No.	Teacher's Sign / Remarks

Exam Title -> Certified Ethical Hacking (CEH)
Exam Code -> 312-50
Availability -> EC-Council Exam portal, VUE
Duration -> 4 hours
Questions -> 125 (MCQ)
Passing Score -> 100

Table of Contents

		Number of question		
724	1. INtroduction to Ethical Hacking	8	->	6%
554	2. Footprinting and Reconnaissance	10	}	21%
777	3. Scanning Networks	10		
777	4. Enumeration	6		
139	5. Vulnerability Analysis	9	}	17%
525	6. System Hacking	6		
281	7. Malware Threats	6		
240	8. Sniffing	3	}	14%
149	9. Social Engineering	5		
185	10. Denial-of-Services	2		
113	11. Session Hijacking	3		
295	12. Evading IDS, Firewall, and Honeypots	5		
107	13. Hacking web Servers	8	}	16%
321	14. Hacking web Applications	8		
83	15. SQL injection	4		
266	16. Hacking wireless Networks	8	->	6%
352	17. Hacking Mobile platforms	4	}	8%
372	18. IOT and OT Hacking	6		
181	19. Cloud Computing	7	->	6%
471	20. Cryptography	7	->	6%
		125Q		100%

8M

Introduction

★ Fundamental Security Concepts

- The whole principle is to avoid Theft, Tampering and disruption of the systems through CIA Triad. (Confidentiality, Integrity and Availability).

Security Triad

- These three concepts are termed as CIA triad to represent fundamental security objective for data and information services shown in below diagram.

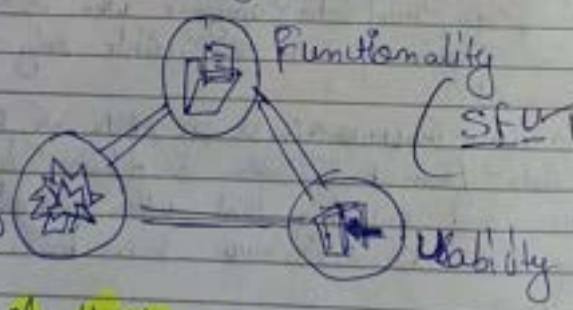
- Confidentiality - Keeping system and data from being access, seen, read to anyone who is not authorized to do so. Information is accessible only to the autorized personnel.
- Integrity - Trustworthiness of data or Resources: protect the data from modification or deletion by unathorized parties, and ensuring that when authorised people make change that should have been made the damage can be undone.
- Availability - Accessible when Required by Authorized users: System, access channels and authentication mechanisms must all be working probably for the information they provid and protect to be available when needed.

Note - In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved.

- Authenticity - Refers to the characteristic of a communication, documents, or any data that ensure the quality genuine.
- Auditing & Accountability Basically keep tracking of everything, like, who's been logging in when are logging in whose access this data.
- Non-Repudiation - Non-Repudiation is the assurance that someone cannot deny the validity of something. Non-repudiation is a legal concept that is widely used in information security and refers to a service, which provides proof of the origin of data and the integrity of the data.

★ Security, functionality and usability balance

- There is an inter dependency between these three attributes. When ~~someone~~ security gossip, usability and functionality come down. Any organization should balance between these qualities to arrive at a balanced information system.



(SFU triangle)

★ Type of Hackers

- Blackhat, - Greyhat, - Whitehat
- Script Kiddie, - State Sponsored Hacker, - Hacktivist

- Black Hat - Hackers that seek to perform malicious activities.
- Gray Hat - Hackers that perform good or bad activities but do not have the permission of the organisation they are hacking against.
- White Hat - Ethical hackers. They use their skills to improve security by exposing vulnerabilities before malicious hackers.
- Script Kiddie/ Skiddies - unskilled individual who use malicious script or programs, such as web shell developed by other to attack computer system and network and deface website
- State-Sponsored Hacker - Hacker that is hired by a government or entity related.
- Hacktivist - Someone who hacks for a cause; political agenda.
- Suicide Hackers - Are hackers that are not afraid of going jail or facing any sort of punishment. Hack to get the job done.
- Cyberterrorist - Motivated by religious or political belief to create fear or disruption.

* Hacking Vocabulary

- Hack Value - Perceived value or worth of a target as seen by the attacker.
- Vulnerability - A system flaw, weakness on the system (on design implementation etc).
- Threat - Exploit a vulnerability.
- Exploit - Exploit are a way of gaining access to a system through a security flaw and

taking advantage of the flaw for their benefit

- payload - Component of an attack; is the part of the private user text which could also contain malware such as worm or Viruses which performs the malicious action; deleting data, sending spam or encrypting data.
- Zero-day attack - Attack that occurs before a Vender knows or is able to patch a flaw.
- Daisy Chaining / pivotting - It involves gaining access to a network and/or Computer and then using the same inform to gain access to multiple network and Computers that contains desirable information.
- DoXXing - publishing PII about an individual usually with a malicious intent.
- Enterprise information security Architecture (EISA) - determines the structure and behavior of organization's information system through processes, requirements, principles and models.

* Threat Categories

Network Threats

- Information gathering
- Sniffing and eavesdropping
- DNS / ARP poisoning
- MITM (Man-in-the Middle)
- DoS / DDoS
- Password-based attacks

- Firewall and IDS attack
- Session Hijacking

Host threats
- Password Cracking
- Malware attacks
- Footprinting
- profiling
- Arbitrary Code execution
- Backdoor access
- Privilege Escalation
- Code Execution

Application Threats
- Injection Attacks
- Improper data/input Validation
- Improper error handling and exception management
- Cryptography issues
- SQL injection
- Phishing
- Buffer Overflow
- ~~Phishing~~
- Information disclosure
- Security Misconfigurations.

* Attack Vectors
path by which a hacker can gain access to a host in order to deliver a payload or malicious outcome.

- APT - Advance persistent threats
  - An advance persistent threat is a stealthy threat is ~~a stealthy~~ actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period; typically uses zero day attacks.

- Cloud Computing / Cloud based technologies
  - Flaw in one client's application cloud allow attacks to access other client's data.

- Viruses, worms, and malware
  - Viruses and worms are the most prevalent networking threat that are capable of infecting a network within seconds.

- Ransomware
  - Restricts access to the computer system's files and folders and demand an online ransom payment to the attacker in order to remove the restriction

- Mobile Device threats.

- Botnets
  - Huge network of compromised system used by an intruder to perform various network attacks.

- Insider attacks
  - Disgruntled employee can damage assets from inside.
  - Huge network of compromised hosts. (used for DDoS)
- Phishing attacks
- Web Application ~~Attacks~~ threats
  - Attack like SQL injection, XSS (cross-site scripting)
- IOT threats

* Attack types

1. Operating system
   Attack targeting OS flaws or security issues inside such as guest accounts or default passwords.
   - Vectors: Buffer overflows, protocol implementations, software defects, patch levels, authentication schemes
2. Application Level
   Attack on programming code and software logic
   - Vectors: Buffer overflow, Bugs, XSS, DoS, SQL injection, MITM.
3. Misconfiguration
   Attack takes advantage of system that are misconfigured due to improper configuration or default configuration.
   - Examples: Improper permissions of SQL users; Access list permit all.

4. Shrink-wrap Code
Act of exploiting holes in unpatched or poorly-configured software.
- Examples: Software defects in Version 1.0; Defect in examples CGI Scripts; Default passwo

* Vulnerabilities

- CVSS - Common Vulnerability Scoring System
  - Places numerical score based on severity.
- CVE - Common Vulnerabilities and Exposures
  - Is a list of publicly disclosed Vulnerabilities and exposures that is maintained by MITRE.
- NVD - National Vulnerabilities Database
  - Is a Database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Govt. Vulnerabilities repository.

* Vulnerability Categories

- Misconfiguration - improperly configuring a service or application.
- Default installation - failure to change setting in an application that come by default.
- Buffer overflow - Code execution flaw.
- Missing patches - Systems that have not been patched.

- Design flaw - flaw inherent to system design such as encryption and data Validation.
- Operating System Flaws - flaws specific to each OS
- Default passwords - leaving default password that come with system/application.

* Pen-Test phases (CEH)

1 Pre-Attack phase - Reconnaissance and data-gathering.

2 Attack phase - Attempts to penetrate the Network and execute attacks.

3 Post-Attack phase - Cleanup to return a system to the pre-attack condition and deliver reports

Note: (for the exam, EC-Council brings his own methodology and that's all you need for the exam, you can check another pentesting methodolies)

* The five Stages of Ethical Hacking

1 Reconnaissance
Gathering evidence about target; there are two type of Recon:

> passive Reconnaissance: Gain information about targeted computer and Network without direct interaction with the Systems.
e.g: Google Search, Public records, News releases, Social media, Wardrive scanning networks around.

* Active Reconnaissance : Envolves direct interaction with the target.
e.g: Make a phone call to the target, Job interview; tools like Nmap, Nessus, OpenVAS, Nikto and Metasploit can be considered as Active Recon

2. Scanning & Enumeration
obtaining more in-depth information about targets.
e.g: Network scanning, port scanning, which version of services are running.

3. Gaining Access
Attacks are lauched in order to gain access to a system.
e.g: Can be done locally (offline) over a LAN or over the internet
e.g: Spoofing to exploit the system by pretending to be a legitimate user on different system, they can send a data packet containing a bug to the target system in order to exploit a vulnerability.
- Can be done using many techniques like command injection, buffer overflow, DoS brute forcing credentials social engineering, misconfiguration etc

4. Maintaining Access
Them put in place to ensure future access.
e.g: Rootkit, Trojan, Backdoor can be used.

5. Covering Tracks
Steps taken to Conceal Success and Intrusion; Not be noticed.
e.g: Clear the logs; obfuscate trojans or malicious backdoors programs.

★ Three types of Active Defense

1. Annoyance
Involves tracking a hacker and leading him into a fake Server wasting his time - and making him easy to detect.

2. Attribution
Identify an attacker; uses tools to trace the Source of an attack back to a specific location, or even an individual hacker.

3. Attack
That is most Controversial. To "hack back", a company accesses an alleged hacker's Computer to delete its data or even to take revenge. Both of these steps are Considered illegal.

★ Information Assurance (IA)
Refers to the assurance of the integrity Availability, Confidentiality, and authenticity of information and information Systems during usage, processing, Storage and transmission of information.

* Processes that help achieving IA:
- Developing local policy, process, and guidence.
- Designing network and user authentication strategy
- Identifying network vulnerabilities and threats (Vulnerabilities assessment outlines the security posture of the network)
- Identifying problems and resource requirements
- Creating plan for identified resource requirements
- Applying appropriate IA Controls
- performing C&A (Certification and Accreditation) process of information system helps to track vulnerabilities, and implement safety measures.
- providing information assurance training to all personnel in federal and private org.

* Information Security Management program
Combination of policies, processes, procedures, standards, and guidelines to establish the required level of information security.
- Designed to ensure the business operates in a state of reduced risk
- It encompasses all organizational and operational processes and participants relevant to information security.

Note:- IA focuses on risk assessment, mitigation side of things. Infosec focuses on actually implementing security measures to safeguard system.

Security Policy				Governance	Compliance
Roles & responsibilities		Security Guidelines & Procedures			
Risk Management	Technical Security Architecture	Assets Classification	Security Management and operation		
Business Resilience					
Business Continuity Management		Disaster Recovery			
Training & Awareness					
Security Metrics & Reporting					

* EI
- set that orga
- Goal
- Help
- Dete
- Prio
- Help
IT a
- Cost such

* Phys
- Prev
e.g:
- Detec
e.g:
- Deter
e.g:
- Reco
e.g:
- Comp

★ EISA - Enterprise Information Security Architecture

- set of requirements, process, principles, and models that determines the structure and behavior of an organisation's information security.

• Goals of EISA
- Help in monitoring and detecting network behaviors
- Detect and recover from security breaches
- Prioritizing resources of an organisation
- Help to perform risk assessment of an organisations IT assets.
- Cost prospective when incorporated in security provisions such as incident response, disaster recovery event correlation

★ Physical Security Controls

• Preventive Control ⇒ Deters the actor from performing the threat
e.g: Fence, Server Locks, Mantraps etc.

• Detective Control ⇒ Recognizes an actor's threat.
e.g: Background check, CCTV.

• Deterrent Control ⇒ Deters the actor from attempting the threat.
e.g: Warning sign.

• Recovery ⇒ Mitigates the impact of a manifested threat.
e.g: Backups

• Compensating Control ⇒ provides alternative fixes to

any of the above function.

- Most of security Controls are preventive phase Controls

Δ • Defense in Depth ⇒ Multiple layers of security Controls failure.

e.g: Image below.

★ Types of Security Controls

Description	Examples
Physical	Guards, light, Cameras, fire extinguishers, flood protection.
Administrative	Training awareness, policies procedures and guidelines to infosec.
Technical	IDS / IPS, Firewall, Encryption Smart Cards, Access Control lists

Description	Examples
preventative	authentication, alarm bells
Detective	audits, backups
Corrective	restore operations

★ Mana
- Risk
occur
dama
impact

★ Risk
- A r
define
of
of
• This
of r

★ Risk
- Is t
risks
of
proba
maxim

★ Phase

★ Managing the Risk

- Risk can be defined as a probability of the occurrence of a threat or an event that may damage, or cause loss or have other negative impact either from internal or external liabilities.

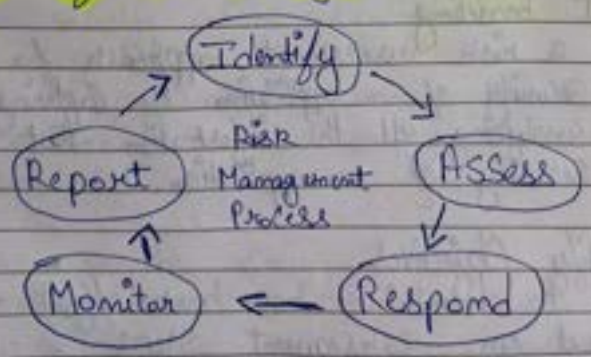
★ Risk matrix

- A risk matrix is used during risk assessment to define the level of risk by considering the category of probability or likelihood against the category of consequence severity.
- This is a simple mechanism to increase visibility of risks and assist management decision making.

★ Risk Management

- Is the identification, evaluation, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability or impact of unfortunate events or to maximize the realization of opportunities.

★ Phases of Risk Management



Risk Identification.
- Identification the Sources, Causes, Consequences of the internal and external risks.

Risk Assessment
- Assessment the Org. Risk and provides an estimate on the likelihood and impact of the risk.

Risk treatment
- Selects and implement appropriate Controls on the identified risks.

Risk tracking
- Ensures appropriate Control are implemented to handle risks and identifies the chance of a new risk occurring.

Risk review
- Evaluates the performance of the implemented risk management Strategies

★ Threat modeling
- Is a risk assessment approach for analyzing the Security of an application by Capturing, organizing and analyzing all the information that affects the Security of an application.

1. Identify Objectives
Helps to determine how much effort needs to be put on Subsequent Steps.

2. Application overview
- Identify the components, data flows, and trust boundaries

3. Decompose Application
- Find more relevant details on threats

4. Identify threats
- Identify threats relevant to your control scenario and context using the information obtained in Step 2 and Step 3

5. Identify Vulnerabilities
- Identify weaknesses related to the threats found using Vulnerability Categories.

★ Security policies

1. Policies - High-level statements about protecting information; Business rules to safeguard CIA triad; Security policies can be applied on users, system, partners network and providers.

• Common security policies examples :-

Password policy
• Meet the password complexity requirements.
• e.g: Minimum 8 char length, upper and lower case and alphanumerical.

Wireless security policy.

AUP - Acceptable use - policy
• How to properly use company's assets
• e.g: "Do's and Don't's" with company computer.

Data Retention policy
- e.g: kep the data for X time.

Access Control policies
- e.g: Accessing Servers; firewalls

2. Procedures - Set of detail steps to accomplish a goal; Intructions for implementation

3. Guidelines - Advice on actions given a situation; Recommended, not mandatory

★ Security policy - Examples

Access Control policy
This defines the resources being protected and the rules that Control access to them.

Remote Access policy
This defines who can have remote access and defines access medium and remote access security controls.

Firewall management policy
This defines access management and monitoring of firewalls in an organization.

Network Connection policy
This defines who can install new resources on the network, approve the installation of new device

document network changes etc.

Password policy
This define guidelines for using strong password protection on available resources.

user Account policy
This defines the account creation process, authority, rights and responsibility of user accounts.

Information protection policy
This defines the sensitivity levels of information, who may have access, how it is stored and transmitted, and how it should be deleted from storage media etc

Email security policy
This policy is designed to govern the proper usage of corporate email.

Acceptable use policy
This defines the acceptable use of system resources.

★ Security policy — Types

1. Promiscuous policy — This policy usually has no restrictions on usage of system resources.

2. Permissive policy — This policy beings wide open and only know dangerous service/attacks or behavior are blocked. This type of policy has to be

update regularly to stay effective.

3. Prudent policy – This policy provides maximum security while allowing known but necessary dangers. This type of policy will block all services and only safe/necessary services are enabled individually. Everything is logged.

4. Paramoid policy – This policy forbids everything. No Internet connection or severely restricted Internet usage is allowed.

★ Security policy – Creation Steps

1. Perform a Risk Assessment
2. Use Security Standards and Frameworks as guid
3. Get management and staff input
4. Enforce the policy. Use penalties for non-compliance.
5. Publish final draft to entire org.
6. Have all staff read/sign that they understood policy
7. Employ tools to help enforce policy
8. Staff training
9. Review and update regularly

★ Incident Management process

- An incident is an event that could lead to loss of, or disruption to, an organization's operations services or functions.

Incident management is a term describing the activities of an organization to identify, analyze, and correct hazards to prevent a future re-occurrence.

1. Preparation: Select people, assign rules, define tools to handle the incident.
2. Detection & Analysis: Determine an incident has occured (IDS, SIEM, AV, Someone reporting etc)
3. Classification and prioritization
4. Notification: Identify minor and major incident; Who and How to notify an incident.
5. Containment: Limit the damage; Isolate hosts; Contact System owners.
6. Forensic Investigation: Investigate the root cause of the incident using forensic tools; System logs, real time memory, network device logs application logs, etc.
7. Eradicate & Recovery: Remove the cause of incident, patch if needed Recovery: get back into production; Monitor affected systems
8. Post-Incident Activities: Document what happen and why; Transfer knowledge.

* Incident Response Team Duties

1. Managing Security issues by taking a proactive approach towards the Customer's Security vulnerability
2. Developing or reviewing processes and procedures that must be followed
3. Managing the response to an incident and ensuring that all procedures are followed correctly in order to minimize and control the damage.
4. Identifying and analyzing what has happened during an incident including impact and threat
5. Providing a Single point of Contact for reporting security incidents and issues.
6. Reviewing change in legal and regulatory requirement to ensure that all processes and procedures are valid
7. Reviewing existing controls and recommending steps and technologies to prevent future incidents
8. Establishing relationship with local law enforcement agency, gov agencies, key partners and Suppliers.

★ SIEM – Security Information and event management

- Collects data points from network, including log files, traffic captures, SNMP messages, and so on, from every host on the network. SIEM can collect all this data into one centralized location and correlate it for analysis to look for security and performance issues, as well nagative trends all in real time.

Aggregation : Collecting data from disparate source and organizing the data into a single format. Any device within a SIEM system that collectes data is called collector or an aggregator.

Correlation : Its the logic that looks at data from disparate sources and can make determinations about events taking place on your network. (could be in-band or out-of-band, depending on the placement of the NIDS / NIPS).

- Alerts – for notification if something goes bad.
- Triggering – Exceeding thresholds.

