Introduction to Ethical Hacking

Footprinting

Scanning Networks

System Hacking

Wireless Networks and Spoofing

Social Engineering

Firewalls and Honeypots

Hacking Web Servers and Web Applications

Cryptography

Introduction to Ethical Hacking

OVERVIEW OF INFORMATION SECURITY

OVERVIEW OF INFORMATION THREATS AND ATTACKS

INTRODUCTION TO HACKING

PROTECTING INFORMATION

PENETRATION TESTING

LAWS, STANDARDS, AND REGULATIONS

COMMON TERMS

To understand the process of hacking, it is important to understand the following terms:

- Hack value

  Hack value is hackers' way of deciding whether something is worth doing or not. If something is considered to be of high value to a hacker, they will put all of their effort and energy into the hack.

- Vulnerability

  Vulnerability is a weakness which can compromise the system and be used for a possible attack.

- Exploit

  Exploit is a piece of code which takes advantage of the identified vulnerability to deliver the malicious code.

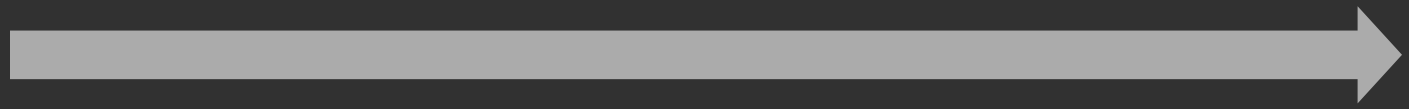
- Payload

  Payload is the malicious code that is executed through the exploit.

COMMON TERMS

- Zero-Day attack

  Exploiting previously unknown vulnerabilities that have not been patched yet is called a zero-day attack.



Introduction to Ethical Hacking

COMMON TERMS

- Daisy chaining

  Daisy chaining is an attack in which hackers gain access to one computer or network and then use that computer to access the next computer or network.

Introduction to Ethical Hacking

COMMON TERMS

- Doxing

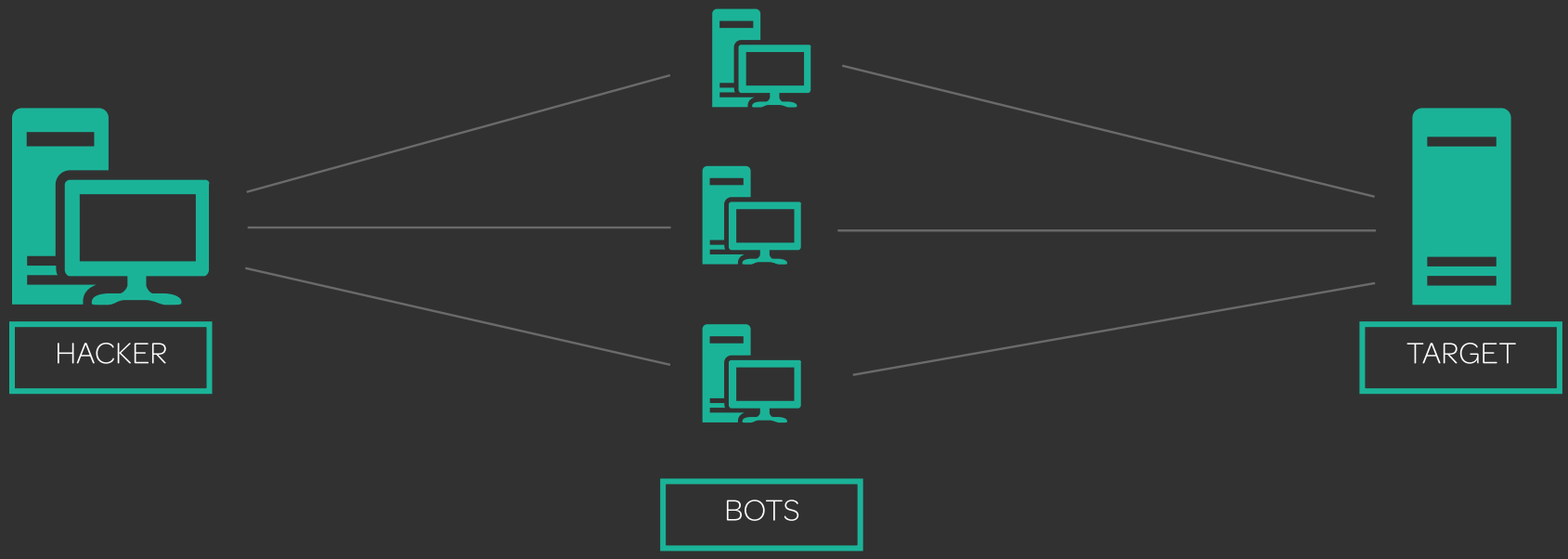
Doxing involves gathering private and valuable information about a person or organization and then misusing that information for different reasons.

Introduction to Ethical Hacking

COMMON TERMS

- Bot

  Bots are malicious programs used by hackers to control the infected machines.



INFORMATION SECURITY

Information security refers to a set of processes and activities performed in order to protect information. The main objective is to prevent unauthorized access to systems and networks.

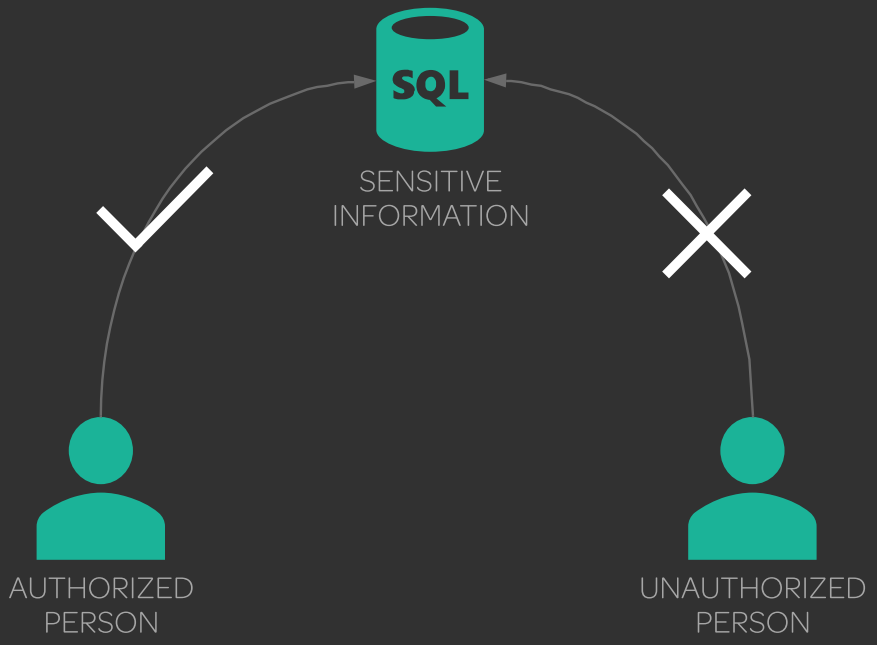
INFORMATION SECURITY

Five elements of information security:

1. Confidentiality
2. Integrity
3. Availability
4. Authenticity
5. Non-repudiation

INFORMATION SECURITY

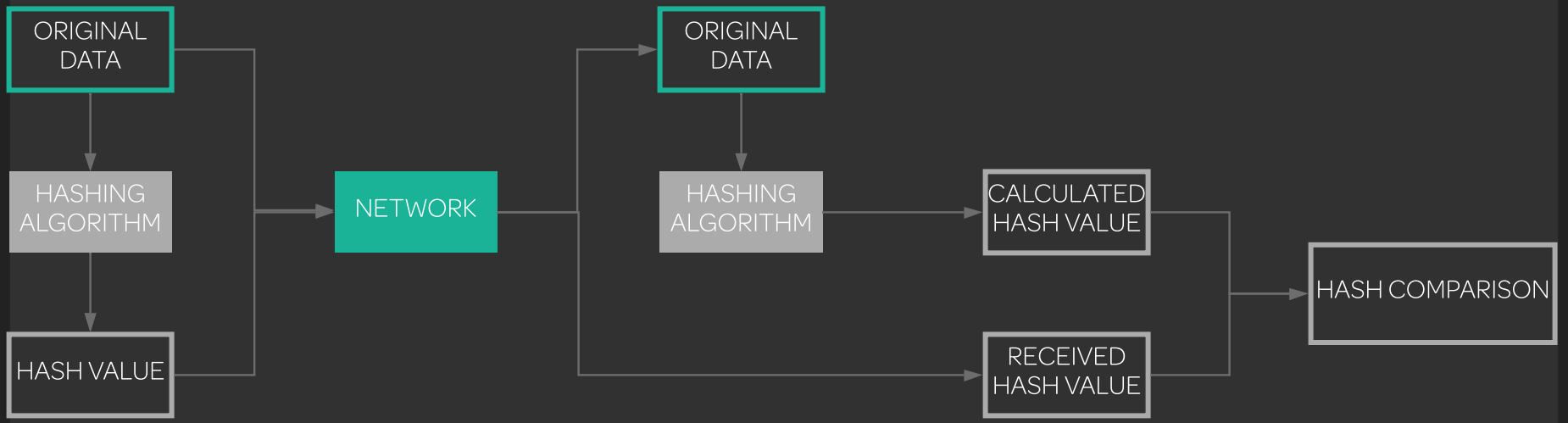
Confidentiality ensures that the information is available only to people who have the authorization to access it.



Introduction to Ethical Hacking

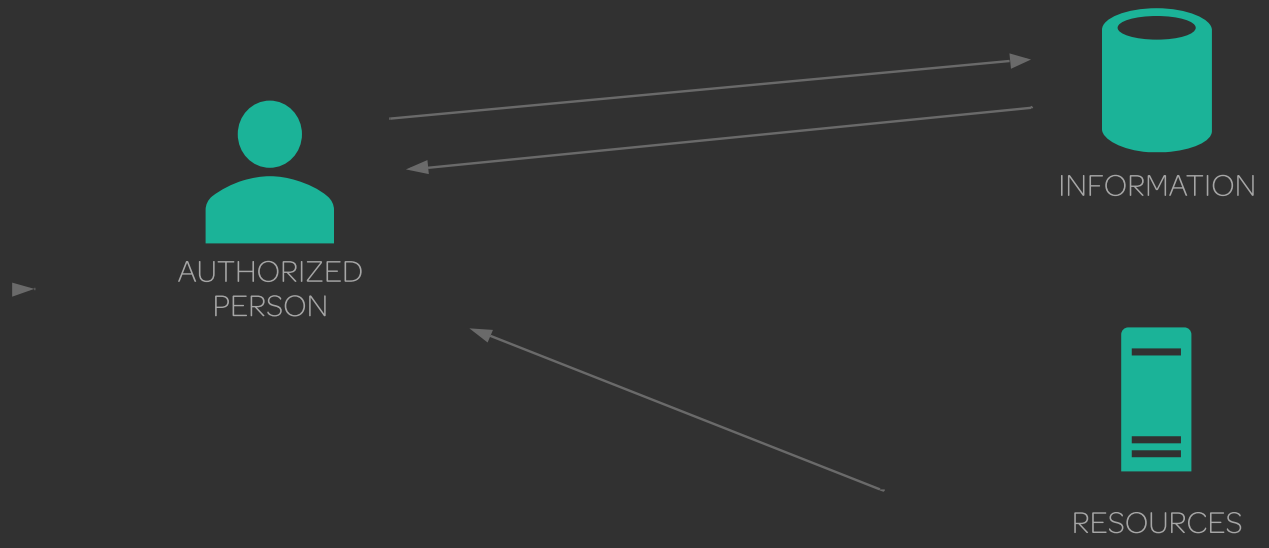
INFORMATION SECURITY

Integrity ensures the accuracy of the information. Using hashing helps in keeping the integrity of information.



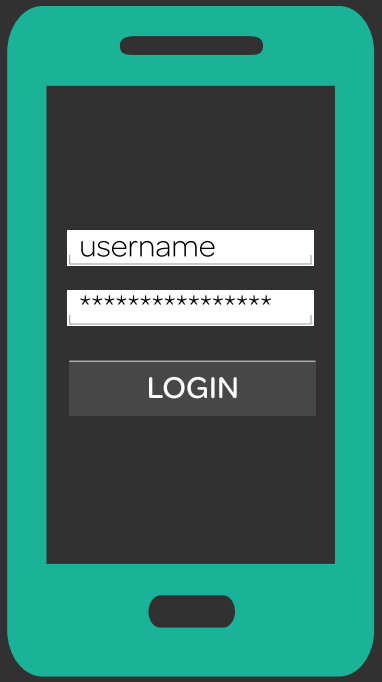
INFORMATION SECURITY

Availability ensures that the resources are available whenever the authorized user needs them.



INFORMATION SECURITY

Authenticity ensures that users are actually who they present themselves to be, or that the document or information presented is not corrupted.



INFORMATION SECURITY

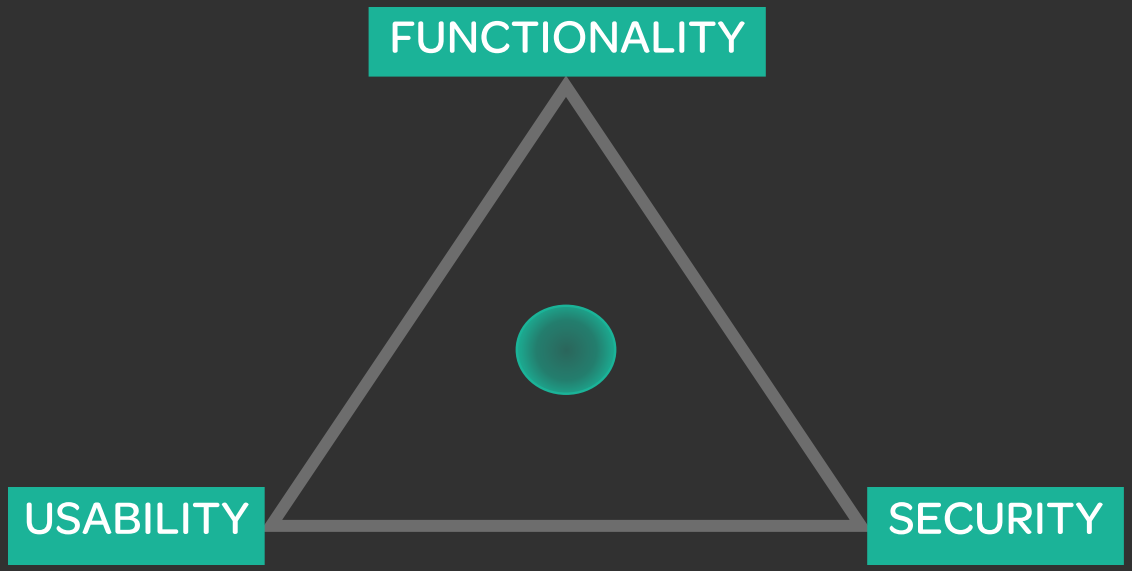
Non-repudiation ensures that a person cannot deny the authenticity of their signature on a document or a message sent by them.

DEFINING THE LEVEL OF SECURITY OF A SYSTEM

Functionality refers to the features of the system.

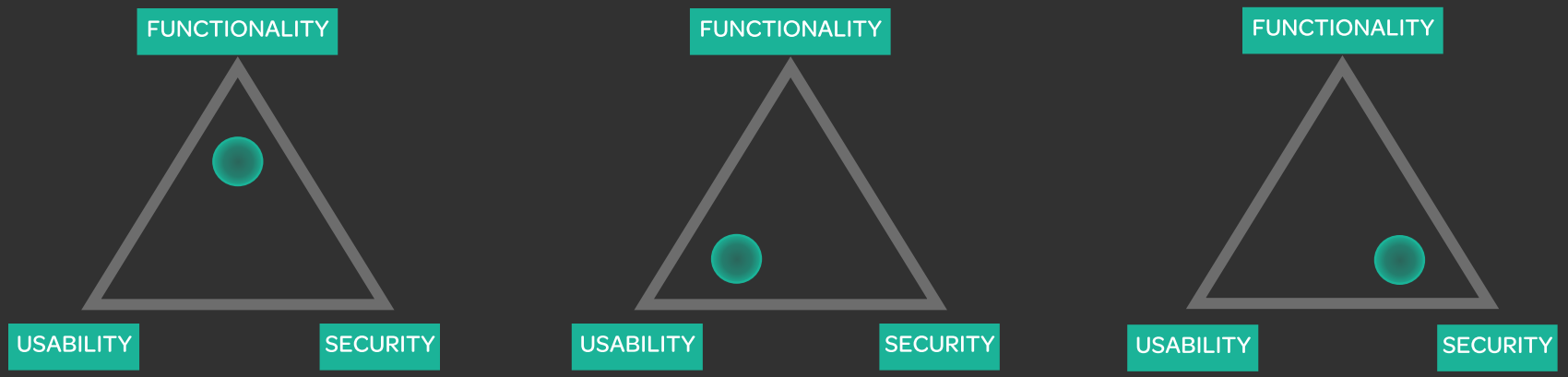
Usability refers to the GUI of the system and how user friendly it is.

Security refers to how the processes of the system are used and who is using them.



Introduction to Ethical Hacking

DEFINING THE LEVEL OF SECURITY OF A SYSTEM



WHY ARE CYBER ATTACKS PERFORMED?

Information security refers to a set of processes and activities performed in order to protect information. The more valuable information is, the higher the threats and chances for an attack are.

Introduction to Ethical Hacking

THREAT vs ATTACK

Security threat refers to anything that has a potential of causing damage to a system.
Security attack (cyber attack) refers to an attempt to gain unauthorized access to a system or network.

WHAT ARE THE MOTIVES BEHIND SECURITY ATTACKS?

Motive comes from the thought that a system has valuable information stored and as such is a potential target for an attack.

Some of the most common motives behind cyber attacks are:

- Revenge
- Ransom
- Interrupting the flow of business activities and processes
- Stealing valuable information
- Data manipulation
- Stealing money

ATTACK VECTORS

Attack vectors are means by which hackers deliver a payload to systems and networks.

COMMON ATTACK VECTORS

- Cloud Computing Threats
- Advanced Persistent Threats
- Viruses and Worms
- Ransomware
- Mobile Threats
- Botnets
- Insider attacks
- Phishing
- Web Application Threats
- IoT Threats

Introduction to Ethical Hacking

ATTACK VECTORS

Cloud Computing Threats | some of the cloud computing threats include stealing information from other cloud users, data loss, and attack on sensitive information

Botnets | malicious programs used by hackers with the intent to perform malicious activities from the machines on which bots run

Advanced Persistent Threats | refer to stealing information without the target being aware of the attack

Insider Threats | performed by a person from within the organization who has authorized access

Viruses and Worms | replicate themselves to programs and documents on the victim machine. They have capabilities to infect systems and networks in a matter of seconds

Phishing | refers to using deceptive emails to gather personal or account information

Ransomware | type of malware in which hackers restrict access to files and folders on the target system until a payment is made

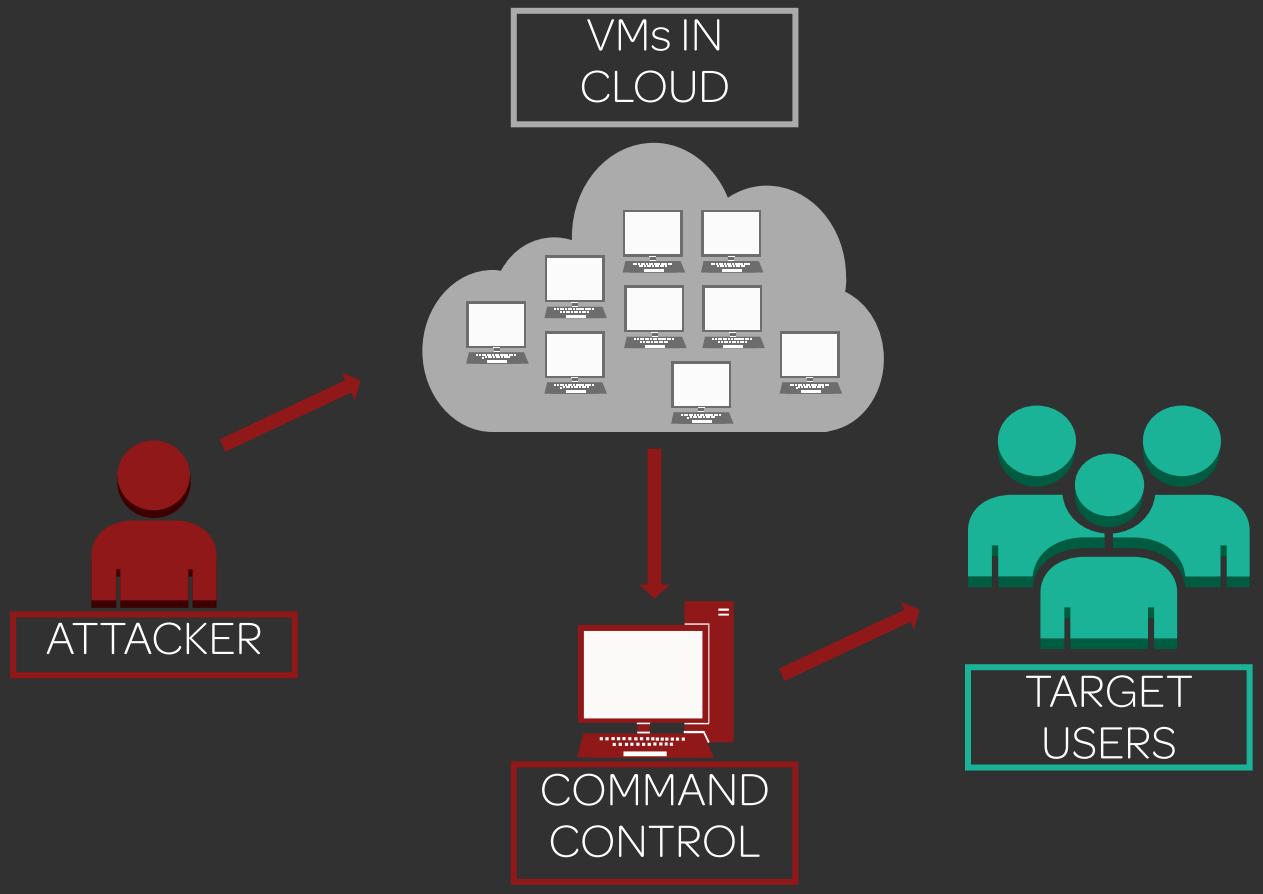
Web Application Threats | take advantage of poorly written code and lack of proper validation on input and output data

Mobile Threats | through malware applications delivered to targets' smartphones, attackers can track their targets and their activities

IoT Threats | take advantage of the lack of security mechanisms in IoT devices due to different hardware constraints

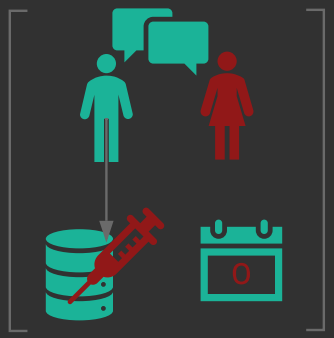
Introduction to Ethical Hacking

CLOUD COMPUTING THREATS



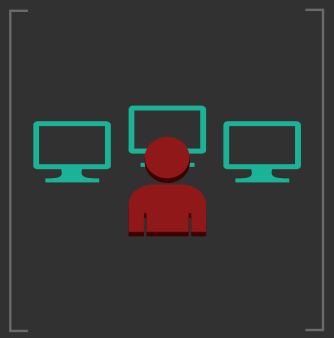
Introduction to Ethical Hacking

ADVANCED PERSISTENT THREATS

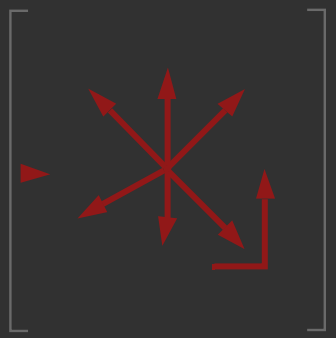


BREACH

EXPLOIT



CONTROL



EXFILTRATION

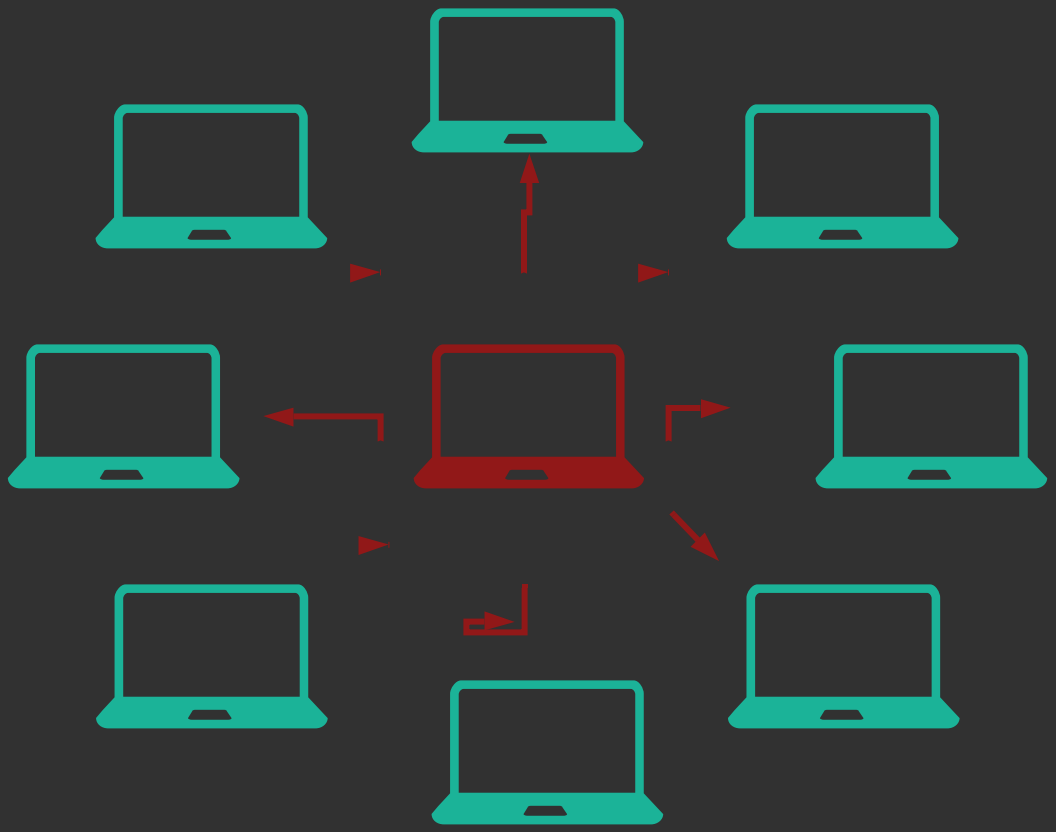
VIRUSES AND WORMS

RANSOMWARE

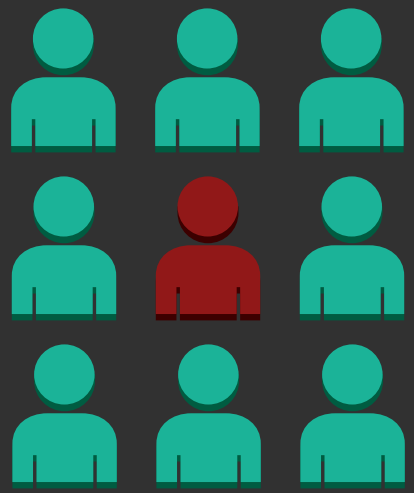
MOBILE THREATS

MOBILE THREATS

BOTNETS



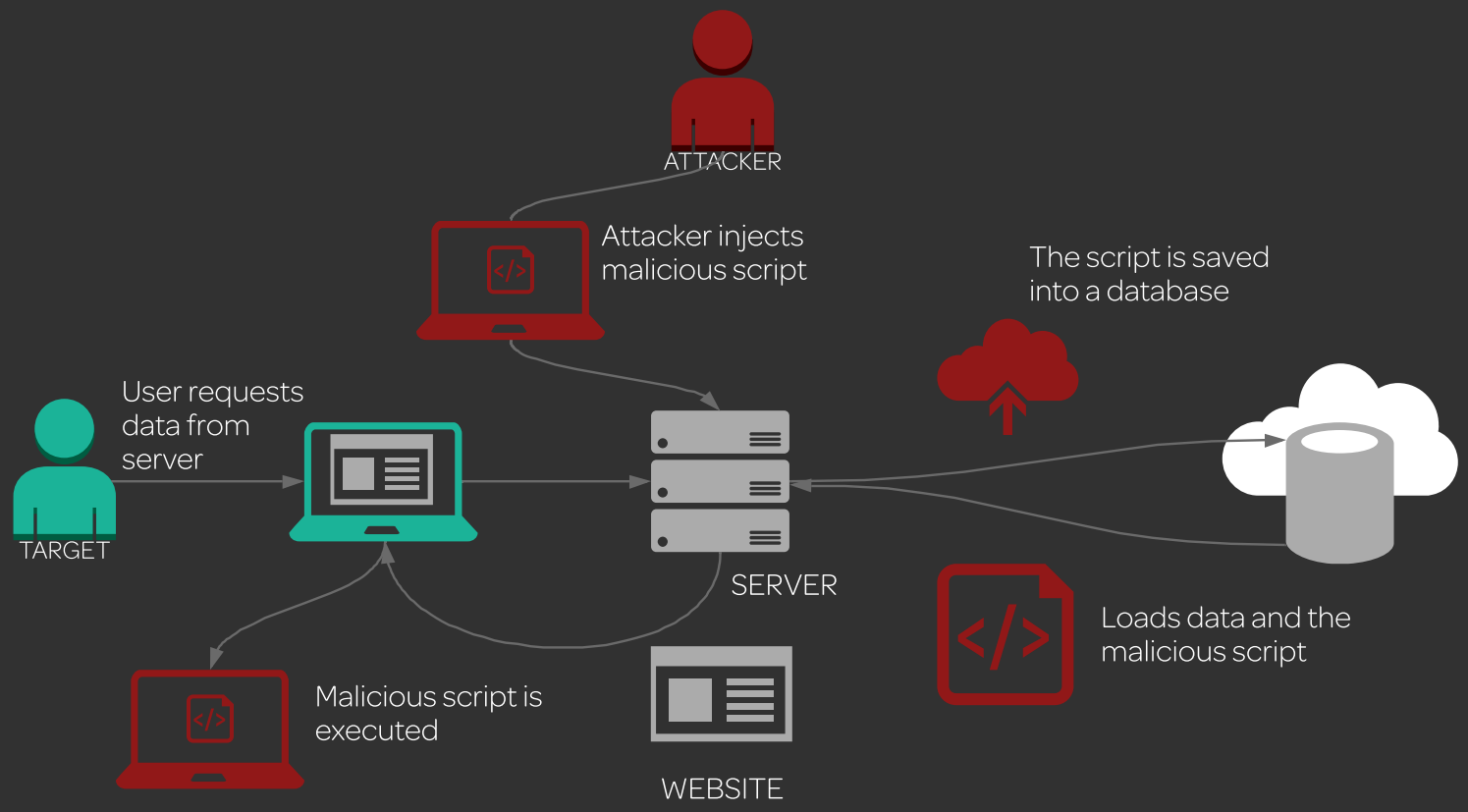
INSIDER ATTACKS



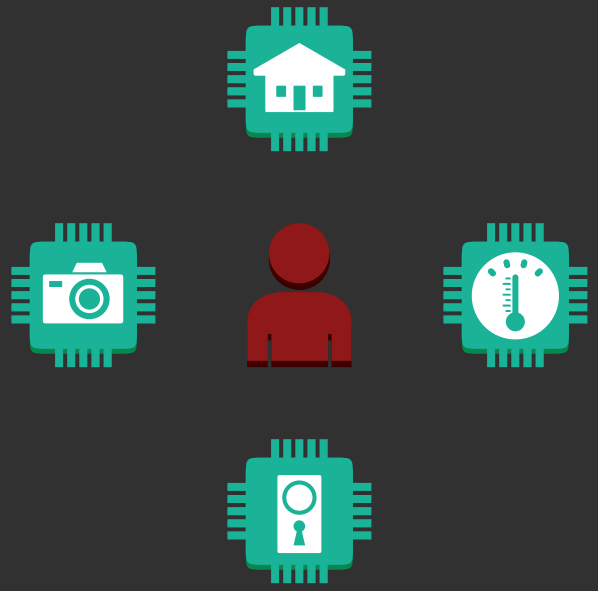
PHISHING

Introduction to Ethical Hacking

WEB APPLICATION THREATS



IoT THREATS



Introduction to Ethical Hacking

THREAT CLASSIFICATION

NETWORK THREATS

Systems exchange information over networks, and during that exchange of information a hacker can break into the communication channel and steal the information that is being exchanged.

