analysis

→ goal ! (detection) !

- Active Attacks
  - Explicit interception and modification
  - Several classes of these Attacks exist
    - masquerade (masking/pretending) - MITM
    - Replay
    - Modification (fails integrity)
    - Denial of Service (message never gets through)

mechanisms used to provide security

⇒ Security Services - gives specific kind of protection to system resource
- Security services implement security policies
- implemented by security mechanisms.
- counter security attacks, secures data processing
- replicates functions found in physical docs.

- X.800 - service provided by protocol layer of communicating open systems, ensures adequate security of systems or data transfers.
- RFC 2828

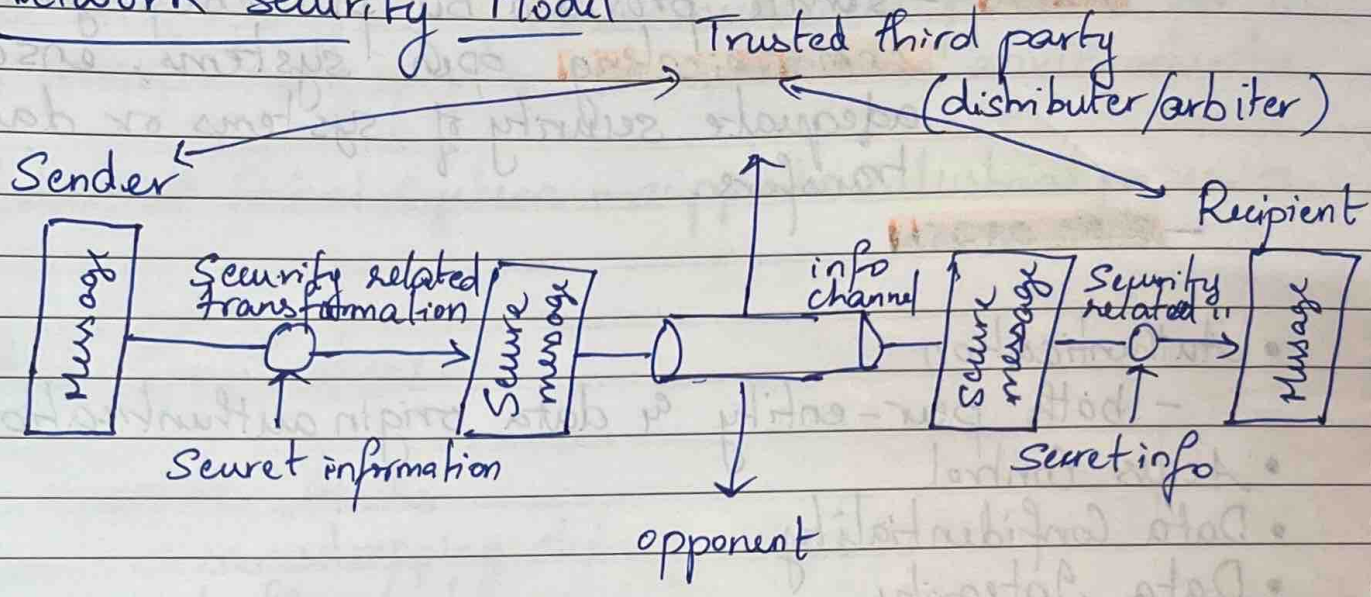
- Authentication
  - both peer-entity & data origin authentication
- Access Control
- Data Confidentiality
- Data Integrity
- Non-Repudiation
- Available

technical

⇒ Security Mechanism (~~security~~ implementation of security policy)
- use security service to enforce security policy.
- implement a specific security policy.

- Specific Security mechanisms - crypto, digital signatures, auss controls, data integrity, authentication exchange, routing control, notarization
- Pervasive Security mechanisms - Trusted functionality, security labels, event detection, security audit trials, security recovery.
- passive security mechanism -

⇒ Network Security Model



⇒ Security Architecture - What needs to be protected?

a) information and data (ex: passwords)
b) communication and data processing services
c) equipment and facilities.

↳ Threats: a) destruction of infor/resources
b) corruption or modification of info
c) theft, removal or loss of info/resources
d) disclosure of info
e) interruption of services.