Normalization : Will actually create multiple tables/ organize in such a way that the data can become more efficient and allows our analysis and report tools to work better.

WORM – Write Once Read Many : The concept being is that log files are precious,

and a lot of times you might want to look at them in an archival way, so that we can use optical media like WORM drive to store them.

★ **Most popular SIEM tools :-**

- → Splunk
- → ArcSight
- → ELK - Elastic Search, Log stash and kibana

★ **Identity and Access Management**

Identification, Authentication, Authorization, and Accounting work together to manage assets security.

Identification

The information on credentials ~~that~~ identifies the user.

Example : Your name, username, ID number, employee number, SSN etc.

Authentication

"Prove you are the legitimate user".

Should always be done with multifactor Authentication!

- Authentication factors :
  - = Something you know (Password)
  - = Something you have (Smart Card)

- Something you are (fingerprint)
- Something you do (android pattern ; manual signing)
- ~~Something~~ Somewhere you are (geolocation)

Note => Multi-/actore authentication generally uses two of this examples.
Ex - Something you know(1) and Something you have(2), never on Same Categery.

Authorization Concepts

what are you allowed to access - we use Access control models, what and how we implement depends on the organization and what our security goals are.

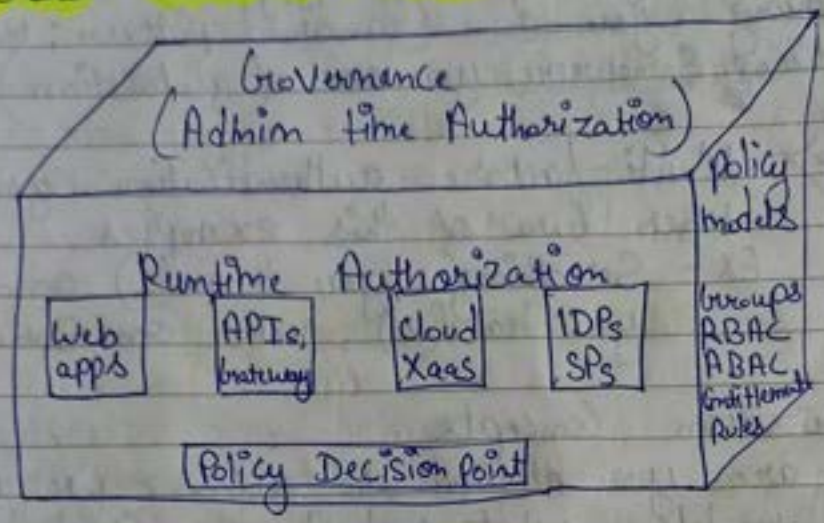
- Permissions :
  Applied to resources
- Right / privileges :
  Assign at system level
- Authorization Strategies :
  Least privileged
  Separation of Duties

Accounting

Trace an Action to a Subjects identity :

- Prove who/what a given action was performed by (non-repudiation) ; logging

★ Access Controls Models



⇒ Mandatory Access Control (MAC):

- Every object gets a label
  - Confidential, Secret, top Secret, etc
- The administrator decision who gets access to what Security level; users Cannot Change these Settings
- Used on old System (e.g: Top Secret Gov. information).

⇒ Discretionary Access Control (DAC):

- used in most OS
- Owner of the data defines access
- Very flexible access ~~defines~~ Control; Very weak Security.

=> Role - based Access Control (RBAC):

- Access to resources is defines by a set of rules defined by a role in your organization/job function (Manager, Director etc)

- Administrators provide access based on the role of the user
  - Rights are gained implicity instead of explicity

- In windows, use Groups to provide role - based access Control
  - e.g: Admin Group -> Right and perms,
  - Sales Group -> Right and perms

Note: "Access is defined by ACL Access Control List". implicity deny prevents access unless specifically permitted.

★ Data Loss prevention (DLP)

Data Loss prevention (DLP) is the practise of detecting and preventing data breaches, exfiltration, or unwanted destruction of sensitive data.
Organization use DLP to protect and secure their data and comply with regulations.

- The DLP term refers to defending organizations against both data loss and data leakage prevention.

Organization typically use DLP to:

- Protect personally identifiable information (PII) and comply with relevant regulations

- Protect Intellectual property critical for the organizations
- Achieve data visibility in large organizations
- Secure mobile workforce and enforce security in Bring your Own Device (BYOD) environments
- Secure data on remote cloud systems.

★ Data Backup

Data backup plays a crucial role in maintaing business continuity by helping org. recover from IT disasters, security breaches, application failures human errors etc.

All regulatory compliance such as COBIT, SSAE, SOC II, PCI-DSS, HIPPA, SOX, FISMA, GDPR etc. require business to maintain data backups of critical data for specified duration.

Backup Strategies

1. Identifying the critical business data
2. Selecting the backup media
3. Selecting a backup technology
4. Selecting the approprite RAID levels
5. Selecting an appropriate backup method

3 Backup methods

1) Cold backup
- Empty Site, no hardware, no data, no people
- It takes weeks to bring online.
- Basic office spaces (e.g building, chairs, AC....)
- No operational equipment
- Cheapest recovery site.

2. Warm backup
- Somewhere between Cold and hot just enough to get going (Big room with rack space, you bring the hardware).
- Hardware is ready and waiting - you bring the Software and data
- It takes days to bring online
- Operational equipment but little or no data.

3. Hot backup
- Exact replica of production systems
- Application and Software are Constantly updated
- Flip a Switch and everything moves
- It take hours to bring online
- Real - time Synchonization
- Almost all data ready to go - Often just a quick update
- Very expensive.

★ Pentration test - Basics

A pentration test, Colloquially know as a pen test, pentest or ethical hacking, is an authorized simulated Cyberattack on a Computer System, performed to evaluate the Security of the System.

Note ⇒ Not to be Confused with a Vulnerability assessm

- Clearly defined, full Scale test of Security Controls

- Phases
  - preparation ⇒ Contracts and team determined
  - Assessment ⇒ All hacking phases (reCannaissance, Scanning, attack, etc)
  - Post-Assessment - Reports & Conclusions

- Types
  - Black Box ⇒ Done without any knowledge of the System or network.
  - White Box ⇒ When the attacker have Complete knowledge of the system provided by the owner / target.
  - Gray Box ⇒ When the attacker has Some knowledge of the System and/or network.

★ Law C

- Crimin

- Civil

- Commo

★ Laws

OSST
"open
maintai

- Legisla

- Contra

- Standa

group
itself

- OSSTI
- OSSTM
1 Auther

2. Identifi

★ Law Categories

- Criminal - Laws that protect public Safety and usually have jail time attached.
- Civil - Private right and remedies.
- Common - Law that are based on Societal Customs.

★ Laws and Standards :

OSSTM Compliance

"open Source Security Testing Methodology Manual" maintained by ISECOM, defines three types of compliance

- Legislative - Deals with government regulations (Such as SOX and HIPAA).
- Contractual - Deals with industry/group requirement (Such as PCI DSS).
- Standards based - Deals with practices that must be followed by members of a given group/organization (Such as ITIL, ISO and OSSTMM itself).
- OSSTM Controls

- OSSTM Class A - Interactive Controls

1. Authentication - Provides for identification and authorization based on Credentials.
2. Identification - Provided Contractual protection against loss or damages.

3. Subjugation - Ensures that interactions occur according to processes defined by the assets owner.
4. Continuity - Maintains interactivity with assets if corruption of failure occurs.
5. Resilience - Protects assets from corruption and failure.

- OSSTM Class B - Process Controls
1. Non-repudiation - Prevents participants from denying its actions.
2. Confidentiality - Ensures that only participants know of an asset
3. Privacy - Ensures that only participant have access to the asset
4. Integrity - Ensures that only participants know when assets and processes change
5. Alarm - Notifies participants when interaction occur

★ PCI - DSS
"Payment Card Industry Data Security Standard" Standard for organizations handling Credit Cards, ATM Cards and other POS Cards.

★ ISO 27001
This international Standard has been prepared to provide requirements for establishing, implementing, maintaining and continually improving an information Security Management System.

★ ISO 2
Based
objective
industry

★ HIPAA
"Heath
a low
patient
between

SoX
"Sarbane
traded
and to

★ DMCA
"The D
enited
1996 t
organiz
-nation
to c
works

★ FISMA
"Federal
A law
Departm
-entation
agen

★ ISO 27002 And 17799
Based on BS799 but focused on security objective and provides security controls based on industry best practise.

★ HIPAA
"Heath Insurance Portability and Accountability Act" a law that set's privacy standards to protect patient medical records and health information shared between doctors, hospitals and insurance providers.

★ SOX
"Sarbanes - Oxley Act" Law that requires publicly traded companies to submit to independent audits and to properly disclose financial information.

★ DMCA
"The Digital Millennium Copyright Act" is a 1998 united states copyright law that implements two 1996 treaties of the World intellectual property organization. It criminalizes production and dissemi-nation of technology, devices, or service intentled to circumvent measures that control access to copyright works.

★ FISMA
"Federal information Security Modernization Ac of 2002" A law updated in 2004 of codify the authority of the Department of Homeland Security with regard to implem-entation of information Security policies. (for Gov. agencies)

★ NIST - 800 - 53
Catalogs security and privacy Controls for federal information system, Created to help implementation of FISMA.

★ FITARA
"Federal Information Technology Acquisition Reform Act" A 2013 bill that was intended to change the framework that determines how the US GoV purchases technology.

★ COBIT
"Control Object for information and Related Technology" IT Governance framework and toolset, Created by ISACA and ITGI

★ GLBA
"U.S Gramm - Leach - Bliley Act" Law that protects the Confidentiality and integrity of personal information that is collected by financial institutions.

★ CSIRT
"Computer Security incident Response Team" CSIRT provided a single point of Contract when reporting Computer Security incidents.

★ ITIL
"Information technology infrastructure Library" - An operational framework develop in the 80's that standardizes IT management procedures

★ Essen

★ OSI
• The

design
system
smalle

• The T
OSI
layers

Layer
7
6
5
4
3
2
1

★ Essential Knowledge

OSI Model and TCP Model

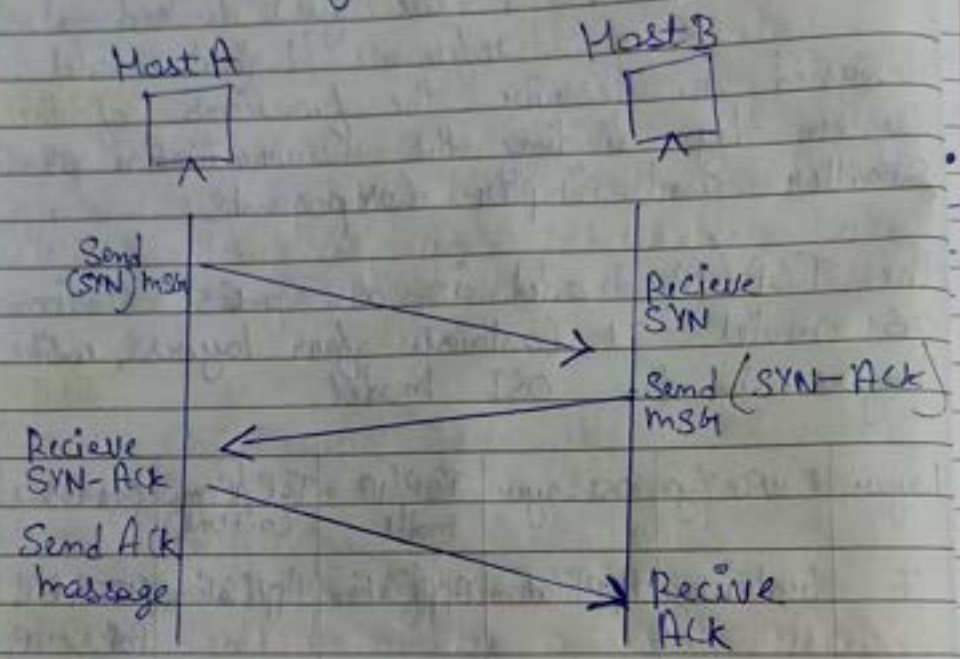
- The OSI Model - we just looked at is just a reference / logical model. It was designed to describe the functions of the communication system by dividing the communication procedure into smaller and simpler components.

- The TCP/IP model is a concise version of the OSI model. It contains four layers, unlike seven layers in the OSI model.

Layer	Device Type	OSI Layer	TCP/IP model	TCP/IP new (actual)	protocols	PDU
7	Gateway	Application	Application	Application	HTTP, FTP, PoP, SMTP, DNS, RIP	Data
6	-	Presentation	Application	Application	HTTP, FTP PoP, SMTP DNS, RIP, MIME	Data
5	-	Session	Application	Application	HTTP, FTP PoP, SMTP, DNS, RIP, SCP	Data
4	-	Transport	Transport	Transport	TCP/UDP	Segments
3	Router	Network	Internet	Network	IP, ARP, ICMP, IGMP	packets
2	Switch/ bridge	Data Link	Link	Data Link	Ethernet, Token Ring	frames
1	Hubs/ Repeater	physical	Link	physical	Ethernet, Token Ring	Bits

* TCP Handshake

The Three-way handshake



TCP Connection Establishment

* TCP Connection establishment process

1. Host A Sends out a SYN (Synchronize) packet with proposed initial sequence number to Host B.
2. Host B receives SYN message it returns a packet with both SYN and Ack flags (SYN-Ack) Set in the TCP header.
3. Host A recived the SYN-Ack, it Sends back Ack (Acknowlledgment) packet.
4. Host B recived Ack and at this stage the Connection is Established.

★ Port Numbers

- Internet Assigned Numbers Authority (IANA) - maintains Services Name and transport protocol port Number Registry which lists all port number reservations.

- Ranges
  - Well-known ports - 0 - 1023
  - Registered ports - 1024 - 49,151
  - Dynamic ports - 49,152 - 65,535

IMP

port Number	protocol	transport Protocol
20/21	FTP	TCP
22	SSH	TCP
23	Telnet	TCP
25	SMTP	TCP
53	DNS	TCP/UDP
67	DHCP	UDP
69	TFTP	UDP
80	HTTP	TCP
110	POP3	TCP
135	RPC	TCP
137-139	NetBIOS	TCP/UDP
143	IMAP	TCP
161/162	SNMP	UDP
389	LDAP	TCP/UDP
443	HTTPs	TCP
445	SMB	TCP
514	SYSLOG	UDP

- A services is said to be listening for a port when it has that specific port open
- Once a service has made a connection, the port is in an establish state

- Netstat command :
→ Shows open ports on computer
→ netstart -b displays executables tried to the open port (admin only)
→ netstart -an displays connection in numerical form.

★ Subnetting

IPv4 main address types
- unicast - acted on by a single recipient
- Multicast - acted on by members of a specific group
- Broadcast - acted on by everyone on the network.
  - Limited - delivered to every system in the Domain (255.255.255.255)
  - Directed - delivered to all devices on a subnet and use that broadcast address.

Subnet mask - determines how many address available on a specific subnets.
- Represented by three methods
  - Decimal - 255.240.0.0

- Binary - 11111111 . 11110000 . 00000000 . 00000000
- CIDR - X.X.X.X/12 (where X.X.X.X is an IP address on that range)

- If all the bits in the host field are 1s, the address is the broadcast.
- If they are all 0s, it's the network address
- Any other combination indicates an address in the range.

Reconnaissance and footprinting

* Footprinting

Footprinting is a part of reconnaissance process which is used for gathering possible information about a target Computer System or network. When used in the Computer security lexicon, 'Footprinting' generally refers to one of the pre-attack phases; tasks performed before doing the actual attack. Some of the tools used for footprinting are Sam Spade - nslookup traceroute, Nmap and neotrace.

* Footprinting Types: Active and pasive

Active - requires attacker to touch the device or network.
- Social engineering and other Communication that requires interaction with target

Pasive - measures to collect information from publicly available sources
- websites, DNS records, business information database

* Footprinting helps to:

Know security posture - The Data gathered will help us to get an overview of the security posture of the Company such as details about the presence of a firewall, security configurations of applications

Reduce Attack Area — Can identify a specific range of system and concentration on particular targets only. This will greatly reduce the number of systems we are focusing on.

Identify Vulnerabilities — we can build an information database containing the vulnerabilities, threats, loopholes available in the system of the target organization.

Draw Network map — help to draw a network map of the networks in the target organization showing topology, trusted routers, presence of server and other information.

★ Footprinting could be both passive and active. Reviewing a company's website is an example of passive footprinting, whereas attempting to gain access to sensitive information through social engineering is an example of active information gathering.
During this phase, a hacker can collect the following information (only high-level information) :-

- Domain name
- IP Addresses
- Namespaces
- Employee information
- Phone numbers
- E-mails
- Job information

Can be:

- Anonymous - information gathering without revealing anything about yourself
- Pseudonymous - Making someone else take the blame for your actions

- Competitive intelligence - information gathered by businesses about compe

- Alexa.Com - resource for statistics about websites.

★ Footprinting objectives

Network

- DNS
- IP networks
- Accessible systems
- Websites
- Access Control
- VPN Endpoints
- Firewall Vendors
- IDS Systems
- Routing/Router protocols
- Phone System (Analog/VoIP)

Organisat
- Org stru
- websites
- Phone nu
- Directory
- Office
- Company
- Business

Hosts
- Listening
- Operating
- Internet
- Enumera
- SNMP,
- users/
- Mobile I

★ Method

★ Search

Netcraft

target

Job job

Organisation
- Org structure
- websites
- Phone numbers
- Directory information
- Office Locations
- Company History
- Business Associations

Hosts
- Listening Services
- Operating System Versions
- Internet Reachability
- Enumerated information
- SNMP info
- users / Groups
- Mobile Device

★ Methods and Tools

★ Search Engines

Netcraft – Blueprint a comprehensive list of information about the technologies and information about target website.

~~Job~~ job Search sites – Information about technologies can be gleaned from job postings.

google Search | Google dorks

- filetype : - looks for file types
- index of - directory listings
- info : - Contains google's information about the page.
- intitle : - String in title
- inurl : - String in URL
- link : - finds linked pages
- related : - finds similar pages
- site : - finds pages specific to that site

Metagoofil => Command line interface that uses google hacks to find information in meta tags (Domain, filetype, etc is a google dorks for terminal)

★ Websites Footprinting

Web mirroring | Websites Cloning — allows for discrete testing offline.

- HTTrack - you can use the CLI version or web interface version
- wget - Linux Command
  wget -mk -w 10
  http://hackthissite.org/
- Black widow
- web Ripper
- Teleport pro
- Backstreet Browser

Archive.org / wayback machine

provides cached websites from various dates which possibly have sensitive information that has been now removed.

★ Email Footprinting

Email header - may show servers and where the location of those servers are

- Email headers can provide : Names, Address (IP, email), Mail Servers, Time Stamps, Authentication and so on.
- Email Tracker pro - is a windows software that trace an email back to its true point of origin

- Email tracking - Services can track various bits of information including the IP address of where it was opened, where it went, etc.

★ DNS Footprinting

Ports
- Name lookup - UDP 53
- Zone transfer - TCP 53

Zone transfer replicates all records
Name resolves answer requests
Authoritative servers hold all records for a namespace
DNS poisoning - changes cache on a machine to redirect request to a malicious server
DNSSEC - helps prevent DNS poisoning by encrypting records
SOA Record fields
- Source Host - hostname of the primary DNS
- Contact Email - email for the person responsible for the zone file
- Serial Number - revision number that increases with each change
- Refresh time - time in which an update should wait on a failure
- Expire time - time in which a zone transfer is allowed to complete.

- TTL - minimum TTL for records within the zone.