- Denial of Service attacks
- Password-based attacks
- Compromised-key attacks
- Firewall and IDS attacks
- DNS and ARP poisoning
- Man in the middle attack
- Spoofing
- Session hijacking
- Information gathering
- Sniffing

HOST THREATS

Host threat refers to the attack on a specific system in an attempt to gain access to the information that resides on the system.

- Password attacks
- Unauthorized access
- Profiling
- Malware attacks
- Footprinting
- Denial of Service attacks
- Arbitrary code execution
- Privilege escalation
- Backdoor attacks
- Physical security threats

APPLICATION THREATS

Application threat refers to the exploit of vulnerabilities that are present in the application due to the lack of proper security measures in the application.

- SQL injection
- Cross-site scripting
- Session hijacking
- Identity spoofing
- Improper input validation
- Security misconfiguration
- Information disclosure
- Hidden-field manipulation
- Broken session management
- Cryptography attacks
- Buffer overflow issue
- Phishing

Introduction to Ethical Hacking

ATTACK CLASSIFICATION

OPERATING SYSTEM ATTACKS

Protecting the system from OS attacks requires regular monitoring of the network as well as being informed about the latest trends in this area of knowledge and expertise.

- Bugs
- Buffer overflow
- Unpatched Operating Systems
- Exploit of the implementation of a specific network protocol
- Cracking passwords
- Breaking filesystem security

APPLICATION-LEVEL ATTACKS

Applications nowadays are prone to vulnerabilities due to the developers' inability to properly and thoroughly test the code. Hackers use different tools and techniques in order to discover and exploit these vulnerabilities and thus gain access to the application information.

- Sensitive information disclosure
- Buffer overflow attack
- SQL injection
- Cross-site scripting
- Session hijacking
- Denial of Service
- Man in the middle
- Phishing

MISCONFIGURATION ATTACKS

Misconfiguration attack happens when a hacker gains access to the system that has poorly configured security. This attack allows hackers to access the system and its files, and perform malicious actions.

SHRINK-WRAP CODE ATTACKS

Shrink-wrap attacks happen because programmers regularly utilize free libraries and code authorized from different sources. If a hacker manages to find vulnerabilities in that code, then that would cause a great deal of problems.

MODERN AGE INFORMATION WARFARE

Information warfare involves the use and management of information and communication technologies in order to gain the advantage over the competitors.

INFORMATION WARFARE CATEGORIES

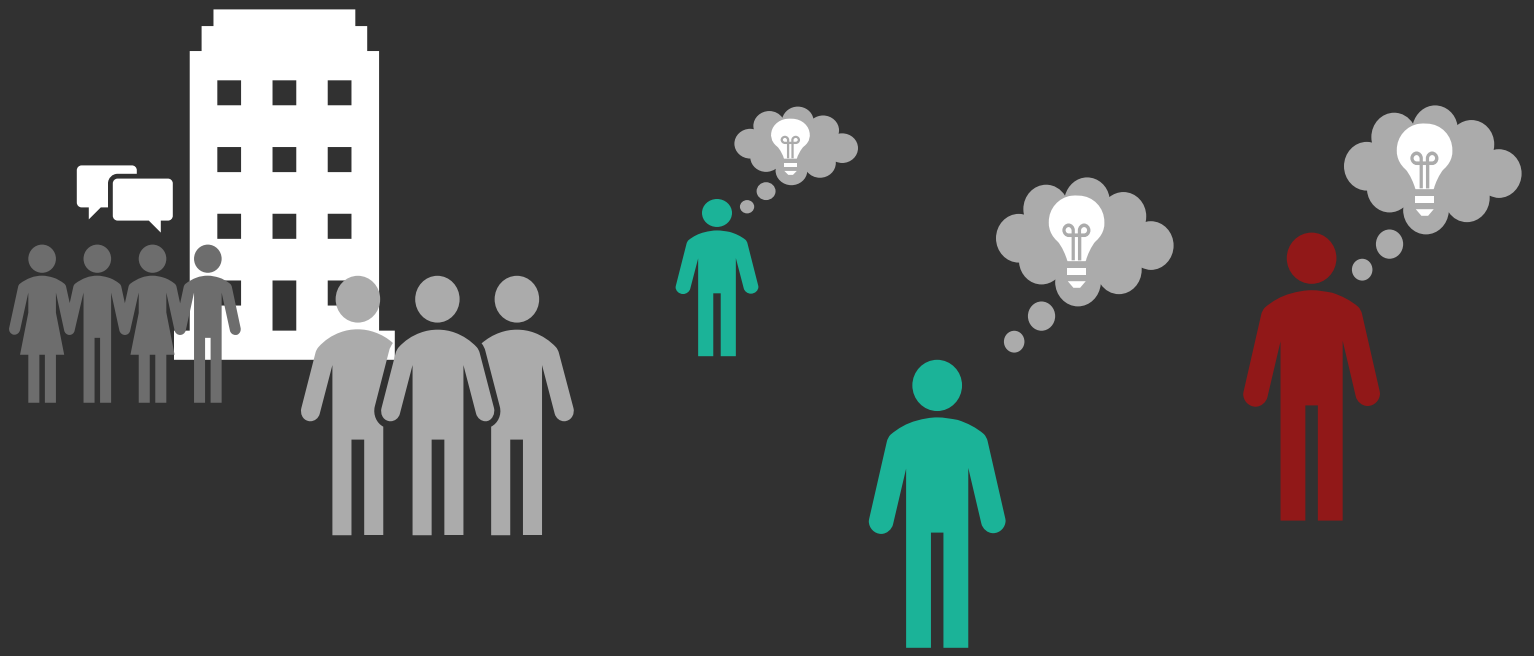
- Command and control warfare
- Intelligence-based warfare
- Electronic warfare
- Psychological warfare
- Hacker warfare
- Economic warfare
- Cyber warfare

INFORMATION WARFARE STRATEGIES

- Offensive strategies
- Defensive strategies

Introduction to Ethical Hacking

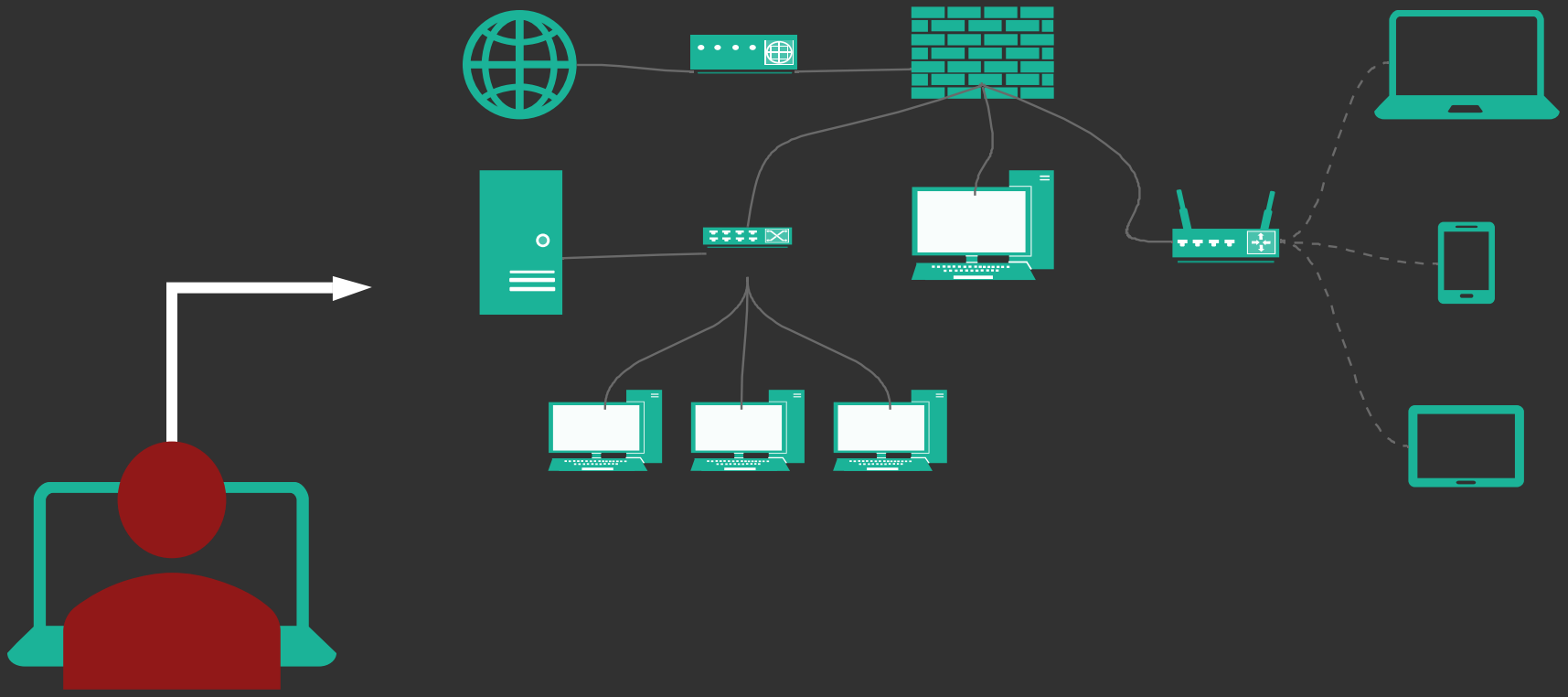
THE HISTORY OF HACKING



Introduction to Ethical Hacking

WHAT IS A HACKER?

A hacker is an individual who uses their computer and technical skills to gain access to systems and networks.



CLASSIFICATION OF HACKERS

TYPES OF HACKERS

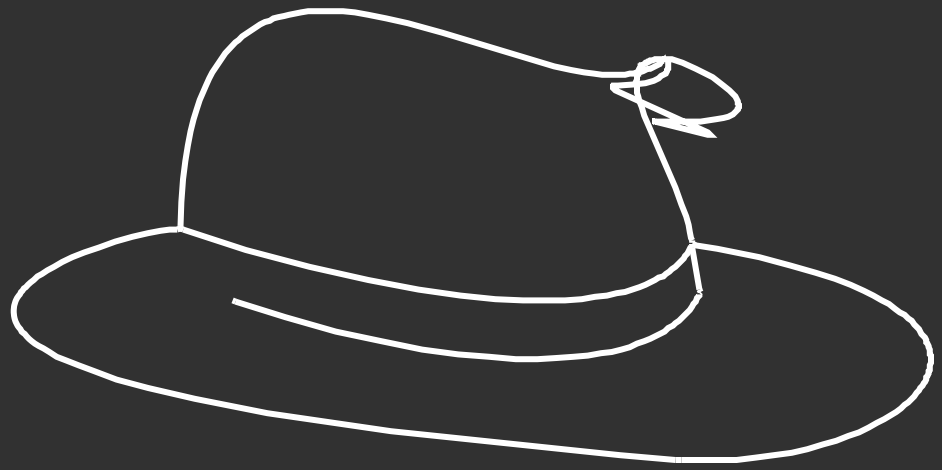
- Black hat hackers
- White hat hackers
- Grey hat hackers
- Suicide hackers
- Script kiddies
- Cyber terrorists
- State-sponsored hackers
- Hacktivists

CLASSIFICATION OF HACKERS

Black hats are hackers who use their knowledge and skills to discover and exploit security vulnerabilities for financial gain or other malicious reasons.

CLASSIFICATION OF HACKERS

White hats are ethical hackers who use their knowledge and skills to improve a system's security by discovering vulnerabilities before black hats do.



CLASSIFICATION OF HACKERS

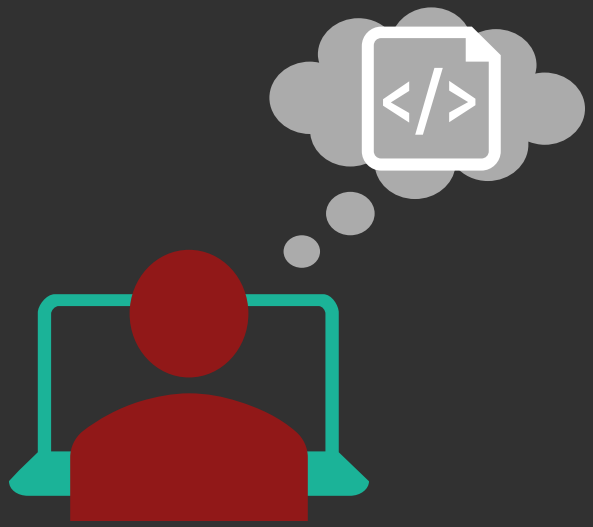
Grey hats are hackers who are not as bad as black hats but not as ethical as white hats.

CLASSIFICATION OF HACKERS

Suicide hackers are hackers who perform attacks for a cause despite the risk of being caught and prosecuted.

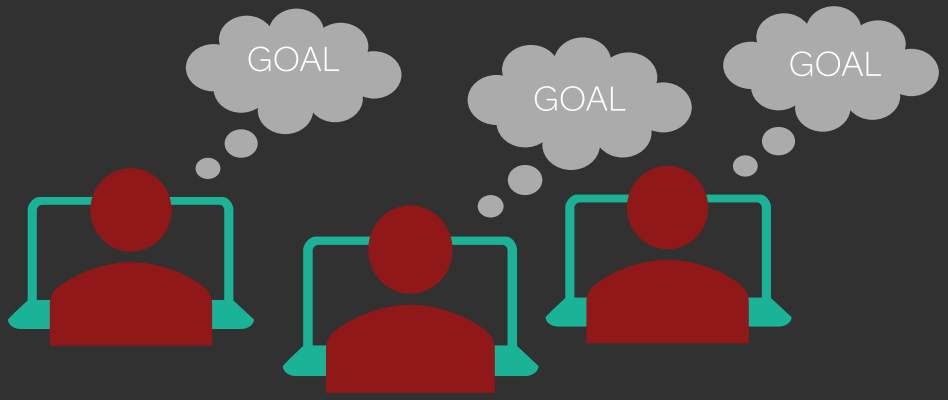
CLASSIFICATION OF HACKERS

Script kiddies are inexperienced hackers who don't have enough knowledge or skills to perform hacks on their own. Instead, they use tools and scripts developed by more experienced hackers.



CLASSIFICATION OF HACKERS

Cyber terrorists are hackers who are influenced by religious or political beliefs. They attempt to disrupt systems and networks in order to promote fear and unrest.



CLASSIFICATION OF HACKERS

State-sponsored hackers are recruited by governments to gain access to classified information about other governments.

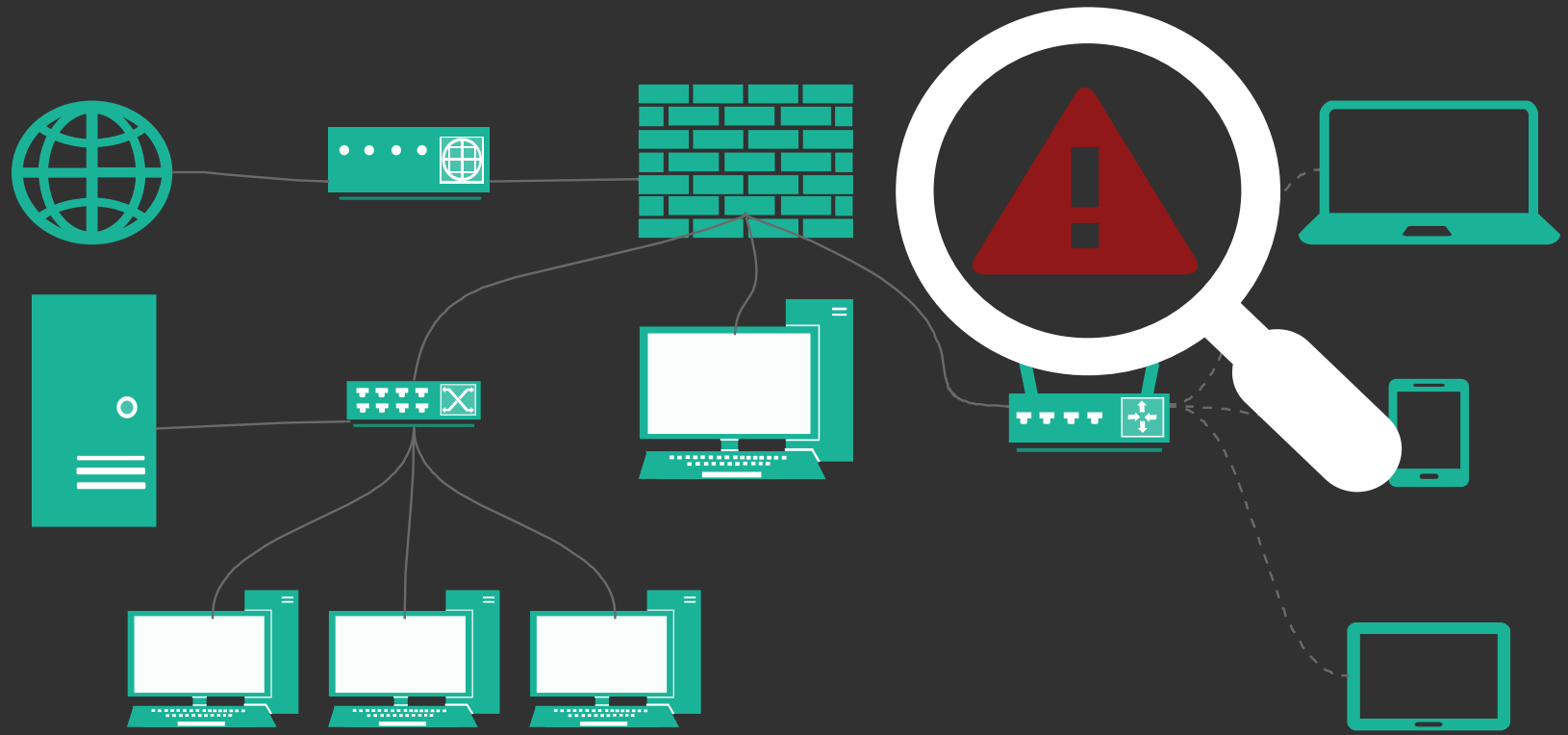
CLASSIFICATION OF HACKERS

Hacktivists break into government and corporate systems out of protest. They use their skills to promote political or social agenda.

Introduction to Ethical Hacking

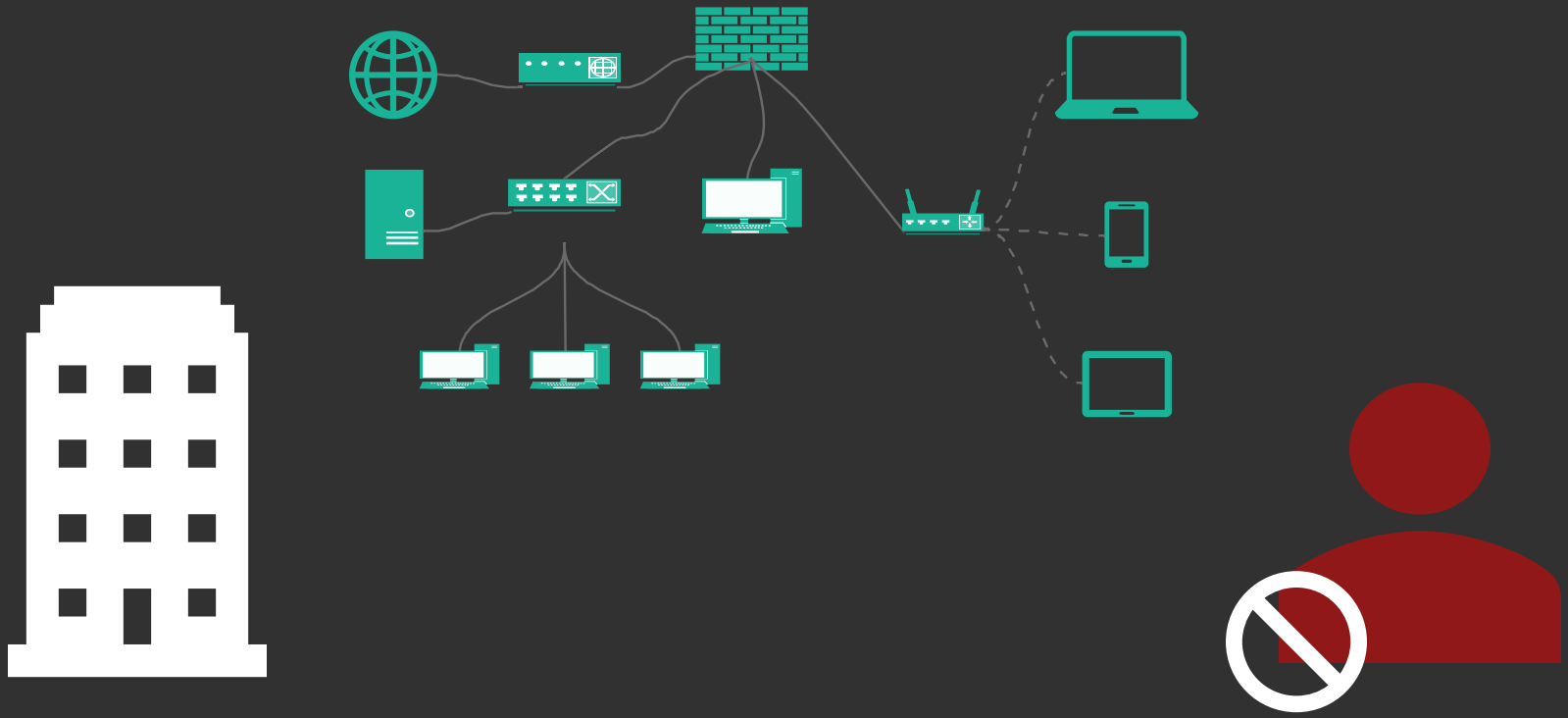
WHAT IS ETHICAL HACKING?

Ethical hacking describes any activities performed by a security specialist to help companies identify vulnerabilities in their networks and systems.



THE PURPOSE OF ETHICAL HACKING

The purpose of ethical hacking is to prevent malicious hackers from breaking into systems and networks.



THE SCOPE OF ETHICAL HACKING

Ethical hackers are usually hired to do a full-scale test of the client's network security while following certain guidelines:

- No test should be performed without appropriate permissions and authorization
- Test results should be kept confidential
- Only those tests that the client requested should be performed

HACKING STAGES

Reconnaissance is the initial phase. This phase involves gathering information to learn as much as possible about the target.

Scanning is the second phase. During this phase, hackers use the information they gathered in the reconnaissance phase to scan the target network.

Gaining access involves finding an entry point to the target's operating system or an application on the system and using it to perform the attack.

Maintaining access is the phase in which hackers try to keep the admin/root privileges so they can continue using the system.

Clearing tracks is the final phase. During this phase, hackers attempt to hide their activities on the system. They do everything they can to cover their tracks and avoid getting caught.

SECURITY CONTROLS

Information assurance is the assurance that the information integrity, availability, confidentiality, authenticity, and non-repudiation is kept during its use, storage, processing, and transfer.

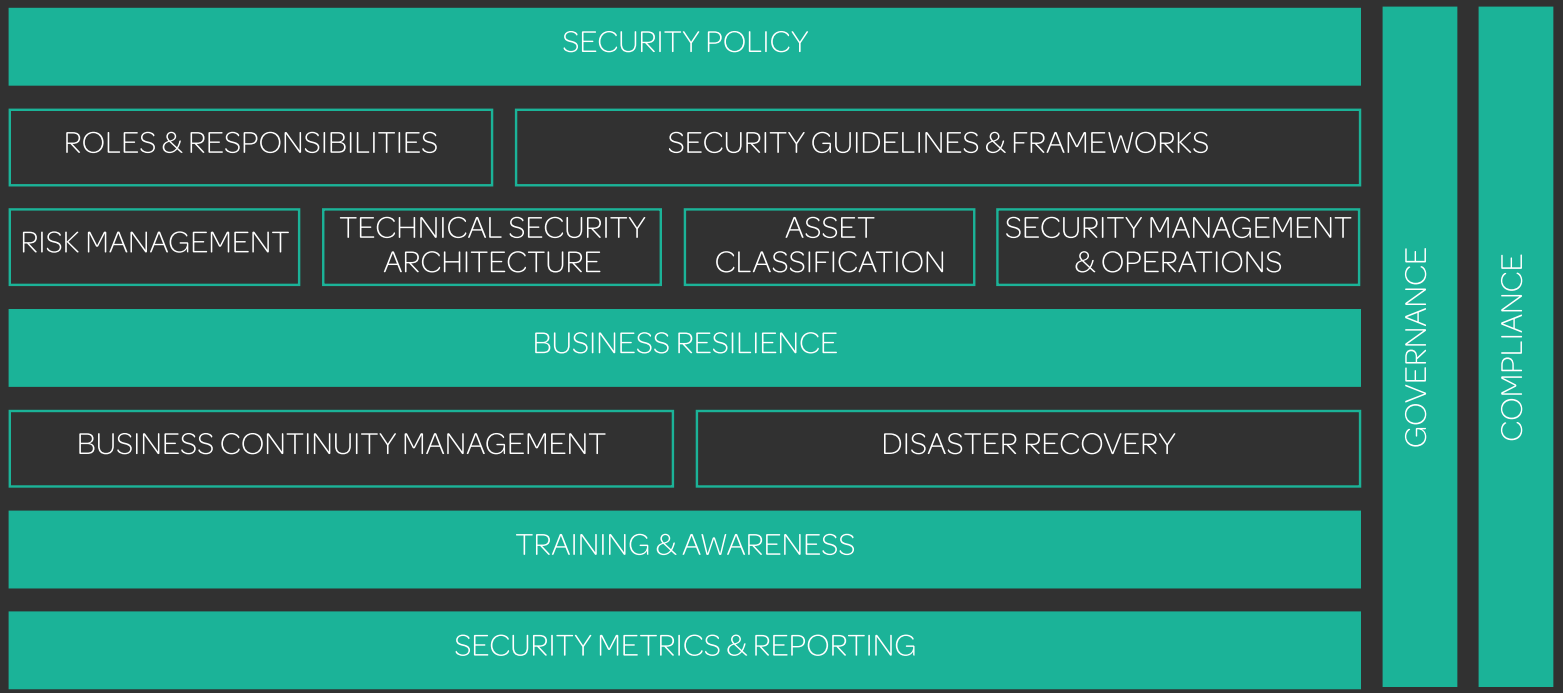
There are several processes defined that help in achieving information assurance:

- Development of security policies that help in maintaining the system security
- Design of the network and user authentication strategy
- Identification of vulnerabilities and threats
- Identification of problems in the system and resource requirements
- Plan design for the identified requirements
- Certification and accreditation to find vulnerabilities and remove them
- Information assurance training for employees

Introduction to Ethical Hacking

SECURITY CONTROLS

Information security management program is an organization-wide program that allows organizations to perform their activities in a secure environment.



SECURITY CONTROLS

Enterprise information security architecture (EISA) refers to a group of requirements, processes, principles, and models that regulate the organization's structure and behavior in terms of system security, processes, and employees.