↳ Attacks: As discussed earlier (passive)
a) Active Attack
- Replay → attack on integrity of system's data (due to its untimely manner - delay/modified)
- DoS → attack on availability

⇒ Malware - Software used to disrupt computer or mobile operations, gather sensitive info, gain acess to private computer systems, or display unwanted ads.

↳ Types : a) Virus (require human interaction to replicate)
b) worms (self replicating malware) (cripples resources and turns computers into zombies)
c) Trojan Horses (hidden malware that damages system)
d) spyware (track and report usage, collect data, browsing history, etc)
e) Adware (code that automatically displays or downloads unsolicited ads)
f) RATs (Remote Acess Trojans - allows to gain unauthorized acess to computer)
g) Rootkit (software intended to take full or partial control of system at lowest level)

• Botnets - set of compromised hosts that enables attackers to exploit computer resources.

h) Key loggers
i) Logic Bombs (triggers at a particular time)
j) APTs (acess and monitor to network to steal info)

⇒ How do we protect against threats?

↳ Technical:
- a) Anti Virus
- b) IPS, IDS, UTM
  - inter operation
  - intrusion detection
  - unified threat management
  } systems
- c) Updates ☺

↳ Administrative:
- a) Policies (password policy)
- b) Training (social engineering training)
- c) Revisions and tracking (everything above are up to date)

⇒ Internet Security threats

→ Mapping: case the joint - find servies implimented on network
: Use ping to determine what hosts have addresses on network
: port Scanning (establish TCP Connection to each port in sequence)

↳ Countermeasures: record traffic entering network
: look for suspicious activity (IP addr, ports)
: Use host scanner and keep inventory of hosts

→ packet Sniffing : promiscuous NIC reads all packets

→ IP Spoofing : generate bogus IP packets (masquerading)
↳ countermeasures : shouldn't forward outgoing packets with invalid source address → ingress filtering

→ Denial of Service (DoS) : flood of packets to swamp receiver.
: DDos — multiple coordinated sources swamp reciever
↳ Countermeasures : filter out packets before reaching host
: traceback to source of floods (most likely an innocent, compromised machine)

→ Host insertions : insider threat, ie, computer 'host' with malicious intent is inserted in sleeper mode on the network
↳ Countermeasures : accurate MAC address inventory
: match discoverable hosts against inventory
: missing hosts are OK.
: new host are NOT OK.

→ Rogue Software process : inserted into host intentionally
: network traffic monitoring
: Exfiltration of sensitive data

⇒ Phases of intrusion kill chain

Reconnaissance
↓
Weaponization
↓
Delivery
↓
Exploitation.
↓
Installation
↓
Command & Control
↓
Actions on Objective

⇒ Phishing → Open Source Phishing framework - GoPhish
↳ Vishing → call phishing

⇒ Books for CyberWar (Websites included)
↳ Countdown to Zero day
↳ CSIS.org

M T W T F S S
Page No.: YOUVA
Date:

W3

⇒ CIA TRIAD

07/09/2022

C → Confidentiality (prevent disclosure of data without prior auth)
I → Integrity (data or its metadata isn't modified by unauthorized entity)
A → Availability (availability of data when needed)

↳ implementations : RAIDs (multiple drives)
: Clusters (maintain different set of servers)
: ISP Redundancy (backup/second internet)
: Backups (data backups for restoration)

Non-Repudiation : valid proof of identity of data sender or reciever

↳ implementations : Digital Signatures
: Logs

Access Management : Access Criteria
- Groups (different groups with diff perms)
- Time frame and specific dates (time specific accessibility only)
- Physical location (specific location accessibility)
- Transaction type (specific perms, ie only read or only write, etc)

: Need to know
- Just access information needed for that role

: Single Sign-on (SSO)
- One time login process

Authentication : Identity proof - username ensures identification
: ~~Kerberos~~ (SSO) - password gives authentication

: Kerberos (SSO)
- protocol used to implement SingleSign On.

: Mutal Authentication
- MS-CHAP v2 (between systems : rely on secret key)

: Security ID in Active Directories
- ID given to objects and objects that uniquly identifies a person or objet.