IP address management
- ARIN - North America
- APNIC - Asia pacific
- RIPE - Europe, Middle East
- LACNIC - Latin America
- AfricNIC - Africa

whois - obtains registration information for the domain from command line or web interface
- on kali whois is pre-installed on CLI; eg:
  whois google.com
- on windows, you can use Smart Whois GUI Software to perform a whois, or any website like domaintools.com

Nslookup - Performs DNS queries; (Nslookup is pre-installed on Kali Linux).
- nslookup
  - www.hackthissite.org
- Server : 192.168.63.0
  address : 192.168.63.1
  - First two lines shows my current DNS server; The IP addresses returned are 'A record', meaning is the IPv4 address of the domain; Bottom line Nslookup queries the specified DNS server and retrieves the requested records that are associated with the domain.

The following types of DNS records are especially useful to use on Nslookup:

- A => The IPv4 address of the domain.
- AAAA => The domain's IPv6 address
- CNAME => The canonical name — allowing one domain name to map on to another. This allows more than one website to refer to a single web server.
- MX => The server that handles email for the the domain.
- NS => One or more authoritative name server records for the domain.
- TXT => A record containing information for use outside the DNS server. The content takes the form name = value. This information is used for many things including authentication schemes such as SPF and DKIM.

Nslookup — Interactive mode Zone transfer (interactive mode allows the user to query name servers for information about various hosts and domains or to print a list of hosts in a domain).

- nslookup
- Server <IP Address>
- Set type = <DNS type>
- <target domain>

Dig - Unix-based Command like nslookup

- dig <target>
- To get email records specify -t MX
  dig <target> -t MX
- To get zone transfer specify axfr

★ Network fonfprinting

⇒ IP address range can be obtained from regional registrar (e.g: ARIN for America, RIPE for Europe, etc)

⇒ use [traceroute] to find intermediary servers
- traceroute uses ICMP echo in windows (tracert)
- traceroute is good for detect firewalls and the network path

usage example :-
- ~~trace~~ traceroute -I nsa.gov
- Specify target : traceroute <target>
- In this case it used ICMP Echo for traceroutting [-I]

Note ⇒ windows Command - tracert
Linux Command - traceroute

★ Other Relevant tools

★ OSRF framework
uses open source intelligence to get information about target. (username checking, DNS lookups, information leaks research, deep web search, regular expressions extraction, and many others.

★ Web Spiders
obtain information from the websites such as pages, etc.

★ Recon-ng
Recon-ng is a web-based open-source reconnaissance tool used to extract information from a target organization and its personnel. provides a powerful environment in which open source web-based reconnaissance can be automated conducted, quickly and thoroughly.

★ Metasploit Framework
The metasploit framework is a tool that provides information about security vulnerabilities and aids in penetration testing and IDS signature development; This is a huge framework that provide Recon tool as well.

★ theHarvester
theHarvester is a OSINT tool; useful for gathering information like :-

- Emails
- Subdomains
- Hosts
- Employee names
- open ports
- Banners from different public sources like search engines, pgp key servers and SHODAN computer database.

Usage example:

- theHarvester -d www.hackthissite.org -n -b google
- Issue theharvester command : theHarvester
- specify the domain : -d <URL>
- perform dns lookup : -n
- specify search engine/source : -b google.

★ Sublist3r

Sublist3r enumerates subdomains using many search engines such as google, Yahoo, Bing, Baidu and Ask. Sublist3r also enumerates subdomains using NetCraft, Virustotal, threatcrowd, DNSdumpster and ReverseDNS.

Usage examples:-

- python3 Sublist3r.py -d hackthissite.org
- Specify the domain : -d <URL>

* DIRB

DIRB is a web content Scanner. It look for existing (and/or hidden) web objects. It basically works by launching a dictionary based attack/brute force attack against a Web Server and analyzing the response.

- useful to find subdirectories on web application

Usage example :-

- dirb https://www.hackthissite.org/user/share/wordlists/dirb/small.txt.
- specify the url by issuing dirb command:
  dirb <url>
- Specify the wordlist : /path/to/wordlist

* Maltego

Maltego is a powerful OSINT tool, you can extract a broad type of information through the networks, technologies and personnel (email, phone number, twitter).

- You able to :-
  - identify IP address
  - identify Domain and Domain Name Schema
  - identify Server Side technology
  - identify Service oriented Architecture (SoA) information
  - identify Name Server
  - identify Mail Exchanger.

- identify geographical Location
- identify Entities
- Discover Email addresses and phone numbers

* Social Engineering framework (SEF)

It's a open Sources Social Engineering framework (Script) that helps generate phising attacks and fake emails, fake email with file attachment and other Stuff that helps you in Social Engineering Attack.

* Web Based ReCon

* NetCraft

NetCraft is a website analyzing server with the help of this website we find basic and important information on the websites like :-

Background - This includes basic domain information.
- which OS, web server is runing which ISP;

Network - This includes information from IP address to Domain names to nameservers.

SSL/TLS - This gives the SSL/tls status of the target.

Hosting History - This gives the information on the hosting history of the target.

Sender policy Framework (SPF) - This describes who can send mail on the domains behalf.

DMARC - This is a mechanism for domain owner to indicate how mail purporting to originate from their domain should be authenticated.

Web trackers - This trackers can be used to monitor individual user behavior across the web site Technology - This section includes details on :-

- Cloud & PaaS
- Server - Side technologies (e.g: Javascript library)
- CDN information
- CMS information (e.g: wordpress, Joomla, etc)
- Mobile Technology.
- web sites (e.g: web analytics, collection, etc
- Character encoding.

★ Shodan

Shodan unlike traditional Search engines such as google, use web crawlers to traverse your entire site but directly into the channel behind the internet, Various types of port equipment audits, and never stop looking for the internet and all associated servers, Camera, printers, routers, and so on.

Some have also described it as a Search engine of Service banners, which are metadata that the Server sends back to the Client.

Shodan works well with basic, Single-term Searches. Here are the basic Search filters you Can use :-

- City : find device in a particular City.
- Country : find device in a particular Country.
- geo : you Can press it Coordinates
- hostname : find Values that match the hostname
- net : Search based on an IP or /x CIDR
- os : Search based on an operating system
- port : find particular ports that are open.
- before / after : find result within a timeframe.

* Censys => Alternative for Shodan.

10M 6M

Scanning and Enumeration Networking

Scanning and Enumeration.

* Scanning and Enumeration.
* Network Scanning – Discovering systems on the network (can be hosts, switches servers, routers, firewall and so on) and looking at what ports are open as well as applications/services and their respective versions that may be running.

In general network scanning have three main objectives :-

1. Scanning for live devices, OS, IPs in use.
   - Server at 192.168.60.30
2. Looking for ports open/closed.
   - The server 192.168.60.30 have TCP port 23 (telnet) running.
3. Search for vulnerabilities on services scanned.
   - The telnet service is cleartext and have many vulnerabilities published.

* Connectionless Communication – UDP packets are sent without creating a connection. Examples are TFTP, DNS (lookup only) and DHCP.

* Connection-oriented Communication – TCP packets require a connection due to the size of the data being transmitted and to ensure deliverability.

★ Slanning Methodology

Check for live systems - ping or other type of way to determine live hosts.
Check for open ports - Once you know live host IPs, Scan them for listening ports.
Scan beyond IDS - if needed, use methods to scans beyond the detection systems; evade IDS using proxies, Spoofing, fragmented packets & so on.
Perform banner grabbing - Grab from Servers as well as perform OS fingerprinting (version of the running services.
Scan for Vulnerabilities - use tools to look at the Vulnerabilities of open Systems.
Draw network diagrams - Shows logical and physical pathways into networks.
Use proxies - Obscures efforts to keep you hidden
pentest Report - Document everything that you find.

★ Identifying Targets

The easiest way to scan for live system is through ICMP.
It has it's Shortcomings and is Sometimes blocked on hosts that are actually live.
Message Types and Returns
- Payload of an ICMP message Can be anything; RFC never Set what it was supposed to be. Allow for Covert channels.

- Ping sweep – easiest method to identify multiple hosts on subnet. You can automate ping sweep with scripting language like Bash script (Linux) or powershell (windows) or use software like advance IP scanner, Angry IP scanner, Nmap, etc.

- ICMP Echo scanning – Sending an ICMP Echo request to the network IP address

- An ICMP return of type 3 with a code of 13 indicates a poorly configured firewall

- Ping scanning tools
  - Nmap
    - nmap -sn 192.168.1.0/24

    This command uses -sn flag (ping scan). This will perform a ping sweep on 256 IP address on this subnet in seconds, showing which hosts are up.

  - hping3
    - hping -1 10.0.0.x --rand-dest -I eth0
    - -1 --> ICMP mode
    - --rand-dest --> random destination address mode.
    - -I <interface> --> network interface name

  - Angry IP Scanner
  - Solar-Winds Engineer toolkit
  - Advance IP Scanner
  - Pinkie.

- Nmap virtually always does a ping sweep with scans unless you turn it off.

Important ICMP Codes.

ICMP message type	Description and Codes
0: Echo reply	- Answer to a type 8 Echo request
3: Destination unreachable	- Error message followed by these Codes: 0 - Destination network unreachable 1 - Destination host unreachable 6 - Network unkown 7 - Host unkown 9 - Network administratively prohibited 10 - Host administratively prohibited. 13 - Communication administratively prohibited.
4: Source Quench	- A Congestion Control message
5: Redirect	- Sent when there are two or more gateway available for the sender to use. Followed by these Codes:- 0 - Redirect datagram for the network 1 - Redirect datagram for the host
8: Echo request	- A ping message requesting an echo reply
11: Time Exceeded	- packet took too long to be routed. (Code 0 is TTL expired)

★ Port Discovery - Basic Concepts

Knocking the door:

- The hacker above sends a SYN packet to port 80 on the server.
  - if server returns SYN - Ack packet = The port is ~~closed~~. Open
  - if server returns RST (reset) packet = The port is closed

Checking if stateful firewall is present:

- The hacker above sends an ACK segment/packet on the first interaction. (without three way handshake).
  - If server returns no respons means that might have a stateful firewall handling proper sessions.
  - If server returns RST packet means that have no stateful firewall

Note: This can be easily achieved by using nmap only

★ Keep in mind the TCP flags & TCP three-way handshake before use nmap!

- TCP Flags

Flag	Name	Function
- SYN	Synchronize	Set during initial communication. Negotiating of parameters & sequence numbers.
- ACK	Acknowledgment	Set as an acknowledgment to the SYN flag. Always set after initial SYN
- RST	Reset	Forces the termination of a connection (in both direction).
- FIN	Finish	ordered close to communications
- PSH	Push	Forces the delivery of data without concern for buffering.
- URG	Urgent	Data inside is being sent out of band. Example is cancelling a message.

Note ⇒ The CEH exam will definitely cover Nmap question. about switches and how to perform a specific type of scan.

★ **Nmap**

Nmap ("Network Mapper") is a free and open source (license) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring service or host uptime. Nmap uses raw IP packets in novel way to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS version) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

★ **Nmap Scan types :**

★ **Stealth Scan**

Half-open scan or SYN scan - only SYN packets sent. Responses same as full.

- useful for hiding efforts and evading firewall
- nmap -sS <target IP>

★ **Full Connect**

TCP connect or full open scan. The first two steps (SYN and SYN/ACK) are exactly the same as with a SYN scan. Then, instead of aborting the half-open connection with a RST packet, kraad acknowledges the SYN/ACK with its own ACK packet.

Completing the Connection.

- Full Connection and then tears down with RST.
- Easiest to detect, but most reliable.
- nmap -sT <target IP>

★ TCP ACK Scan / Flag probe - multiple methods

- TTL Version - if TTL of RST Packet < 64, port is open.
- window Version - if the windows on the RST packet is anything other than 0, port open.
- Can be used to check filtering. if Ack is sent and no response, stateful firewall present.
- nmap -sA <target IP> (ACK Scan)
- nmap -sW <target IP> (window Scan)

★ Null, FIN and Xmas Scan

A uses FIN, URG or PSH flag.

- Open gives no response. closed gives RST/Ack
- nmap -sN <target IP> (Null Scan)
- nmap -sF <target IP> (FIN Scan).
- Xmas Scan - sets the FIN, PSH, and URG flags, lighting the packets up like a Christmas tree.
- Responses are same as Inverse TCP Scan.
- Do not work against windows machines
- nmap -sX <target IP>

Note → The key advantage of these Scan types (Null, FIN or Xmas Scan) is that they can break through certain non-stateful firewalls and packet filtering routers.

★ IDLE Scan

uses a third party to check if a port is open

- Looks at the IPID to see if there is a response
- Only works if third party isn't transmitting data
- Sends a request to the third party to check IPID id; then sends a spoofed packet to the target with a return of the third party; sends a request to the third party again to check if IPID increased.
  - IPID increased of 1 indicates port closed
  - IPID increase of 2 port open.
  - IPID increase of anything greater indicates the third party was not idle.

- nmap -sI <Zombie host> <target IP>

★ Spoofing

- Delay:
  - nmap -Pn -D <spoofed IP> <target>
    This will perform a spoofed ping scan.
- Source Address spoofing:
  - nmap -e <network interface> -S <IP Source> <target>
    Example: nmap -e eth0 -S 10.0.0.14 10.0.0.165

- MAC address Spoofing:
  - nmap --spoof-mac <mac|vendor> <target>
    Example -> nmap --spoof-mac Cis 10.0.0.104

Note -> Decoys will send spoofed IP address along with your IP address.

★ Firewall Evasion

- Multiple Decoy IP addresses :-
  This command is used to scan multiple decoy IP addresses. Nmap will send multiple packets with different IP addresses, along with your attacker's IP address.
  - nmap -D RND: <number> <target>
    Example -> nmap -D RND: 10. 192.168.62.4

- IP fragmentation :-
  used to scan tiny fragment packets
  - nmap -f <target>

- Maximum transmission unit:
  This command is used to transmit smaller packets instead of sending one complete packet at a time.
  - nmap --mtu 8 <target>
    Maximum transmission unit (--mtu) and 8 bytes of packets.

-T0 through -T2 => Serial scans. T0 is slowest
-T3 through -T5 => Parallel scans. T3 is slowest

★ Timing & performance

- Paranoid
  Paranoid (0) Intrusion Detection System evasion.
  - nmap <target> -T0

- Sneaky
  Sneaky (1) Intrusion Detection System evasion
  - nmap <target> -T1

- Polite
  Polite (2) slows down the scan to use less bandwidth and use less target machine resources
  - nmap <target> -T2

- Normal
  Normal (3) which is default speed
  - nmap <target> -T3

- Aggressive
  Aggressive (4) speeds scan; assumes you are on a reasonably fast and reliable network
  - nmap <target> -T4

- Insane
  - Insane (5) speeds scan; assumes you are on an extraordinarily fast network
  - nmap <target> -T5

★ UDP Scan

Most popular services runs over the TCP, but there are many common services that also uses UDP: DNS(53), SMTP(25), DHCP(67), NTP(123), NetBIOSsesn (137), etc

- nmap -sU <target>

You also can specify which UDP port:

- nmap -sU -p U:53,123 <target>

Also you can fire up both TCP and UDP scan with port specification:

- nmap -sU -sS -p U:53,123 T:80,443 <target>

★ List of Switches

IMP

Switch

- -sA ⇒ ACK scan
- -sF ⇒ FIN scan
- -sI ⇒ IDLE scan
- -sL ⇒ DNS scan (list scan)
- -sN ⇒ Null scan
- -sO ⇒ protocol scan
- -sP/-sn ⇒ ping scan
- -sR ⇒ RPC scan
- -sS ⇒ SYN scan
- -sT ⇒ TCP connection scan
- -sW ⇒ window scan
- -sX ⇒ XMAS scan

- -PI ⇒ ICMP ping
- -Pn ⇒ No ping
- -PO ⇒ No ping
- -Ps ⇒ SYN ping
- -PT ⇒ TCP ping
- -oN ⇒ Normal output
- -oX ⇒ XML output
- -n ⇒ Never do DNS resolution resolu
- -f ⇒ --mtu: fragment packets
- -D ⇒ IP address Decoy: <decoy1, decoy2 [ME]...>: Cloak a scan with decoys

- -A ⇒ OS detection, version detection, script, scanning and traceroute
- -sV ⇒ Determine only service/version info
- -F ⇒ fast mode - Scan fewer ports than the default scan.

Notes:
- Nmap run by default at a T3 level (3 - Normal)
- Nmap run by default TCP Scan.
- Nmap ping the target first before the port scan by default, but if the target have a firewall, maybe the scan will be blocked. To avoid this, you can use -Pn to disable ping.
- If you're in LAN and you need to disable ARP ping, use:
  - --disable-arp-ping
- You can add a input from external lists of hosts / networks:
  - -iL hosts-example.txt
- Fingerprinting - another word for port sweeping and enumeration.

★ More useful Information about Nmap :-

Switch	Example	Description
-p	nmap 192.168.1.1 -p21	port scan for port x
-p	nmap 192.168.1.1 -p21-100	port Range
-p	nmap 192.168.1.1 -p U:53,T:21-25,80	port scan multiple TCP and UDP ports
-p-	nmap 192.168.1.1 -p-	port scan all ports
-p	nmap 192.168.1.1 -p http,https	port scan from service name
-F	nmap 192.168.1.1 -F	fast port scan (100 port)

→ --top ports	→ nmap 192.168.1.1 --top-ports 2000	port scan the top x ports
→ -p- (65535)	→ nmap 192.168.1.1 -p-65535	Leaving off initial port in range makes the scan start at port 1
→ -p0-	→ nmap 192.168.1.1 -p0-	Leaving off end port in range makes the scan go through to port 65535.

#2 Service and Version Detection.

Switch	Example	Description.
→ -sV	→ nmap 192.168.1.1 -sV	Attempts to determine the version of the service running on port.
→ -sV-- (Version intensity)	→ nmap 192.168.1.1 -sV-- Version-intensity8	Intensity level 0 to 9. Higher number increases possibility of correctness.
→ -sV-- (Version light)	→ nmap 192.168.1.1 -sV-- Versionlight	Enable light mode. Lower possibility of correctness faster.
→ -sV-- (version-all)	→ nmap 192.168.1.1 -sV-- Version-all	Enable intensity level 9. Higher possibility of correctness slower.
→ -A	→ nmap 192.168.1.1 -A	Enables OS detection, Version detection, Script scanning and traceroute.

#3> OS Detection

Switch	Example	Description
=> -O	=> nmap 192.168.1.1 -O	Remote OS detection using TCP/IP stack fingerprinting
=> -O -- (osscan-limit)	=> nmap 192.168.1.1 -O --osscan-limit	If at least one open and one closed TCP port are not found it will not try OS detection against host
=> -O -- (osscan-guess)	=> nmap 192.168.1.1 -O --osscan-guess	Makes Nmap guess more aggressively
=> -O -- (max-os-tries)	=> nmap 192.168.1.1 -O --max-os-tries1	Set the maximum number X of OS detection tries against a target.
=> -A	=> nmap 192.168.1.1 -A	Enable OS detection, version detection, script scanning and traceroute.

#4> Timing and performance

Switch	Example	Description
=> --host-timeout <time>	=> 1s; 4m; 2h	give up on target after this long.
=> --min-rtt-timeout/max-rtt timeout/initial-rtt-timeout <time>	=> 1s; 4m; 2h	Specifies probe round trip time
=> --min-hostgroup/max-hostgroup <size>	=> 50; 1024	Parallel host scan group sizes
=> --min-parallelism/max-parallelism <num probes>	=> 10; 1	probe parallelization
=> --scan-delay/--max-scan-delay <time>	=> 20ms; 2s; 4m; 5h	Adjust delay between probes

=> --max-

=> --min-

=> --max

#5> NS

NSE

a digi

default

tradi

One

let u

mat

Switch

=> -sC

=> --script

default

=> --scripts

=> --scrip

=> --script

=> --scrip

=> --scripts

args

=> --max-retries <tries> => 3	Specify the maximum number of port scan probe retrans-missions
=> --min-rate <number> => 100	Send packets no slower than <number> per second
=> --max-rate <number> => 100	Send packets not faster than <numbers> per second.