ENTERPRISE INFORMATION SECURITY ARCHITECTURE GOALS

- Real-time monitoring of the organization's network
- Security breach detection and recovery
- Ensuring cost efficiency of security provisions
- Helping the IT department function properly
- Risk assessment of IT assets

NETWORK ZONING

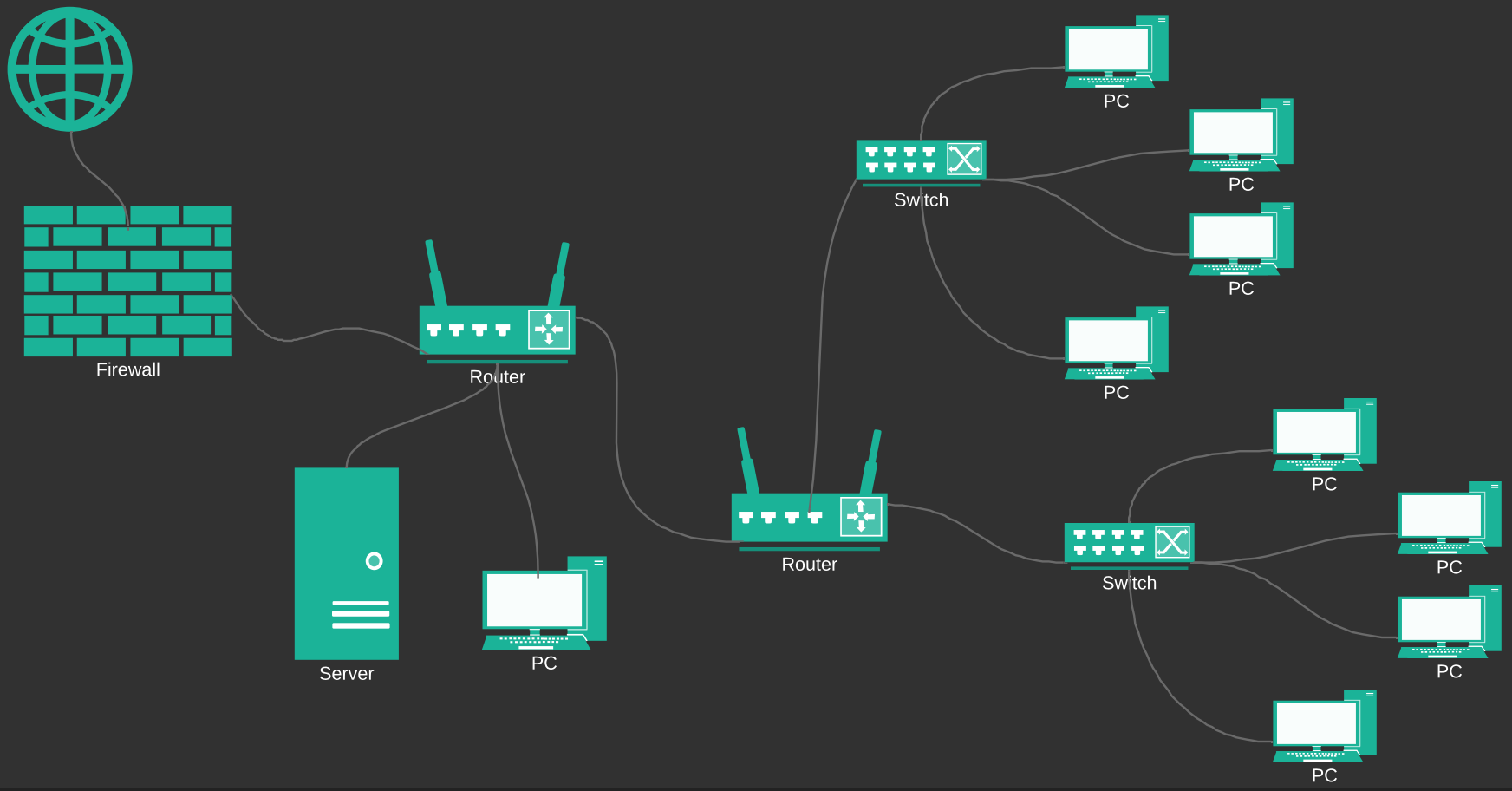
Network zoning is a mechanism that allows efficient management of an organization's different network zones.

Properties of a security zone are:

- Active security policies in regard to the network traffic
- Detection and blocking of malicious traffic
- List of known IP addresses and address sets
- List of the zone interfaces

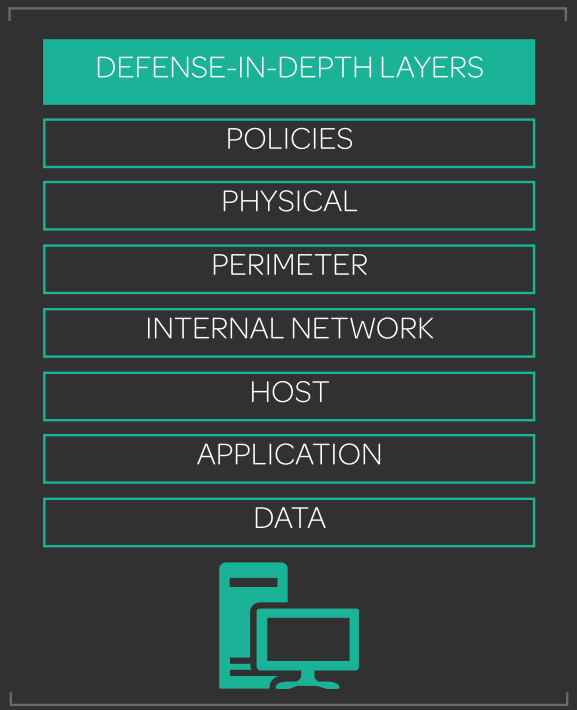
Introduction to Ethical Hacking

NETWORK ZONING



DEFENSE-IN-DEPTH

Defense-in-depth is a strategy which uses a number of layers of protection. The idea is that having multiple protection layers is better and more secure than having just one, so that attackers cannot easily break into the system. Using this strategy, direct attacks on the system and its data are prevented.

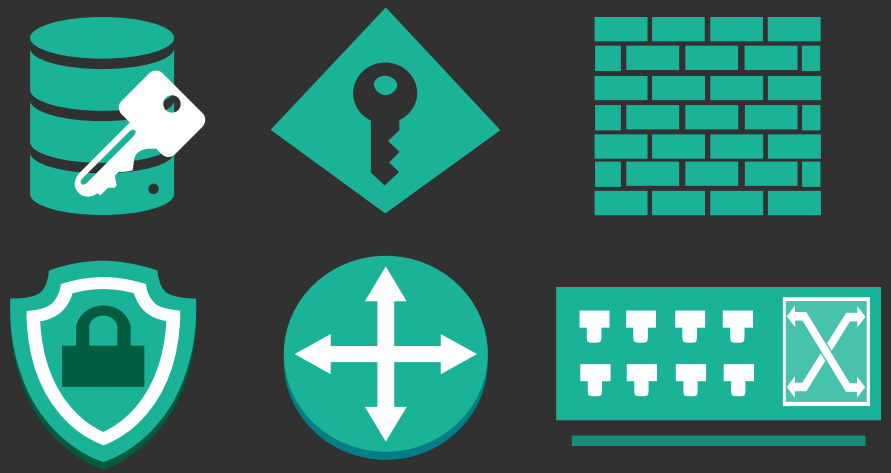


SECURITY POLICIES

Security policies are the core of every security infrastructure because they define rules and requirements that the system has to have in order to protect organization's information systems.

Security policies should cover the following:

- Encryption
- Access control
- Authentication
- Firewalls
- Antiviruses
- Websites
- Gateways
- Routers and switches



SECURITY POLICIES

PROMISCUOUS POLICY

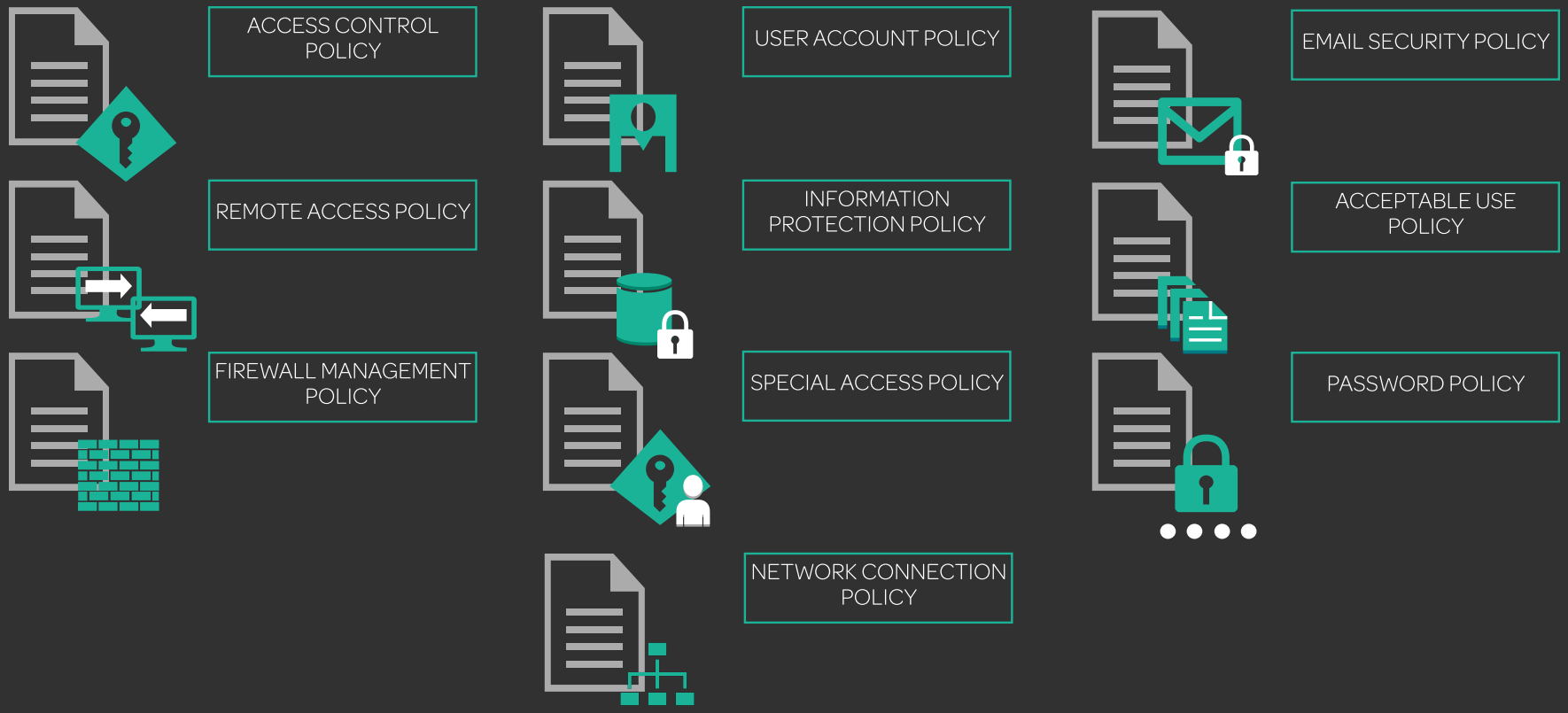
PERMISSIVE POLICY

PRUDENT POLICY

PARANOID POLICY

Introduction to Ethical Hacking

SECURITY POLICIES



SECURITY POLICIES

Privacy policies at workplace include:

- Inform employees about what information is being collected about them and reasons for it
- Collect only required information
- Use the collected information with consent only
- Allow employees to access their information
- Keep the collected information secure

SECURITY POLICIES

IMPLEMENTATION STEPS

1	PERFORM RISK ASSESSMENT	4	DEFINE SANCTIONS	7	ENFORCE POLICIES
2	UTILIZE STANDARD GUIDELINES	5	DISTRIBUTE THE FINAL VERSION	8	EDUCATE AND TRAIN EMPLOYEES
3	INCLUDE SENIOR MANAGEMENT	6	ENSURE THAT EMPLOYEES HAVE READ THE POLICY	9	REVIEW AND UPDATE THE POLICY

SECURITY POLICIES

Human Resource department has the responsibility to educate and train the employees in practices defined by the company's security policies, monitor the implementation of the policies, and enforce penalties.

PHYSICAL SECURITY

Physical security refers to the protection of all assets of an organization from all sorts of threats and attacks.

Physical security helps in:

- Preventing unauthorized access to the system
- Preventing any kind of data manipulation and theft
- Protecting the system against malicious activities such as espionage, damage, and theft
- Protecting employees and preventing social engineering attacks

PHYSICAL SECURITY CATEGORIES

NATURAL THREAT	MAN-MADE THREAT
	

PHYSICAL SECURITY CONTROL

Reconnaissance is the initial phase. This phase involves gathering information to learn as much as possible about the target.

PREVENTIVE CONTROLS

Preventive controls enforce different access control mechanisms and prevent violations in regard to the security of the system.

DETECTIVE CONTROLS

Detective controls detect violations in security as well as any attempts of intrusion.

DETERRENT CONTROLS

Deterrent controls are used to warn intruders to stay away from the system.

RECOVERY CONTROLS

Recovery controls are used after a violation has happened and system needs to be restored to its persistent state.

COMPENSATING CONTROLS

Compensating controls do not prevent attacks. Instead, they are used when everything else fails. In this type of control, the goal is to restore everything back to normal.

RISK MANAGEMENT

Risk refers to the probability or threat of damage or loss. Risk assessment is used to evaluate the impact an event had on a network. In order for a risk to be evaluated, it is necessary to define the level of risk, that is, the probability of an event happening and the consequences it has.

RISK LEVEL	CONSEQUENCE	ACTION
EXTREME/HIGH	Serious danger	Steps should be taken to reduce the risk immediately.
MEDIUM	Medium danger	Steps should be taken to reduce the risk as soon as possible.
LOW	Negligible danger	Preventive measures should be taken to mitigate the risk.

RISK MANAGEMENT

The risk matrix considers the probability of the risk happening as well as its impact on the system. By designing the risk matrix, it is possible to visualize possible risks and how their occurrence might affect the system

PROBABILITY	CONSEQUENCES				
	INSIGNIFICANT	MINOR	MODERATE	MAJOR	SEVERE
VERY HIGH PROBABILITY	Low	Medium	High	Extreme	Extreme
HIGH PROBABILITY	Low	Medium	High	High	Extreme
EQUAL PROBABILITY	Low	Medium	Medium	High	High
LOW PROBABILITY	Low	Low	Medium	Medium	High
VERY LOW PROBABILITY	Low	Low	Medium	Medium	High

RISK MANAGEMENT

Risk management refers to the process of identifying, assessing, and acting on potential risks. It is an ongoing process, designed to help reduce the risk level and keep it at an acceptable level.

Objectives of risk management are:

- Identify potential risks
- Identify the ipacts of those risks
- Create a risk management strategy and plan
- Assign priorities to risks
- Analyze the risks
- Control the risk
- Develop strategies and plans for long lasting risks

THREAT MODELING

Threat modeling is an assessment approach in which the security of an application is analyzed. It helps in identifying threats that are relevant to the application, discovering application vulnerabilities, and improve the security.

Threat modeling process consists of five steps:

1. Identify security objectives
2. Create application overview
3. Decompose applicatio
4. Identify threats
5. Identify vulnerabilities

INCIDENT MANAGEMENT

Incident management refers to the process of identifying, analyzing, prioritizing, and solving security incidents.

Introduction to Ethical Hacking

INCIDENT MANAGEMENT

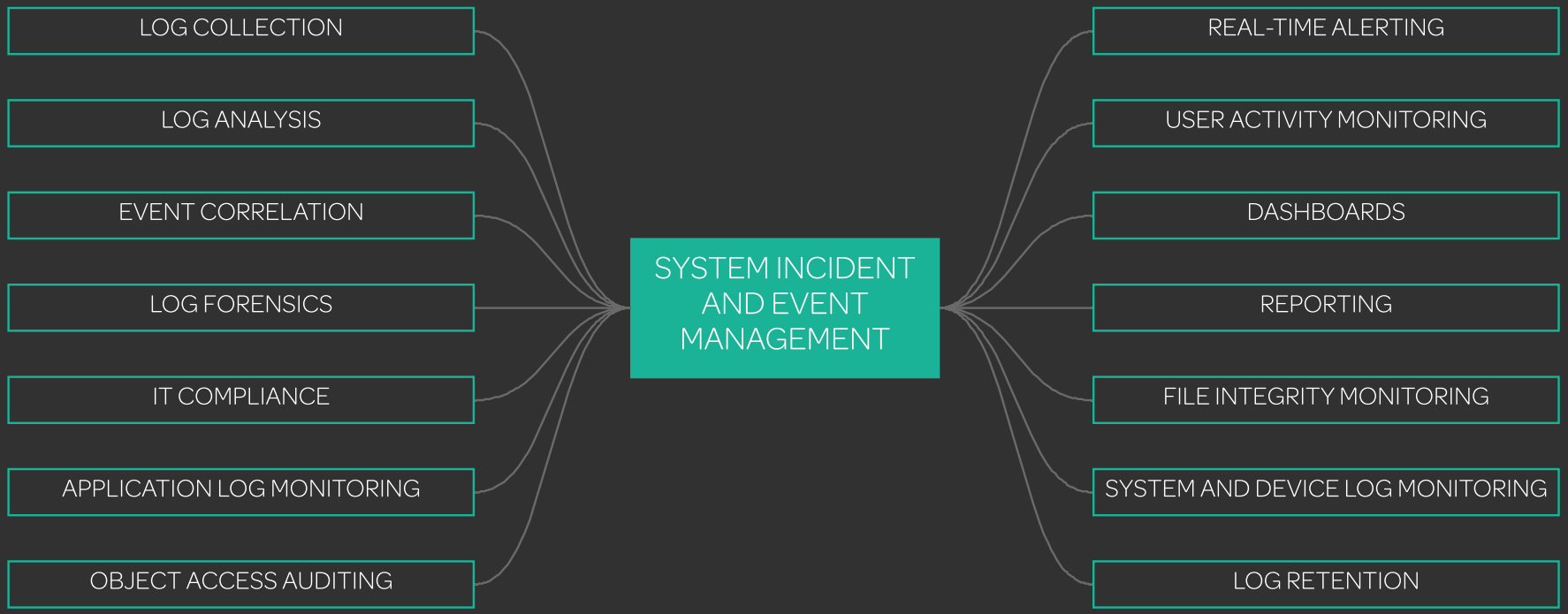
1	PREPARATION FOR INCIDENT HANDLING AND RESPONSE	This step involves familiarizing the employees with the guideline and plan of actions that is to be followed, establishing different policies, and training people to take effective actions.
2	DETECTION AND ANALYSIS	In this step, incidents and their signatures are identified, analyzed, recorded, and prioritized.
3	CATEGORIZATION AND PRIORITIZATION	In this step, each incident that has ocurred is classified and prioritized, so that the situation is handled promptly and efficiently.
4	REPORTING	Upon the identification and classification of the incident, individuals that are in charge of handling such situations are notified about the issue.
5	CONTAINMENT	In this step, the objective is to prevent the occurring incident from causing any additional damage.
6	FORENSIC INVESTIGATION	In this step, an investigation is performed to determine the main cause of the incident, to understand what really happened on the system.
7	RECOVERY	In this step, the ystem is restored to its original state. It is important to perform the cleanup and notify the people working the incident response team about the taken recovery steps.
8	POST-INCIDENT ACTIVITIES	In this step, the final review of the incident is conducted. A post incident report is generated upon the completion of the review.

INCIDENT MANAGEMENT

INCIDENT RESPONSE TEAM RESPONSIBILITIES			
1	Manage security issues and respond to security incidents	5	Provide a point of contact for incident reports
2	Create a plan to be followed in case of an incident	6	Stay up-to-date with regulations and requirements
3	Manage the response and make sure the plan is being followed	7	Take steps to prevent future incidents
4	Identify the cause and impact of the incident	8	Establish relationships with the individuals and agencies that play a role in the organization's security

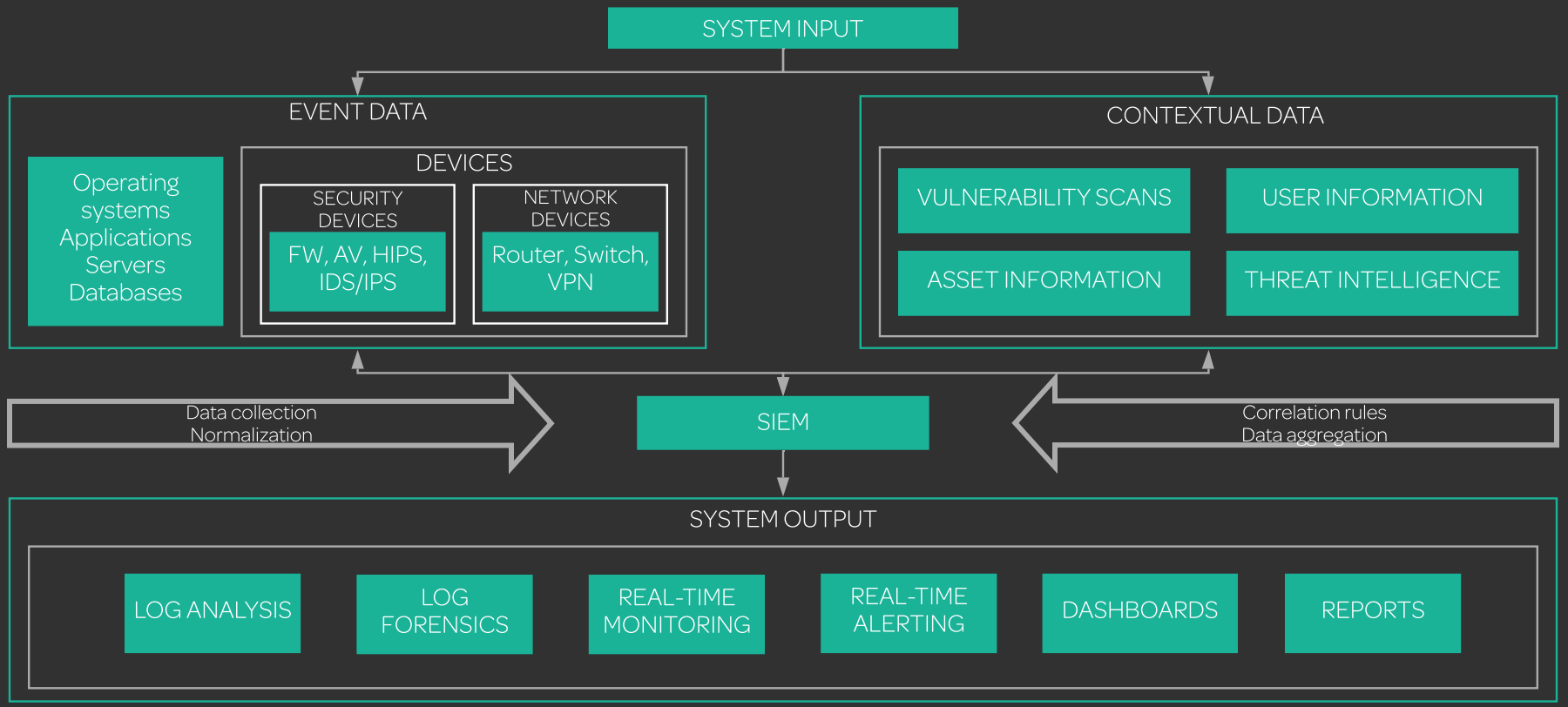
SECURITY INCIDENT AND EVENT MANAGEMENT

Security incident and event management is responsible for identifying, monitoring, recording, inspecting, and analyzing security incidents, performing threat detection and incident resposnse activities, and real-time tracking of suspicious activities.



Introduction to Ethical Hacking

SIEM ARCHITECTURE



USER BEHAVIOR ANALYTICS

User behavior analytics refers to the pprocess of monitoring user behavior in an attempt to discover potential threats and attacks.

USER BEHAVIOR ANALYSIS

The activity needs to be investigated

Suspicious activity detected

User behavior analysis confirms suspicion

Suspicious activity detected

NETWORK SECURITY CONTROLS

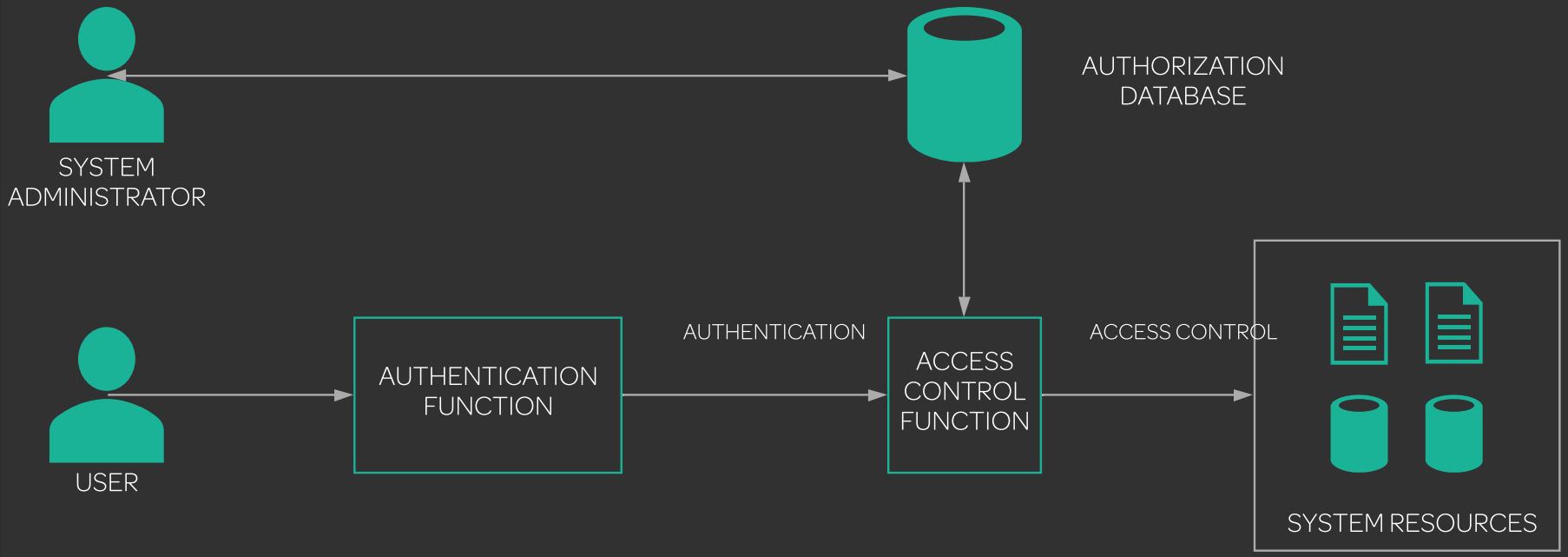
Network security controls can be considered as a safeguard that minimizes security risks.

1	ACCESS CONTROL	2	IDENTIFICATION
3	AUTHENTICATION	4	AUTHORIZATION
5	ACCOUNTING	6	CRYPTOGRAPHY
7	SECURITY POLICY		

Introduction to Ethical Hacking

NETWORK SECUIRTY CONTROLS

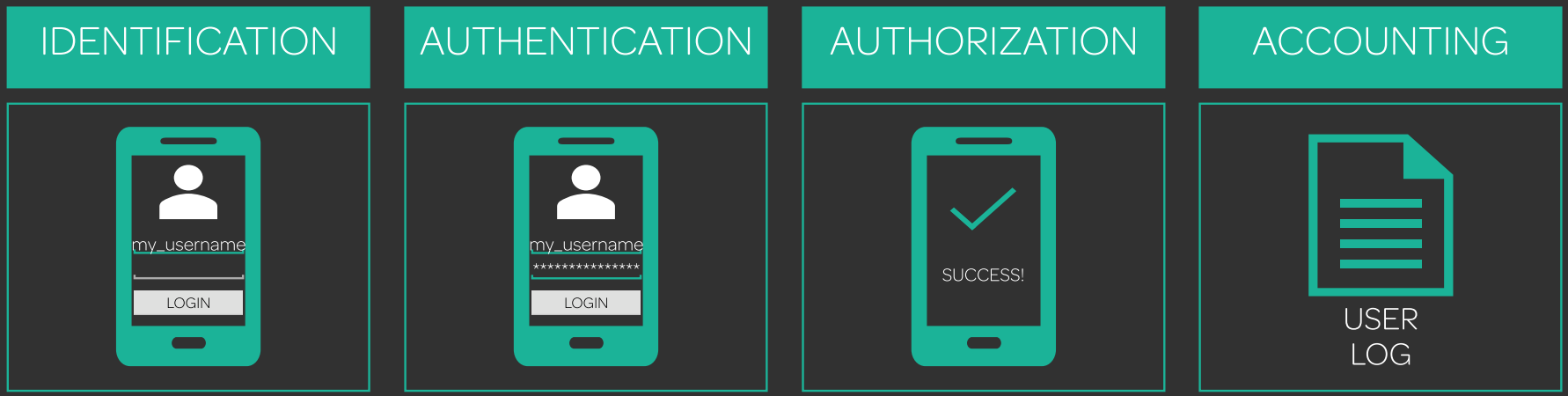
Access control refers to the restrictions placed upon the system/network. These restrictions determine who has access to a resource and who does not. By placing these restrictions, the organization protects its information assets.



NETWORK SECURITY CONTROLS

Access control involves identification, authentication, authorization, and accountability.

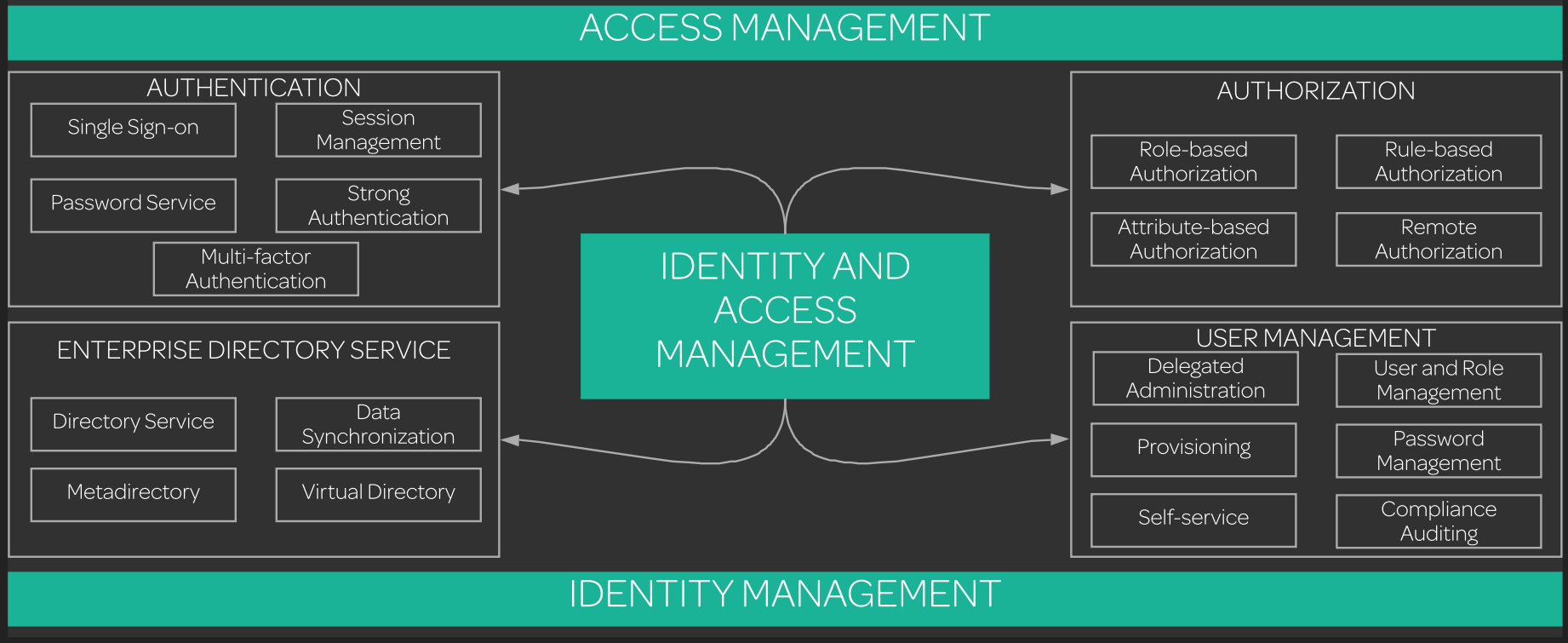
- Identification is the confirmation of the identity of a user or a device that is accessing the network. Confirming the identity is usually done through the verification of credentials such as an ID or username.
- Authentication refers to the verification of the provided user ID/username and password.
- Authorization is the process of giving access permissions to authenticated users.
- Accounting is the process of tracking user activity on the network



Introduction to Ethical Hacking

IDENTITY AND ACCESS MANAGEMENT

Identity access management is a framework which makes sure that the right users have access to the right resources at the right time. The framework includes users, procedures, and software that manage users' access to the organization's resources.