: Discretionary Acuss Control List
- User provides Acuss perms to files or objects.

⇒ Incident Response

- managment procuss that involves monitering and dituction of security events on a computer or computer network and emuution of proper resources to those events.

- Key Components → • Event : observed change to normal behaviour, en: firewall policy pushed.
• Incident : event that negatively effects CIA at an orgonization
• Response team : team that ~~reports~~ recieves report of security breaches, conducts analysis of

reports and responds to sender.
CSIRT may be an established group or an ad hoc assembly.

[computer security [I.R.T]]

necessary

- Investigation: seeks to determine circumstances of incident. Every incident warrants or require investigation. Collect evidence. Keep in mind the chain of custody

Key Concepts →

- E-Discovery: helps to get current tech status of data, systems and info in our network. helps to understand how to control data retention and backup

- Automated Systems: Using SIEM, SOA, Splunk, Qradar, ArcSight, user-behaviour analysis, honeypots, AI, etc. These enhance to detect and control incidents that could compromise the tech environment.

- BCP and Disaster Recovery: Business continuity plan must be implemented in order to prevent or guide IRT and the entire organization. good to have clear understanding of

critical Business areas.
Disaster recovery is the process needed to implement or follow in order to be able to recover all areas if disaster occurs.
↓
cyberattacks

- Post Incident : Root cause analysis, understand difference between error, problem and isolated incident.
  Reports → Key !

⇒ Incident Response processes

phase 1 → prepare :
- conduct critical assessment for org
- Carry out cyber security threat Analysis
- Consider implications of people, process tech and info
- Create an appropriate control framework
- Review state of readiness in C.S incident response.

Phase 2 → Respond :
- Identify cyber security incident
- Define objectives and investigate situation
- Take appropriate action
- Recover data, systems and connectivity.

phase 3 → follow up:
- investigate incident more thoroughly
- Report incident to stakeholders
- Carry out post incident review
- Communicate and build on lessons learned
- Update key info, controls and processes
- perform trend Analysis.

!! Top 3 cost reducing factors — Incident Response Team
- Extensive use of encryption
- Employee Training.

⇒ Audits

- Define audit scope and limitations
- look for info, gathering info
- Do the audit
- feedback based on findings
- Deliver a report
- Discuss the results.

⇒ IT Governance plans
- ~~Strategy~~
- Tactical plans
- Policies
- Audits
- Governance

⇒ Pentest - Ethical Hacking (simulating attacks on Computer system or network)

↳ MILE2 CPTE TRAINING ⇒ Footprinting
↓
Scanning
↓
Enumeration
↓
Penetration
(failed) → Denial of Service Attack
(successful) → Privilage escalation
↓
Data manipulation
↓
Cover Tracks
↓
Leave Back doors

Offensive Security Scan

⇒ OWASP Top 10 Report gives all information about the Vulnerabilities.

Top 10 → Open Web Application Security Project

M T W T F S S
Page No.: YOUVA
Date:

W4

07/09/2022

⇒ Firewalls

- isolates organization's internal net from larger Internet, allowing some packets to pass, blocking others.
  - prevents DoS Attacks
  - prevent illegal modification/accus of internal data.
  - allow only authorized accus to inside network
  - two types of firewalls:
    - → application-level
    - → packet-filtering

↳ Packet filtering

- scans all packets (or filter)
- internal network connected to Internet via router firewall
- router filters packet-by-packet, decision to forward/drop packets based on:
  - source IP, destination IP
  - TCP/UDP source and destination port no.s
  - ICMP message type
  - TCP SYN and ACK bits

↳ Application gateway

7th layer of OSI

- filters packets on application data as well as on IP/TCP/UDP fields.

eg: Allow select internal users to telnet outside. (through gateway)

↳ limitations: IP spoofing, client software must know how to contact gateway,

↳ XML Gateway ∞

[Convuntional] ↑ firewall without inspection.

- XML traffic passes through
  - across normal 'web ports'
- XML gateway examins payload of XML mussage
  - no executable code.
  - Target IP makes sense
  - Source IP is known

↳ 2 types → stateless firewalls ①
→ stateful firewalls ②

→ ①
- paket filter (AKA)
- filters paikets based on layer 3 and 4 (IP and port)
- less secure.