#5> NSE Scripts

NSE stands for nmap scripting Engine and it's basically a digital library of nmap scripts that helps to enhance the default Nmap features and report the result in a traditional Nmap output.

One of the best things about NSE is its ability to let users write and share their own scripts, so you're not limited to relying on the Nmap default NSE scripts.

Switch	Example	Description.
=> -sC	=> nmap 192.168.1.1 -sC	Scan with default NSE scripts considered useful for discovery and safe.
=> --script default	=> nmap 192.168.1.1 --script default	Scan with default NSE scripts considered useful for discovery and safe.
=> --scripts	=> nmap 192.168.1.1 --script = banner	Scan with a single script. Example banner.
=> --script	=> nmap 192.168.1.1 --script = http*	Scan with a wildcard. Example http
=> --script	=> nmap 192.168.1.1 --script = http,banner	Scan with two scripts. Example http and banner
=> --script	=> nmap 192.168.1.1 -- Script "not intrusive"	Scan default, but remove intrusive scripts.
=> --scripts-args	=> nmap 1 --script snmp-sysdescr --script-args snmpcommunity = admin) 192.168.1.1	=> NSE script with arguments

#6) Useful NSE Script Examples

Command	Description
=> nmap -Pn --script=http -sitemap-generator scanme.nmap.org	http site map generator
=> nmap -n -Pn -P80 --open -sV -vvv --script banner,http -title -iR 1000	Fast search for random web servers
=> nmap -Pn --script=dns-brute domain.com	Brute forces DNS hostnames guessing subdomains
=> nmap -n -Pn -vv -o -sV --script smb-enum*, smb-ls, smb-mbenum, smb-os-discovery, smb-s*, smb-vuln*, smbv2* -vv 192.168.1.1	Safe SMB script to run.
=> nmap --script whois* domain.com	Whois query
=> nmap -P80 --script http -unsafe-output-escaping scanme.nmap.org	Detect Cross site Scripting Vulnerabilities
=> nmap -p80 --script http -sql-injection scanme.nmap.org	Check for SQL injections.

★ hping

Hping3 is a Scriptable program that uses the Tcl language, whereby packets can be recived and sent via a binary or string representation describing the packets.

- Another powerful ping sweep and port scanning tool
- Also can craft UDP/TCP packets. • you can make a TCP flood
- hping3 -1 IP address.

Switch		Description
=> -1	=>	Set ICMP mode
=> -2	=>	Set UDP mode.
=> -8	=>	Set Scan mode. Expects port range without -p flag
=> -9	=>	Listen mod. Expects signature (e.g. HTTP) and interface (-I eth0)
=> --flood	=>	Send packets as fast as possible without showing incoming replies
=> -Q	=>	Collects sequence numbers generated by the host.
=> -p	=>	Set port numbers
=> -F	=>	Set the FIN flag
=> -S	=>	Set the SYN flag
=> -R	=>	Set the RST flag
=> -P	=>	Set the PSH flag.
=> -A	=>	Set the ACK flag.
=> -U	=>	Set the URG flag.
=> -X	=>	Set the XMAS Scan flags

★ Evasion Concepts

- To evade IDS, sometimes you need to change the way you scan
- One method is to fragment packets (nmap -f switch)
- OS fingerprinting
  - Active – Sending crafted packets to the target
  - Passive – Sniffing network traffic for things such as TTL windows, DF flags and ToS fi
- Spoofing – Can only be used when you dont expect a response back to your machine.
- Source routing – Specifies the path a packet should take on the network; most system dont allow this anymore.
- IP Address Decoy – Sends packets from your IP as well as multiple other decoy to confuse the IDS/firewall as to where the attack is really coming from.
  - nmap -D RND:10 X.X.X.X
  - nmap -D decoyIP1, decoyIP2..., SourceIP... (target)
- Proxy – hides true identity by filtering through another computer. Also can be used for other purposes such as content blocking evasion, etc.
  - proxy chains – Changing multiple proxies together
    - proxy switcher
    - proxy workbench
    - proxy chains

- Tor – a specific type of proxy that uses multiple hops to a destination; endpoint are peer computers.
- Anonymizers – hides identity on HTTP traffic (port 80)

★ **Banner Grabbing**

Banner grabbing can be used to get information about OS or specific server info (such as web server, mail server, etc).

- Active – sending specially crafted packets and comparing responses to determine OS
- Passive – reading error messages, sniffing traffic or looking at page extensions
- Easy way to banner grab is connect via telnet on port (e.g. 80 for web server).
- NetCat tool
  - "Swiss army knife" of TCP/IP hacking
  - provides all sorts of control over a remote shell on a target
  - Connect via nc -e <IP address> <port>
  - from attack machine nc -l -p 5555 opens a listening port on 5555
  - can connect over TCP or UDP, from any port
  - offers DNS forwarding, port mapping and forwarding and proxying
  - NetCat can be used to banner grab:
    nc <IP address or FQDN> <port number>

- Example of Banner grabbing on netcat – extracting request HTTP header.

i. nc Command with target IP address and port 80

ii. Issue the GET /HTTP/1.0 (this GET request will send to the web server).

iii. The server responded with some interesting information: (Code likha hua h).

★ Vulnerabilities

★ Vulnerability Categories:

- Misconfiguration – improperly configuring a service or application.
- Default installation – failure to change setting in an application that come by default.
- Buffer overflow – Code execution flaw
- Missing patches – System that have not been patched
- Design flaws – flaws inherent to system design such as encryption and data validation
- Operating System flaws – flaws specific to each OS
- Default password – leaving default password that come with system/application

★ Vulnerability Assessment

Scans and tests for vulnerabilities but does not intentionally exploit them.

- Find the vulnerabilities so we can categorize them (OS, misconfigurations, patch management, third-party, etc).

* Vulnerability Management Life-Cycle

The vulnerability Management Life cycle is intended to allows organization to identity System security weaknesses; priaritize assets; assess, report, and remediate the weaknesses; and Verify that they have been eliminated.

1. Discover : Inventory all assets across ~~the~~ the network and identity host details inclding operating System and open services to identify vulnerabilities. Develop a network baseline. Identify Security Vulnerabilities on a regular automated Schedule

2. Prioritize Assets : Categorize assets into group or business units, and assign a business value to asset group based on their criticality to your business operation.

3. Assess : Determine a baseline risk profile So you Can eliminate risks based on asset criticality vulnerability threat, and asset classification.

4. Report : Measure the level of business risk associated with your assets according to your security policies. Document a Security plan monitor suspicious activity, and describe known vulnerabilities.

5. Remediate : Prioritize and fix vulnerabilities in order according to business risk. Establish Control & demonstrate progress

6. Verify : Verify that threats have been eliminated through follow-up audits.

★ Vulnerability Scanning
Can be complex or simple tools run against a target to determine Vulnerabilities.

• Type of Vulm. Assessment tools :-

- Host - based
- Depth - based (Fuzzer tools)
- Application - layer tools (software, databases, etc)
- Active Scanning
- Passive Scanning.
- Scope tools.

• Tools :
- Industry standard is Tenable's Nessus.
- GFI LanGuard.
- Nikto - CLI; is a web server assessment tool. It is designed to find various default and insecure files, configurations and programs on any type of web server.
- OpenVAS - Best Competitor to Nessus and is free.
- WpScan - CLI; scan word press websites.
- MBSA - Microsoft Baseline Security Analyzer
- FreeScan - Well known for testing websites and applications.
- Qualys.

★ CVSS and CVE

→ CVSS - Common Vulnerability Scoring System
- None - white (0.0)
- Low - green tones (0.1 - 3.9)
- Medium - Yellow/light orange (4.0 - 6.9)
- High - orange (7.0 - 8.0)
- Critical - red (9.0 - 10.0)

→ CVE - Common Vulnerabilities and Exposures is a list of publicly disclosed vulnerabilities and exposures that is maintained by MITRE.

→ NVD - National Vulnerabilities Database is a database, maintained by NIST, that is fully synchronized with the MITRE CVE list; US Gov. vulnerabilities respositary.

★ Proxychains

Proxychains is open-sources software that is available free and most of linux distro it is pre-install. If you are using the latest version of kali linux it is pre-installed in it.
proxychains is a tool that redirects the TCP (Transmission Control protocol) connection with the help of proxies like TOR, HTTP(s), and SOCKS, and it creates a proxy chain server.

→ proxychains features :-

- Support SOCKS5, SOCKS4, and HTTP/HTTPs connect proxy servers.

- Proxychains can be mixed up with a different proxy types in a list
- Proxychains also supports any kinds of chaining options methods, like: random, which takes a random proxy in the list stored in a configuration file, or chaining proxies in the exact order list, different proxies are separated by a new line in a file. There is also a dynamic option, that lets proxychains go through the live only proxies, it will exclude the dead or unreachable proxies, the dynamic option often called smart options.
- Proxychains can be used with servers, like squid, sendmail, etc.
- Proxychains is capable to do DNS resolving through proxy.
- Proxychains can handle any TCP client application, ie. nmap, telnet.

★ Enumeration Concepts

Enumeration is the process of extracting users names, machine name, network resources, shares and services from a system, and its conducted in an intranet environment.

- Get user names using email IDs.
- Get information using default password.
- Get user names using SNMP
- Brute force AD
- Get user group from windows

In this phase, the attacker creates an active connection to the system and performs directed queries to gain more information about the target. The gathered information is used to identify the vulnera-bilities or weak points in system security and tries to exploit in the system gaining phase.

- Defined as listing the items that are found within a specific target
- Always is active in nature.
- Direct access.
- Gain more information.

★ SNMP Enumeration

SNMP enumeration is the process of enumerating the users accounts and device on a SNMP enable computer

- SNMP service comes with two password, which are used to configure and access the SNMP agent from the management station (MIB):

i. Read community staring
ii. Read/write community string.

- These strings (password) come with a default value, which is same for all the systems.

- They become easy entry points for attackers if left uncharged by administrator.

⇒ Attackers enumerate SNMP to extract information about network resources such as hosts, router, device shares (...) Network information such as ARP tables, routing tables, device specific information and traffic statistics

- Runs on port 161 UDP
- Management information Base (MIB) - database that stores information.
- Object identifiers (OID) - identifiers for information stored in MIB.
- SNMP GET - gets information about thy system
- SNMP SET - Sets informations about the system.
- Types of objects
- Scalar - Single object
- Tabular - multiple related objected that can be grouped together.

- SNMP uses community string which function as passwords.
- There is a read-only and a read-write version
- Default read-only string is public and default read-write is private.
- These are sent in cleartext unless using SNMP V3
- CLI Tools.
- Snmap-Check --> SNMP device enumerator comes pre-installed on kali linux machine; Snmp-Check supports a huge type of enumerations :- • contact and user account • devices • domain • hardware and storage information • hostname • IIS statistics • listening UDP ports and TCP connections. • mold (banner) • network interfaces and network services • routing information

- Metasploit module, Snmp-enum
- MSF Snmp-enum (pratical lab).
- Snmpwalk

- GUI Tools
  - Engineer's Toolset
  - SNMP Scanner
  - opUtils 5
  - SNScan

    Example of SNScan :-

    Note :- the first Slanned item is a printer running SNMP.

★ Windows System Basics

- Everything runs within Context of an account
- Security Context - users identity and authentication information
- Security identifier (SID) - identifies a user, group or computer account
- Resource identifier (RID) - portion of the SID identifying a specific user, group or computer.
- The end of the SID indicates the user number.
- Example SID : S-1-5-21-3874928736-3675328774-129833 7465-500
- Administrator Account - SID of 500
  - Command to get SID of local user:
    - Whic 'username' where name = 'username' get sid
- Regular Accounts - Start with a SID of 1000
- Linux systems used user IDs (UID) and group IDs (GID) found in /etc/passwd

- SAM Database – file where all local passwd are stored (encrypted)
  - Stored in
    C:\Windows\System32\Config

- Linux Enumeration Commands in powershell or Cmd prompt
  - Finger – info on user and host machine
  - rpcinfo and rpcclient – info on RPC in the environment
  - showmount – displays all shared directories on the machine.

- Look for share resources (NetBIOS):
  - net view \\sysName

- Windows SysInternals is a Websites and suite that offers technical resources and utilities to manage, diagnose, troubleshoot, and monitor
  - Lots of resources for enumerating, windows administration tools, etc.

★ NetBIOS Enumeration

- NetBIOS provides name servicing, connectionless communication and some session layer stuff
- The browser service in windows designed to host information about all machine within domain or TCP/IP network segment
- NetBIOS name is a 16-character ASCII string used to identify devices.

Enumerating NetBIOS :

- You can use nmap or zenmap to check which os the target is using, and which ports are open:
  - nmap -O <target>

- If theres any UDP port 137 or TCP port 138/139 open, we can assume that the target is running some type of NetBIOS service.

- On windows is nbtstat command:
  nbtstat display protocol statistics and current TCP/IP connections using NetBIOS over TCP/IP.
  - nbtstat gives your own info
  - nbtstat -a list the remote machine's name table given its name
  - nbtstat -A list the remote machine's name table given its IP address.
  - nbtstat -n gives local table
  - nbtstart -c gives cache information.

Code	Type	Meaning
<1B>	UNIQUE	Domain master browser
<1C>	UNIQUE	Domain Controller
<1D>	GROUP	Master browser for subnet
<00>	UNIQUE	Hostname
<00>	GROUP	Domain name
<03>	UNIQUE	Service running on system.
<20>	UNIQUE	Server service running

- NetBIOS name resolution doesn't work on IPv6
- other tools for NetBIOS enumeration:-
  - SuperScan
  - Hyena
  - NetBIOS Enumerator (is a nbstat with GUI)
  - NS Auditor.

★ Linux System Basics.

- Enum4linux is a tool for enumerating information from windows and Samba systems:
  - enum4linux -u CEH -p password -u 192.168.2.23
    - -u username, -p password, -U users information
  - Key features :-
    - RID cycling (when RestrictAnonymous is set to 1 to windows 2000)
    - user listing (when RestrictAnonymous is set to 0 on windows 2000)
    - Listing of group membership information.
    - Share enumeration.
    - Detecting if host is in a workgroup or a domain
    - Identifying the remote operating system.
    - Password policy retrieval (using polenum)
- finger -> who is currently logged in, when and where.
- w -> Show who is logged on and what they are doing.

★ LDAP Enumeration.

- Runs on TCP ports 389 and 636 (over SSL)
- Connects on 389 to a Directory System Agent (DSA)
- Returns information such as valid user names, domain information, addresses, telephone numbers, system data, organization structure and other items
- To identify if the target system is using LDAP services you can use nmap with -sT flag for TCP connect/full scan and -O flag for OS detection.
- sudo nmap -sT -O <target>

- Tools for Enumeration LDAP :
  - Softerra
  - JXplorer
  - Lex
  - LDAP Admin tool

- JXplorer example :-

★ NTP Enumeration.

- Runs on UDP 123
- Querying can give you list of systems connected to the server (name and IP)
- Tools
  - NTP Server Scanner
  - AtomSync
  - Can also use Nmap and wireshark.

- Commands include ntptrace, ntpdate, ntpdc and ntpq

-> Nmap example for NTP enumeration :-
- -sU UDP scan
- -pU port UDP 123 (NTP)
- -pn treat all hosts as online --skip host discovery
- -n Never do DNS resolution.
- The nmap script ntp-monlist will run against the ntp service which only runs on UDP 123.
- nmap -sU -pU:123 -Pn -n --script=ntp-monlist <target>

- As you can see on the output above, information of all clients that is using NTP services on the network shown IPv4 and IPv6 addresses.

★ SMTP Enumeration.

• Ports used :-
- SMTP: TCP 25 --> [outbound email]
- IMAP : TCP 143/993 (over SSL) --> [inbound email]
- POP3 : TCP 110/995 (over SSL) --> [inbound email]

In simple words : users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving e-mail.

• Enumerating with nmap :-
- -P25 port 25 (SMTP)
- --script smtp-commands nmap script - attempts

- EXPN ⇒ asks for a confirmation about the identification of a mailing list.

other tools:- . smtp-user-enum
— username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT To.

to use EHLO and HELP to gether the Extended Command Supported by an SMTP Server
- nmap -p25 --script smtp-Commands <target IP>

• It is possible to Connect to SMTP through telnet Connection, instead using port 23 (telnet) we Can Set the port 25 (SMTP) on the telnet Command :-
- telnet <target> 25
• Case we got Connected, we Can use the SMTP Commands to explore as Shown below:
• Both of emails are Valid to an attacker explore further attacks like brute forcing etc.

★ Some SMTP Commands :-

- HELO ⇒ It's the first SMTP Command : is Starts the Conversation identifying the Sender Server and is generally followed by its domain name.
- EHLO ⇒ An alternative Command to Start the Conversation underlying that the Server is using the Extended SMTP protocol.
- MAIL FROM ⇒ with this SMTP Command the operations begin: the Sender States the Source email address in the "From" field and actually start the email transfer.
- RCPT To ⇒ It identifies the recipient of the email
- DATA ⇒ with the DATA Command the email Content begins to be transferred; its generally followed by a 354 reply Code given by the Server, giving the permission to Start the actual transmission.
- VRFY ⇒ The Server is asked to Verify whether a particular email address or username actually exists.

Vulnerability Analysis

★ **Def.**
Attackers perform VA to identify security loophole in the target's network, and end device. The identified Vulnerabilities are used by attacker to further exploit the target network.
VA Researchers VA has an important role to play in an organization's security from different internal and external threats. To secure a network, an administrator needs to perform patch management, install proper antivirus software, check configuration, solve known issues in third-party application, and troubleshoot hardware default configuration. All these activities together constitute vulnerability assessment.

In this section we will learn :-
- Vulnerability Assessment Concepts
- Vulnerability Classification and Assessment types
- Vulnerability Assessment Solutions and tools
- Vulnerability Assessment Reports

★ **Vulnerability Assessment Concepts :-**
There are two causes of Vulnerable System in a network :-
1. Misconfiguration in Software or Hardware
2. Poor Programming practices.

Attackers leverage these Vulnerabilities to perform different attackers on an organizational resources. We will be covering Vulnerability Assessment, Vulnerability Scoring Systems, Vulnerability database

and the Vulnerability assessment life cycle.

* **Vulnerability Research**

It is the process of analyzing protocols, services, and configurations to discover the vulnerabilities and design flaw that will expose an OS and its application to exploit, attack or misuse.

An administrator needs Vulnerability Research :-

- To gather information about security trends, newly discovered threats, attack surface, attack vectors and techniques
- To find weaknesses in the OS and application and alert the network administrator before a network attack.
- To understand information that helps prevent security problems.
- To know how to recover from a network attack

An ethical hacker needs to keep up with the most recently discovered vulnerabilities and exploits to say one step ahead of the attackers through vulnerability research which includes :-

- Discovering the system design faults and weaknesses that might allow attackers to compromise a system.
- Stay update about new products and technologies and reading news related to current exploits
- Checking underground hacking web sites (Deep and Dark websites) for newly discovered vulnerabilities and exploits.
- Checking newly released alerts regarding relevant innovation and product improvement for security system

Security expert and Vulnerability Scanners Classify Vulnerabilities by :-

- Severity level (low, medium, high).
- Exploit range (local or remote)

★ **Resources for Vulnerability Research**

The following are Some of the online websites used to perform Vulnerability research :-

- Microsoft Vulnerability Researc (MSVR)
- Dark Readin
- Security Tracker
- Trend Micr
- Security Magazin
- Pentest Magazin
- SC Magazin
- Exploit Databas
- Security Folu
- help Net security
- Hackerstorm
- Computerworld
- windowssecurity
- D'Crypt

★ **What is Vulnerability Assessment?**

A Vulnerability assessment is an in depth examination of the ability of a System or application, including current security procedures and controls to withstand exploitation. It Scans network for known Security weaknesses, and recognizes, measures, and classifies security vulnerabilities in Computer Systems, networks and Communication channels.