DATA LEAKAGE

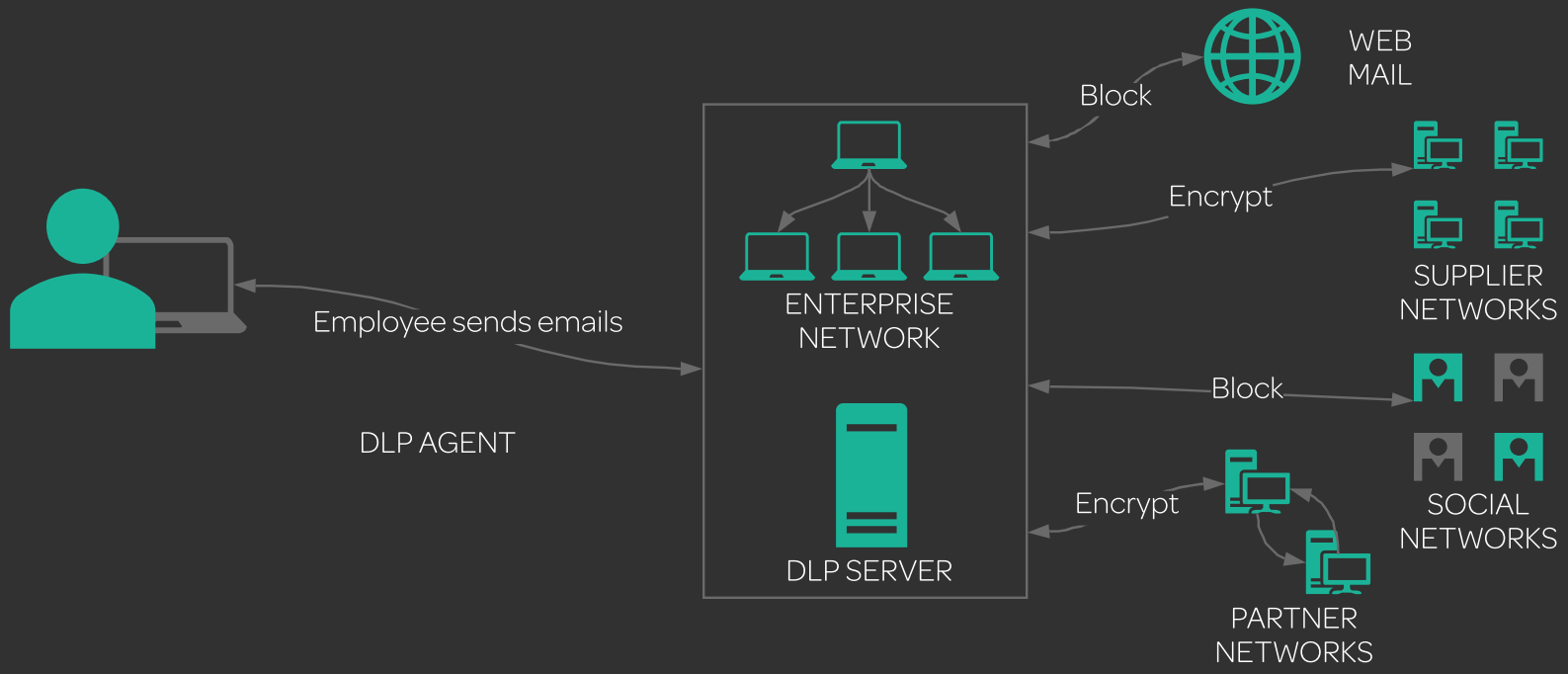
Data leakage is the unauthorized transfer of sensitive information from the organization to the outside world.

Data leakage threats are classified into insider and external threats. Insider threats are caused by the people who work in the organization. External threats are attackers who are continuously looking for vulnerabilities and ways to gain access to the system/network.

Introduction to Ethical Hacking

DATA LOSS PREVENTION

Data Loss Prevention is the process of identification and monitoring of important information that is not to be shared outside the organization. DLP combines different techniques of data access control. The goal is to protect the sensitive data and provide a secure data transmission.



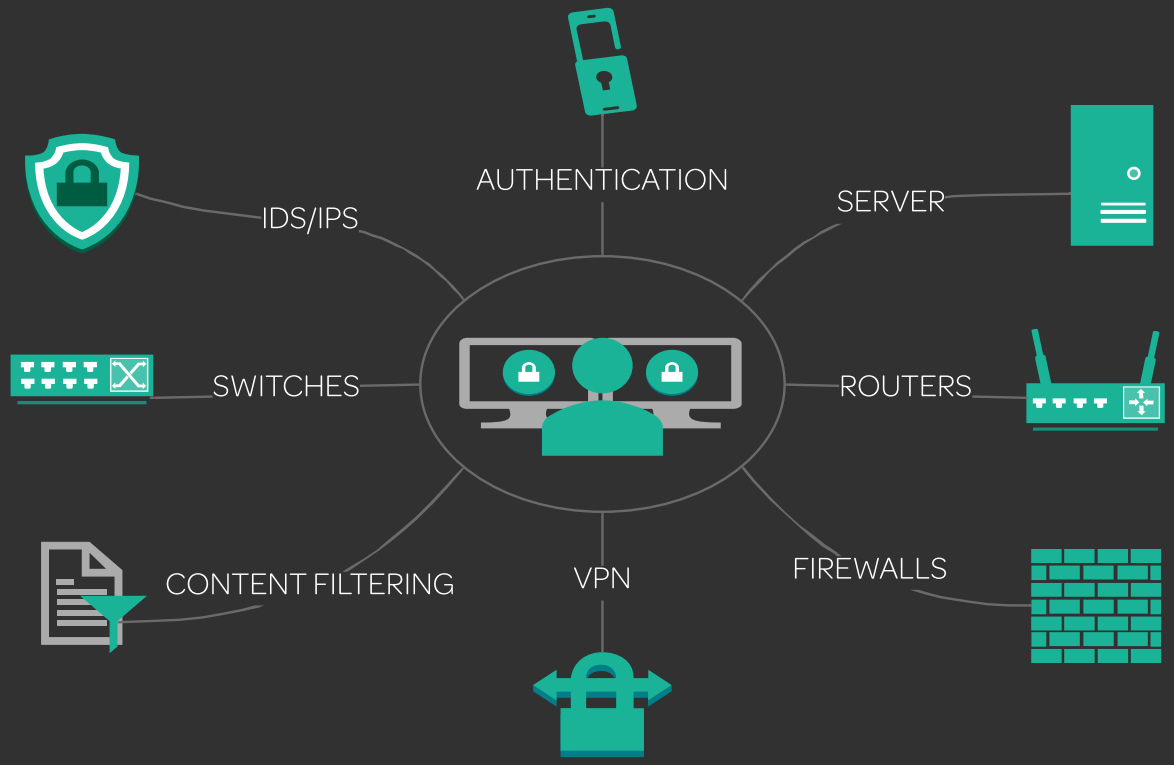
DATA BACKUP AND RECOVERY

Data backup is the process of creating and storing a copy of important data that can be used in case an incident occurs and original data is lost. Data backup is used for two main reasons: to restore the system to its normal state and to recover data in case of data loss or corruption.

Data recovery refers to the process of retrieving the lost or corrupted data. This process depends on the way the data was lost and, in most cases, the lost data can be recovered.

WHAT IS PENETRATION TESTING?

Penetration testing refers to the simulation of a security attack in which the objective is to discover vulnerabilities and evaluate the security of the system/networks that is being tested.



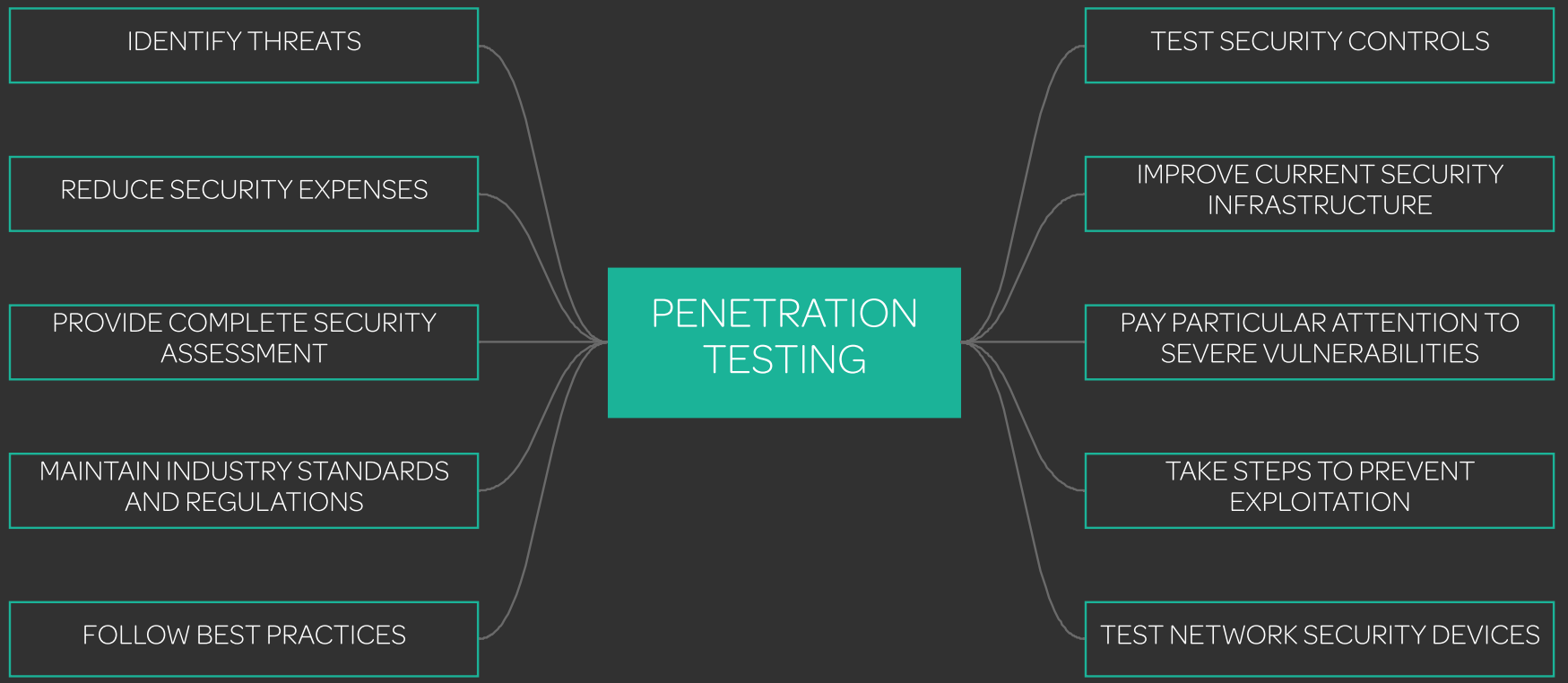
WHAT IS A GOOD PENETRATION TEST?

Activities that make up a good penetration test include:

- Defining the penetration test parameters
- Engaging skilled penetration testers
- Following nondisclosure agreement
- Selecting appropriate tests
- Using and following a methodology
- Documenting the results of the test
- Creating a final report

Introduction to Ethical Hacking

PURPOSE OF PENETRATION TESTING



AUDIT vs VULNERABILITY ASSESSMENT vs PENETRATION TESTING

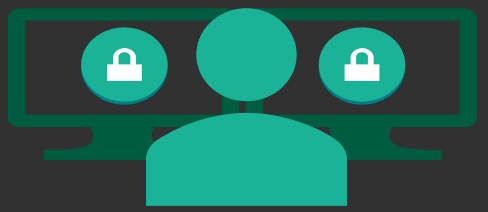
SECURITY AUDIT

A security audit only determines whether or not an organization is following security standards and policies.

VULNERABILITY ASSESSMENT

A vulnerability assessment only deals with identifying vulnerabilities in a system/network.

PENETRATION TESTING



Penetration testing encompasses both a security audit and a vulnerability assessment. It also demonstrates how attackers can exploit the identified vulnerabilities.

BLUE AND RED TEAMING

To perform a security assessment, penetration testers often use either blue teaming approach or red teaming approach.

BLUE TEAM

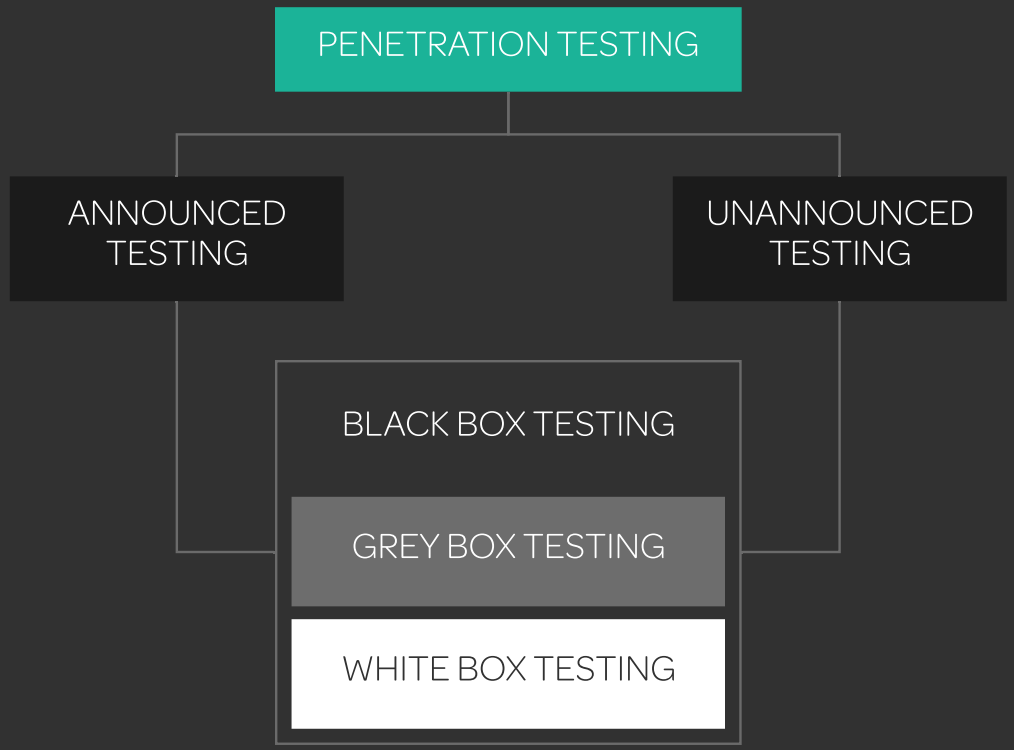
The role of the blue team is to detect the red team and predict their attacks.

RED TEAM

The role of the red team is to find vulnerabilities in the system/network and attempt to bypass security as real attackers would.

Introduction to Ethical Hacking

PENETRATION TESTING TYPES



PENETRATION TESTING PHASES

PRE-ATTACK PHASE

The pre-attack phase mainly includes activities such as preparation and planning, and information gathering. The objective is to gather as much information about the target as possible.

ATTACK PHASE

Attack phase is the phase in which the target gets compromised. During this phase, the tester uses the information gathered in the previous one and tries to carry out an attack

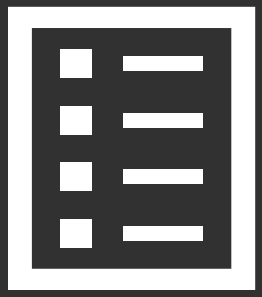
POST-ATTACK PHASE

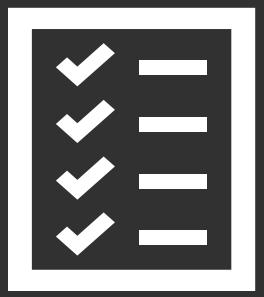
In this phase, the tester restores the system to the pretest state. The tester should also report where the security flaws are as well as document all activities and results.

Introduction to Ethical Hacking

PRE-ATTACK PHASE

Rules of Engagement refers to the formal agreement and permission to perform a penetration test. ROE is a guideline for testers and as such should clearly state what is and isn't allowed.

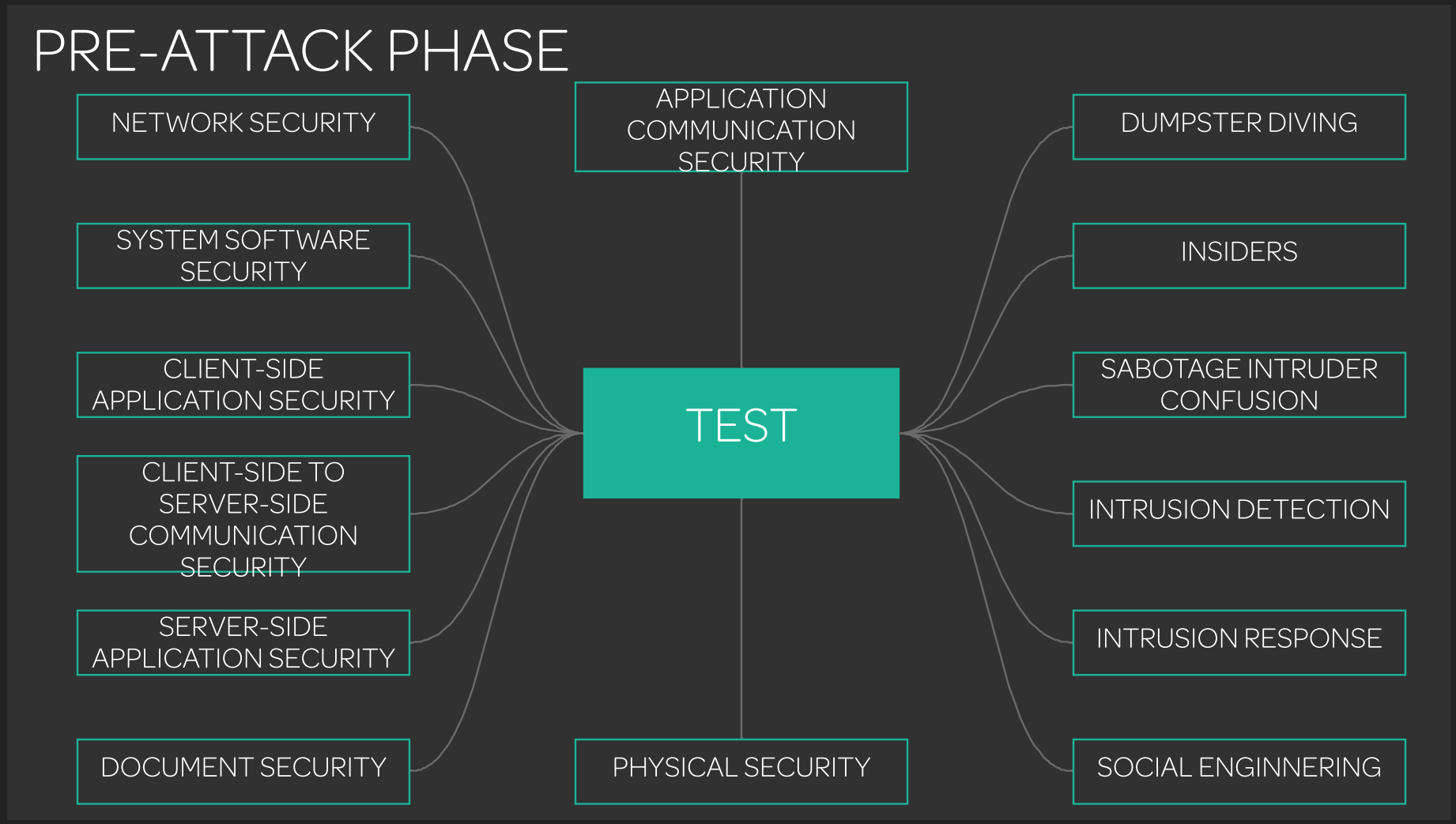




Understanding the client's requirements is of great importance as it ensures that the penetration test is thorough and the client is satisfied. It is considered good practice to create a checklist of the testing requirements to determine what the client wants to be tested.

The scope of the penetration test should be defined to ensure that requirements are fulfilled and objectives are met.

Introduction to Ethical Hacking

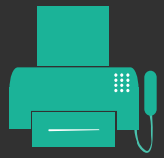


Introduction to Ethical Hacking

PRE-ATTACK PHASE

The goal of the pre-attack phase is to gather as much information as possible. The collected information is used to map out the target's network and plan the attack

PHYSICAL AND LOGICAL LOCATION



ANALOG CONNECTIONS

INFORMATION GATHERING

CONTACT INFORMATION

INFORMATION ABOUT OTHER ORGANIZATIONS

PRE-ATTACK PHASE

RECONNAISSANCE TYPES

PASSIVE

- News & job postings
- WHOIS databases
- Document sifting
- Social engineering

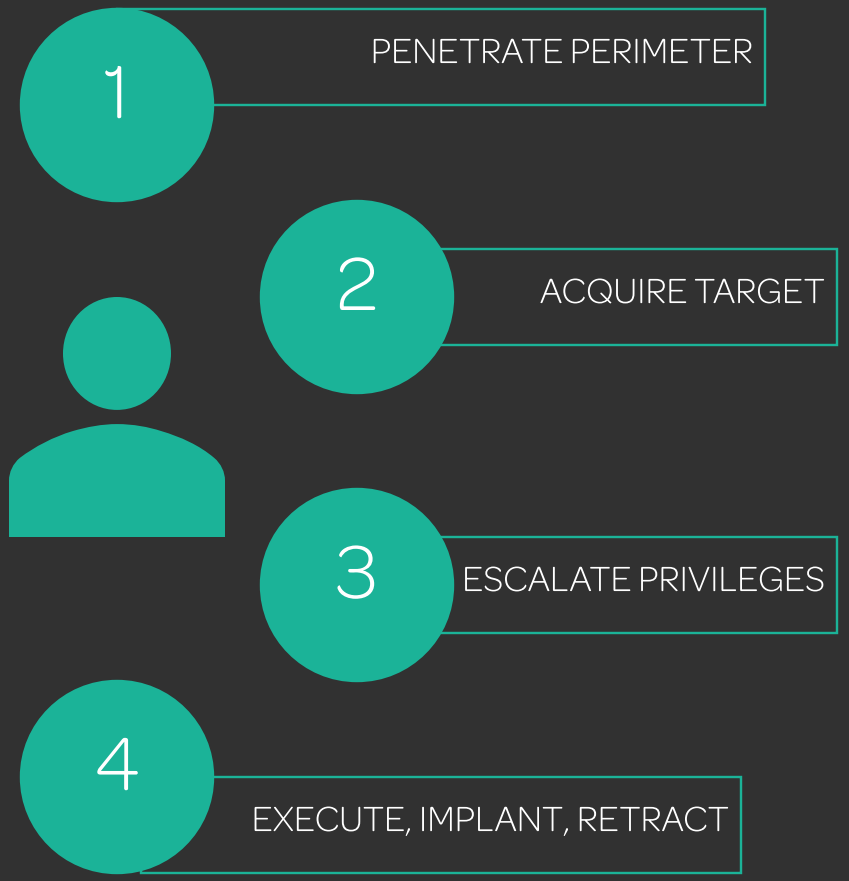
ACTIVE

- Network mapping
- Perimeter mapping
- Port scanning
- Web profiling

ATTACK PHASE

This is the phase in which the target gets compromised.

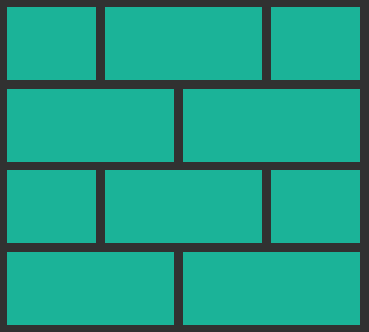
During this phase, the tester uses the information gathered in the previous one and tries to carry out an attack.



Introduction to Ethical Hacking

ATTACK PHASE

1 PENETRATE PERIMETER



FIREWALL TESTING

- ICMP PROBES
- CHECKING ACCESS CONTROL
- EVALUATING PROTOCOL FILTERING RULES
- EVALUATING IDS

ENUMERATING DEVICES

- DEVICE ID
- HOSTNAMES
- PHYSICAL LOCATIONS
- IP AND MAC ADDRESSES

Introduction to Ethical Hacking

ATTACK PHASE

2 ACQUIRE TARGET

- ACTIVE PROBING ASSAULTS
- RUNNING VULNERABILITY SCANS
- TRUSTED SYSTEMS AND TRUSTED PROCESS ASSESSMENT

Introduction to Ethical Hacking

ATTACK PHASE

3 ESCALATE PRIVILEGES

- PASSWORD CRACKERS
- TROJANS
- SOCIAL ENGINEERING

Introduction to Ethical Hacking

ATTACK PHASE

4 EXECUTE, IMPLANT, RETRACT

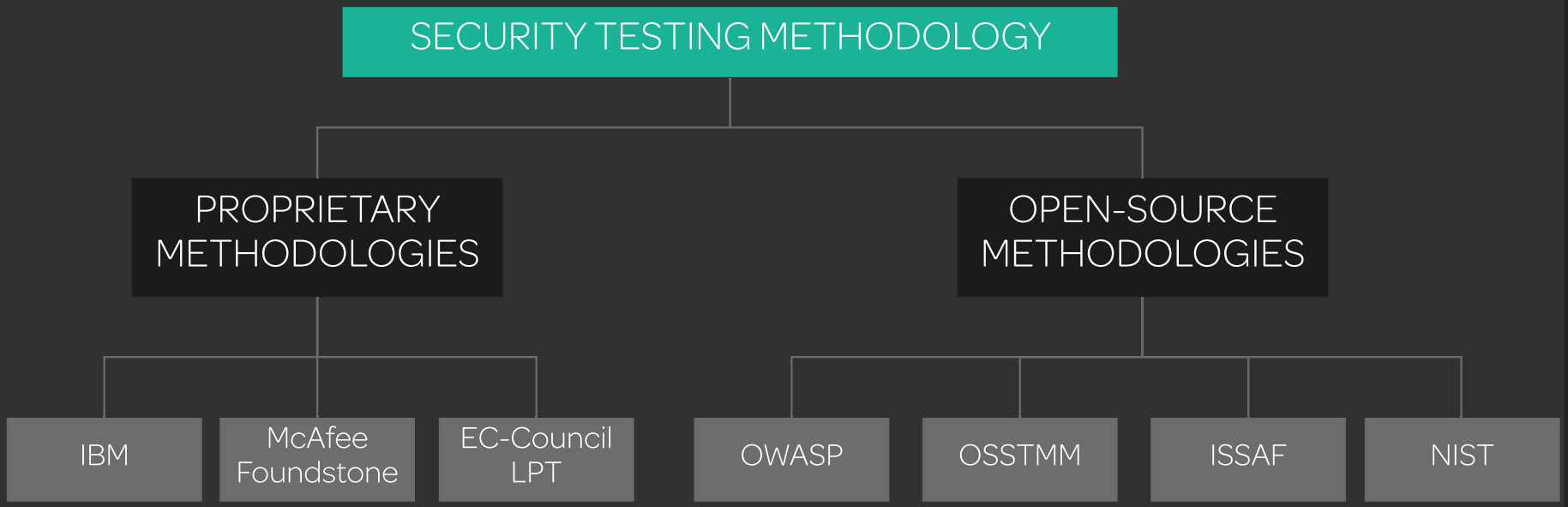
- DoS ATTACKS
- BUFFER OVERFLOWS
- VIRUSES, TROJANS, ROOTKITS
- INSTALLING BACKDOORS

POST-ATTACK PHASE

In this phase, the tester restores the system to the pretest state. The tester should also report where the security flaws are. All activities and results must be documented.

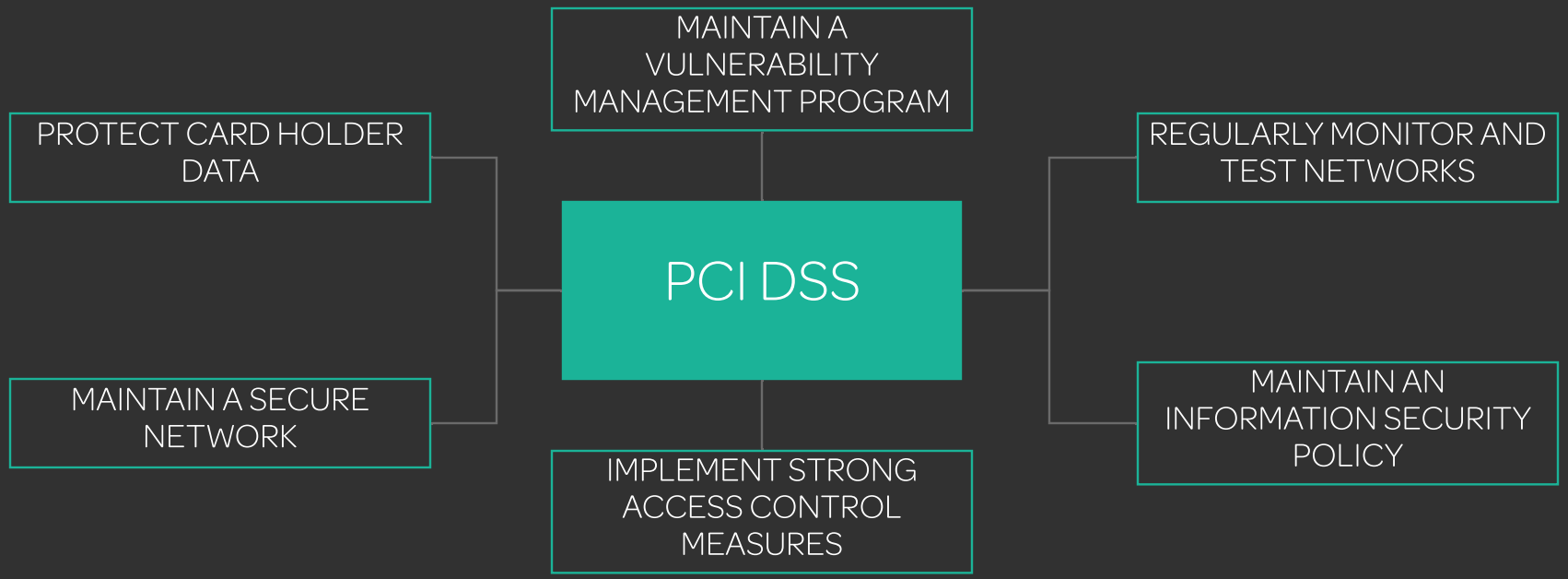
SECURITY TESTING METHODODLOGIES

Security testing methodology is an approach which attempts to find vulnerabilities in the system's security mechanisms. The goal is to enable the system administrators to protect the data and information by applying appropriate security controls.



PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

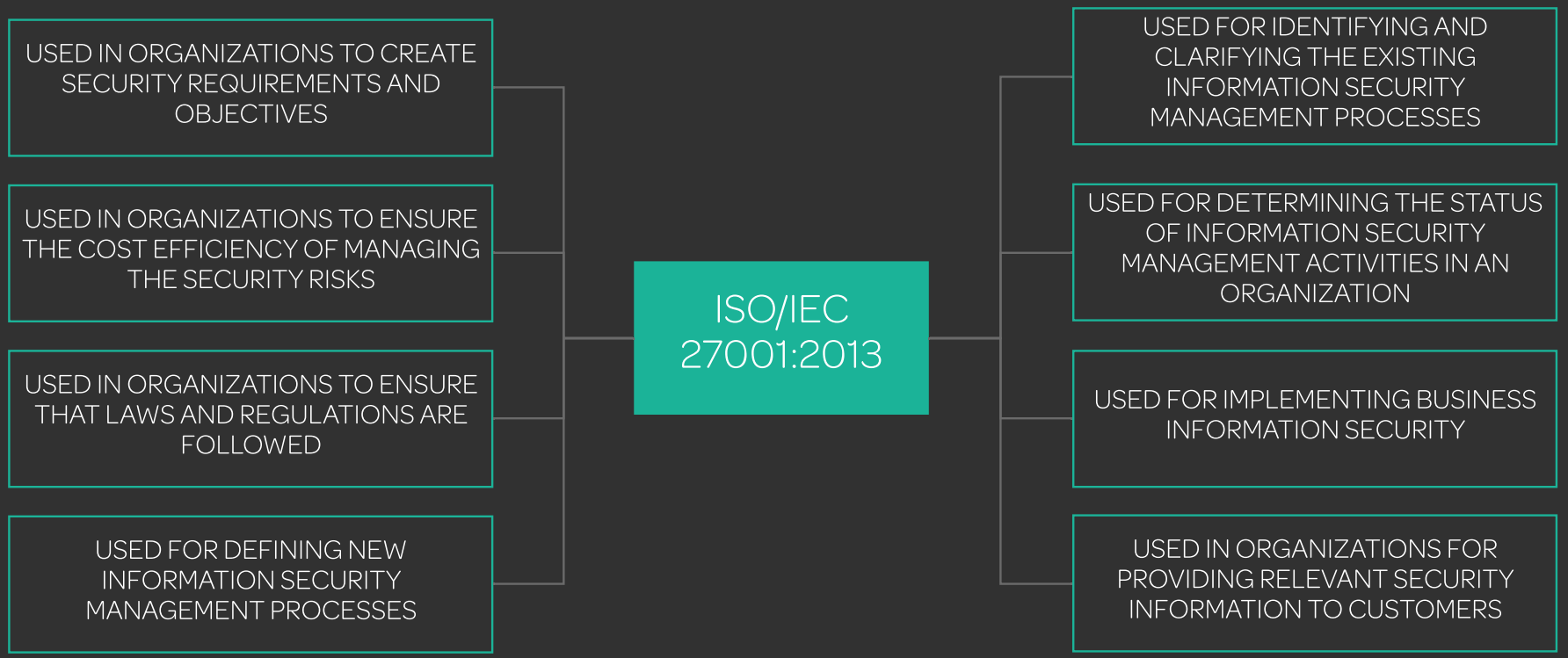
The PCI DSS standard covers any organization that directly accepts credit or debit card payments and applies to all entities involved in the process of card payment.



Introduction to Ethical Hacking

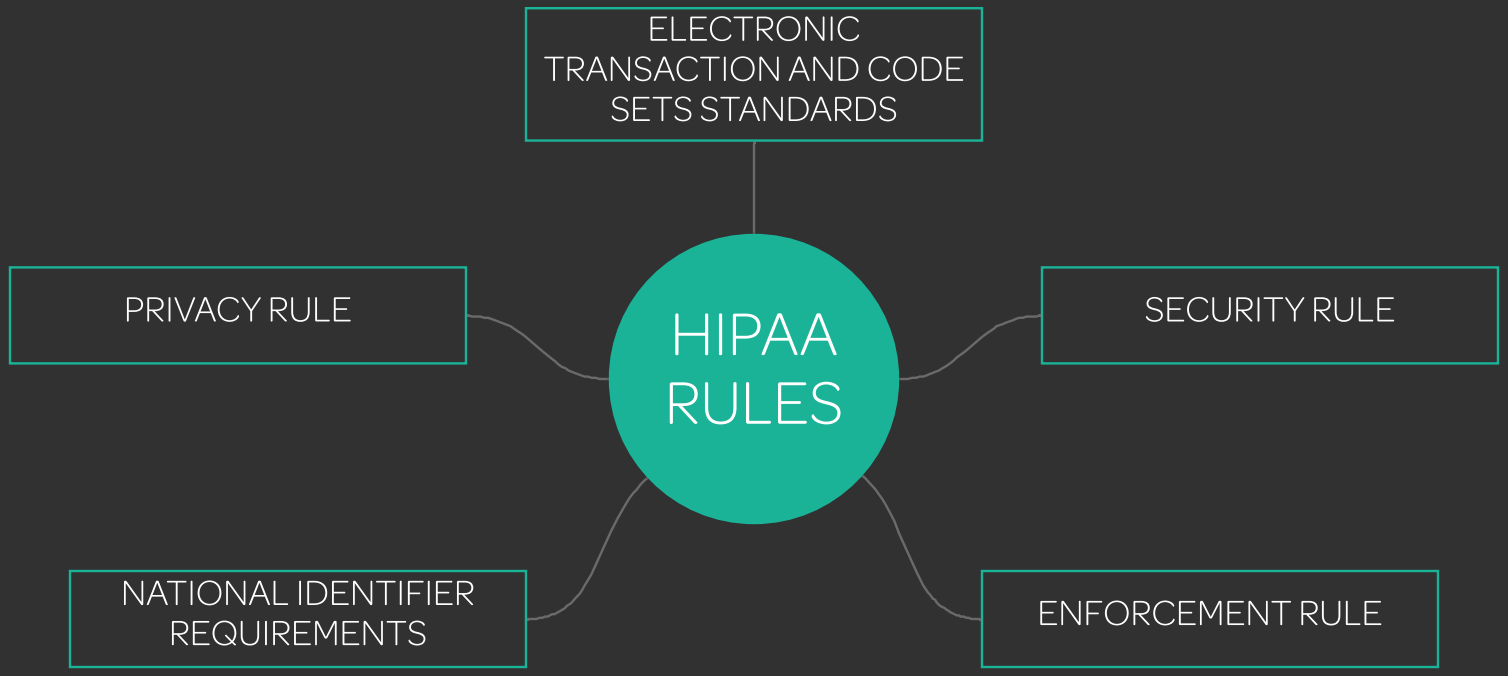
ISO/IEC 27001:2013

This standard defines the requirements for the establishment, implementation, maintenance, and continuous improvements in the organization's information security management system.



HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA)

HIPAA provides data privacy and protection of medical information. It specifies administrative, physical, and technical protection for all entities involved.



SARBANES OXLEY ACT (SOX)

The Sarbanes Oxley Act describes what records organizations must keep and for how long, thus increasing the accuracy and reliability of corporate disclosures and protecting investors and the public.

The act contains 11 titles:

1. Public company accounting oversight board
2. Auditor independence
3. Corporate responsibility
4. Enhanced financial disclosures
5. Analyst conflicts of interest
6. Commission resources and authority
7. Studies and reports
8. Corporate and criminal fraud accountability
9. White-collar-crime penalty enhancement
10. Corporate tax returns Corporate fraud accountability

DIGITAL MILLENIUM COPYRIGHT ACT (DMCA)

The DMCA is a copyright law in the United States of America which implements the WIPO (World Intellectual Property Organization) Copyright Treaty and WIPO Performances and Phonograms Treaty.

The act contains five titles:
1. WIPO Treaty Implementation
2. Online Copyright Infringement Liability Limitation
3. Computer maintenance or repair
4. Miscellaneous provisions Protection of certain original designs

FEDERAL INFORMATION SECURITY MANAGEMENT ACT

FISMA protects government information, operations, and assets against various threats.

FISMA FRAMEWORK

STANDARDS FOR CATEGORIZING INFORMATION AND INFORMATION SYSTEMS BY MISSION IMPACT

STANDARDS FOR MINIMUM SECURITY REQUIREMENTS FOR INFORMATION AND INFORMATION SYSTEMS

GUIDANCE FOR CHOOSING APPROPRIATE SECURITY CONTROLS FOR INFORMATION SYSTEMS

GUIDANCE FOR ASSESSING SECURITY CONTROLS IN INFORMATION SYSTEMS

GUIDANCE FOR THE SECURITY AUTHORIZATION OF INFORMATION SYSTEMS

Footprinting and Reconnaissance

ABOUT FOOTPRINTING

SEARCH ENGINES AND GOOGLE HACKING

FOOTPRINTING TYPES

Footprinting

WHAT IS FOOTPRINTING?

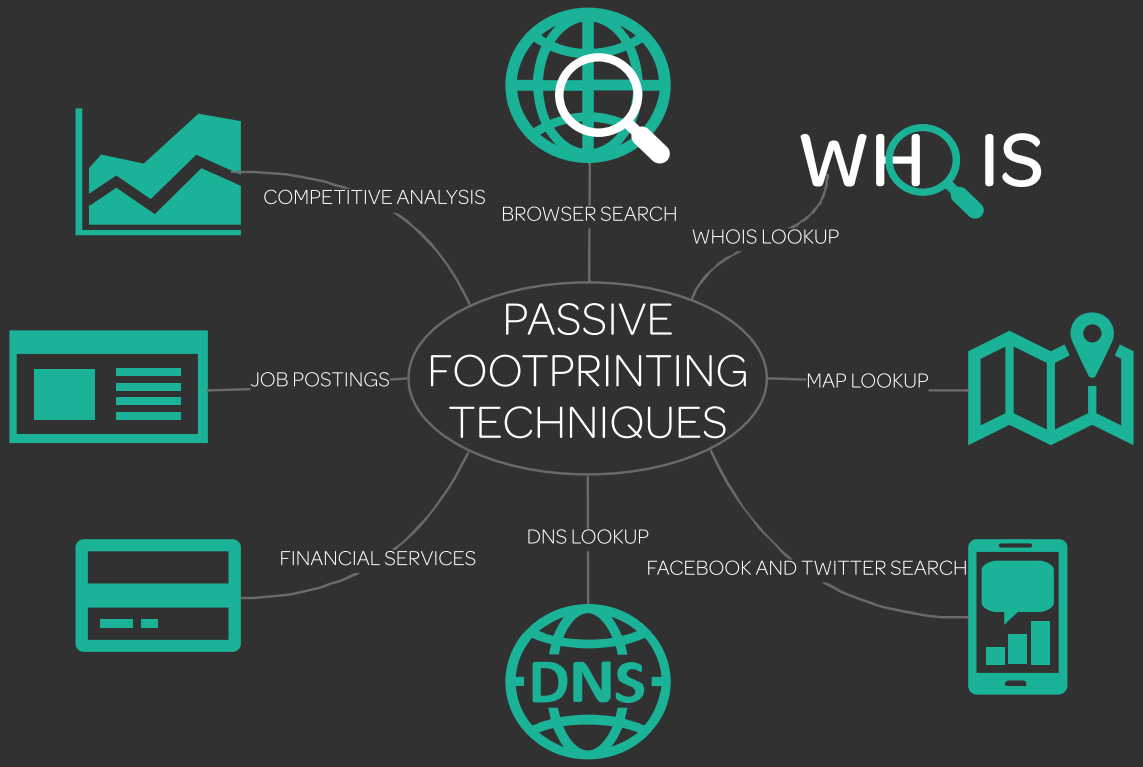
Footprinting refers to the process of gathering information about a target system. It is the first step of an attack in which the attacker tries to learn as much as possible about the target in order to find a way to break into the system.

PASSIVE	ACTIVE
Information is collected with no direct contact with the target.	Information is collected with direct contact with the target.

Footprinting

PASSIVE FOOTPRINTING

Passive footprinting means collecting information without interacting with the target directly. This type of footprinting is used when information gathering must not be detected by the target.



Footprinting

ACTIVE FOOTPRINTING

Active footprinting means collecting information by interacting with the target directly. With this type of footprinting there is a chance that the target becomes aware of the information gathering.

Footprinting

INFORMATION GATHERED IN FOOTPRINTING

NETWORK INFORMATION

WHOIS

Collected information:

- domains
- subdomains
- IP addresses
- Whois and DNS records

SYSTEM INFORMATION

Collected information:

- OS on web servers
- server locations
- users
- passwords

ORGANIZATION INFORMATION

Collected information:

- employee information
- organization's background
- phone numbers
- locations

Footprinting

FOOTPRINTING OBJECTIVES

LEARN SECURITY POSTURE

Analyze the security posture of the target, find loopholes, and create an attack plan.

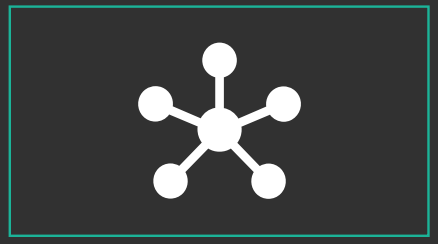
IDENTIFY FOCUS AREA

Using different tools and techniques, narrow down the range of IP addresses.

FIND VULNERABILITIES

Use the collected information to identify weaknesses in the target's security.

MAP THE NETWORK



Graphically represent the target's network and use it as a guide during an attack.

Footprinting

THREATS MADE THROUGH FOOTPRINTING

SOCIAL ENGINEERING

SYSTEM AND NETWORK ATTACKS

DATA LEAKAGE

LOSS OF PRIVACY

CORPORATE ESPIONAGE

LOSS OF BUSINESS

SEARCH ENGINES AND GOOGLE HACKING

Search engines can be used to extract information about the target organization. Search results can include information about the target organization's employees, intranet, login pages, and other information that could be useful to attackers.

Google hacking is a technique which attackers use to perform a complex search and extract important information about their targets. It involves using a set of search operators and building complex queries.

Google dorks is the name used for the operators used in Google hacking.

Footprinting

DORKS

[site:]

This operator limits the results to the specified domain.

Example:
[course site: www.linuxacademy.com]

[inurl:]

This operator limits the results only to those pages that have the query term in the URL.

Example:
[inurl:linuxacademy]

[intitle:]

This operator limits the results only to those pages that have the query term in the title.

Example:
[intitle:linux]

[allinurl:]

This operator limits the results to the pages that have all the query terms in the URL.

Example:
[allinurl: search google]

[allintitle:]

This operator limits the results to the pages that have all the query terms in the title.

Example:
[allintitle: linux academy security]

[inanchor:]

This operator limits the results to the pages that have the query term in the anchor text of the page.

Example:
[course inanchor:linuxacademy]

Footprinting

DORKS

[allinanchor:]

This operator limits the results to the pages that have all the query terms in the anchor text of the page.

Example:
[allinanchor: linux academy cloud]

[link:]

This operator limits the results to the pages that contain the queried link.

Example:
[link:www.linuxacademy.com]

[location:]

This operator returns information about the queried location.

Example:
[location: vegan restaurant]

[cache:]

This operator displays cached versions of the queried page.

Example:
[cache:www.linuxacademy.com]

[related:]

This operator shows sites that are similar or related to the queried URL.

Example:
[related:www.linuxacademy.com]

[filetype:]

This operator limits the results to the specified domain.

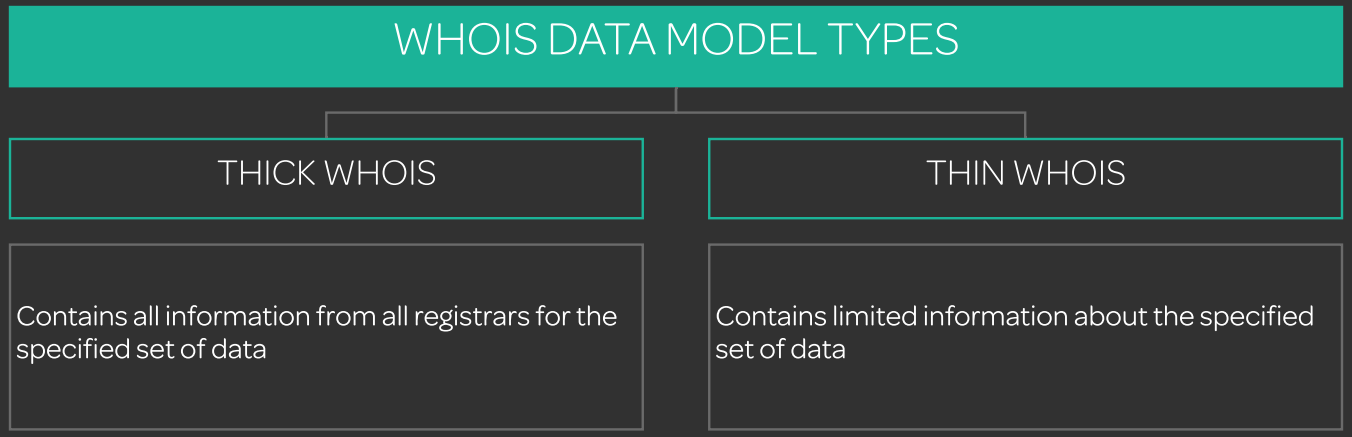
Example:
[filetype:pdf linuxacademy]

WHOIS FOOTPRINTING

Whois refers to a query and response protocol (port 43) which is used for retrieving information about assigned Internet resources.

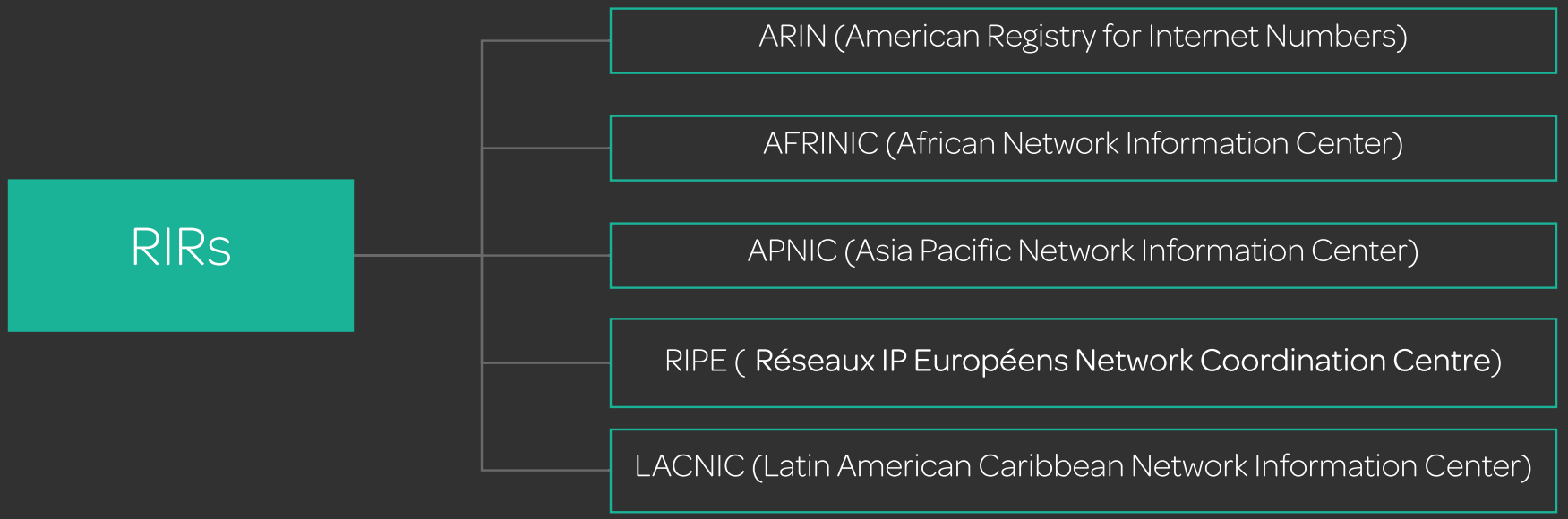
Whois query results typically include:

- Domain details
- Domain owner details
- Domain server
- Net range
- Domain expiration Creation and last update dates



WHOIS FOOTPRINTING

Whois databases are maintained by the Regional Internet Registries (RIRs) which contains personal information about the domain owners.



Footprinting

IP GEOLOCATION

IP geolocation helps find location information about a target such as country, city, postal code, ISP, and so on. With this information, hackers are able to perform social engineering attacks on the target.

DNS FOOTPRINTING

DNS footprinting refers to collecting information about DNS zone data, which includes information about key hosts in the network. DNS interrogation tools help attackers to perform DNS footprinting. Using these tools, attackers are able to obtain information about server types and their locations.

EMAIL FOOTPRINTING

Email footprinting refers to collecting information from emails by monitoring the email delivery and inspecting the headers.

Email headers contain information about the sender, subject, and recipient. All this information is valuable to hackers when planning to attack their target.

Email tracking tools have the capability of tracking emails and inspecting their headers to extract useful information. The sender is notified of the email being delivered and opened by the recipient.

INFORMATION GATHERED IN EMAIL FOOTPRINTING	INFORMATION CONTAINED IN HEADERS
• IP Address of the recipient • Geolocation of the recipient • Delivery information • Visited links • Browser and OS information • Reading time	• IP/Email address of the sender • Mail server • Mail server authentication system • Send and delivery timestamps • Unique number of the message • Sender's name

Footprinting

WEBSITE FOOTPRINTING

Website footprinting is a technique in which information about the target is collected by monitoring the target's website. Hackers can map the entire website of the target without being noticed. Additional ways to gather information is through HTML Source Code and cookie examination.

Web spider refers to a program which is designed in such a way to methodically browse a website in search of specific information. Information collected this way can help hackers perform social engineering attacks.

INFORMATION GATHERED IN WEBSITE FOOTPRINTING

- Software
- Operating system
- Subdirectories
- Contact information
- Scripting platform
- Query details

INFORMATION CONTAINED IN HEADERS

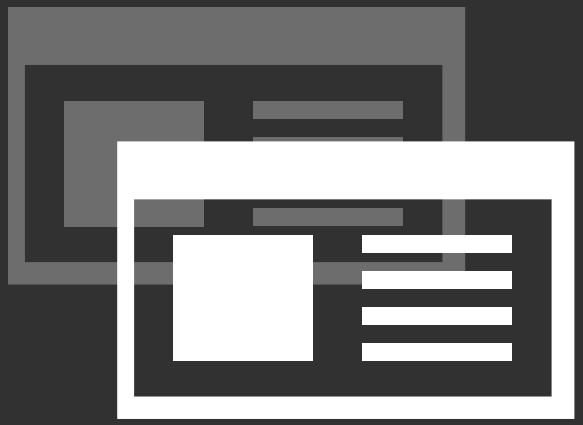
- Content-Type
- Accept-Ranges
- Connection Status
- Last-Modified Information
- X-powered-by Information
- Web Server Information

WEBSITE FOOTPRINTING

Website mirroring refers to the process of duplicating a website. Mirroring a website helps in browsing the site offline, searching the website for vulnerabilities, and discovering valuable information.

Websites may store documents of different format which in turn may contain hidden information and metadata that can be analyzed and used in performing an attack.

Monitoring websites for updates and changes can be done using website monitoring tools which have the capability to send notifications on detected changes.



NETWORK FOOTPRINTING

Network footprinting refers to the process of collecting information about the target's network. During this process, attackers collect network range information and use the information to map the target's network.

Network range gives attackers an insight into how the network is structured and which machines belong to the network

NMAP	TRACEROUTE
Nmap is a tool used for network discovery. It uses raw IP packets to determine the available hosts on the network, the services offered by those hosts, operating systems they are running, firewall types that are being used, and other important characteristics. Nmap features include the ability to scan large networks as well as mapping out networks.	Traceroute programs are used for discovering routers that are on the path to the target host. Traceroute uses ICMP protocol and the TTL field in the IP header to discover the route. It records IP addresses and DNS names of discovered routers. The results of a traceroute help attackers collect information about network topology, trusted routers, as well as firewall locations.

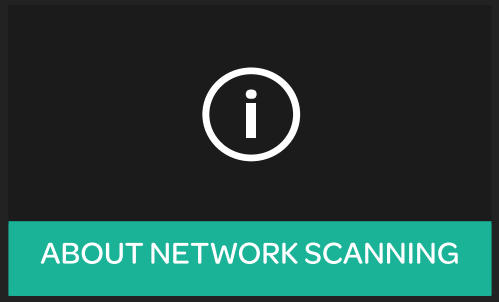
FOOTPRINTING COUNTERMEASURES

- Restrict access to social media
- Enforce security policies
- Educate employees about security threats
- Encrypt sensitive information
- Disable protocols that are not required
- Configure services properly

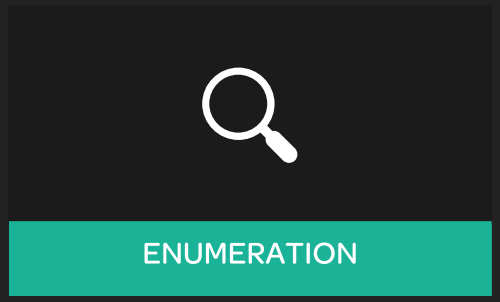
FOOTPRINTING REPORTS

Footprinting reports should include details about the performed tests, used techniques, and test results. It should also include a list of vulnerabilities and how they can be fixed. These reports should be kept highly confidential, so that they do not fall into wrong hands.

Scanning Networks



ABOUT NETWORK SCANNING



ENUMERATION

VULNERABILITY

Scanning Networks

NETWORK SCANNING

Network scanning refers to the process of obtaining additional information and performing a more detailed reconnaissance based on the collected information in the footprinting phase. In this phase, several different procedures are used with the objective to identify hosts, ports, and services in the target network.

The purpose is to identify vulnerabilities in communication channels and then create an attack plan.

Scanning has three types:

- Port scanning - used to list open ports and services
- Network scanning - used to list IP addresses
- Vulnerability scanning - used to discover the presence of known vulnerabilities

Scanning Networks

SCANNING TECHNIQUES

Scanning techniques represent different categories which are used based on protocol types.

SCANNING TECHNIQUES		
Scanning ICMP Network Services	Scanning TCP Network Services	Scanning UDP Network Services
ICMP Scanning	TCP Connect	IDLE/IPID Header Scan
Ping Sweep	Stealth Scan	UDP Scanning
ICMP Echo Scanning	Inverse TCP Flag Scanning	SSDP and List Scanning
	Xmas Scan	
	ACK Flag Probe Scanning	

Scanning Networks

SCANNING ICMP NETWORK SERVICES

ICMP Scanning	ICMP scanning is used for identifying active devices and determining whether ICMP can pass through a firewall.
Ping Sweep	Ping sweep is used to determine the range of IP addresses that is mapped to active devices. It allows hackers to calculate subnet masks and identify the number of present hosts in the subnet, and thus create an inventory of active devices in the subnet.
ICMP Echo Scanning	ICMP Echo Scanning is used to determine which hosts are active in a target network by pinging all the machines in the network.

Scanning Networks

SCANNING TCP NETWORK SERVICES

TCP Connect	TCP connect scan used for detecting open ports upon the completion of the three-way handshake. It works by establishing a full connection and then dropping it by sending an RST packet.
Stealth Scan	Stealth scan is used for bypassing firewall and logging mechanisms. It works by resetting the TCP connection before the three-way handshake is completed, which in turn makes the connection half open.
Inverse TCP Flag Scanning	Inverse TCP flag scanning works by sending TCP probe packets with or without TCP flags. Based on the response, it is possible to determine whether the port is open or closed.
Xmas Scan	Xmas scan works by sending a TCP frame with FIN, URG, and PUSH flags set to the target device. Based on the response, it is possible to determine whether the port is open or closed.
ACK Flag Probe Scanning	ACK flag probe scanning works by sending TCP probe packets with ACK flag set in order to determine whether the port is open or closed. This is done by analyzing the TTL and WINDOW field of the received RST packet's header.

Scanning Networks

SCANNING UDP NETWORK SERVICES

IDEL/IPID Header Scan	IDLE/IPID header scan works by sending a spoofed source address to the target to determine which services are available. Based on the IPID of the packer (fragment identification number), it is possible to determine whether the port is open or closed.
UDP Scanning	UDP scanning uses UDP protocol to test whether the port is open or closed. ICMP is used to determine if the port is open or not. So, if the ICMP port unreachable packet is returned, then the port is closed. If there is no response, then the port is open.
SSDP and List Scanning	SSDP service responds to queries sent over IPv4 and IPv6 broadcast addresses. Attackers use this scan to exploit UPnP vulnerabilities and carry out buffer overflow or DoS attacks. List scanning works by listing out IP addresses and names without pinging the hosts and performing a reverse DNS resolution to identify the names of the hosts.

Scanning Networks

BYPASSING IDS AND FIREWALLS

PACKET FRAGMENTATION	Packet fragmentation works by sending fragmented probe packets to the server which then reassembles them once all packets are received.
SOURCE ROUTING	Source routing works by specifying which path the malformed packet will take to get to the target host.
IP ADDRESS DECOY	IP address decoy works by generating decoy IP addresses and thus preventing the IDS/Firewall from determining the real IP address.
IP ADDRESS SPOOFING	IP address spoofing works by changing the IP address of the source and thus making the packet appear to come from someone else.
PROXY SERVER	Proxy server works by using a series of proxy servers to conceal the real source of the scan.

Scanning Networks

BANNER GRABBING

Banner grabbing refers to determining the operating system of the target. Knowing the operating system help attackers exploit known vulnerabilities as well as form an attack plan.