→ ②
- State tables that allow firewall to compare current paikets with previous one
- slower but secure
- Application firewall make decision based on layer 7.

→ Proxy firewall

- acts as intermediary servers
- terminate connections and initiate new ones (like MITM)
- 2 'three-way' handshakes between 2 devices

⇒ Anti Virus / Antimalware

- detect, prevent and destroy virus or malware.
- user malware definitions (to be compared to search for matches)

⇒ Cryptography

- stream cipher encrypt or decrypt bit per bit
- Block cipher encrypt or decrypt in blocks or several sizes.

↳ 3 types - Symmetric Encryption ①
Asymmetric Encryption ②
Hash functions ③

① • same key to encrypt and decrypt
• bigger key - stronger
• ex: DES, Triple DES, AES

② • uses 2 keys
• public key and private key.
• one for encryption, one for decryption
• one-way algo used to generate 2 keys.
• slower than ①
• ex: HTTPs website

③ • uses an algo and no key.
• plaintext is hashed
• hash changes, plaintext also changes (integrity check)
• SHA-1, MD5 - prone to collisions (old algos) (2 different P.T having same hash - collision)
• SHA-2 - newer and recommended.

⇒ Cryptographic Attacks

millions of previously recorded data

- Brute force (based on trial and error)
- Rainbow tables (likewise to brute force using limited info)
- Social engineering
- known plaintext
- known Ciphertext

↳ Symmetric key crypto: DES (Data Encryption Standard)

- 56-bit symmetric key
- 64-bit plaintext input → ingests text in 64 bit chunks
- Use 3 keys sequentially (3-DES)
- Use cipher block chaining

: AES (Advanced Encryption Standard)

- process data in 128 bit blocks
- 128, 192 or 256 bit keys
- brute force takes 149 trillion years for AES.

⇒ Hackers

- White hat : work done under contract for security reasons
- Grey hat : look for vulnerabilities in an unauthorized manner and report back to possible victim
- Black hat : personal agenda

⇒ Pentest Methodologies

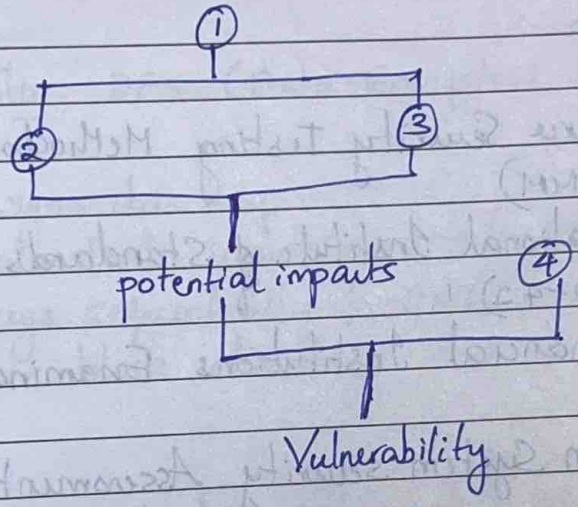
- Open Source Security Testing Methodology Manual (OSSTMM)
- NIST National Institute of Standards and Technology (SP 800-42)
- Federal financial Institutions Examination Council (FFIEC)
- Information System security Assessment framework (ISSAF)

↳ pen testing execution

- pre-engagement interations
- Intelligence gathering
- Threat Modelling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

⇒ Vulnerability Assessment test

1) Identify indicators
2) Exposure
3) Sensitivity
4) Adaptive capacity



⇒ Digital forensics

- includes identification, recovery, investigation, validation and presentation of facts regarding digital evidence found on computers or digital storage media devices.

↳ **Tools** : Hardware
- Faraday Cage (block magnetic fields)
- forensic Laptops, tool sets, digital camera, Case folder, empty hard drives, ~~Hardware~~ write blockers

~~Hardware~~ → hardware

: **Software**
- Volatility
- FTK
- Enlax
- dd (bit by bit copier)
- Autopsy
- Bulk extractor, etc..

→ **Notable website**

- **Securityintelligence.com** – to review all up to date info contributed by cyber security experts globally.