It identifies, quantifies, and ranks possible vulnerability to threats in a system. Additionally, it asits security professionals in securing the network by identifying security loopholes or vulnerabilities in the current security mechanism before attackers can exploit them.

A Vulnerability assessment may be used to :-

- Identify weaknesses that could be exploited.
- Predict the effectiveness of additional security measures in protecting information resources from attack.

Typically, vulnerability-scanning tools search network segments for IP-enable devices and enumerate systems, operating systems, and applications to identify vulnerabilities resulting from vendor negligence, system or network administration activities, or day-to-day activities.

Vulnerability-scanning software scans the computer against the Common Vulnerability and Exposures (CVE) index and security bulletins provided by the software vendor.

Vulnerability scanners are capable of identifying the following information :-

- The OS version running on computers or devices
- IP and Transmission Control protocol/user Datagram protocol (TCP/UDP) ports that are listening.
- Applications installed on computers.
- Accounts with weak passwords
- Files and folders with weak permissions
- Default services and applications that might have to be uninstalled.
- Errors in the security configuration of common applications

- Computers exposed to known or publicly reported vulnerabilities.
- EOL/EOS Software information
- Missing patches and hotfixes
- Weak network configuration and misconfigured or risky ports.
- Help to verify the inventory of all devices in the network.

* There are two approaches to network vulnerability scanning :-

- Active scanning :- The attacker interacts directly with the target network to find vulnerabilities. Active scanning helps in simulating an attack on the target network to uncover vulnerabilities that can be exploited by the attacker.

Example :- An attacker sends probes and specially crafted requested to the target host in the network to identify vulnerability

- Passive scanning : The attacker tries to find vulnerabilities without directly interacting with the target network. The attacker identifies vulnerabilities via information exposed by systems during normal communications. Passive scanning identifies the active operating systems, applications, and ports throughout the target network, monitoring activity to determine its vulnerabilities. This approach provides information about weakness but does not

provides a path for directly launching attacks.
Examples : An attacker guesses the operating systems information, applications, and application and service versions by observing the TCP connection setup and teardown.

★ Vulnerability - Management life - cycle

The process helps identify remediate any potential security weaknesses before they can be exploited.

- Identify assets and create a baseline

This phase identifies critical assets and prioritize them to define the risk based on the criticality and value of each system. This creates a good baseline for vulnerability management. This phase involves the gathering of information about the identified systems to understand the approved ports, software, drivers, and basic configuration each system in order to develop and maintain a system baseline.

- Vulnerability Scan

This phase is very crucial in vulnerability management. In this step, the security analyst perform the vulnerability scan on the network to identify the known vulnerabilities. Vulnerability scans can also be performed on applicable compliance templates to assess the organization infrastructure weaknesses against the respective compliance guidelines.

- Risk Assessment

In this phase, all serious uncertainties that are associated with the system are assessed and

prioritized, and remediation is planned to permanently eliminate System flaws. The risk assessment summarizes the vulnerability and risk level identified for each of the selected assets. It determines whether the risk level for a particular asset is high, moderate, or low. Remediation is planned based on the determined risk level. For example, vulnerabilities ranked high-risk are targeted first to decrease the chances of exploitation that would adversely impact the organization.

- Remediation.

Remediation is the process of applying fixes on vulnerable systems in order to reduce the impact and severity of vulnerabilities. This phase is initiated after the successful implementation of the baseline and assessment steps.

- Verification

In this phase, the security team perform a re-scan of system to assess if the required remediation is complete and whether the individual fixes have been applied to the impacted assets. This phase provides clear visibility into the firm and allows the security team to check whether all the previous phases have been perfectly employed or not. Verification can be performed by using various means such as ticketing systems, scanners, and reports.

- Monitor

Organization need to performed regular monitoring to maintain System security. They use tool such as IDS/IPS and firewall. Continuous monitoring identifies potential threats and any new vulnerabilities that have evolved. As per security best practices, all phases of vulnerabilities management must be performed regularly.

- Base line
- Vulnerability Scan
- Risk assessment
- Remediation
- Verification
- Monitor

} Vulnerability life-cycle management

System Hacking

★ Goals :-

1. Gaining access - uses information gathered to exploit the system.

- Password Attacks :-
  - Non-electronic attacks
  - Active online attacks
  - Passive online attacks
  - Offline attacks

2. Escalating privileges - Granting the account you've hacked admin or pivoting to an admin account.

3. Executing Applications - Putting back door into the system so that you can maintain access.

4. Hiding files - Making sure the files you leave behind are not discoverable

5. Covering Tracks - Cleaning up everything else (log files, etc)
   - Clearev - Meterpreter shell command to clear log files (issue inside Metasploit framework)
   - Clear MRU list in windows
   - In Linux, append a dot in front of a file to hide it.

★ Password Attacks

Note => Check out the practical labs on Dumping and Cracking SAM Hashes (1), Rainbow Tables Basics (2), and LLMNR/NBT-NS (3).

* Non-electronic - Non-technical attacks.
- Social engineering attacks - most effective.
- Shoulder surfing
- Dumpster diving
- Snooping around
- Guessing

* Active online - done by directly communicating with the victim's machine
- Includes Dictionary and Brute-force attacks, hash injections, phishing, Trojans, Spyware, keyloggers and password guessing.

* LLMR / NBT-NS poisoning - attack based off windows technologies that caches DNS locally. Responding to these poisons the local cache. If an NTLMv2 hash is sent over, it can be sniffed out & then cracked.
- LLMNR / NBT-NS practical lab
- LLMNR uses UDP 5355
- NBT-NS uses UDP 137
- Responder is the tool to sniff the access logs from LLMNR / NBT-NS
- Keylogging - process of using a hardware device or software application to capture keystrokes of a user
- Active online attack are easier to detect and take a longer time
- Tools for Active online Attack :-
  - Medusa
  - Hydra
  - NBNSproof
  - Pupy
  - MetaSploit

- Responder – LLMNR and NBT-NS responder, it will answer to specific NBT-NS (Netbios Name Service) queries based on their name suffix. By default, the tool will only answer to file Server service request, which is for SMB.

- Can combine 'net' commands with a tool such as NetBIOS Auditing tool or Legion to automate the testing of User IDs and password.
- Tools for NetBIOS attack :-
- Hydra
- Metasploit

★ Passive online – Sniffing the wire in hopes of intercepting a password in clear text or attempting a replay attack or man-in-the-middle attack.
- Tools for passive online Attack :-
- Cain and Able – Can poison ARP and then monitor the Victim's traffic; Also used for cracking hash passwords (LM, NTLM), Sniff network packets for password, sniff out for local stored passwords
- EtterCap – MITM tool for LAN's DNS spoofing. Help against SSL encryption; Intercept the traffic on a network segment, capture passwords, and conduct an active eavesdropping against a number of common protocols.
- KerCrack – built-in sniffer and password cracker looking for port 88 Kerberos traffic

- SloopLM – specifically looks for windows authentication traffic on the wire and has a password cracker.

Note :- Service / protocols that uses clear text:

Service	port
FTP	20/21
TELNET	23
SMTP	25
HTTP	80
POP3	110
IMAP4	143
NetBIOS	139, 445
SNMP	161, 162
SQLnet	1521

★ Passive offline :- When the hacker steals a copy of the password file (plaintext or Hash) and does the cracking on a separate system.

- Dictionary Attack – uses a word list to attack the password. Fastest method of attacking password.

- Wordlist – A wordlist or a password dictionary is a collection of password dictionary is a collection of passwords stored in plain text. It's basically a file with a bunch of passwords in it. one popular example of wordlist is the rockyou.txt containing 14,341,564 unique passwords.

- You also can generate your own wordlist with given parameters like length, combining letters and numbers, profiling etc. Tool for generate wordlists :- ① CeWL ② Crunch

- Brute force attack - Tries every combination of characters ~~(such as at least 7 characters, should have a special character, etc.)~~ to crack a password
- Can be faster if you know parameters (such as at least 7 character, should have a special character, etc)

- Hybrid attack - Takes a dictionary attack and replace characters (such as a 0 for an o) or adding numbers to the end

- Rainbow tables - uses pre-hashed password to compare against a password hash. Is faster because the hashes are already computed.

- Tools for cracking password files (CLI):-
- John the Ripper - works on unix, windows and kerberos; compatible with MySQL, LDAP and MD4.
- Hashcat - Advance password recovery tool; provides several option like hash modes OS's documents, password managers... (MD5, SHA-family, RIPE-MD, NTLM, LM, Bitlocker, OSX, MD5 salted or iterated, and the list goes on).

- Tools for Cracking password files (NV1):
- Cain & Abel – windows software; crack hash passwords (LM, NTLM), sniff network packets for password, sniff out for local stored password, etc.
- LOphCrack – paid software; Extract and crack hashes; uses brute force or dictionary attack;
- Ophcrack – Free open-Source; crack windows log-in passwords by using LM hashes through rainbow tables.
- Legion – Legion automates the password guessing in NetBIOS sessions. Legion scans multiple IP address ranges for windows shares and also offers a manual dictionary attack tool.
- KerbCrack – Crack Kerberos passwords.
- Mimikatz – Steal Credentials and escalate privileges (windows NTLM hashes and Kerberos tickets (Golden ticket Attack); 'pass-the-hash' and 'pass-the-ticket')
- Fgdump – Dump SAM databases on windows machines.
- Pwdump7 – Dump SAM databases on windows machines.

- CHNTPW – chntpw is a software utility for resetting or blanking local password used by windows NT, 2000, XP, Vista, 7, 8, 8.1 and 10. It does this by editing the SAM database where windows stores password hashes.

i) physical access to victim's computer
ii) Startup on BIOS and allow boot to CD or USB.

iii) Modify the SAM user account information through the CHNTPW

⚠ -> ntgen, winntgen — Tools for generate your own rainbow tables

⚠ -> SAM (Security Account Manager) is a database file present in windows machines that stores user accounts and security descriptors for users on a local computer. It stores users password in a hashed format (in LM hash function is one-way, this provides some measure of security for the storage of the passwords.

⚠ -> /etc/shadow is where hashed password data is stored in linux systems (only user with high privileges can access).

⚠ -> Password attack countermeasures :-

- Length of password is good against brute-force attacks.
- Password complexity is good against dictionary attacks.

★ Authentication

- Three Different Types

- Something you are — Uses biometrics to validate identity (retina, fingerprint, etc)
- Downside is there can be lots of false negatives.
- False acceptance rate (FAR) — Type II — Likelihood that an unauthorized user will be accepted (This would be bad)

- False Injection rate (FPR) - Type I - likehood that an authorized user will be rejected
- Crossover error rate (CER) - Combination of the two; the lower the CER, the better the system.
- Active - requires interaction (retina scan or finger-print scanner)
- passive - Requires no interaction (iris scan)

- Something You have - usually consists of a token of some kind (swipe badge, ATM card, etc).
  - This type usually requires something alongside it (such as a PIN for an ATM card)
  - Some tokens are single factor (such as a plug-and play authentication).

- Something You know - Better know as a password
  - Most system use this because it is universal and well-known.

- Two-factor - when You have two types of authentication such as something You know (password) and something you have (access card)

- Strength of passwords - Determined by length and complexity.

- ECC says that both should be combined for the best outcome.
- Complexity is defined by number of character sets used (lower case, upper case, numbers, symbols, etc.)

- Default passwords – always should be changed and never left what they came with. Databases such as cirt.net default-password info and open sez inc all have databases of these.

★ **Windows Security Architecture**

- Authentication Credentials stored in Sam file
- File is located at C:\Windows\System32\Config
- Older System use LM hashing current uses NTLM V2 (MD5)
- Windows network authentication uses Kerberos

★ **LM Hashing**

- Splits the password up. If it's over 7 characters, it is encoded in two sections.
- If one section is blank, the hash will be AAD3B435B51404EE
- Easy to break if password is 7 character or under because you can split the hash
- SAM file presents as
  Username : SID : LM_Hash : NTLM_Hash : : :

★ **Ntds.dit**

Database file on a domain controller that stores passwords

- Located in %SystemRoot%\NTDS\Ntds.dit or
- Located in %SystemRoot%\System32\Ntds.dit
- Includes the entire Active Directory.

Uses

★ Kerberos (AD DS

- Step
1. Client ticket
2. Server This
3. If cl to th (TGS)
4. Server to ac
- Tools
- KerbSni
- kerbbri
- Both

★ Regis

- Called make
- Made
- Root
- HKE and
- HKE asso
- HKE the
- HKEY infor

Uses TCP/UDP Port 88

★ Kerberos for Active Directory Domain Services (AD DS)

- Step of exchange

1. Client asks key Distribution Center (KDC) for a ticket. Sent in clear text.
2. Server responses with Ticket Granting Ticket (TGT). This is a secret key which is hashed by the password copy stored on the server.
3. If client can decrypt it, the TGT is sent back to the server requesting a Ticket Granting Service (TGS) service ticket.
4. Server sends TGS service ticket which client uses to access resources.

- Tools
  - KerbSniff
  - kerbcrack
  - Both take a long time to crack

★ Registry

- Collection of all settings and configurations that make the system run
- Made up of keys and values
- Root level keys
  - HKEY_LOCAL_MACHINE (HKLM) - information on hardware and software
  - HKEY_CLASSES_ROOT (HKCR) - information on file associates and OLE classes
  - HKEY_CURRENT_USER (HKCU) - profile information for the current user including preferences
  - HKEY_USERS (HKU) - specific user configuration information for all currently active users

- HKEY_CURRENT_CONFIG (HKCC) - points to HKEY_LOCAL_Machine\SYSTEM\CurrentControlSet\Hardware profiles\Current

• Type of Values
- REG_SZ - Character String
- REG_EXPAND_SZ - expandable string Value
- REG_BINARY - a binary Value
- REG_DWORD - 32-bit unsigned integer
- REG_LINK - symbolic link to another Key

• Important Locations
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServiceOnce
- HKEY_LOCAL_MACHINE\Software\Microsoft\Microsoft\Windows\CurrentVersion\RunService
- " " " " \CurrentVersion\RunOnce
- " " " " \CurrentVersion\Run

• Executables to edit
- regedit.exe
- regedt32.exe (preferred by Microsoft).

★ MMC
• Microsoft Management Console - used by windows to administer system.
• Has "Snap-ins" that allow you to modify sets (such as Group policy Editor)

★ Sigverif.exe

- File Signature Verification (sigverif.exe) detects signed files and allows you to :-
  - View the certificates of signed files to verify that the file has not been tampered with after being certified.
  - Search for signed files.
  - Search for unsigned files.

★ Linux Security Architecture

★ Linux Directory Structure

- Linux root is just a slash (/)
- Important locations
  - / - root directory
  - /bin - basic Linux commands
  - /dev - contains pointer locations to various storage and input/output systems
  - /etc - all administration files and passwords. Both password and shadow files are here
  - /home - holds the user home directories
  - /mnt - holds the access location you've mounted
  - /sbin - system binaries folder which holds more administrative commands
  - /usr - holds almost all of the information, commands and files unique to the users

★ Linux Common Commands

→ adduser, Cat, Cp, ifconfig, kill, ls, ~~Cloning~~ man, passwd, ps, rm, su, pwd, chmod,

There are some much command in linux that's why I'm not able to write here.

★ Privilege Escalation and Executing Application

★ Vertical - Lower level user executes code at a higher privilege level (e.g: Common user to root / administrator)

★ Horizontal - executing code at the same user level but from a location that would be protected from that access

- Crack the password of an admin primary or
- Taking advantage of an OS Vulnerability
- One way to perform a priv esc is using CVE's in order to perform bind shells, web shells and so on.
- Examples :-
  - Linux : DirtyCow race-condition Vulnerability
  - Windows : EternalBlue exploits the old Samba version 1 to leverage a Remote Code execution

- DLL Hijacking - replacing a DLL in the application directory with your own version which gives you the access you need

- In linux machines is possible to look for Crontabs and find misconfigurations on privilege

- In Linux, insecure Sudo can lead a privilege escalation to root; You can check this by typing: Sudo -L. if there's any system command that allows NOPASSWD option this may lead to escalation.

- Nmap old versions you can start interactive mode and issue the !/bin/bash to delete root priveleges.

- Use a tool that will provide you the access such as Metasploit

- Social engineering a user to run an application
- ECC refers executing application as "owning" a system
- Executing applications - Starting things such as key-loggers, Spyware back doors and crackers.

★ Covert data gathering
★ Keyloggers - record keys strokes of a individual computer keyboard or a network of computers.
- Keylogger when associated with spyware, helps to transmit your information to an unknown third party.
- Types of Keyloggers :-
→ Hardware Keyloggers
- PC/BIOS embedded
- Keyboard
- External device → PS/2 and USB, Acoustic/CAM, Bluetooth, wi-fi

- Hardware Keylogger Tools :-
  - KeyGrabber - electronic device capable of capturing keystrokes from PS/2 USB keyb

⇒ Software Keylogger
- Application
- Kernel
- Hypervisor-based
- Form Grabbing based (records from web form data)
- Software Keylogger Tools :-
  - KeyCarbon
  - Keyllama Keylogger
  - Keyboard logger
  - Key Ghost

★ **Spywares** — Watching user's actions and logging them without the user's knowledge.
- Hide its process, files and other objects
- Spywares can tracks user's PII, monitors activity, display annoying pop-ups, redirect web pages to ads, changes the browser setting steal passwords, modifies the DLLS, changes firewall setting and so on.
- Types of Spyware :-
  - Desktop
  - Email
  - Internet
  - Child-monitoring
  - Screen Capturing
  - USB
  - Audio and Video
  - Printers
  - Mobile device / Telephones / Cellphones
  - GPS

- Spyware Tools :-
  - SpyAgent - allows you to secretly monitor and record all activities on your computer which is completely legal.
  - Power Spy - allows you to securetly monitor and record all activities on your computer, which is completely legal.
  - mSpy - GPS spyware that track the location of particular mobile devices.
  - USBdeview - monitors and analyzes data transferred between any USB device connected to a computer.

★ Defending against keyloggers and spywares

- Restrict physical access to computer systems
- Use anti-keylogger between the keyboard and its driver
- Use pop-up blocker and avoid opening junk mails
- Use anti-spyware / antivirus
- Firewall and anti-keylogging software (Zemana)
- Update and patch!
- Recognize phishing emails
- Host-based IDS
- Automatic form-filling password manager or virtual keyboard.