Operating system can be identified by reading the values of TTL (time to live) and TCP window size in the IP header of the first packet. These values are different for different operating systems.

Banner grabbing can be prevented by disabling banners and by hiding web page extensions.

ACTIVE BANNER GRABBING

Active banner grabbing works by sending malformed packets to the OS and then recording the responses. Because different operating systems have different TCP/IP stack implementations, each response is analyzed to determine the operating system.

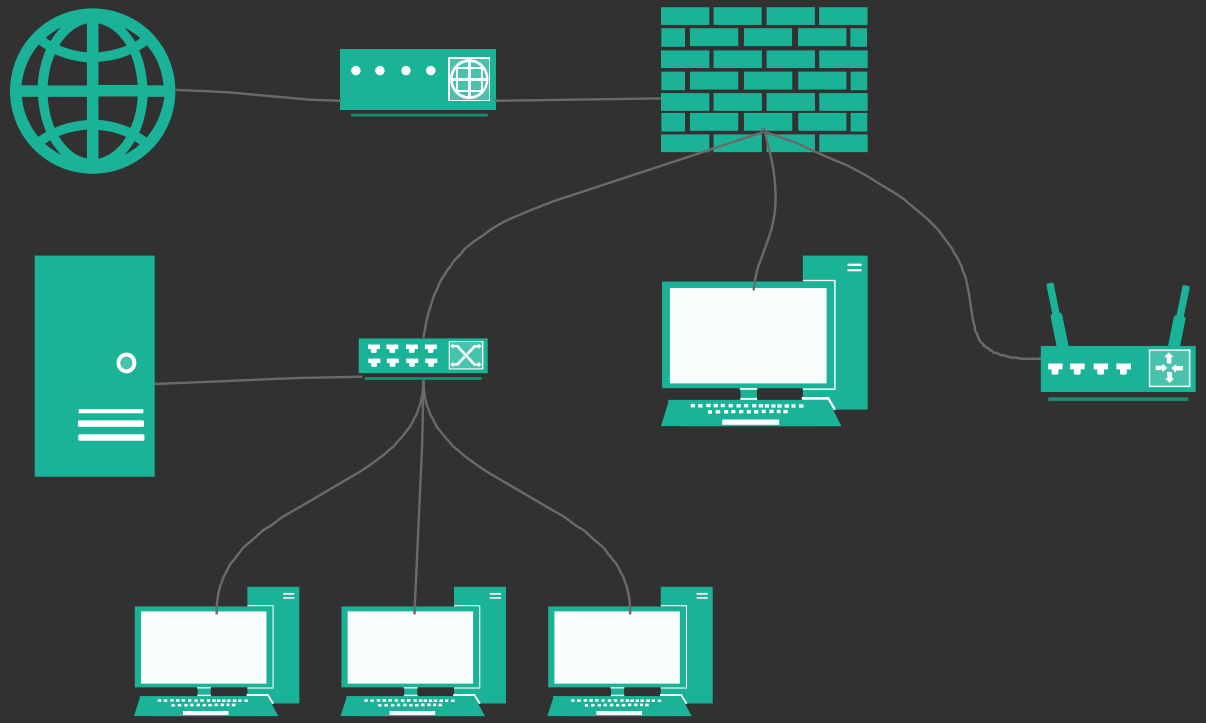
PASSIVE BANNER GRABBING

Passive banner grabbing uses sniffing to determine the operating system. It includes analyzing error messages, sniffing the traffic on the network, and examining page extensions.

Scanning Networks

NETWORK DIAGRAMS

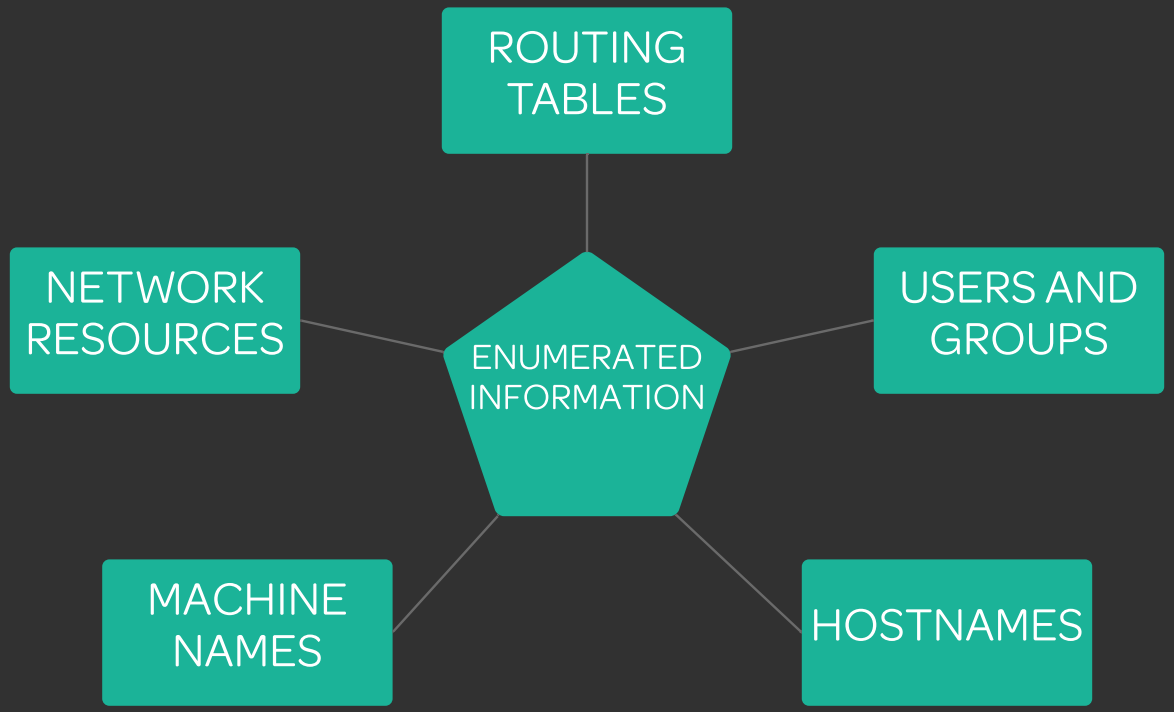
Network diagrams are useful when it comes to identifying and understanding the topology of the target network. The diagram can tell the attacker how firewalls, IDSs, routers, and other devices are arranged in the network.



Scanning Networks

ENUMERATION

Enumeration is the process of extracting information from a system or a network by creating active connections and performing queries. The information collected through this process is used to discover vulnerabilities in the system and then exploit them.



Scanning Networks

ENUMERATION TYPES

NetBIOS Enumeration

NetBIOS is easily exploitable and often used by hackers when attacking a target. NetBIOS enumeration helps attacker collect information about all computers that belong to one domain, individual host shares in the network, as well as passwords and policies.

SNMP Enumeration

SNMP enumeration works by using SNMP to enumerate users and devices on a target system. Using SNMP enumeration, attackers can extract information about hosts, routers, devices, routing tables, and other network resources.

LDAP Enumeration

LDAP has access to directory services. Querying LDAP may return information about usernames, addresses, servers, and other sensitive information which can help the attacker perform an attack.

NTP Enumeration

NTP enumeration provides hackers with information about the hosts that are connected to NTP server as well as IP addresses, system names, and operating systems of the clients.

SMTP Enumeration

SMTP stands for Simple Mail Transport Protocol and is used for sending emails. SMTP enumeration helps identify valid users on the SMTP server.

DNS Enumeration

DNS enumeration helps locate the target's DNS server and records. Attackers can collect information about DNS server names, hosts, usernames, machine names, IP addresses, and so on. The objective here is to retrieve a copy of the domain's zone file.

SCANNING FOR VULNERABILITIES

Vulnerability research helps identify vulnerabilities which could compromise the system.

Vulnerabilities are typically categorized into one of the following categories:

- Misconfiguration
- Default installations
- Buffer overflows
- Unpatched servers
- Design flaws
- Operating system flaws
- Application flaws
- Open services
- Default passwords

Scanning Networks

VULNERABILITY ASSESSMENT

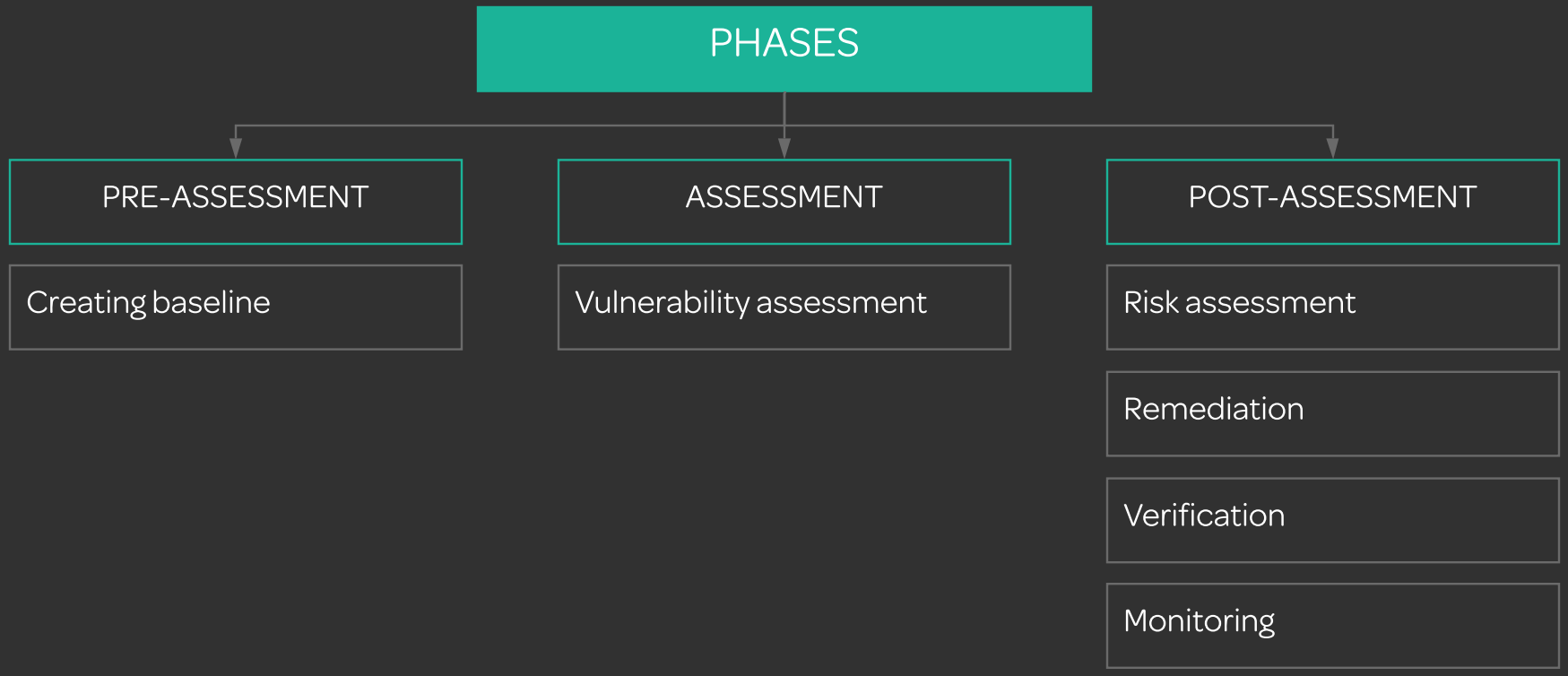
Vulnerability assessment examines the system and its ability to resist an attack by scanning the network and looking for vulnerabilities.

ASSESSMENT TYPES	
Active Assessment	Utilizes network scanners to discover hosts, services, and vulnerabilities
Passive Assessment	Discovers hosts, services, and vulnerabilities by sniffic the traffic
External Assessment	Discovers vulnerabilities and threats that are accessible from the outside
Internal Assessment	Discovers vulnerabilities and threats that are present internally
Host-Based Assessment	Discovers vulnerabilities and threats on a specific server
Network Assessment	Identifies potential attacks on the network
Application Assessment	Examines the configuration of the web infrastructure
Wireless Network Assessment	Discovers vulnerabilities and threats in the organization's wireless network

Scanning Networks

VULNERABILITY MANAGEMENT

Vulnerability management refers to the evaluation and control of the risks and vulnerabilities in the system.



Scanning Networks

VULNERABILITY SCORING SYSTEMS

Vulnerabilities that are identified are stored into databases and given certain scores based on their severity and risk.

CVSS	CVE	NVD
The Common Vulnerability Scoring System (CVSS) provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. *	CVE is a list of common identifiers for publicly known cybersecurity vulnerabilities. *	NVD includes databases of security checklist references, security related software flaws, misconfigurations, product names, and impact metrics. *
*https://www.first.org/cvss/	*https://cve.mitre.org/about/index.html	* https://nvd.nist.gov/general

System Hacking

CRACKING PASSWORDS

PRIVILEGE ESCALATION AND REMOTE ACCESS

HIDING FILES AND COVERING TRACKS

MALWARE

SYSTEM HACKING

Hacking a system is done in three steps. Attackers first collect enough information which can be used to gain access to the system. Once they have the right privileges, their goal is to maintain the access for as long as possible during which time they execute malicious programs, steal information, or simply tamper with the system. After they are done with their attack, attackers hide their tracks by modifying the system logs.

The objectives of system hacking are to:

- Gain access to the target system
- Escalate privileges
- Execute applications
- Hide files
- Cover tracks

1 Gain Access

2 Maintain Access

3 Cover Tracks

CRACKING PASSWORDS

Cracking passwords refers to recovering passwords from the transmitted or stored data on computer systems

Non-electronic Attacks	Active Online Attacks	Passive Online Attacks	Offline Attacks
Dumpster Diving	Dictionary Attack	Wire Sniffing	Rainbow Table Attack
Shoulder Surfing	Brute Force Attack	MITM Attack	Distributed Network Attack
Social Engineering	Rule-based Attack	Replay Attack	
	Password Guessing		
	Trojan/Spyware/Keylogger		
	Hash Injection		
	LLMNR/NBT-NS Poisoning		

System Hacking

NON-ELECTRONIC ATTACKS

Dumpster Diving	Dumpster diving is a technique which requires going through the target's trash bins, printer trash bins, and work desks and looking for notes or anything that can help in cracking the password.
Shoulder Surfing	Shoulder surfing refers to observing the target while they type in their passwords, that is, looking at their keyboard or screen.
Social Engineering	Social engineering requires the attacker to interact with the target and trick them into revealing their passwords.

System Hacking

ACTIVE ONLINE ATTACKS

Dictionary Attack	Dictionary attack loads a dictionary file into a password cracking program which then checks the passwords against user accounts
Brute Force Attack	Brute force attack requires the attacker to run every combination of characters until the password is cracked
Rule-based Attack	Rule-based attack is used when the attacker has some information about the password, such as the length, if there are any digits, and similar
Password Guessing	In this attack, the attacker uses all information they have gathered about the target to create a list of possible passwords and then tries each password on the target's machine
Trojan/Spyware/Keylogger	Attackers install trojans, spyware, and keyloggers so that they could get the target's passwords and usernames
Hash Injection	Hash injection attack is an attack on systems that use hash functions for the user authentication
LLMNR/NBT-NS Poisoning	In this attack, attackers exploit the vulnerability when DNS fails to resolve name queries.

System Hacking

PASSIVE ONLINE ATTACKS

Wire Sniffing	Wire sniffing is an attack in which attackers sniff credentials by capturing packets that are being transmitted. During the packet transmission, attackers are able to capture packets and extract sensitive information such as passwords and emails and thus gain access to the target system.
MITM Attack	Man-in-the-middle attack is an attack in which the attacker gains access to the communication channel between the target and server. Then, the attacker is able to extract information and data they need to gain unauthorized access.
Replay Attack	Replay attack involves using a sniffer to capture packets and authentication tokens. Once the relevant data is extracted, the tokens are placed back on the network in an attempt to gain unauthorized access.

System Hacking

OFFLINE ATTACKS

Rainbow Table Attack	Rainbow table refers to a table of word and brute force lists and their hashes. The attack requires the attacker to create a rainbow table prior to the attack, and then use the information from the table to crack the password.
Distributed Network Attack	Distributed network attack utilizes the processing power of machines that are on the network in order to decrypt the password. This attack is used for recovering passwords from hashes. It works by installing a DNA manager in a central location from which it is possible to coordinate the attack by allocating portions of the key search to machines which are on the network.

PRIVILEGE ESCALATION

Privilege escalation refers to taking advantage of the operating system and software vulnerabilities which enable the attacker to gain admin privileges. Becoming an admin on the target system allows the attacker to perform all sorts of malicious activities.

Horizontal Privilege Escalation	Vertical Privilege Escalation
Horizontal privilege escalation refers to acquiring the privileges of the same level.	Vertical privilege escalation refers to acquiring higher privileges.

REMOTE ACCESS

Once the attacker has gained access to the system and elevated privileges, they proceed to the next step in which they remotely execute malicious programs.

Programs that attackers install include:

- Backdoors to collect information and gain unauthorized access to the system
- Crackers to crack passwords
- Keyloggers to record keystrokes
- Spyware to capture screenshots and send them to the attacker

KEYLOGGERS

Keylogger is a program or hardware device designed to record every keystroke on the target's keyboard, logs them into a file, and sends them to a remote location.

Hardware Keylogger

Hardware keyloggers are devices that look like USB drives and are designed to record keystrokes, which are stored on the device. They are placed between a keyboard plug and USB socket and cannot be detected by antispyware or antivirus programs.

Software Keylogger

Software keyloggers are programs installed on the target's machine. Recorded keystrokes are logged into a log file on the target's machine which is then sent to the attacker using email protocols.

System Hacking

HARDWARE KEYLOGGERS

PC/BIOS EMBEDDED	PC/BIOS Embedded keylogger refers to modifying the BIOS level firmware to capture the keystrokes
KEYLOGGER KEYBOARD	Keylogger keyboard refers to attaching the hardware circuit with the keyboard cable connector
EXTERNAL KEYLOGGER	External keylogger refers to attaching the keylogger between a keyboard and computer

SOFTWARE KEYLOGGERS

APPLICATION KEYLOGGER	Application keylogger is designed to observe the target's activity whenever type something
KERNEL, ROOTKIT, DEVICE DRIVER KEYLOGGERS	Kernel keylogger is designed to exist on a kernel level and act as a keyboard device driver, which allows it to record everything that is typed on the keyboard. Rootkit keylogger refers to a forged Windows device driver which records keystrokes. Device driver keylogger is designed to replace the driver that has the keylogging functionality, logs the keystrokes, and send the file to a remote location
HYPERVISOR BASED KEYLOGGER	Hypervisor-based keylogger is designed to work within a malware hypervisor that is operating on the OS
FORM GRABBING BASED KEYLOGGER	Form grabbing based keylogger is designed to record web browsing when the Submit event is triggered

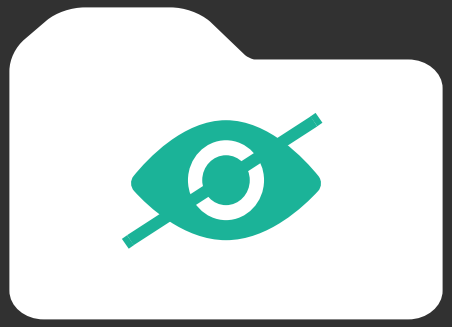
System Hacking

SPYWARE

Spyware is a stealthy program designed to record the target's interaction with the computer and Internet and then send the recorded data to the attacker. This program is also able to take and send screenshots. The program is hidden when installed

HIDING FILES

Hiding files is a process in which the attacker attempts to cover their tracks in order to ensure future access to the system.



ROOTKITS

Rootkit is a program designed to help the attacker gain access to a system without being detected. It is designed to create a backdoor to the system and thus enable the attacker to access the system and perform malicious activities.

The objectives of a rootkit include:

- Gaining remote backdoor access
- Hiding traces of the attack
- Collect confidential data
- Install other malicious programs on the machine

System Hacking

ROOTKIT TYPES

HYPERVISOR LEVEL ROOTKIT	Hypervisor level rootkit is designed to act as a hypervisor and load the target OS as a virtual machine
HARDWARE/FIRMWARE ROOTKIT	Hardware/Firmware rootkit is designed to conceal itself in hardware devices that are not inspected
KERNEL LEVEL ROOTKIT	Kernel level rootkit is designed to add malicious code or replace portions of the core operating system with some modified code
BOOTLOADER LEVEL ROOTKIT	Boot loader level rootkit is designed to replace the original bootloader with a malicious one
APPLICATION LEVEL ROOTKIT	Application level rootkit is designed to change the behavior of the target application
LIBRARY LEVEL ROOTKIT	Library level rootkit is designed to replace the original system calls in order to hide the attacker's activities

NTFS DATA STREAMS

NTFS data streams are two data streams that help NTFS store files. One data stream stores data about the file, and the other stream stores the file data.

Alternate data stream contains file metadata such as file attributes, author, access, and word count. Alternate data stream enables attackers to inject malicious code into files and execute it. This is not easily detectable by the system admin because the file size and the contents remain the same, despite the size of the added ADS. The only way of discovering that the file has been tampered with is to check the file timestamps

STEGANOGRAPHY

Steganography refers to a technique which hides a message within another message. The hidden message is extracted when it arrives to its destination. This technique is used for maintaining information confidentiality.

Steganalysis refers to discovering of the hidden data in a medium. Steganalysis uses steganography to detect hidden messages. It has two phases: detection, in which the analyst detects the existence of hidden information, and distortion, in which the analyst tries to extract the hidden message.

COVERING TRACKS

Covering tracks is a phase in which the attacker attempts to hide their presence on the system. To avoid detection, the attacker needs to modify the system logs and delete their activity during the attack, and also ensure that future activities are not logged too. It is very important that the system appears uncompromised.

REVERSE HTTP SHELLS	Reverse HTTP shells are designed to ask the master system for commands which, when received, are executed on the target's machine
REVERSE ICMP TUNNELS	Reverse ICMP tunnel is a technique in which the attacker accesses the system by using ICMP echo and reply packets as carriers of TCP payload
DNS TUNNELING	DNS tunneling refers to adding data payload to the target's DNS server in order to create a back channel through which it is possible to steal information from the server
TCP PAREMETERS	TCP parameters refers to using TCP parameters for payload distribution. Fields in which data can be hidden are IP identification field, TCP acknowledgement number, and TCP initial sequence number

System Hacking

MALWARE

Malware refers to a malicious program designed to cause damage to systems. Attackers use malware to gain access to target systems.

TROJAN	Trojan is a program which contains malicious code and has the ability to cause damage to the target system. They are contained inside seemingly harmless programs and activated when such programs are executed
CRYPTER	Crypter is a program which hides malware from antiviruses by encrypting the program's original binary code.
VIRUS	Virus is a program designed to replicate itself to other programs and documents on the infected machine. Viruses spread to other computers with the transfer of the infected files or programs. They are transmitted through file transfers, infected flash drives, and email attachments.
WORM	Worm is a program which replicates itself across network connections. Worms are designed to exploit vulnerabilities on the victim machines and then spread to other computers as the infected files are transferred.
RANSOMWARE	Ransomware is a type of malware in which hackers restrict access to files and folders on the target system until a payment is made. Victims are usually required to pay a certain sum of money in order to be able to access their files.

MALWARE ANALYSIS

Malware analysis refers to a process of reverse engineering of a malware program. The purpose of the analysis is to determine how the malware works and assess the potential damage it could cause.

STATIC MALWARE ANALYSIS

Static analysis refers to analyzing the malware without running or installing it. The malware's binary code is examined to determine if there are any data structures or function calls that have malicious behavior.

DYNAMIC MALWARE ANALYSIS

Dynamic analysis requires the malware program to be running in a monitored environment, such as a sandbox or virtual machine. This type of analysis helps in understanding how the malware works by monitoring its activities on the system.

ANTI-MALWARE SOFTWARE

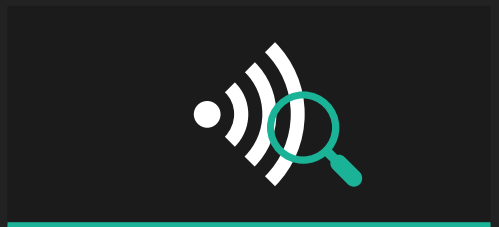
Anti-malware software helps detect, prevent, and remove malware on the system. It also helps repair any damage that the malware may have caused.

Signature-based Detection	Signature-based detection refers to comparing the hash of a suspicious code against a database of already known malware.
Behavior-based Detection	Behavior-based detection refers to detecting the malware based on its behavior and characteristics.
Sandboxing	Sandboxing refers to running unknown applications or possible threats in an isolated environment and monitoring the behavior. If the application appears to be malicious, then it gets terminated.

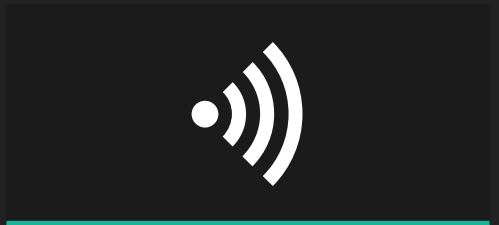
ANTIVIRUS vs ANTI-MALWARE

ANTIVIRUS	ANTI-MALWARE
Antivirus is designed to detect and remove viruses from the system. It focuses more on already known and older viruses, trojans, and worms.	Anti-malware is designed to detect and protect the system from all malware, including viruses, worms, trojans, rootkits, and so on. The focus is shifted to the latest threats that could be even more dangerous than the ones that already exist.

Wireless Networks and Spoofing



SNIFFING



WIRELESS NETWORKS

Wireless Networks and Spoofing

SNIFFING

Packet sniffing refers to the process of capturing data packets on a network using a program or a device.

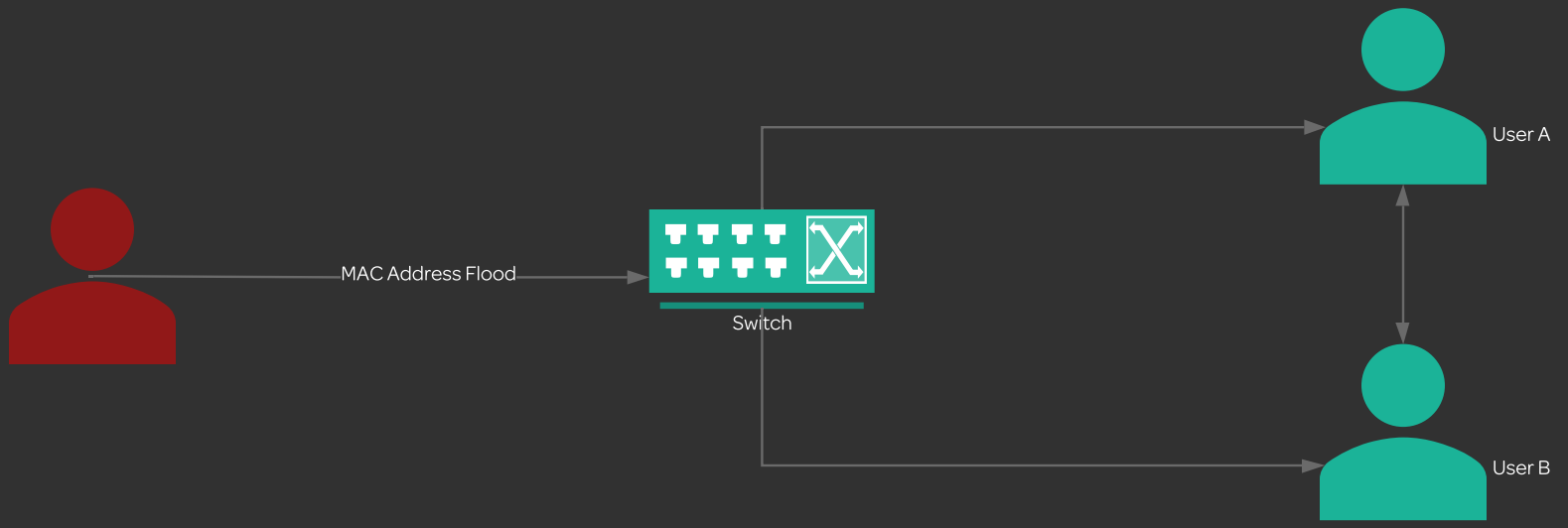
Packet sniffing programs are called sniffers and they are designed to capture packets that contain information such as passwords, router configuration, and traffic.

Passive Sniffing	Active Sniffing
Passive sniffing is used in networks which use hubs to connect systems. Such networks allow their hosts to see all the traffic passing through the network, which makes it easy for attackers to capture that traffic. Passive sniffing does not require any packets to be sent. Instead, the packets coming into the network are monitored and captured.	Active sniffing is used in networks which use switches. Switches require a packet to have a source and destination addresses in order to be sent to its destination, which makes it more difficult for attackers to sniff. However, it is possible to sniff a switch by flooding its Content Addressable Memory (CAM) table, which contains the information of which port belongs to which host. Flooding the CAM table is done by actively injecting ARP traffic into a LAN and then capturing the traffic.

Wireless Networks and Spoofing

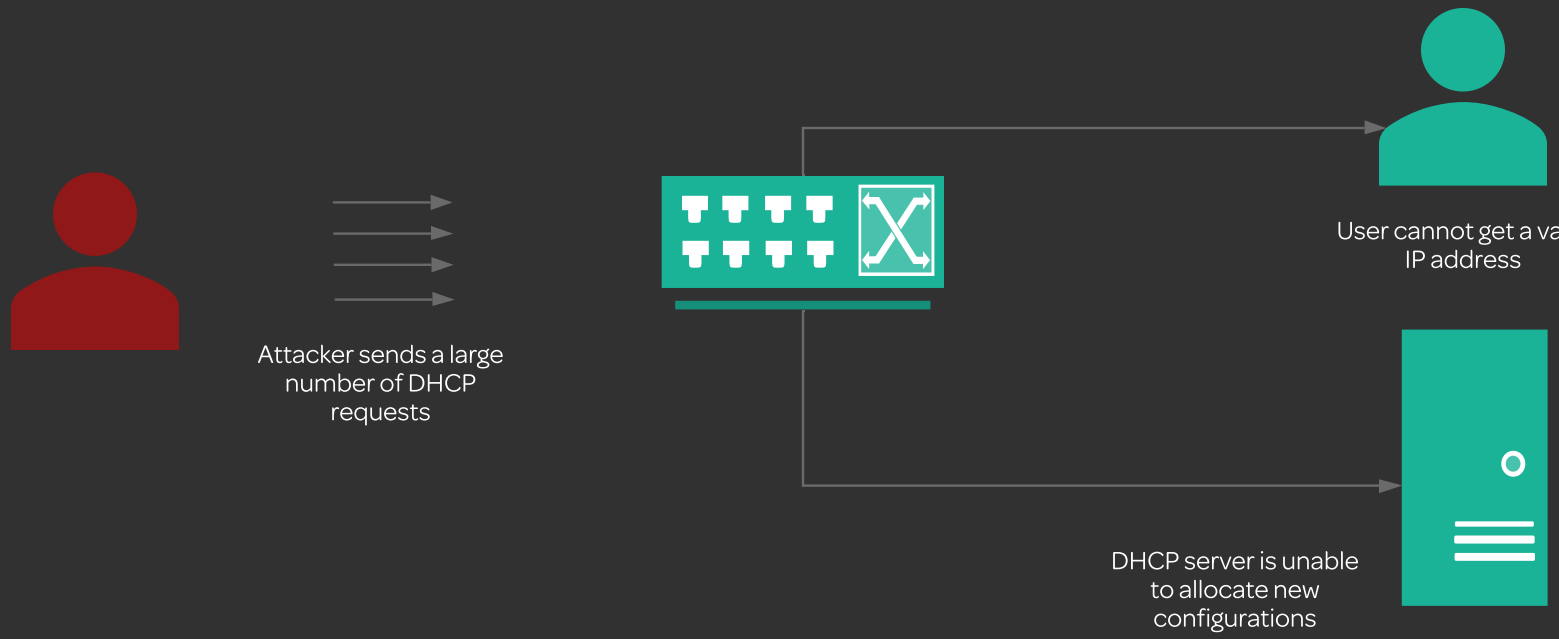
MAC FLOODING

MAC flooding is an attack in which a switch is forced to behave as a hub. This is possible due to the fixed size of the MAC table. By sending a large number of fake MAC addresses to the switch, the CAM table eventually becomes full. When that happens, switch enters the so-called fail-open mode in which it broadcasts the incoming traffic to all ports on the network.



DHCP STARVATION

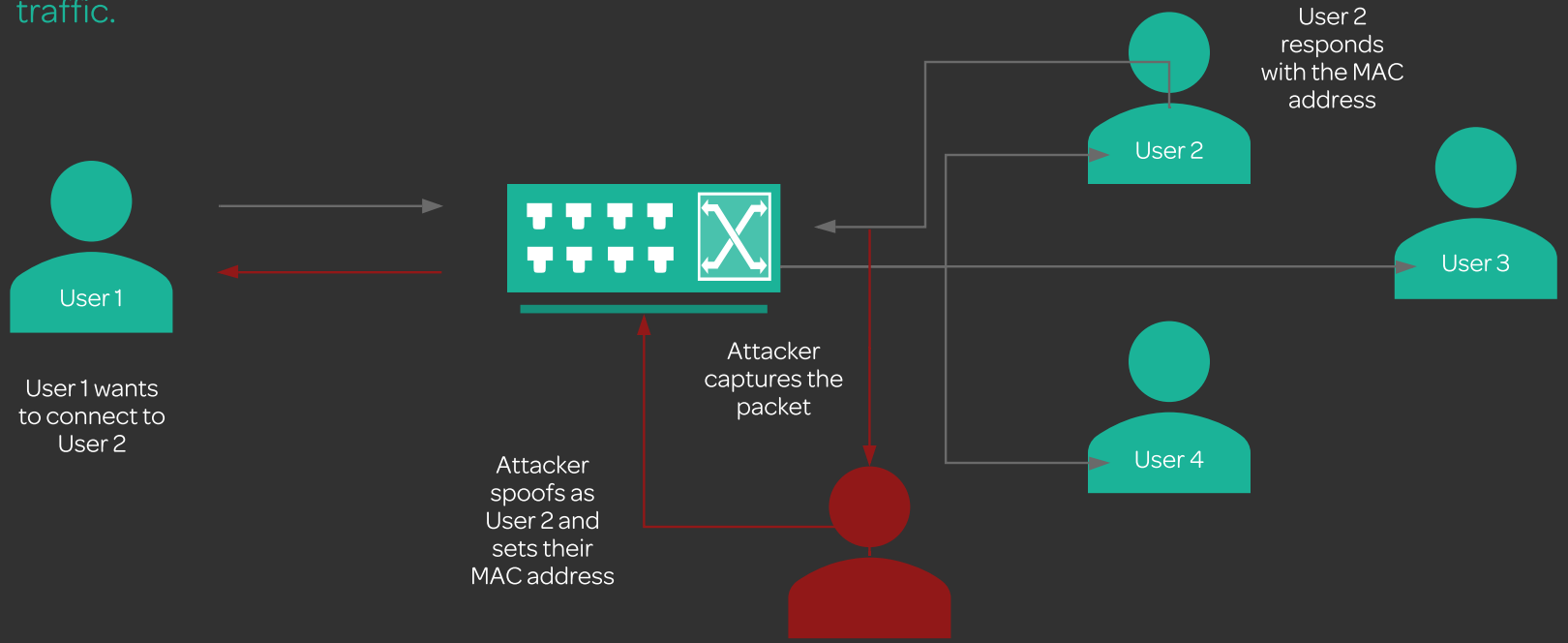
DHCP starvation is an attack in which the attacker floods the DHCP server so that it cannot provide IP addresses. This is a Denial of Service attack in which the attacker sends a huge number of DHCP requests to the point where the DHCP server is unable to allocate configurations to new clients and issue any IP addresses.



Wireless Networks and Spoofing

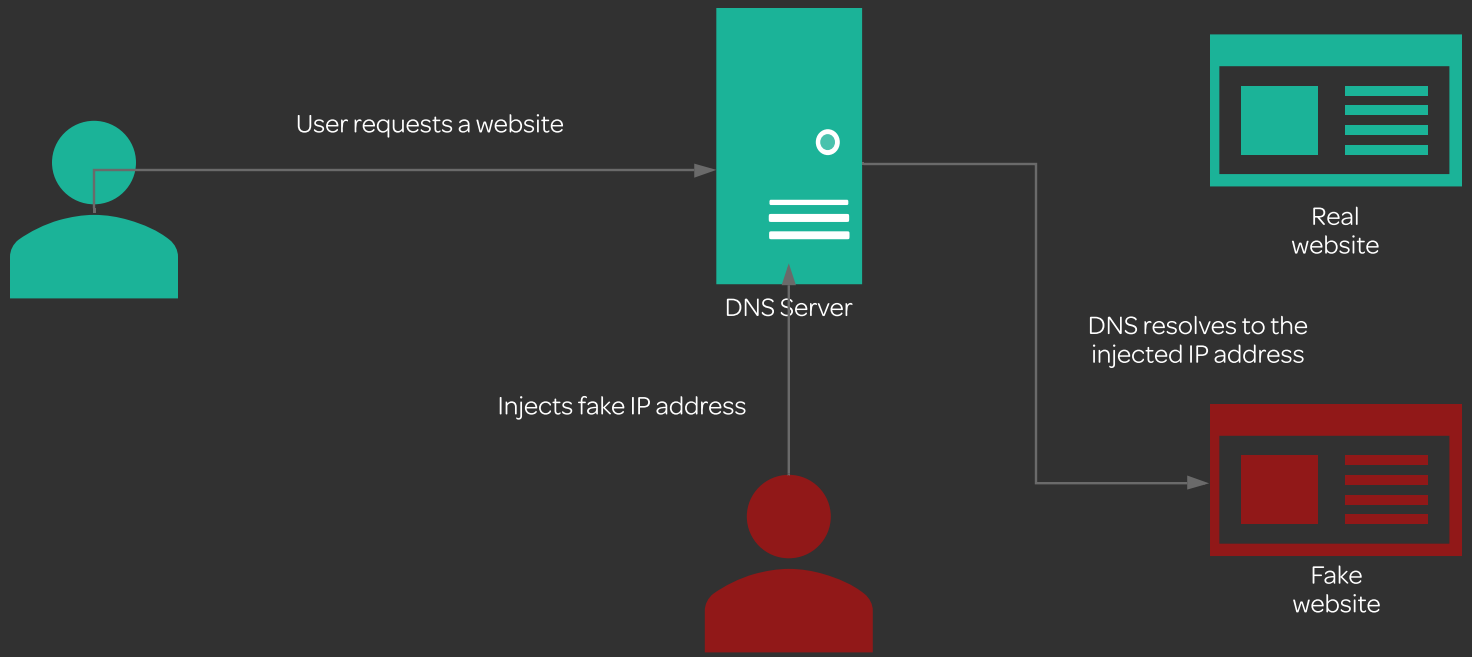
ARP POISONING

ARP spoofing or ARP poisoning is an attack in which the attacker forges ARP request and reply packets and sends a huge number of them to overload the switch. ARP does not verify the device authenticity, so the machine that sent a request simply assumes the reply came from the right device. Attackers use this flaw to sniff the network and create a forged ARP reply which is accepted by the machine that sent the request. The attacker then floods the victim's ARP table and sets the switch in forwarding mode. This enables the attacker to sniff the network traffic.



DNS POISONING

DNS poisoning is an attack in which the attacker manipulates the DNS table by replacing a legitimate IP address with a malicious one. When the target tries to access the website, whose data has been manipulated in the DNS table, the target is then redirected to the malicious URL and connected to the attacker's server.



WIRELESS NETWORKS

Wireless network (Wi-Fi) is a Wireless Local Area Network (WLAN) based on the IEEE 802.11 standard in which devices that are in the range of an access point are allowed to access the network.

A wireless network can be identified by its SSID (Service Set Identifier), which is a unique name for a wireless network and acts as an identifier between clients and the access point.

Wi-Fi AUTHENTICATION MODES

OSA

Open System Authentication (OSA) process refers to a process of accessing a Wi-Fi network which uses WEP protocol. A client sends an authentication request to the access point (AP). The AP responds with a randomly generated authentication code. The client accepts the authentication code and connects to the network.

SKA

Shared Key Authentication (SKA) process refers to a process of accessing a Wi-Fi network which uses WEP protocol and a shared secret key. A client sends an authentication request to the access point (AP). The AP responds with a challenge text. The client uses its WEP key to encrypt the challenge text and sends the encrypted text back to the AP. The AP decrypts the text and compares the decrypted text with the original one. If they match, the AP sends the authentication code to the client. The client accepts the authentication code and connects to the network.

Wireless Networks and Spoofing

WIRELESS ENCRYPTION

WEP

WEP, Wired Equivalent Privacy, is a security protocol which provides security and privacy on wireless networks. It encrypts data using RC4 encryption algorithm. It also relies on a 24-bit initialization vector and a 40-bit or 104-bit key, which combined form a 64-bit or 128-bit secret keys which are shared between a client and AP. The secret key is used for encryption and decryption of the data. CRC-32 checksum is used for integrity checks of the packets in transit.

WPA

WPA, Wi-Fi Protected Access, is a security protocol which provides stronger encryption than WEP. It uses TKIP (Temporal Key Integrity Protocol) which employs the RC4 algorithm with 128-bit keys and 64-bit Message Integrity Checks (MIC). MIC ensures that the transmitted packets are not changed or resent. TKIP uses a different key for each packet thus providing stronger encryption.

WPA2

WPA2, Wi-Fi Protected Access 2, is an upgrade to WPA. It uses AES encryption (Advanced Encryption Standard) and CCMP protocol (Counter Mode Cipher Block Chaining Message Authentication Code Protocol). WPA2-Personal encryption uses a pre-shared key (PSK) to protect the network access. WPA2-Enterprise uses Extensible Authentication Protocol (EAP) and RADIUS authentication.

Wireless Networks and Spoofing

WIRELESS HACKING METHODOLOGY

A wireless hacking methodology provides steps to be followed in order to successfully break into a wireless network. The objective is to compromise a Wi-Fi network and gain unauthorized access to its resources.

1. Discover potential Wi-Fi networks and choose one to attack
2. Create a map and a database of discovered networks
3. Analyze the traffic on the discovered wireless network and find vulnerabilities
4. Launch an attack
5. Break the security of the network
6. Compromise the network

BREAKING WEP ENCRYPTION

To break the WEP encryption, it is necessary to collect as many IVs as possible. In order to do so, the attacker needs to listen to the network traffic. They can also inject packets to speed up the process.

1. Listen to the traffic
2. Test the AP for packet injection
3. Perform fake authentication with the AP
4. Run a sniffer and collect IVs
5. Inject packets to collect more IVs
6. Run a cracking tool to extract encryption keys from the collected IVs

BREAKING WPA/WPA2 ENCRYPTION

WPA encryption is not as exploitable as WEP, but it can be cracked if the right packets are captured.

WPA PSK Attack	WPA PSK is a technique which exploits the weakness of the password being shared in the 4-way handshake. This means that, when a client tries to connect to an AP, they go through a 4-step process of authentication in which the password is exchanged. If the attacker manages to grab the password during this process, then they can attempt to crack it.
Offline Attack	Offline Attack is a technique in which the attacker captures the authentication handshake and then attempts to crack the WPA keys offline.
De-authentication Attack	De-authentication attack is a technique in which the attacker forces an actively connected client to disconnect from the AP. When the client tries to reconnect, the attacker captures the authentication packet. This packet includes the PMK (Pairwise Master Key) which can be cracked to get the WPA key.
Brute Force WPA Keys Attack	Brute-Force WPA Keys is a technique in which the attacker uses dictionary or cracking tools to break WPA encryption keys. This attack takes a lot of time to break the key.

Social Engineering

Social Engineering

SOCIAL ENGINEERING

Social engineering is a technique which relies on human interaction in order to obtain sensitive information. Attackers use social engineering to extract important information about their targets.

Social Engineering

SOCIAL ENGINEERING TYPES

Human-Based Social Engineering

Human-based social engineering involves interaction with people related to the organization with a goal to extract sensitive and important information about the target organization.

Computer-Based Social Engineering

Computer-based social engineering involves using computers and information systems for collecting sensitive and important information.

Mobile-Based Social Engineering

Mobile-based social engineering involves using malicious mobile apps to collect sensitive and important information.

Social Engineering

HUMAN-BASED SOCIAL ENGINEERING

Impersonation	Impersonation is a technique in which the attacker pretends to be someone else in order to learn the information they need.
Shoulder Surfing	Shoulder surfing is a technique in which the attacker gathers sensitive information such as passwords and codes by looking at the keyboard/keypad as the target types the data in.
Dumpster Diving	Dumpster diving is a technique in which the attacker collects information from the target's trash bins by looking for bills, financial information, sticky notes, and manuals.
Reverse Social Engineering	Reverse social engineering is an attack in which the attacker creates a problem for an employee and then presents themselves as someone who is able to fix the problem.
Piggybacking	Piggybacking is a technique in which the attacker gains access to the target organization's building or secured area by convincing an authorized employee to let them pass.

Social Engineering

COMPUTER-BASED SOCIAL ENGINEERING

Phishing

Phishing is a technique in which the attacker sets up a malicious website and then mails the link of the website to their target.

Spam Mail

Attackers send spam mail and malicious attachments in order to obtain sensitive information from the target or infect the target's machine

Chat Messenger

Attackers use chat messengers to interact with their target and learn personal information which they can later use for the attack on the target's accounts.

Pop-up Windows

Attackers use pop-ups to urge the target into clicking on links to malicious websites or downloading malware.

MOBILE-BASED SOCIAL ENGINEERING

Malicious Apps

Attackers **create and publish malicious apps** to get users to install them and thus infect their phones with malware which is designed to send the victim's credentials to the attackers.

App Repackaging

Attackers **repackage legitimate apps with malware** and upload the repackaged app to a third-party app store.

Fake Security Apps

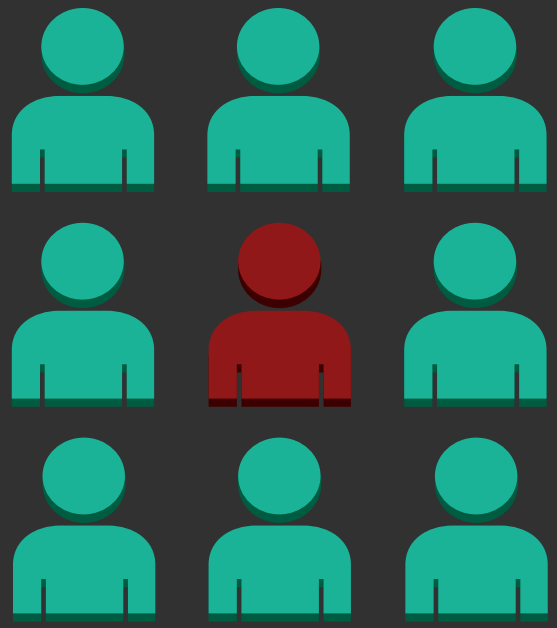
Attacker tricks users into downloading the app that the attacker had created and use that app to securely log on to their bank accounts, thus p**roviding the attacker with the account credentials**.

SMS Phishing

Attackers use SMS phishing to **send malicious links through SMS messages** and urge their targets to take action, which leads to the target giving their personal and sensitive information to the attacker.

INSIDER ATTACKS

Insider attack is an attack in which an authorized person unintentionally or intentionally compromises the security of a system. Insider attacks are usually performed by privileged users, former employees, dissatisfied employees, and uneducated employees who have access to sensitive information.



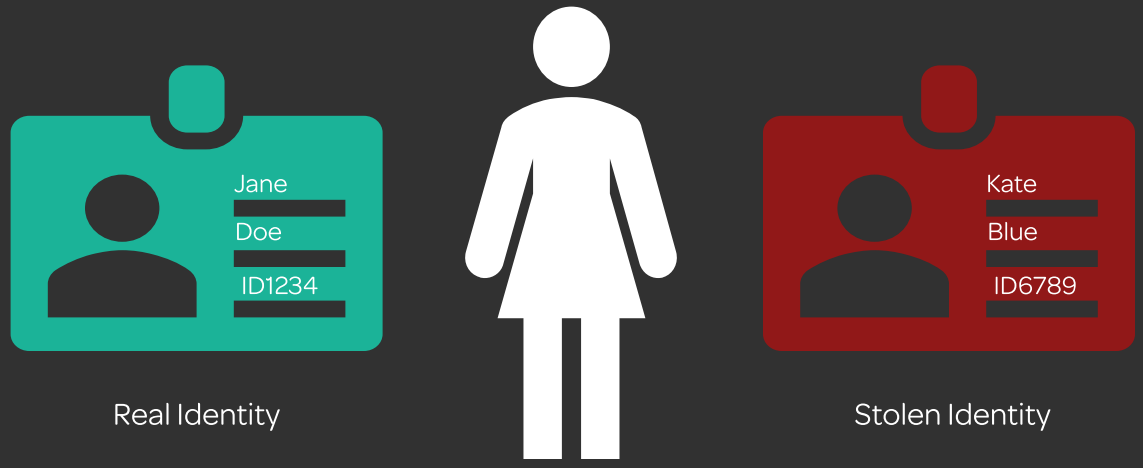
Insiders are categorized into:

- Malicious insiders
- Negligent insiders
- Professional insiders
- Compromised insiders

Social Engineering

IDENTITY THEFT

Identity theft refers to using someone else's identity and posing as that person. This includes stealing someone's personal information to commit some sort of a criminal act.

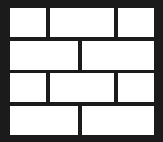


Real Identity

Stolen Identity

Firewalls and Honeypots

INTRUSION DETECTION SYSTEM



FIREWALLS

HONEYPOTS

INTRUSION DETECTION SYSTEM

Intrusion Detection System or IDS refers to software or hardware designed to monitor, detect, and protect networks and systems from attacks by inspecting the incoming and outgoing traffic and looking for suspicious activities and signatures.

Firewalls and Honeypots

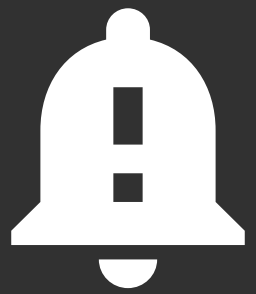
INTRUSION DETECTION METHODS

Signature Recognition

Signature recognition compares incoming and outgoing traffic to the signatures of already known attacks and raises an alarm if an intrusion is detected.

Anomaly Detection

Anomaly detection analyzes the behavioral characteristics of the system's users and components and looks for deviations in the behavior.



Protocol Anomaly Detection

Protocol anomaly detection identifies anomalies specific to a protocol. This method designs models which analyze the different ways in which different vendors deploy the TCP/IP protocol.

Firewalls and Honeypots

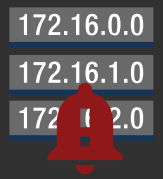
INTRUSION TYPES

Filesystem Intrusion

Signs of a filesystem intrusion:

- New files
- Missing files
- Unfamiliar programs
- Modified file permissions
- Unfamiliar extensions

Network Intrusion



Signs of a network intrusion:

- Attempted logins from remote hosts
- Connections coming from strange locations
- Increase in bandwidth consumption

System Intrusion

Signs of a system intrusion:

- Modified logs
- Missing logs
- Changes in the system performance
- Modified configuration files
- Unfamiliar processes

Firewalls and Honeypots

IDS TYPES

Network-based IDS

Network-based IDS inspects each incoming packet for anomalies. It inspects all incoming traffic and looks for suspicious patterns. It is able to detect DoS attacks, port scans, or break in attempts.

Host-Based IDS

Host-based IDS analyzes behavior and events on a particular host. It is able to detect both anomalies and unauthorized changes in the filesystem.

Firewalls and Honeypots

ALERT TYPES

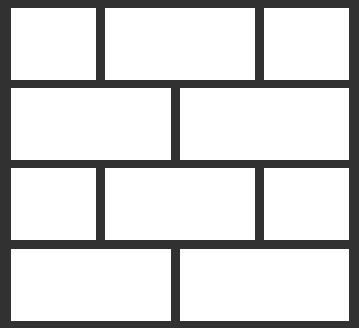
Attack occurred and alert has been raised	True Positive
False Positive	Attack did not occur, but alert has been raised
Attack did not occur and alert has not been raised	True Negative
False Negative	Attack occurred, but alert has not been raised

Firewalls and Honeypots

FIREWALL

Firewall is a program or a device that monitors network traffic and allows or blocks traffic in accordance with the defined set of rules. Firewalls act as filters between a network/system and the Internet. Their purpose is to define a set of rules based on which the incoming and outgoing traffic is filtered. These rules ensure that only allowed incoming and outgoing traffic can pass through the firewall, and everything else is blocked.

Hardware Firewall	Hardware firewall is a device placed on the network's perimeter and uses packet filtering technique to filter the traffic. It can come either as a standalone device or part of a router.
Software Firewall	Software firewall is a program designed to filter traffic on the machine on which it is installed and protect the machine from unauthorized access, trojans, viruses, and worms.

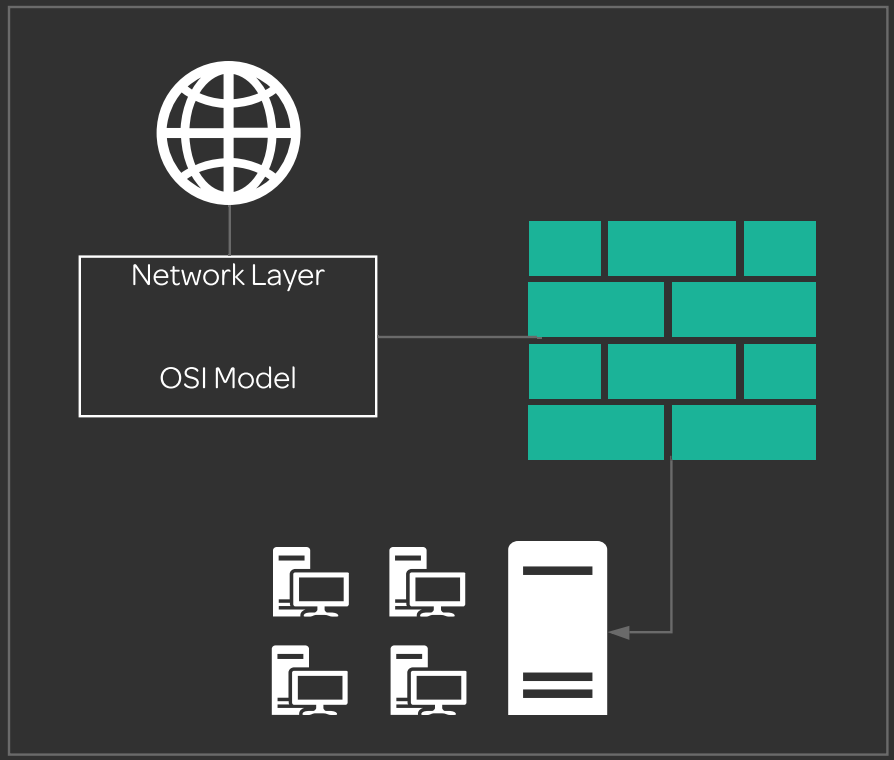


PACKET FILTERING FIREWALL

Packet filtering firewalls are implemented on the Network Layer and designed to analyze each packer individually by applying a set of filters.

This firewall type examines the packet's source, destination, protocol, and destination port number.

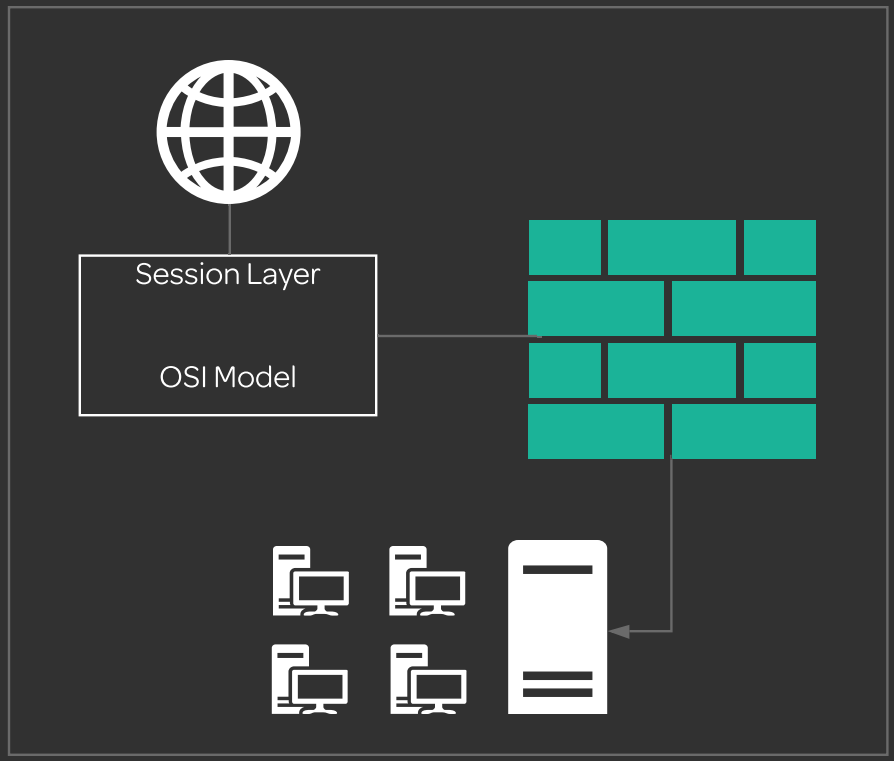
If the packet does not comply with the defined set of rules, then it is dropped and not forwarded to its destination.



CIRCUIT LEVEL GATEWAY FIREWALL

Circuit level gateway firewalls are implemented on the Session Layer.

They are designed to monitor TCP handshakes to determine if the requested connection should be allowed or not.

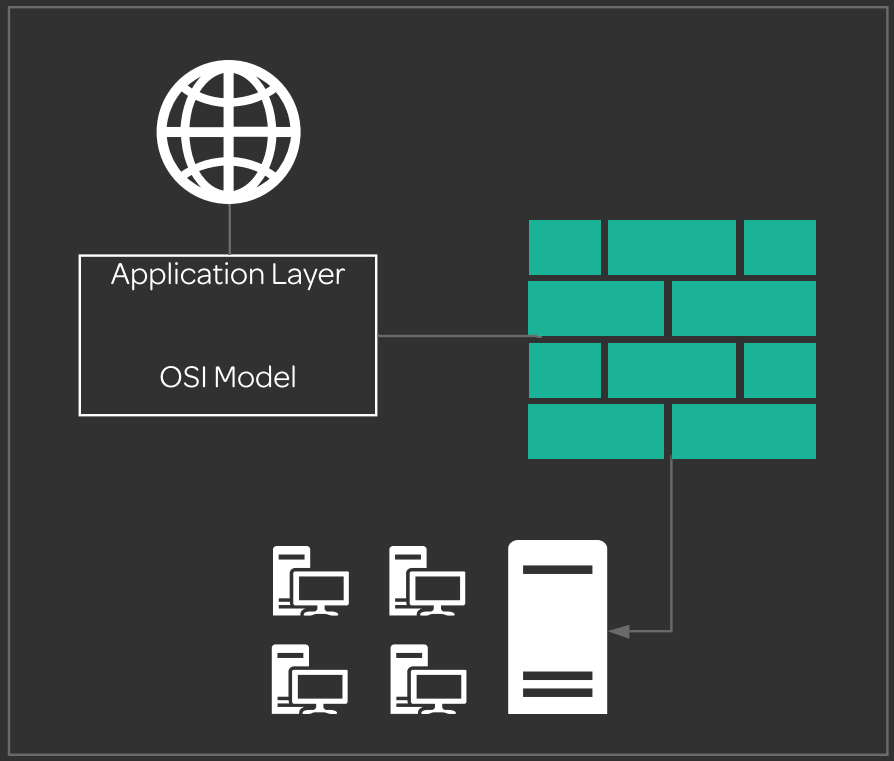


APPLICATION LEVEL FIREWALL

Application level gateway firewalls filter traffic only for the protocols for which they are configured.

They use proxies on one firewall for different applications.