★ Steganography :-

- Steganography - practice of concealing a message inside another medium so that only the sender and recipient know of its existence.
- Ways to identify
  - Text - character positions are key - blank spaces, text patterns
  - Image - file larger in size; some may have colour palette faults
  - Audio & Video - require statistical analysis
- Methods
  - Least significant bit insertion - changes least meaningful bit
  - Masking and filtering (grayscale images) - likes watermarking
  - Algorithmic transformation - hides in mathematic functions used in image compression
- Tools
  - QuickStego
  - gifShuffle
  - SNOW
  - Steganography Studio
  - openStego

★ Hiding Files

- In windows, you can use Alternate Data Stream (ADS) to hide files :-
  - Hide a file from directory listing on an

NTFS file system
- type badfile.exe :> plaintext.txt : badfile.exe
- Next create a symlink - mklink normalapp.exe readme.txt : badfile.exe

- You can also clear out all ADS by copying files to a FAT partition
- To show ADS, dir /r does the trick;
  - You can use streams from sysinternals to show streams.
  - Also you can use FTK (forensics Toolkit) to look for this

- You can also hide files by attributes
- In windows :- attrib +h filename
- In Linux, simply add a . to the beginning of the filename (.file.tar)

- Can hide data and files with Steganography
- Tools for Steganography :-
  - CLI (Linux) -> steghide
  - GUI (window) -> Snow, Openstego, Openpuff

★ Rootkits
- Software put in place by attacker to obscure system compromise
- Hides processes and files
- Also allows for future access
- Examples:- ① Horsepill - Linux kernel rootkit inside initrd
  ② Crayfish - windows rootkit that injects in boot record
  ③ Firefly - multi-component family of malware ④ AZZale
  ⑤ Alotar ⑥ Necurs ⑦ Zero Access

- Hypervisor level - rootkits that modify the boot sequence of a host system to load a VM as the host OS
- Hardware - hide malware in devices of firmware
- Boot loader level - replace boot loaders with ones controlled by hacker
- Application level - directed to replace valid application files with Trojans
- Kernel level - attacks boot sectors and kernal level replacing kernel code with back-door code; most dangerous.
- Library level - use system-level calls to hide themselves.
- One way to detect rootkits is to map all the files on a system and then boot a system ~~and~~ from a clean CD version and compare the two file systems.

★ **Covering Tracks**

Clearing logs is the main idea behind covering tracks.

1. Find and clear the logs.
2. Falsify / modify logs.

★ **On Linux :-**

- Linux keep the command line history on .bash_history
- To clear out the command line history use rm -f to force remove. You also can use shred -zu that deletes the file and overwrite on memory.
- You can also use history -c to clear all command history on entire system or history -w to clear

out all Session history.

- Turn off the Command logs :-
- export HISTSIZE =0
- echo $HISTSIZE will return 0 limiting the number of Commands which can be saved in $HISTFILE.
- Clearev - Meterpreter Shell Command to clear logfiles (issued inside Metasploit Framework).

> Most Common logs on linux :-

- /Var/log/messages or /Var/log/Syslog
  - General messages, as well as system-related information
- /Var/log/auth.log or /Var/log/Secure
  - Store authentication logs, including both Successful and failed logins and authentication methods.
- /Var/log/boot.log
  - Related to booting and any message logged during Startup
- /Var/log/maillog or Var/log/mail.log
  - Stores all logs related to mail Server.
- Clearing and Modifying logs on linux :-
  - It is possible to echo whitespace to clear the event log file :-
  - echo " " > /Var/log/auth.log
  - Also you can perform this by using "black hole dev/null":
  - echo /dev/null > auth.log
  - To tamper/modify the log files, you can use Sed Stream editor to delete, replace and insert data
  - Sed -i '/opened/d' /Var/log/auth.log - this Command will delete every line that contains the 'opened' word, that refers to opened sessions on linux system.

★ On windows :-

- To clear out all command line history :-
  - on Cmd prompt : press [alt] + [F7]
  - on powershell : type clear - history

In windows, you need to clear application, system logs.

- Auditpol for changing setting on log files (used for manipulate audit policies).
- main commands :-
  - auditpol /get /category:* --> display all audit policies in detail all audit policies in detail if it enable (object Access, System, Logon /Logoff, privilege use, and so on.)
  - auditpol /clear --> reset (disable) the system audit policy for all subcategories.
  - auditpol /remove --> remove all per-user audit policy setting and disables all system audit policy setting.
- MRU (Most Recently used) programs list registry recently used programs /files and saves on windows Registry.
- Is possible to manually clear the log on event viewer

★ Conclusion on Covering Tracks

- option is to corrupt a log file - this happens all the time
- Best option is be selective and delete the entries pertaining to your actions.
- Can also disable auditing ahead of time to prevent logs from being captured
- Tools :- • CCleaner --> automate the system cleaning. Scrub online history, log files, etc. [windows] • MRC [illegible]

★ Meterpreter on MSF have clearev to clear all event logs remotely. [Kali Linux using MSF]

Malwares Threats

* What is Malware?

→ Any Software intentionally designed to cause damage to a Computer, Server or Computer network. The Code is described as Computer Viruses, Worms, Trojan horses, ransomware, Spyware, adware, and Scareware among other forms. Malware has a malicious intent acting against the interest of the computer user.

* Types of Viruses and Worms

- How it works?

i. Infection Phase – a virus planted on a target system and replicates itself and attaches to one or more executable files.

ii. Attack phase – the infected file is executed accidentally by the user, or in some way is deployed and activated

- Virus – Designed to spread from host to host and has the ability to replicate itself. They cannot reproduce/spread without help. They operate by inserting or attaching itself to a legitimate program or document in order to execute its code.
- Macro Virus – Written in a macro language (e.g: VBA) and that is platform independent.
- Compression Viruses – Another type of virus that appends itself to executables on the system and compresses them by user's permissions.
- Stealth Virus – Hides the modification it has made; trick antivirus software; intercepting its requests to the OS and provides false and bogus

information

- Polymorphic Virus – Produces varied but operational copies of itself. A polymorphic virus may have no parts that remain identical between infections, making it very hard to detect using signatures.
- Multipart Virus – Attempts to infect both boot sector and files; generally refers to viruses with multiple infection methods.
- Self-garbling (metamorphic) Virus – Rewrites itself every time it infects a new file.
- Other virus types
  - Boot Sector Virus – Known as System Virus; moves boot sector to another location and then inserts its code int he original location.
  - Shell Virus – wraps around an application's code, inserting itself before the applications
  - Cluster Virus – modifies directory table entries so every time a file or folder is opened, the virus runs
  - Encryption Virus – Uses encryption to hide the code from antivirus
  - Cavity Virus – Overwrite portions of host file as to not increase the actual size of the file uses null content sections
  - Sparse Infector Virus – only infects occasionally (e.g. every 10th time)
  - File Extension Virus – Changes the file extensions of files to take advantage of most people having them turned off (readme.txt.vbs show as readme.txt)

- Virus Makers
  - Sonic Bat
  - Poison Virus Maker
  - Sahil's Virus Generator
  - JPS Virus Maker

  } Virus makers software

- Worm – Self-replicating malware that sends itself to other computers without human intervention
  - usually doesn't infect files – just resides in active memory
  - often used in botnets

- Ghost Eye Worm – hacking tool that uses random messaging on facebook and other sites to perform a host of malicious efforts.
- Logic Bomb – Executes a program when a certain event happens or a date and time arrives.
- Rootkit – Set of malicious tools that are loaded on a compromised system through stealthy techniques; very hard to detect;
- Ransomware – malicious software designed to deny access to a computer until a price is paid; usually spread through email
  - WannaCry – famous ransomware; within 24 hours had 230,000 victims; exploited unpatched SMB vulnerability
- Other Examples
  - Cryptorbit
  - CryptoLocker
  - CryptoDefense
  - Police-themed

Viruses needs help/interaction
Worms self propagates.

- Trojan horse – A program that is disguised as another legitimate program with the goal of carrying out malicious activities in the background without user's knowledge
  - RAT – Remote Access Trojans – Malicious programs that run on system and allow intruders to access and use a system remotely
- Immunizer – Attaches code to a file or application which would fool a virus into 'thinking' it was already infected (e.g. like human vaccine)
- Behavior blocking – Allowing the suspicious code to execute within the OS and watches its interactions looking for suspicious activities.

★ Major characteristics of Viruses

1. Infecting other files
2. Alteration of data
3. Transforms itself
4. Corruption of files and data
5. Encrypts itself
6. Self replication

★ Stages of Virus Lifecycle :-

1. Design
2. Replication
3. Latch
4. Delivery

5. Incorporation – A.-V. figures out the virus pattern to build signatures to identify and eliminate the virus
6. Execution of the damage routine A.V to the rescue

★ Malware Basics
- How is malware distributed?
  - SEO manipulation
  - Social Engineering / Click jacking
  - Phishing
  - Malvertising
  - Compromising legitimates sites
  - Drive-by downloads
  - Spam

- Malware – Software designed to harm or secretly access a computer system without informed consent
  - Most is downloaded from the internet with or without the user's knowledge
- Overt channels – legitimate communication channels used by programs
- Covert channels – used to transport data in unintended ways
- Wrappers – programs that allows you to bind an executable to an innocent file.

★ **Basic Components of Malware**

1. Crypters – use a combination of encryption and code manipulation to render malware undetectable to security program; protects from being scanned or found during analysis.
2. Downloader – used to download additional malware
3. Dropper – used to install additional malware into the target system.
4. Exploit – Malicious code used to execute one specific vulnerability
5. Injector – used to expose vulnerable process in the target system to the exploit.
6. Obfuscator – used to conceal the true purpose of the malware
7. Packers – used to bundle all of the malware files together into a single executable.
8. Payload – used to take over the target machine
9. Malicious Code – used to define the abilities of the malware.

⇒ Exploit Kits – help deliver exploits and payloads

- Infinity
- Bleeding Life
- Crime pack
- Black hole Exploit kit

★ Trojans

- Software that appears to perform a desirable function but instead performs malicious activity
- To hackers, it is a methods to gain and maintain access to a system
- Trojans are means of delivery whereas a backdoor provides the open access
- Trojans are typically spread through Social Engineering.

- Types of Trojans :-
  - Defacement trojan
  - Proxy Server trojan
  - Botnet trojan
    - Chewbacca
    - Skynet
  - Remote access trojans
    - RAT
    - MoSucker
    - optiX Pro
    - Blackhole
  - E-banking trojans
    - Zeus
    - Spyeye
  - IoT Trojans
  - Security Software Disable trojans
  - Command Shell trojan → provides a backdoor to launch to through Command-line access.
    - Netcat
  - Covert Channel Tunneling trojan (CTT) – A RAT trojan
    Creates data transfer channels in previously authorized data streams.

★ **Infection Process:-**

1. Creation of a Trojan using trojan Construction kit
2. Create a Dropper
   - used to install additional malware into the target system.
3. Create a Wrapper
   - Wrapper - programs that allow you to bind an executable to an innocent file
4. Propagate the Trojan
5. Execute the Dropper

★ **Trojan Port numbers:-**

Trojan Name	TCP port
=> Death	2
=> Senna Spy	20
=> (Blade Runner, Doly Trojan, Fore, Invisible FTP, WebEx, Winsock)	21
=> Shaft	22
=> Executor	80
=> Hackers Paradise	31, 456
=> TCP wrappers	421
=> Pro-killer	555
=> Doom, Santa's Back	666
=> Silencer, WebEx	666
=> Doly Trojan	1001
=> RAT	1011
=> SubSeven	1095-98
=> Shiva-Burka	1243
=> Trojan Cow	1600
=> Deep Throat	2001
	6670-71

Note:-

★

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

★

Tini	7777
Duhere.Y	10000
SubSeven 1.0 - 1.8 MyDoom.B	10080
VooDoo Doll, Netbus 1.X, Backorifice (Bill Gates, X Bill)	12345
Whack a Mole	12321-3
NetBus	17300
Back orifice	31337,8
SubSeven, PhatBot, AgoBot, Kraobot	65506

Note: Its not necessary to know every possible trojan port in the history for the CEH exam, it's good for understanding.

★ Trojan Countermeasures

1. Avoid clicking on unusual or suspect email attachments
2. Block unused ports
3. Monitor network traffic
4. Avoid downloading from untrusted sources
5. Install & update anti-virus software
6. Scan removable media before use
7. Validate file integrity of all externally sourced software
8. Enable auditing
9. Configure Host Based firewalls
10. Use IDS

★ Techniques

- netstat -an - Shows open ports in numerical order
- netstat -b - displays all active connection and

the processes using them
- Process Explorer – Microsoft tool that shows you everything about running processes
- Registry Monitoring tools
  - SysAnalyzer
  - Tiny Watcher
  - Active Registry monitor
  - Regshot
- MSConfig – windows program that shows all programs set to start on startup
- Tripwire – integrity verifier that can act as a HIDS in protection against trojans
- SIGVERIF – build into windows to verify the integrity of the system.
  - Log file can be found at C:\Windows\System32\sigverif.txt
  - Look for drivers that are not signed

★ Malware Analysis

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit or backdoor.

★ Types of Malware analysis :-

1. Static (Code Analysis) – performed by fragmenting the binary file into individual elements that can be analyzed without executing them.
   - File fingerprinting

- Local & online scanning of elements to see if they match know malware profiles
- Identifying packers / obfuscators used
- Identifying the PE's (portable executable) information
- Identify dependencies
- Malware disassembly

2. Dynamic (Behavioral Analysis) - Performed by executing the malware to see what effect it has on the system
- System baselining
- Host integrity monitoring

- Tools for Disassembling | Debugging | Reverse Engineering
- IDA Pro
- Olly Dbg
- Ghidra by NSA

- Sheepdip - Dedicated computer which is used to test files on removable media for viruses before they are allowed to be used with other computers

★ Steps
1. Make sure you have a good test bed
- Use a VM with NIC in host-only mode and no open shares
2. Analyze the malware on the isolated VM in a static state
- Tools - bin Text and UPX help with looking at binary
3. Run the malware and check out processes
- Use process monitor, etc to look at processes

- Use NetResident, TcPview or even wireshark to look at network activity
4. Check and see what files were added, changed, or deleted.
- Tools - IDA Pro, Virustotal, Anubis, threat Analyzer

- Preventing Malware
  - Make sure you know what is going on in your system
  - Have a good antivirus that is up to date
  - Airgapped - isolated on network

★ Rootkits (Done before) (repeat)
- Software put in place by attacker to obscure system compromise
- Hides processes and files
- Also allows for future access
- Examples
  - Horsepill - Linux kernal rootkit inside initrd
  - Crayfish - windows rootkit that injects in boot record
  - Fireloff - multi-component family of malware
  - Azazel
  - Avatar
  - Nelurs
  - Zero Access

3M

Sniffing

★ **Sniffing**

Sniffing is the process of monitoring and capturing all the packets passing through a given network using sniffing tools. It is a form of "tapping phone wires" and get to know about the conversation. It is also called wiretapping applied to the computer networks.

★ **Active and passive sniffing**

- Passive sniffing - watching network traffic without interfering only works for same collision domain
- Active sniffing - uses methods to make a switch send traffic to you even though it isn't destined for your machine.
- Span port - switch configuration that makes the switch send a copy of all frames from other port to a specific port
  - Not all switches have the ability to do this
  - Modern switches sometimes don't allow span ports to send data - you can only listen
- Network tap - special port on a switch that allows the connected device to see all traffic
- Port mirroring - another word for span port

★ **Basics**

- Sniffing is capturing packets as they pass on the wire to review for interesting information
- MAC (Media Access Control)
  Physical or burned-in address assigned to NIC for communications at the Data link layer
  - 48 bit long (6 bytes)
  - Displayed as 12 hex characters separated by colons

- First half of address is the organizationally unique identifier - identifies manufacturer
- Second half ensures no two cards on a subnet will have the same address

- NICs normally only process signals meant for it
- Promiscuous mode - NIC must be in this setting to look at all frames passing on the wire
- CSMA/CD - Carrier Sense Multiple Access/Collision Detection - used over Ethernet to decide who can talk
- Collision Domains
- Traffic from your NIC (regardless of mode) can only be seen within the same collision domain
- Hubs by default have one collision domain.
- Switch have a collision domain for each port

★ Protocols Susceptible

Some of the protocols that are vulnerable to sniffing attacks.

- IMAP, POP3, NNTP and HTTP all send over clear text data
- SMTP is sent in plain text and is viewable over the wire. SMTP V2 limits the information you can get, but you can still see it.
- FTP sends user ID and password in clear text
- TFTP passes everything in clear text
- TCP shows sequence numbers (usable in session hijacking)
- TCP and UCP show open ports

- IP shows source and destination addresses

★ ARP

- Stands for Address Resolution protocol
- Resolves IP address to a MAC address
- Packets are ARP_REQUEST and ARP_REPLY
- Each computer maintains its own ARP cache, which can be poisoned
- Commands
  - arp -a displays current ARP cache
  - arp -d clears ARP cache
- works on a broadcast basis - both requests and replies are broadcast to everyone
- Gratuitous ARP - special packet to update ARP cache even without a request
  - This is used to poison cache on other machines

★ IPv6

- Uses 128-bit address (16 byte)
- Has eight groups of four hexadecimal digits
- Sections with all 0s can be shorted to nothing (just has start and end colons)
- Double colon can only be used once
- Loopback address is ::1

IPv6 Address type	Description
• Unicast	Addressed and intended for one host interface
• Multicast	Addressed for multiple host interfaces
• Anycast	Large number of hosts can receive; nearest host opens

IPv6 Scopes	Description
• Link local	Applies only to hosts on the same subnet (Address block FE80 :: /10)
• Site local	Applies to hosts within the same organization (Address block FEC0 :: /10)
• Global	Includes everything

- Scope applies for multicast and anycast
- Traditional network scanning is computationally less feasible.

★ **Wiretapping**

Wiretapping, also known as telephone tapping, is the process of monitoring telephone and Internet conversations by a third party, often by covert means.

- Lawful interception – Legally intercepting communication between two parties
- Active – Interjecting something into the communication.
- Passive – only monitors and records the data
- PRISM – System used by NSA to wiretap external data coming into US

★ **MAC Flooding**

- Switches either flood or forward data
- If a switch doesn't know what MAC address is on a port, it will flood the data untill it finds out

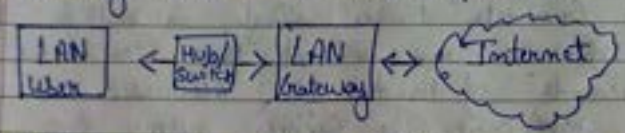
- CAM table – the table on a switch that stores which MAC address is on which port
- If table is empty or full, everything is sent to all ports
- MAC flooding will often destroy the switch before you get anything useful, doesn't last long and it will get you noticed. Also, most modern switches protect against this.
- CAM table overflow Attack – occurs when an attacker connects to a single or multiple switch ports and then run a tool that mimics the existence of thousands of random MAC addresses on those switch port. The switch enters these into the CAM table, and eventually the CAM table, and eventually the CAM table, fills to capacity. (This works by sending so many MAC addresses to the CAM table that it can't keep up). This attack can be performed by using macof.
- Tools for MAC flooding
  - Etherflood
  - Macof
  - Dsniff

★ Switch port Stealing
Tries to update information regarding a specific port in a race condition
1. ARP flood
- Source MAC address same a victim
- Destination MAC is attacker's
- CAM updates port info (stolen)

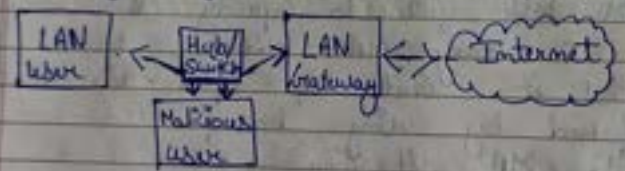
2. Attacker now intercepts Victim traffic
3. Attacker stops flooding
4. Victim reclaims port
5. Attacker retransmits captured data
6. Attacker repeats flooding.

★ ARP Poisoning

=> Routing under normal operation



=> Routing Subject to ARP Cache poisoning



- ARP Spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution protocol) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network.
- Also called ARP Spoofing or gratuitous ARP
- This can trigger alerts because of the constant need to keep updating the ARP cache of machines

- Changes the Cache of machines so that packets are sent to you instead of the intended target
- Countermeasures
  - Dynamic ARP inspection using DHCP Snooping
  - Can use static ARP ACL to map
  - Header to payload validation
  - XArp Software can also watch for this
  - Default gateway MAC can also be added permanently into each machine's cache
- Tools for ARP poisoning
  - Cain and Abel
  - Win Arp Attacker
  - Ufasoft
  - dsniff

★ DHCP Starvation

Is an attack that targets DHCP servers whereby forged DHCP requests are crafted by an attacker with the intent of exhausting all available IP addresses that can be allocated by the DHCP server

- Attemp to exhaust all available addresses from the server
- Attacker sends so many requests that the address space allocated is exhausted
- DHCPv4 packets - DHCPDISCOVER, DHCPOFFER, DHCPREQUEST, DHCPACK
- DHCPv6 packets - Solicit, Advertise Request (Confirm Reply), Reply

- DHCP Steps
1) Clints Sends DHCPDISCOVER
2) Server responds with DHCPOFFER
3) Client Sends request for IP with DHCPREQUEST
4) Server Sends address and Config via DHCPACK

- Tools
- Yersinia
- DHCPstarv

- Mitigation is to Configure DHCP Snooping
- Rogue DHCP Server - setup to offer address instead of real server. Can be combined with starvation to real server.

★ Spoofing

- MAC Spoofing → Changes your MAC address Benefit is CAM table use most recent address.
- Port Security Can slow this down, but doesn't always stop it.
- MAC Spoofing makes the switch send all packets to your address instead of the intended one until the CAM table is updated with the real address again.
- IRDP Spoofing - Attacker Sends ICMP Router Discovery Protocol message advertising a malicious gateway.

- DNS Poisoning - changes where machines get their DNS info from allowing attacker to redirect to malicious websites.

* Sniffing Tools

* Wireshark

Wireshark is the world's foremost and widely-used network protocol analyzer. It lets you see what's happening on your network at a microscopic level.

- With Wireshark you can inspect and detect ARP poisonings, Rogue DHCP Servers, Broadcast Storm etc.
- - Previously know as Ethereal
  - Can be used to follow streams of data
  - Can also filter the packets & so you can find a specific type or specific source address
- Wireshark filters :-
  - ! (arp or icmp or dns)
  - Filters out the "noise" from ARP, DNS and KMP requests
  - ! - Clears out the protocols for better inspection
  - tcp.port == 23
    Look for specific ports using tcp.port
  - ip.addr == 10.0.0.165
    Look for specific IP address
  - IP.addr == 172.17.15.12 && tcp.port == 23
    Displays telnet packets containing that IP
  - IP.Src == 10.0.0.224 && IP.dst == 10.0.0.156
    See all packets exchanged from IP source to destination IP

- http. request
  Displays HTTP GET requests
- tcp Contains String
  Displays TCP Segments that Contain the Word 'String'
- tcp. flags = 0X16
  Filters TCP request with ACK flag set

★ **tcpdump**

Tcpdump is a data-network packet analyzer Computer program that runs under a Command line interface. It allows the user to display TCP/IP and other packets being transmitted or received over a network to which the Computer is attached.

- Syntax
- <tcpdump flag (S) interface>
- tcpdump -i eth1
  puts the interface in listening mode
- WinDump is a windows version similar to tcpdump.

★ **tcptrace**

Analyzes files produced by packet Capture programs such as wireshark, tcpdump and Etherpeek

★ **Other Tools**

- EtherCap - also Can be used for MITM attacks, ARP poisoning. Has active and passive Sniffing.

- Capsa Network Analyzer
- Snort - usally discussed as an intrusion Detection application
- Sniff-o-Matic
- Etherpeek
- WinDump
- WinSniffer

★ Defending and Countermeasures techniques against sniffing :-

- Disable ARP Dynamic
- ARP spoofing detection tools
- Encrypt all the traffic that leaves your system
- Avoid public wi-fi spots
- Network Scanning and monitoring
- Reverse DNS lookup's on logs == Sniffer
- Ping Suspect client with wrong MAC address
  - If Suspect accepts the packet, is a good indication that he is Sniffing the network using NIC in promiscuous mode.
- Use Nmap with nse-script for Sniffer Detect :

-nmap --script == Sniffer - detect <target>

Social - Engineering

★ **Social Engineering**

Social Engineering is the act of manipulating a person or group into providing information or a service they would otherwise not have given.

★ **Phases**

1. Research target Company
   - Dumpster dive, Visit Websites, tour the Company etc
2. Select the Victim
   - Identify frustrated employee or other target
3. Build a relationship
   - Develop relationship with target employee
4. Exploit the relationship
   - Collect Sensitive information and Current technologies

★ **Principles**

1. Authority
   Impersonate or imply a position of authority
2. Intimidation
   Frighten by threat
3. Consensus / Social proof
   To Convince of a general group agreement
4. Scarcity
   The Situation will not be this way for long

5. Urgency
works alongside scarcity / act quickly, don't think
6. Familiarity
To imply a closer relationship
7. Trust
To assure reliance on their honesty and integrity.

★ Behaviors
- Human nature / Trust - Trusting others
- Ignorance of social engineering efforts
- Fear of consequences of not providing the information
- Greed - promised gain for providing requested information.
- A sense of moral obligation.

★ Companies Common Risks :-
- Insufficient training
- Lack of controls
- Technical
  e.g: Firewall rule, ACL rules, patch management (...)
- Administrative
  e.g: Mandatory Vacations, Job Rotation, Separation of Duties (...)
- Physical
  e.g: Proper Lighting, Cameras, Guards, Mantraps (...)
- Size of the company Matters
- Lack of policies
  ① prohibitous policy

(2) permisive policy
(3) prudent policy
(4) paramoid policy

★ Social Engineering Attacks :-

★ Human - Based Attacks

- Dumpster Diving - Looking for Sensitive information in the trash.
  - Shredded papers can sometimes indicate Sensitive info.

- Impersonation - pretending to be Someone you're not.
  - Can be anything from a help desk person up to an authoritative figure (FBI agent)
  - Posing as a tech Support professional can really quickly gain trust with a person.

- Shoulder Surfing - Looking over Someone's Shoulder to get info.
  - Can be done long distance with binoculars etc.

- Eavesdropping - Listening in on conversation about Sensitive information

- Tailgating - Attacker walks in behind Someone who has a valid badge. (e.g: Holding boxes or Simply by following without getting notice).

- Piggybacking – Attacker pretends they lost their badge and asks someone to hold the door.

- RFID identity Theft (RFID skimming)
  - stealing an RFID card signature with a specialized device

- Reverse Social Engineering – Getting someone to call you and give information.
  - often happens with tech support – an email is sent to user stating they need them to call back (due to technical issue) and the user calls back.
  - can also be combined with a DoS attack to cause a problem that the user would need to call about
  - Always be pleasent – it gets more information

- Insider Attack – An attack from an employee generally disgruntled
  - Sometimes subclassified (negligent insider, professional insider).

★ **Computer – Based Attacks**

Can begin with sites like Facebook where information about a person is available; for instance if you knew Bob is working on a project, an email crafted to him about that project would seem quite normal if you spoof it from a person on his project.

- Phising - Crafting an email that appears legitimate but contains links to fake websites or to download malicious code
  - Ways to Avoid phishing
    - Beware unknown, unexpected or suspicious originators
    - Beware of who the email is addressed to
    - Verify phone numbers
    - Beware bad spelling or grammar
    - Always check links

- Spear phishing - Targeting a person or a group with a phising attack.
  - Can be more useful because attack can be targeted

- Whaling - Going after CEOs or other C-level executives.

- Pharming - Make a user's traffic redirects to a clone websites ; may use DNS poisoning

- Spamming - Sending Spam over instant message.

- Fake AntiVirus - Very prevalent attack; pretends to be an anti-virus but is a malicious tool.

★ Tools

- SET (Social Engineering Toolkit) - pentest tool design to perform advanced attacks against human by exploiting their behavior.
- PhishTank - for phishing detection
- Wifiphisher - Automated phishing attacks against wifi networks in order to obtain credentials or injects malware.
- SPF Speedphish framework - Quick recon and deployment of simple social eng. exercises.

★ Mobile - Based Attacks

- ZitMo (Zeus-in-the-Mobile) - banking malware that was ported to android
- SMS messages can be sent to request premium services
- Attacks
  - Publishing malicious apps
  - Repackaging legitimate apps
  - Fake security applications
  - SMS (Smishing)

★ Prevention

- Separation of duties
- Rotation of duties
- Controlled Access → Least Privilege
- Logging & Auditing.
- Policies.

★ Physical Security Basics

- Physical measures – everything you can touch, taste, smell or get shocked by
  - Includes things like air quality, power concerns, humidity control systems
- Technical measures – Smartcards and biometrics
- Operational measures – policies and procedures you set up to enforce a security-minded operation.
- Access Controls – physical measures designed to prevent access to controlled areas
  - Biometrics – measures taken for authentication that come from the "Something you are" concept
    - False rejection rate (FRR) – when a biometric rejects a valid user
    - False acceptance rate (FAR) – when a biometric accepts an invalid user
    - Crossover error rate (CER) – combination of the two determines how good a system is
- Even though hackers normally don't worry about environmental disasters, this is a something to think of from a pentest standpoint (hurricanes, tornadoes, floods, etc)

2M

Denial of Service

★ DoS

A Denial of Service (DoS) is a type of attack on a service that disrupts its normal function and prevents other users from accessing it. The most common target for a DoS attack is an online service such as a websites, through attacks can also be launched against networks, machines or even a single program.

DoS attacks can cause the following problems:-

- Ineffective Services
- Inaccessible Services
- Interruption of network traffic.
- Connection interference.

★ DDoS

A distributed denial of service (DDoS) attack is launched from numerous compromised devices, often distributed globally in what is referred to as a botnet.

Goal :-

Seeks to take down a system or deny access to it by authorized users.

★ Botnet

Network of zombie computers a hacker uses to start a distributed attack.

- Botnets can be designed to do malicious tasks including sending spam, stealing data, ransomware, fraudulently clicking on ads or

distributed denial-of-service (DDoS) attack.

- Can be controlled over HTTP, HTTPs, IRC, or ICQ
- Botnet Scanning Methods:
  - Random ⇒ Randomly looks for vulnerable devices
  - Hitlist ⇒ Given a list of devices to scan for vulnerabilities
  - Topological ⇒ Scan hosts discovered by currently exploited devices
  - Permutation ⇒ Scan list of devices created through pseudorandom permutation algorithm.

★ Three type of DoS/DDoS

1. Volumetric attacks

- Consumes the bandwidth of target network or service.
- Send a massive amount of traffic to the target network with the goal of consuming so much bandwidth that users are denied access.
- Bandwidth depletion attack: Flood attack and Amplification attack.

Attacks:-

- UDP flood attack
- ICMP flood attack
- Ping of Death attack
- Smurf attack (IP)

Note:- Volumetric attack is measured in bits per second (Bps).

- Fraggle (UDP)
- Malformed IP packet flood attack.
- Spoofed IP packet flood attack.

2. Protocol Attacks

- Consume other types of resources like connection state tables present in the network infrastructure component such as load balancers, firewalls, and application servers.

Attacks :-

- SYN flood attack
- Fragmentation attack
- Ack flood attack
- TCP State exhaustion attack
- RST attack

~~Note :- Volumetric attacks is measured in bits per second (bps).~~

protocol attack is measured in packets per second (pps).

3. Application Layer Attacks

- Includes low-and-slow attacks, GET/POST flood attacks that target Apache, windows or openBSD vulnerabilities and more.
- Consume the resources necessary for the application to run.
- Target web servers, web application and specific web-based apps.
- Abuse higher-layer (7) protocols like HTTP/HTTPS and SNMP.

Attacks :-
- HTTP GET/POST attack
- Slowloris attack

Note: Application layer attack is measured {is requested per second (RPS)}

Note {Application level attacks are against weak code.}

★ Attacks explanation

★ IP fragmentation attacks

- IP/ICMP fragmentation attack is a common form of volumetric DoS. In such an attack datagram fragmentation mechanisms are used to overwhelm the network.

- Bombard the destination with fragmented packets causing it to use memory to reassemble all those fragments and overwhelm a targeted network

- Can manifest in different ways :-
- UDP flooding - attacker sends large volumes of fragments from numerous sources.
- UDP and ICMP fragmentation attack - only part of the packets is sent to the target. Since the packets are fake and can't be reassembled the server's resources are quickly consumed.

- TCP fragmentation attack — also know as a Teardrop attack ; target TCP/IP reassembly mechanisms ; fragmented packets are prevented from being reassembled. The result is that data packet overlap and the targeted server become completely overwhelmed.

★ **TCP State — exhaustion attack**

- Attempt to consume connection state table like: Load balancers, firewalls and application servers.

★ **Slowloris attack**

Is an application layer which operates by utilizing partial HTTP requests. The attack functions by opening connection to a targeted web server and then keeping those connection open as long as it can.

★ ⟶ (Complete HTTP request - Response cycle) ⟶ (Incomplete HTTP Requests)

- The attacker first opens multiple connections to the targeted server by sending multiple partial HTTP request headers.
- The target opens a thread for each incoming request.
- To prevent the target from timing out the connection the attacker periodically sends partial request headers to the target in order to keep the request alive. In essence saying "i'm still here!"

I'm just slow", please wait for me".

- The targets server is never able to release any of the open partial connections while waiting for the termination of the request.

- Once all available threads are in use, the server will be unable to respond to additional requests made from regular traffic, resulting in denial-of-service

★ SYN attack

- Sends thousands of SYN packets
- uses a fake source address / spoofed IP address.
- The server then responds to each one of the connection request and leaves an open port ready to receive the response.
- Eventually engages all resources and exhaust the machine.

★ SYN flood (half-open attack).

- Sends thousands of SYN packets
- While the server waits for the final ACK packet, which never arrives, the attacker continues to send more SYN packet causes the server to temporarily maintain a new open port connection for

a Certain length of the time, and once all the available port have been utilize the system is unable to function normally.
- Eventually bogs down the computer runs out of resources.

★ ICMP flood
- Sends ICMP Echo packets with a spoofed address; eventualy reaches limit of packets per second sent.
- Is possible to use hping3 to perform ICMP flood:
- hping -1 --flood --rand-source <target>

★ Smurf attack
- The smurf attack is a distributed denial of service attacks in which large numbers of ICMP packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP broadcast address.
- Is possible to use hping3 to perform this attack and bash script to loop through the subnet.
- hping3 -1 -c 1000 10.0.0.$i --fast -a <spoofed>

★ Fraggle
- Same concept as smurf attack but with UDP packets (UDP flood attack)
- is possible to use hping3 to perform fraggle attack (UDP flood.
- hping3 --flood --rand-source --udp -p <target>

★ Ping of Death
- Fragments ICMP messages; after reassemble, the ICMP packet is larger than the maximum size and crashes the system.
- Performs by sending an IP packet larger than the 65,536 byte allowed by the IP p
- old technique that can be acceptable to old systems.

★ Teardrop
- Overlaps a large number of garbled IP fragments with oversized payloads; causes older system to crash due to fragment reassembly

★ Peer to peer
- Clients of peer-to-peer file-sharing hub are disconnected and directed to connect to the target system

★ Multi-Vector attack
- Is a combination of volumetric, protocol, and application-layer attacks.

★ Phlashing / Permanent DoS
- A DoS attack that causes permanent damage to a system
- Modifies the firmware and can also cause a system to brick.
- e.g.: Send fraudulent hardware update to victim; crashing BIOS.

★ LAND attack

- Sends a SYN packet to the target with a spoofed IP the same as the target; if vulnerable, target loops endlessly and crashes.

★ DoS / DDoS Attack Tools :-

- Low orbit Ion Cannon (LOIC) - DDoS tool that floods a target with TCP, UDP or HTTP requests
- High orbit Ion Cannon (HOIC) - More powerful version of LOIC; Targets TCP and UDP; The application can open up to 256 simultaneous attack sessions at once, bringing down a target system by sending a continuous stream of junk traffic until legitimate requests are no longer able to be processed.
- Other tools
  - Hulk
  - Metasploit
  - Nmap
  - Tsunami
  - Trinity - Linux based DDoS tool
  - Tribe flood network - uses voluntary botnet system to launch massive flood attacks
  - RUDY (R-U-Dead-Yet?) - DoS with HTTP POST via long-form field submissions

★ Mitigations

- Traffic analysis
- ACLs
- Filtering
- Reverse proxies
- Firewalls
- Load Balancers
- Rate limiting - limiting the maximum number of connections a single IP address is allowed to make)
- DoS prevention software

3M

Session Hijacking

★ The Session Hijacking

The Session Hijacking attack Consists of the exploitation of the web session Control mechanism which is normally managed for a Session the

- HTTP Communication uses many different TCP Connections, the web Server needs a method to recognize every user's Connections.
- The most useful method depends on a token that the web Server Sends to the Client browser after a Successful client authentication.
- A Session token is normally Composed of a string of Variable width and it Could be used in different ways

-like in the URL, in the header of the HTTP requisition as a Cookie, in other parts of the header of the HTTP request, or Yet in the body of the HTTP requisition.

The Session Hijacking attack Compromises the Session token by Stealing or predicting a Valid Session token to gain unauthorized access to the web Server.

★ The Session token Could be Compromised in different ways; the most Common are:

predictable Session token

- The Session ID information for a Certain application is normally Composed by a string of fixed width. Randomness is Very imp to avoid its prediction.

- Example: Session ID Value is 'user01', which

corresponds to the username. By trying new values for it, like 'user02', it could be possible to get inside the application without prior authentication.

★ **Session Sniffing**

- Sniffing can be used to hijack a session when there is non-encrypted communication between the web server and the user, and the session ID is being sent in plain text.
- wireshark and kismet can be used to capture sensitive data packets such as the session ID from the network.

★ **Cross-Site Scripting (XSS)**

- A server can be vulnerable to a Cross-Site Scripting exploit, which enables an attacker to execute malicious code from the user's side, gathering session information. An attacker can target a victim's browser and send a scripted Javascript link, which upon opening by the user, runs the malicious code in the browser hijacking sessions.

★ **CSRF** - Cross-Site Request forgery

- Forces an end user to execute unwanted actions on a web application in which they're currently authenticated, with a little help of social engineering (such as sending a link via email or chat), an attacker may trick the users of a web application into executing actions of the attacker's choosing;

- CSRF attack can force the user to perform state changing requests like transferring funds, changing their email address, and so forth. If the victim is an administrative account CSRF can compromise the entire web application.

- CSRF Scenario :-

i. Visit your bank's site, log in.
ii. Then visit the attacker's site (e.g. sponsored ad from an untrusted organization).
iii. Attacker's page includes form with same field as the bank's "Transfer funds" form.
iv. Form fields are pre-filled to transfer money from your account to attacker's account.
v. Attacker's page includes Javascript that submits form to your bank.
vi. When form gets submitted, browser includes your cookies for the bank site, including the session token.
vii. Bank transfers money to attacker's account.
viii. The form can be in an iframe that is invisible, so you never know the attack occurs.

★ Session Fixation

- Session fixation is an attack that permits an attacker to hijack a valid user session. The attack explores a limitation in the way the web application manages the session ID, more specifically the vulnerable web application

- Session fixation Scenario :-

i. The attacker accesses the web application login page and receives a session ID generated by the web application.

ii. The attacker uses an additional technique such as CRLF injection, man-in-the-middle attack, Social engineering, etc. and gets the Victim to use the provided session identifier.

iii. The Victim accesses the web application login page and logs in to the application. After authenticating, the web application treats anyone who uses this Session ID as if they were this user.

iv. The attacker uses the session ID to access the web application, take over the user session, and impersonate the victim.

★ Man-in-the-browser attack

- The man-in-the-Browser attack is the same approach as Man-in-the-middle attack, but in this case a Trojan Horse is used to intercept and manipulate calls between the main applications executable.

★ Man-in-the-middle attack

- MITM attack is a general term for when a perpetrator positions himself in a conversation between a user and an application - either to eavesdrop or to impersonate one of the parties making it appear as if a normal exchange of information is underway.

★ Other attacks

- Compression Ratio info-leak made Easy (CRIME):
  - Is a security exploit against secret web Cookies over Connections using the HTTPS and SPDY protocols that also use data compr. when used to recover the Content of Secret authentication cookies, it allows an attacker to perform Session hijacking.
- BREACH:
  - Is a Security exploit against HTTPS when using HTTP Compression (SSL/TLS Compression). BREACH is built based on the CRIME Security exploit.

⚠ Note → SPDY protocol manipulates HTTP traffic with particular goals of reducing web page load latency and improving web Security.

- Forbidden Attack Vulnerability in TLS that informs reuse the Same Cryptographic nonce when data is encrypted. TLS specifications are Clear that these arbitary pieces of data Should be used only once. When the Same one is used more than once, it provides an opportunity to Carry out the forbidden attack.

★ Network Layer attacks

- TCP Hijacking: TCP/IP Hijacking is when an authorized user gains access to a genuine network Connection of another user. It is done in order to bypass the password authentic

which is normally the start of a session.
- e.g: TELNET hijacking using Ettercap, Shijack
making a blind hijacking.

★ Tools
- Ettercap – MITM tools and packet sniffer on steroids
- Hunt – Sniff, hijack and reset connections
- T-Sight – easily hijack sessions and monitor network connection.
- Zaproxy • Burp suite • paros • Shijack-Tulp
- Juggernaut • Hamster • Ferret

★ Countermeasures
- Session IDS – using unpredictable (randomized) session IDs
  – Never use URL's with sessions IDs – Don't Re-use session IDs
- use HTTP – only on Cookies preventing XSS (cross-site scripting)
- Don't use HTTP protocol without encryption ⇒ use TLS/SSL [HTTPS]
- Limiting incoming connections
- Minimizing remote access
- Regenerating the session key after authentication
- Time – absolute / inactive (e.g 1h of inactivity the user will automatically log off)
- use MFA
- Use IPSec to encrypt.

★ IP Sec

- Transport Mode - payloads and ESP trailer are encrypted ; IP header is not
- Tunnel Mode - everything is encrypted; Cannot be used with NAT.
- Architecture protocols
- Authentication Header - guarantees the integrity and authentication of IP packet sender
- Encapsulating Security payload (ESP) - provides Origin authenticity and integrity as well as Confidentiality
- Internet Key Exchange (IKE) - produces the keys for the encryption process
- Oakley - uses Diffie Hellman to create master and session keys
- Internet Security Association Key management protocol (ISAKMP) - Software that facilitates encrypted communication between two endpoints

Port = 500

(5M)

Evading IDS, Firewalls and Honeypots

* IDS / IPS – Basic Concepts

* Intrusion prevention system (IPS) – ACTIVE monitoring of activity looking for anomalies and alerting / notifying AND taking action when they are found.

* Intrusion Detection System (IDS) – PASSIVE monitoring of activity looking for anomalies and alerting / notifying when they are found.

* Deployment types – HIDS & NIDS & WIDS :

1. Host based – Monitors activity on a single device/host by being installed locally.
2. Network based – Monitors activity across a Network using remote sensor that report back to a central system. Often paired with a Security Information & SIEM System for analysis. Often Reverse ARP or Reverse DNS lookups are used to discover the source

* Knowledge & Behavior – Based Detection :-

1. Knowledge Based (Signature Based / pattern Matching) – is Most Common form of detection. uses a database of profiles, or signatures to assess all traffic against.
2. Behavior Based (Statistical / Anomaly / Heuristic) – Starts by creating a baseline of behaviour for the monitored system / network and then compares all traffic against that

looking for deviations. Can be labeled an AI or Expert System.

★ Types of IDS Alerts

- True positive --> Attack - Alert ☑ ☑
- False positive --> No Attack - Alert ☒ ☑
- False Negative --> Attack - No Alert ☑ ☒
- True Negative --> No Attack - No Alert ☒ ☒

★ Firewalls - Basic Concepts

Firewalls are often seen as NAC devices. Use of rule sets to filter traffic can implement security policy.

★ Firewalls types :-

- Stateful (Dynamic packet filtering) - layer 3+4 (Network + transport layer)
- Stateless (Static packet filtering) - Layer 3 (Network)
- Deep packet Inspection - Layer 7 (Application layer)
- proxy firewall - Mediates communications between untrusted and trusted end-points (Server/host Clients). A proxy firewall is a network security system that protects network resources by filtering messages at the Application layer 7. A proxy firewall may also be called an application firewall or gateway firewall.

* Proxy Types :-

- Circuit - level proxy - Firewall that works on layer 5 (Session layer); They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- Application - level proxy - Any service or server that act as a proxy for client computer requests at the application's protocols.

An application - level proxy is one that know about the particular application it is providing proxy service for; it understands and interprets the contents in the application protocol. A circuit - level proxy is one that creates a circuit between the client and the server without interpreting the application protocol.

- Multi - homed firewall (dual - homed) - Firewall that has two or more interface; One interface is connected to the untrusted network and another interface is connected to the trusted network. A DMZ can be added to a multi-homed firewall just by adding a third interface.
- Bastion hosts - Endpoint that is exposed to the Internet but has been hardened to withstand attacks; Hosts on the Screened Subnet designed to protect internal resources.

- Screened host – Endpoint that is protected by a firewall.
- Packet-filtering – Firewall that only looked at headers.

Note ⇒ Only uses rules that implicity denies traffic unless it is allowed.

Note ⇒ Oftentimes uses network address translation (NAT) which can apply a one-to-one or one-to-many relationship between external and internal IP addresses.

Note ⇒ Private Zone – hosts internal hosts that only respond to requests from within that zone.

★ Honeypots

Honeypots are decoy systems or servers deployed alongside production systems within your network. When deployed as enticing targets for attackers, honeypots can add security monitoring opportunities for blue teams and misdirect the adversary from their true target.

- Honeynet – Two or more honeypots on a network from a honeynet. Honeynets and honeypots are usually implemented as part of larger Network intrusion Detection Systems
- A Honeyfarm is a centralized collection of honeypots and analysis tools.

* Types of Honeypots :-

1. Low - interaction -> Simulates / imitate Service and System that frequently attract Criminal Attention. They offer a method for collecting data from blind attack such as botnets and Worms Malware.
2. High interaction -> Simulates all services and applications and is designed to be completely compromised.
3. Production -> Serve as decoy systems inside fully operating networking networks and serving often as part of an intrusion detection System(IDS). They deflect Criminal attention from the real System while analyzing malicious activity to help mitigate vulnerabilities.
4. Research -> Used for educational purpose and security enhancement. They contain trackable data that you can trace when stolen to analyze the attack.

- Honeypot Tools :-
  - Spector
  - Honeyd
  - Kf Sensor (Honeypot IDS)

* Evading with Nmap

* Useful Switches for Evading and Stealthy :-

(P.T.O)

Nmap Switch		Information
-V	=>	Verbose level
-sS	=>	TCP SYN Scan
-T	=>	Time template for performance
-f	=>	use fragmented IP packets
-f --mtu	=>	use fragmented IP packets
-D	=>	IP address Delay: <delay1,delay2[ms]> Scan with delays.
-S	=>	Spoof the Source IP address
--Send-eth	=>	Ensures that we use Ethernet level packets. bypassing the IP layer and sending raw Ethernet frames within the frame
--data-length	=>	Specify the length of data/frame
--Source-port	=>	Specify a randomized port that you will communicate

★ Example :-

- Sends IPv4 fragmented 50-byte packet size; The packets are too small to send data and to detect as a probe /Scanning technique :

=> nmap -V -SS -f -mtu 32 --Send-eth -data-length 50 --Source-port 8965 -T5 192.168.0.22

Note => Fragmentation is the heart of the IDS/Firewall Evasion techniques.

* Using SNORT

SNORT is an open Source Network intrusion detection System (NIDS). Snort is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies.

- Snort is a widely deployed IDS that is open source
- Includes a sniffer, traffic logger and a protocol analyzer
- Runs in three different modes
  - Sniffer - watches packets in real time
  - Packet logger - Saves packets to disk for review at a later time.
  - NIDS - Analyzes network traffic against various rule sets.
- Configuration is in /etc/snort on Linux and C:\snort\etc in windows; the file is snort.conf

* SNORT basics Commands :-

Operational modes :-

- Snort as Sniffer -> Snort -V
- Snort as packet logger -> Snort -l
- Snort as NIDS -> Snort -A or Snort -c <path_to_conf_file>

? Example of usage :-

- Snort -i 4 -l C:\Snort\log -c C:\Snort\etc\Snort.conf -l

- This Command will test Snort Configuration and rules and check if there is any error without starting up.
- -i4 -> interface specifier, in case is interface 4.
- -l -> for logging.
- -c -> use Snort rules file specifying path
- -T -> only for testing, this prevent Snort from start up; Essentially to check if there is any errors and if the rules are good.

- Snort -i4 -c
  C:\Snort\etc\Snort.Conf -l
  C:\Snort\log -K ascii
- This Command will fire up Snort NIDS and log everything in ASCII.

Basic Command

Flag	Information
-> -A	-> Set alert mode: fast full, console, test
-> -b	-> Log packets in tcpdump format (binary)
-> -B <mask>	-> obfuscate IP addresses in alert and packet dump using CIDR mask
-> -c <rules>	-> use Rules file
-> -C	-> print out payload with character data only (no hex)
-> -l	-> Specifies the logging directory (all alert and packet logs are placed in this directory.
-> -i<interface number>	-> Specifies which interface Snort should
-> -K	-> Logging mode (pcap [default], ascii, none)
-> -?	-> List all switches and options and then ex

★ SNORT Rules

SNORT has a rules engine that allows for customization of monitoring and detection capabilities.

- There are three available rule actions.
  - i. Alert
  - ii. Pass
  - iii. Log

- And three available IP protocols :-
  - i. TCP
  - ii. UDP
  - iii. ICMP

★ Breaking down a Snort rule :-

- alert ICMP any any -> $HOME_NET any (Msg: "ICMP test"; Sid : 100001 ; rev : 1 ; Classtype : icmp-event;)

Rule part	Information
	Rule Header ★
→ alert icmp any any → $HOME_NET any	Rule action Snort will generate an alerts when the set condition is met.
→ alert	Source IP. Snort will look at all sources
→ any (1st)	Source port. Snort will look at all port.
→ any (2nd)	Direction. From source to destination.
→ ->	Destination IP. we are using the HOME_NET
→ $HOME_NET	Value from the Snort.conf file which means a variable that defines the network or networks you are trying to protect.

-> any (3rd)	Destination port. Snort will look at ports on the protected Network
-> (msg: "ICMP test"; sid: 1000001; rev: 1; classtype: icmp-event;)	Rule options
-> msg: "ICMP test"	Snort will include this message with the alert.
-> sid: 1000001	Snort rule ID. Remember all numbers < 1,000,000 are reserved, this is why we are starting in 1000001 (you may use any number, as long as it's greater that 1,000,000)
-> rev: 1	Revision number. This option allows for easier rule maintenance.
-> Classtype: icmp-event	Categorizes the rule as an "icmp-event" one of the predefined Snort Categories. This option helps with the rules organization

★ Rules examples:

- alert tcp 192.168.x.x any -> $HOME_NET 21 (msg: "FTP Connection attempt"; sid: 100002; rev: 1;)

- TCP alert in a Source IP address 192.168.x.x with any port; HOME_NET destination on port 21
- alert tcp $HOME_NET 21 -> any any (msg: "FTP failed login"; content: "login or password incorrect"; sid: 100003; rev: 1;).

- TCP alert in HOME_NET port 21 (FTP) as a Source to any destination IP address and port.

- alert tcp !HOME_NET any -> $HOME_NET 31337 (msg : "BackDoor ATTEMPTT - Backorifice)

- This alerts about trafic coming out from an external network to the internal one on port 31337.

* Example output
- 10/19 -14 : 48 : 38 . 543734 0:48:542:2A:67 -> 0:10:B5:3C:34:C4 type:0X800 len:0X5EA
- XXX -> XXX TCP TTL:64 TOS : 0X0 ID: 18112 IPLen: 20 DgmLen: 1500 DF
- Important info is bolded.

* Evasion Concepts and Techniques.

- Insertion Attack - Attacker forces the IDS to process invalid packets.
- Evasion - An endpoin accepts a packet that the IDS would normally reject.

Typically executed via fragmentation of the attack packets to allow them to be moved through the IDS.

- obfuscation - Encoding the attack packets in such a way that the target is able to decode them, but the IDS is not.
- unicode
- polymorphic code
- Encryption
- path manipulation to cause signature mismatch.

- False positive Generation Events – Crafting malicious packets designed to set off alarms with hope of distracting/overwhelming IDS and operators.
- Session Splicing – just another type of fragmentation attack.
- Unicode encoding – Works with web request using unicode characters instead of ascii can sometimes get past.
- Fragmentation attack – splits up packets so that the IDS can't detect the real intent.
- Overlapping fragments – Generate a bunch of tiny fragments overlapping TCP sequence numbers.
- Time-to-Live (TTL) Attack – Requires the attacker to have inside knowledge of the target network to allow for the adjustment of the TTL values to control who get what packets when.
- Invalid RST Packets – Manipulation of the RST flag to trick IDS into ignoring the communication session with the target.
- Urgency flag – URG – Manipulation URG flag to cause the target and IDS to have different sets of packets, because the IDS processes all packets irrespective of the URG flag whereas the target will only process URG traffic.
- Polymorphic Shellcode – Blows up the pattern match by constantly changing.

- ASCII ShellCode - use ASCII charecters to bypass pattern matching
- Application - Level Attack - Taking advantage of the compression used to transfer large files and hide attacks in compressed data, as it cannot be examined by the IDS.
- Desynchronization - Manipulation the TCP SYN to fool IDS into not paying attention to the sequence number of the illegitimate attack traffic, but rather, give it a false set of sequences to follow.
- Encryption - using encryption to hide attack.
- Flood the network - Trigger alerts that aren't your intended attack so that you confuse firewall / IDS and network admins; overwhelming the IDS.

Note :> Slow down - Faster scanning such as using nmap's -T5 switch will get you caught. pros use -T1 switch to get better results.

Tools for Evasion
- Nessus - Also a vulnerability scanner
- ADMmutate - Creates scripts not recognizable by signature files
- NIDSbench - Older tool for fragmenting bits
- Inundator - Flooding tool

★ Firewall Evasion

- Firewalking – using TTL Values to determine gateway ACL filters and allows for mapping of internal networks by analyzing IP packet responses; going through every port on a firewall to determine what is open.
- Banner Grabbing – Looking for FTP, TELNET and web server banners
- IP Address Spoofing – Hijacking technique allowing attacker to masquerade as a trusted host.
- Source Routing – Allows the sender of a packet to partially or fully specify the route to be used.
- Tiny Fragments – Sucessful with firewall when they only check for the TCP header info, allowing the fragmentation of the information across multiple packets to hide the true intention of the attack.
- ICMP Tunneling – Allows for the tunneling of a backdoor shell via the ICMP echo packets because the RFC (792) does not clearly define what kind of data goes in the data protection of the frame, allowing for attack traffic to be seen as acceptable when inserted. If firewalls do not examine the payload section of the dataframe, they would let the data through, allowing the attack.
- HTTP Tunneling – use of HTTP traffic to hide attacks.

- ACK Tunneling – use of the ACK flag to trick firewall into allowing packets, as many firewall do not check ACK packets.
- SSH Tunneling – use of SSH to encrypt and send attack traffic.
- MITM Attack – use of DNS and routing manipulation to bypass firewalls.
- XSS Attack – Allows for the exploitation of vulnerabilities around the processing of input parameters from the end user and the server responses in a web application. The attacker injects malicious HTML/JS code into website to force the bypassing of the firewall once executed.
- Use IP in place of a URL – may work depending on nature of filtering in place.
- Use proxy Server/Anonymizers – May work depending on nature of filtering in place.
- ICMP Type 3 Code 13 will show that traffic is being blocked by firewall
- ICMP Type 3 Code 3 tells you the client itself has the port closed.
- Tools
  - Covert TCP
  - ICMP Shell
  - 007 Shell
- The best way around a firewall will always be a compromised internal machine.

★ How to detect a Honeypot

Probe Services running on them; ports that show a service is available, but deny a three-way handshake may indicate that the System is a honeypot.

- Layer 7 (Application) – Examine latency of responses from Server
- Layer 4 (Transport) – Examine the TCP windows size, looking for continuous Acknowledgement of incoming packets even when the windows size is set to 0.
- Layer 2 (Data link) – if you are on the same network as the honeypot, look for MAC addresses in packets that indicate the presence of a 'Black Hole' (0:0:f:ff:ff:ff)

Note ① => The exam will not cover every information presented but is good to have a general idea.

- If Honeypot is virtualized, look for the Vendor assigned MAC address ranges as published by IEEE.
- If Honeypot is the Honeyd type, use time based TCP fingerprinting method to detect.
- Detecting User-Mode Linux (UML) honeypot, analyze proc/mounts, proc/interrupts and proc/cmdline which would have UML specific settings and information.
- Detecting Sebek-based honeypots, Sebek will log everything that is allessed via read() before sending to the network, causing congestion that can be anomalous.
- Detecting Snort-inline honeypots, analyze the outgoing packets by capturing the Snort-inline modified packets through another.

Type of firewall.

CVSS chart dekhna h.

Type of SSL inspection

Tier-1 -> Developer machines - image creation testing and accreditation.

Tier-2 -> Testing and accreditation System - Verification & validation of image contents, signing image & sending them to registries

Tier-3 -> Registries - Storing images and distributing image to the Orchestrators based on requests

Tier-4 -> Orchestrators - transforming image into containers and deploying containers to hosts

Tier-5 -> Hosts - operating and managing containers as instructed by the orchestrator.

* Vulnerability management life-cycle management
1. Identify assets and creat a baseline
2. Vulnerability scan
3. Risk assesment
4. Remediation (Stop krna)
5. Verification
6. Monitor

* 2017 OWASP Top 10 list

-> A01 : 2017 - Injection
-> A02 : 2017 - Broken Authentication.
-> A03 : 2017 - Sensitive Data Exposure
-> A04 : 2017 - XML External Entities (XXE)
-> A05 : 2017 - Broken Access Control
-> A06 : 2017 - Security misconfiguration
-> A07 : 2017 - Cross Site Scripting (XSS)
-> A08 : 2017 - Insecure Deserialization
-> A09 : 2017 - Using Components with known Vulnerabilities
-> A10 : 2017 - Insufficient logging & monitoring

OWASP Top 10

=> The OWASP Top 10 is a Standard awareness document for developers and web application security.
It represents a broad consensus about the most critical security risks to web applications.

Companies should adopt this document and start the process of ensuring that their web applications minimize these risks, using the OWASP Top 10 is perhaps the most effective first step towards changing the software development culture within your organization into one that produces more secure code.

★ Top 10 web application security Risks :-
There are three new categories, four categories with naming and slaping changes, and some consolidation in the Top 10 for 2021.

=> A01:2021 - Broken Access Control
=> A02:2021 - Cryptographic failures
=> A03:2021 - Injection
=> A04:2021 - Insecure Design.
=> A05:2021 - Security misconfiguration.
=> A06:2021 - Vulnerable and outdated Components
=> A07:2021 - Identification and Authentication failures.
=> A08:2021 - Software and Data Integrity failures.
=> A09:2021 - Security Logging and monitoring failures
=> A10:2021 - Server Side Request forgery (SSRF)