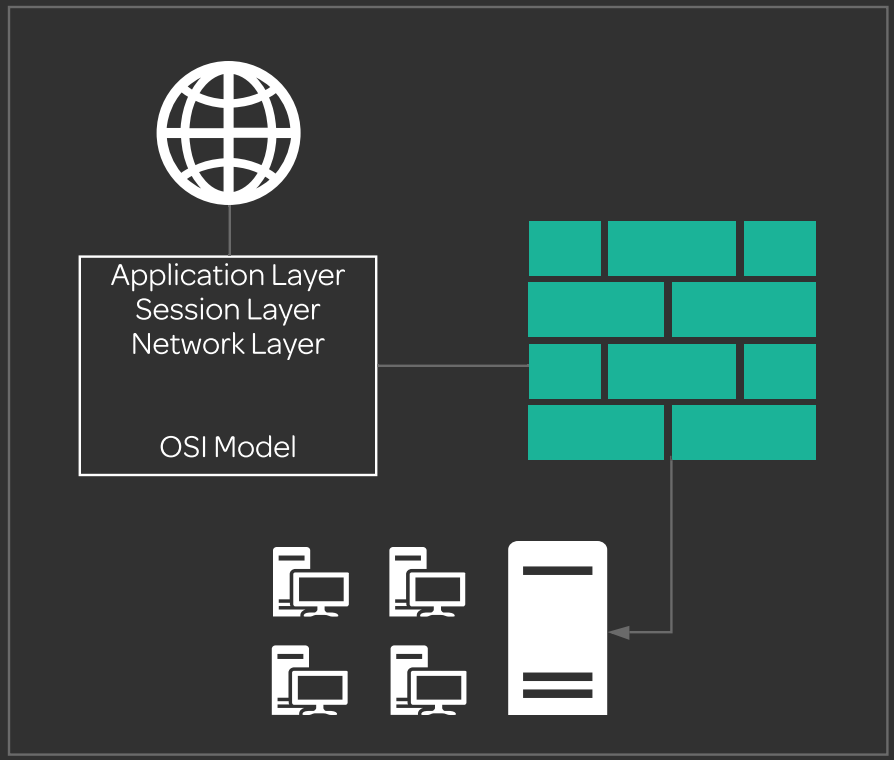
Proxy firewalls force both the client and the server to conduct a session through a proxy server. If the connection to the proxy does not satisfy the defined set of rules, the connection is dropped.



STATEFUL MULTILAYER INSPECTION FIREWALL

Stateful multilayer inspection firewall is a combination of packet filtering, circuit level gateway, and application level firewalls.

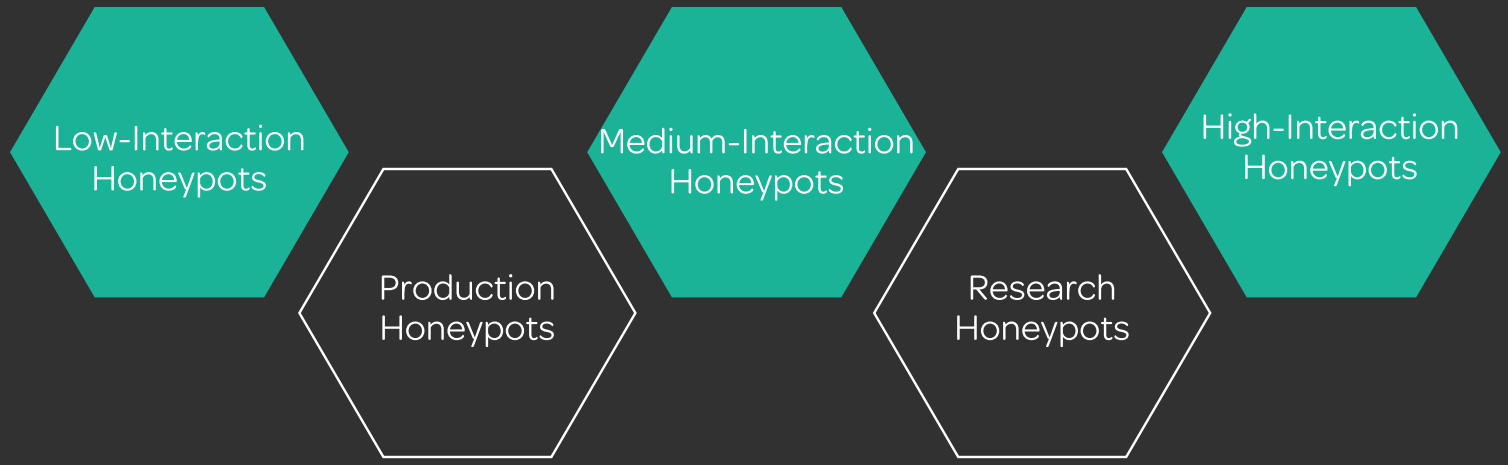
This firewall filters packets on the Network Layer, verifies legitimate sessions on the Session Layer, and evaluates the packets on the Application Layer.



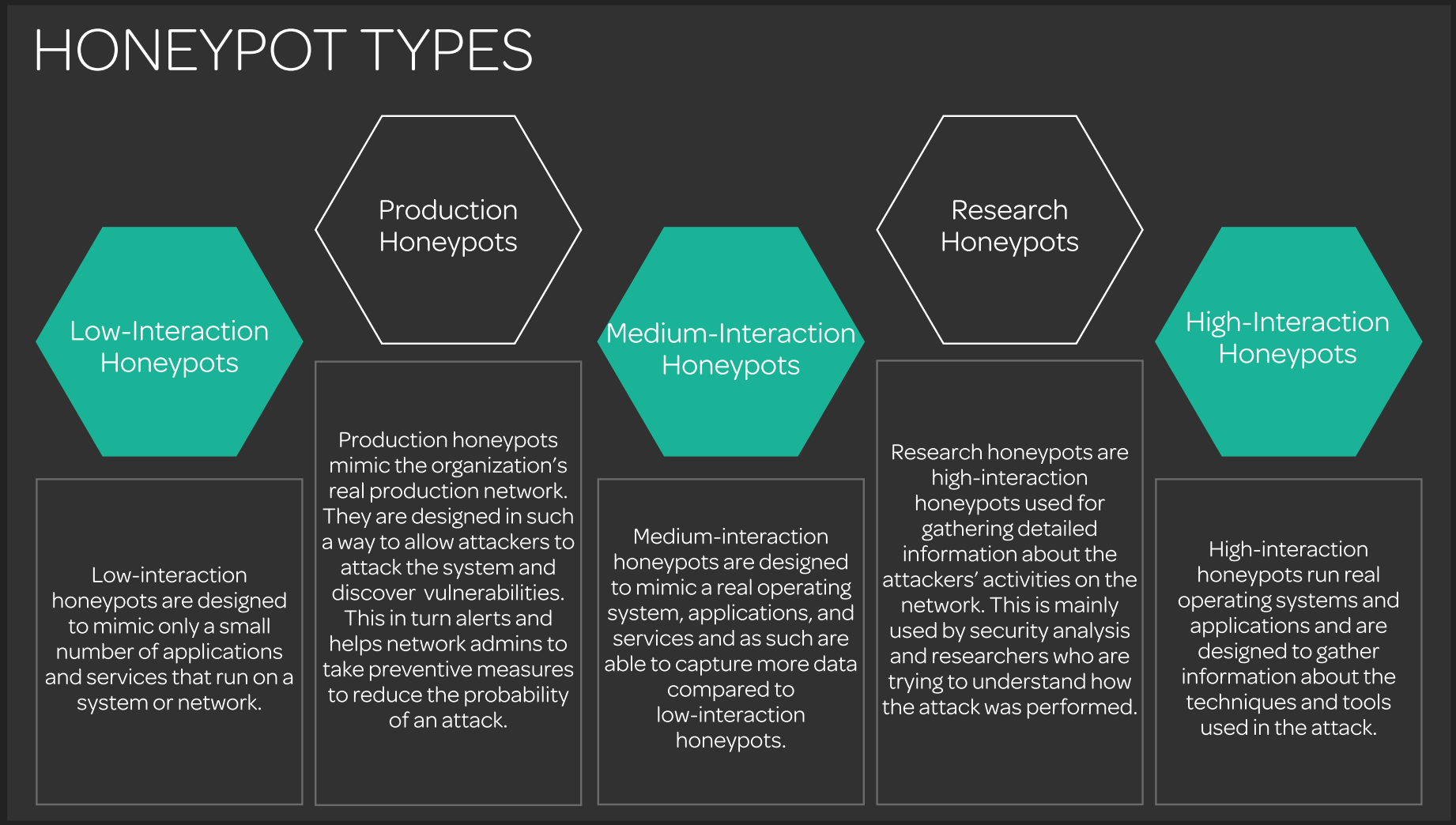
Firewalls and Honeypots

HONEYPOT

Honeypot is designed as a trap for attackers who try to access the network. It is set up in such a way that any traffic to it is considered to be a probe or an attack. So, any interaction with a honeypot points to a malicious activity.

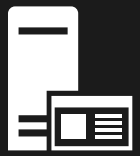


Firewalls and Honeypots



Hacking Web Servers and Web Applications

HACKING WEB SERVERS



HACKING WEB APPLICATIONS

DENIAL OF SERVICE

SESSION HIJACKING

SQL INJECTION

WEB SERVER

Web server is a system used for storing, processing, and delivering websites. It is designed to host web applications, allowing clients to access those applications. It implements client-server model architecture, in which it has the server role, and the browser has the client role.

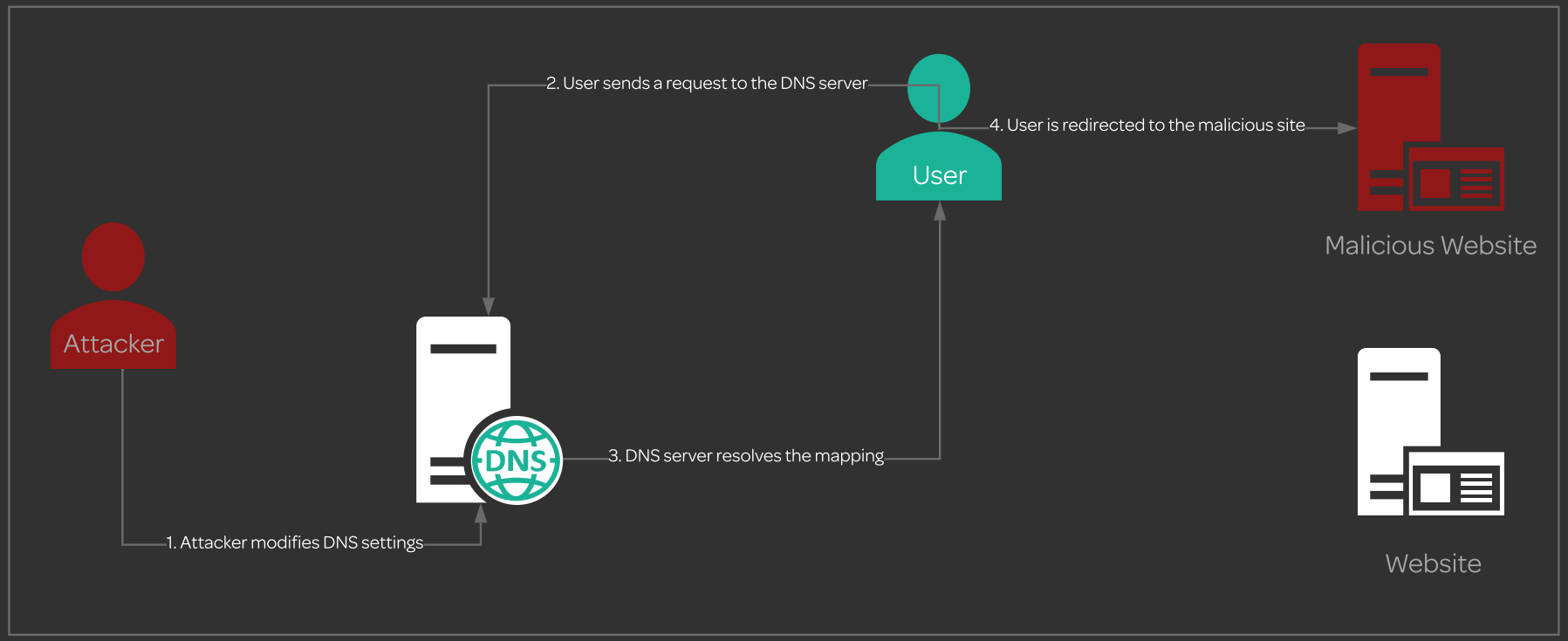
It consists of:

- Document root is a folder which stores HTML files of a website
- Server root is a folder which stores configuration, log, and executable files
- Virtual document tree is a type of storage located on a different disk and used when the original disk becomes full
- Virtual hosting is hosting more than one domain on a single server
- Web Proxy is a server placed between the client and server, which means that all requests coming from the client go through the proxy to the server, instead of directly going to the server

Hacking Web Servers and Web Applications

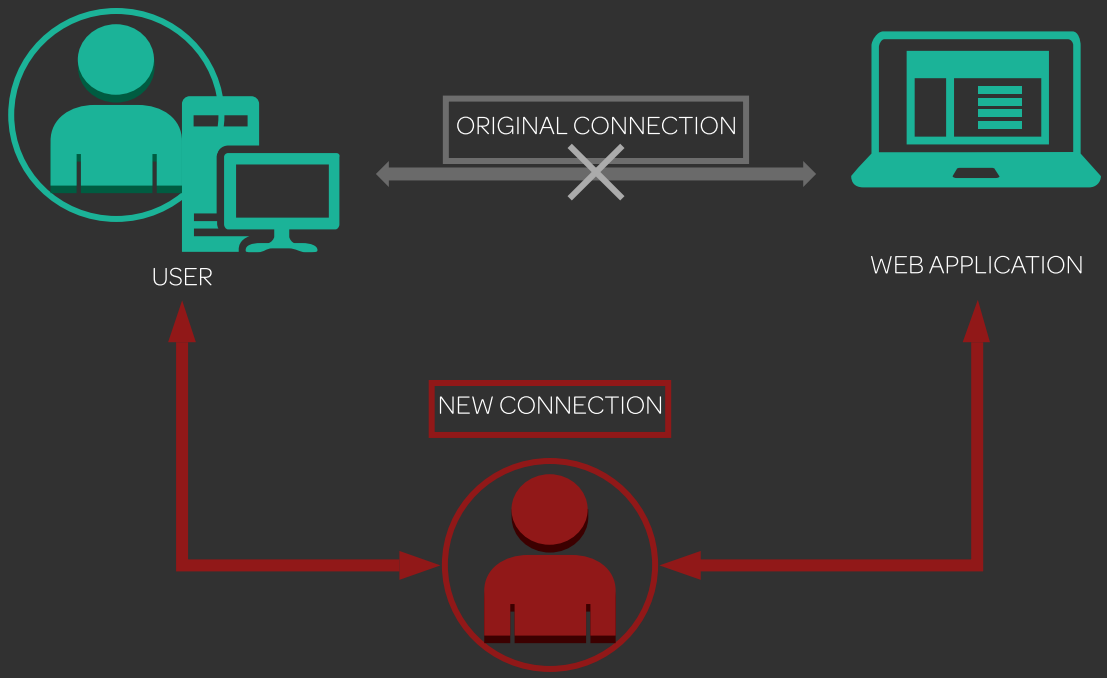
DNS SERVER HIJACKING

DNS server hijacking attack is an attack in which the attacker targets a DNS server and tempers with its mapping settings making it redirect clients to the attacker's rogue server which serves the attacker's malicious website.



MAN-IN-THE-MIDDLE ATTACK

Man-in-the-middle attack is an attack in which the attacker intercepts the traffic that is going from the client to the server and back. They do so by tricking the client into thinking that the attacker is a proxy. Once the client accepts the connection from the attacker, the entire communication between the client and the server goes through the attacker, allowing them to steal information.

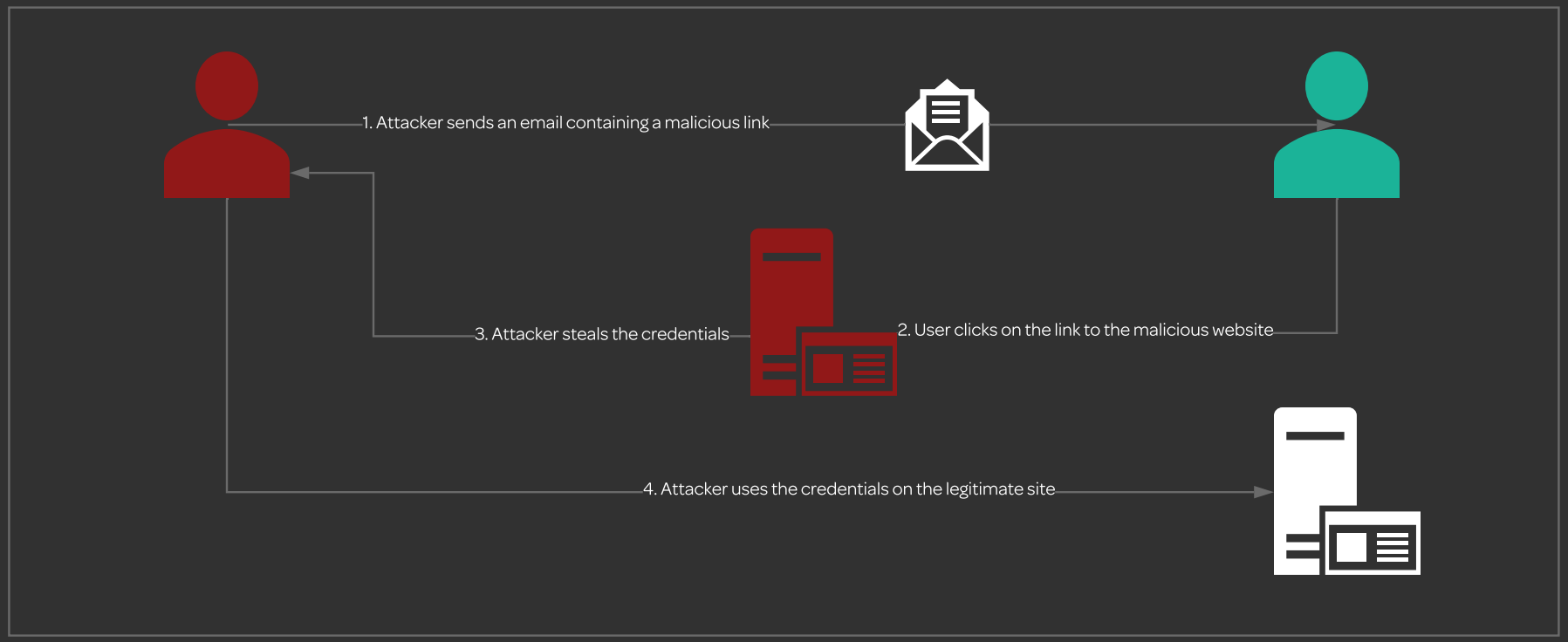


MAN IN THE MIDDLE

Hacking Web Servers and Web Applications

PHISHING ATTACK

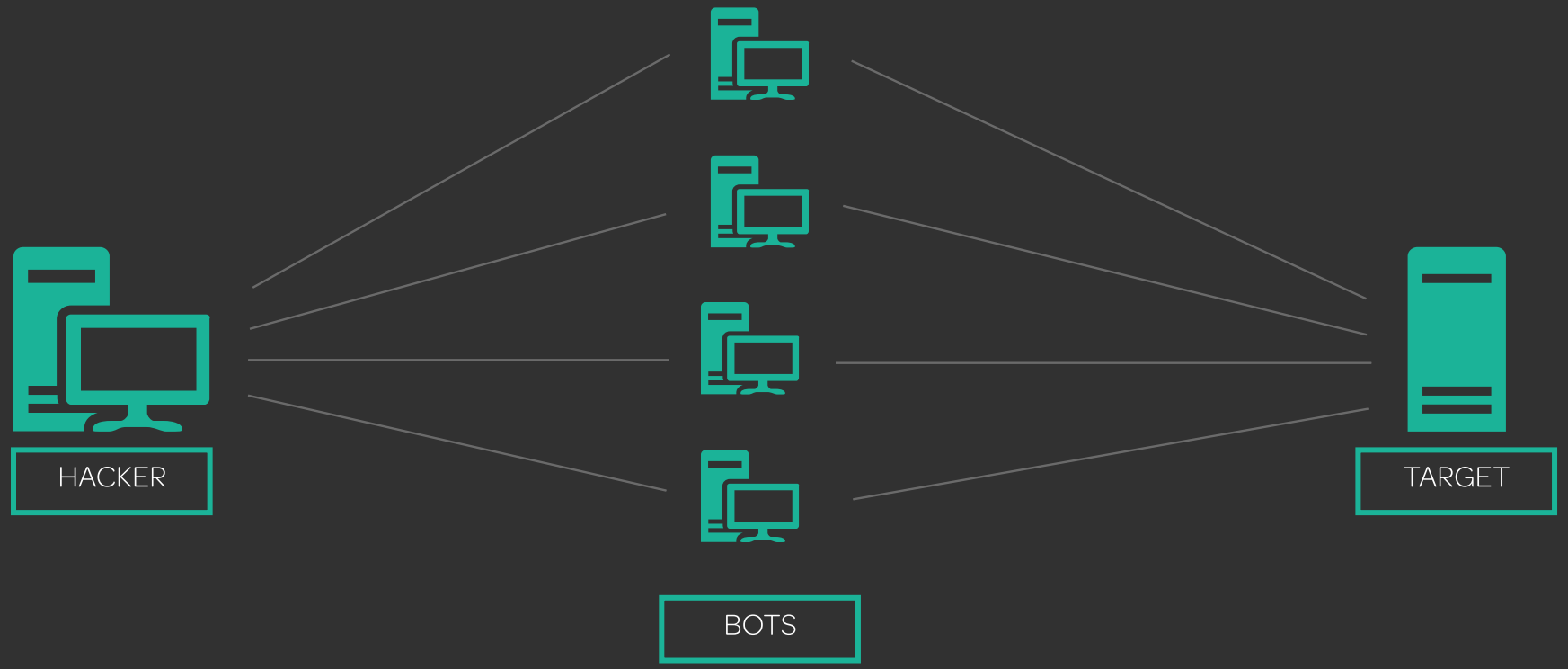
Phishing attack is an attack in which the attacker emails the target with malicious links. Once the target clicks on the link, they are redirected to a malicious website which prompts them to provide sensitive information. The attacker then steals this information.



Hacking Web Servers and Web Applications

DoS ATTACK

DoS/DDoS attack is an attack in which the attacker sends a large number of requests to the target web server to prevent the server from functioning properly.



WEB SERVER HACKING METHODOLOGY

Web Server Hacking Methodology provides attackers with steps to follow to execute a successful attack.

1. Gather information about the target web server
2. Learn about the server's remote access capabilities, ports, and services
3. Mirror the target website to browse it offline
4. Discover vulnerabilities
5. Perform session hijacking and password cracking attacks

WEB APPLICATION

Web applications are programs that allow users to interact with web servers.
They are run on web browsers with the help of client- and server-side scripts.

The web application architecture consists of:

- Client/Presentation layer
- Business logic layer
- Database layer

The client/presentation layer consists of devices on which the application runs.
Such devices include laptops, tablets, smartphones, etc.
The business logic layer has two layers:

- Web-server logic layer consists of components that handle requests and responses, and the coding that reads and returns data to the browser
- Business logic layer contains the application data

The database layer consists of a B2B layer and a database server in which the organization's data is stored.

Hacking Web Servers and Web Applications

VULNERABILITY STACK

Vulnerability stack is comprised of seven layers with each layer describing an element or service of a web application. This vulnerability stack is used to assess the vulnerabilities of the application by looking at its layers. Attacker also use the vulnerability stack to find vulnerabilities, exploit them, and launch attacks on the web application.

WEB APPLICATION	7	Technical vulnerabilities
THIRD PARTY APPLICATION	6	Open Source / Commercial
WEB SERVER	5	Apache / IIS
DATABASE	4	MySQL / Oracle
OS	3	Linux / Windows / OS X
NETWORK	2	Router / Switch
SECURITY	1	IDS

OWASP TOP 10

OWASP is an open community dedicated to enabling organizations to conceive, develop, acquire, operate, and maintain applications that can be trusted.

OWASP Top 10 project produces a document that describes top 10 application security threats. The latest document lists the following top 10 security threats[1]:

- Injection
- Broken authentication
- Sensitive data exposure
- XML External Entity
- Broken Access Control
- Security Misconfiguration
- Cross-Site Scripting (XSS)
- Insecure Deserialization
- Using components with known vulnerabilities
- Insufficient logging and monitoring

[1] www.owasp.org

WEB APPLICATION HACKING METHODOLOGY

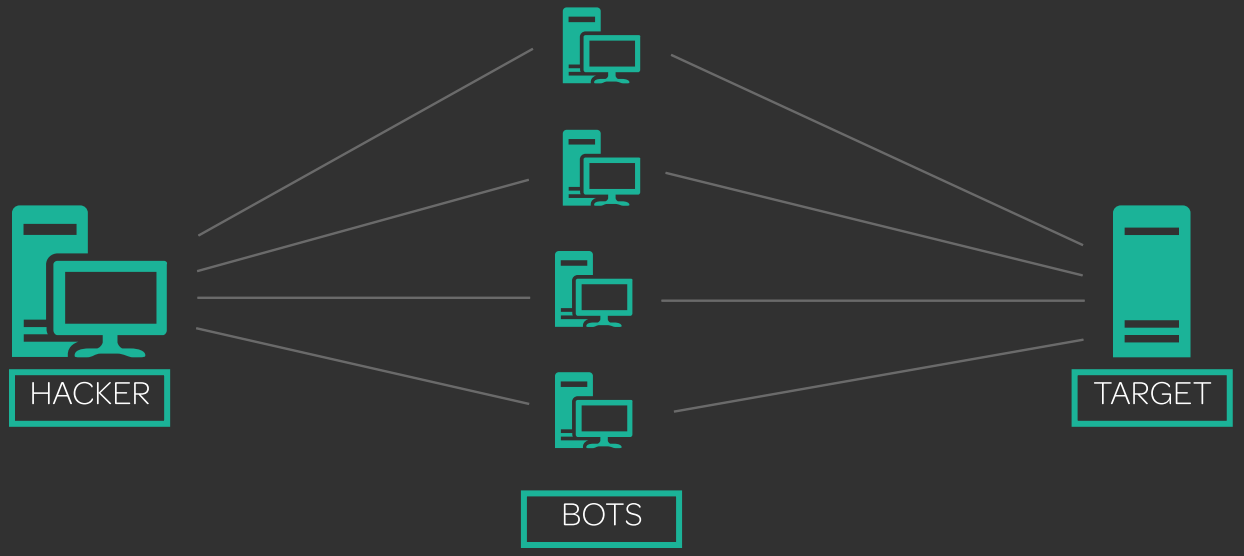
Web Application Hacking Methodology provides attackers with steps to follow to execute a successful attack.

1. Gather information about the target web infrastructure
2. Perform analysis of the gathered information about the application
3. Exploit the application vulnerabilities and execute different attacks
4. Attack the database connection
5. Attack web services

DENIAL OF SERVICE

Denial of Service or DoS attack is an attack in which the attacker overloads the target system with fake requests or traffic resulting in the server being unable to function properly. The objective of a DoS attack is to render the target system useless and prevent users from accessing its resources.

Distributed Denial of Service or DDoS attack is an attack in which the attacker uses botnets to perform a DoS attack. The objective is to first compromise as many systems as possible and then use those systems to launch a DoS attack on their target.



Hacking Web Servers and Web Applications

ATTACK VECTORS

Volumetric Attacks

Volumetric attack is an attack in which the attacker attempts to use up the target network or service's bandwidth, which results in the users being deprived of the said resources.

Techniques used in this attack:

- UDP flood attack
- ICMP flood attack
- Ping of death attack
- Malformed IP packet flood attack
- Spoofed IP packet flood attack

Protocol Attacks

Protocol attack is an attack in which the attacker attempts to consume the resources of a particular target device. This attack targets connection state tables and overloads them in such a way that new connections cannot be made.

Techniques used in this attack:

- SYN flood attack
- ACK flood attack
- TCP connection flood attack
- TCP state exhaustion flood attack
- Fragmentation attack
- RST attack

Application Layer Attacks

Application layer attack is an attack in which the attacker targets the vulnerabilities in the application and attempts to exhaust the application resources with a huge number of open connections so that new connection cannot be made.

Techniques used in this attack:

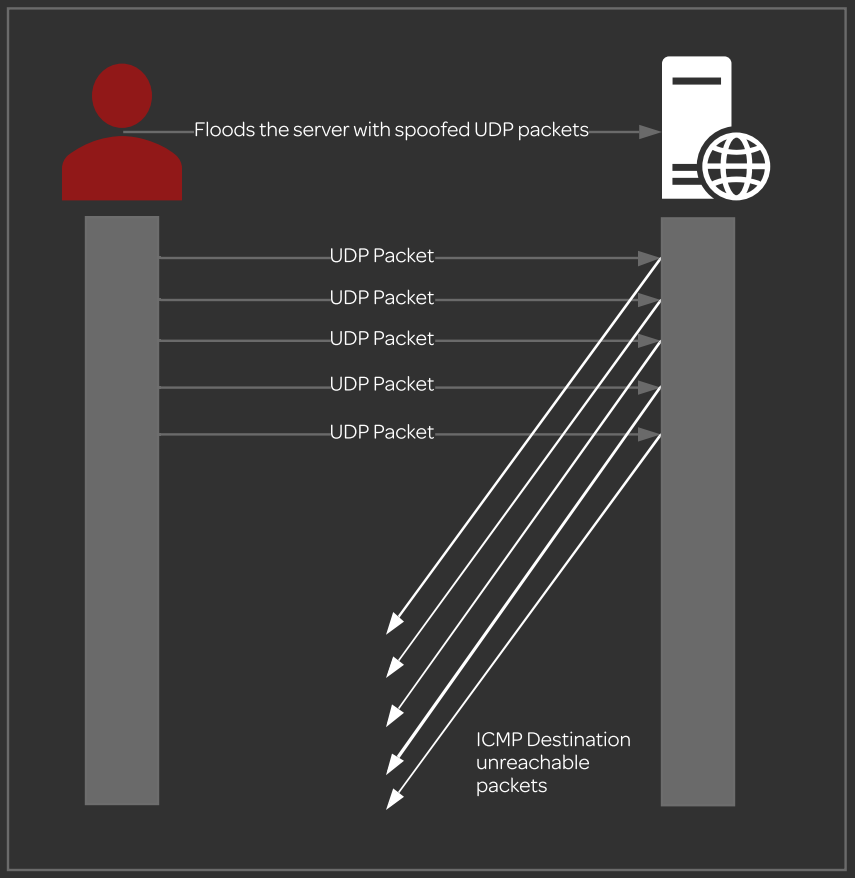
- HTTP flood attack
- Slowloris attack

UDP FLOOD ATTACK

UDP flood attack is an attack in which the attacker floods random ports of the target server with a huge number of spoofed UDP packets causing the server to continuously check for applications on the ports.

Being unable to find any application associated with the packet, the system responds with an ICMP Destination Unreachable packet.

With so many spoofed packets received and answered, the system eventually becomes unable to respond to legitimate applications.



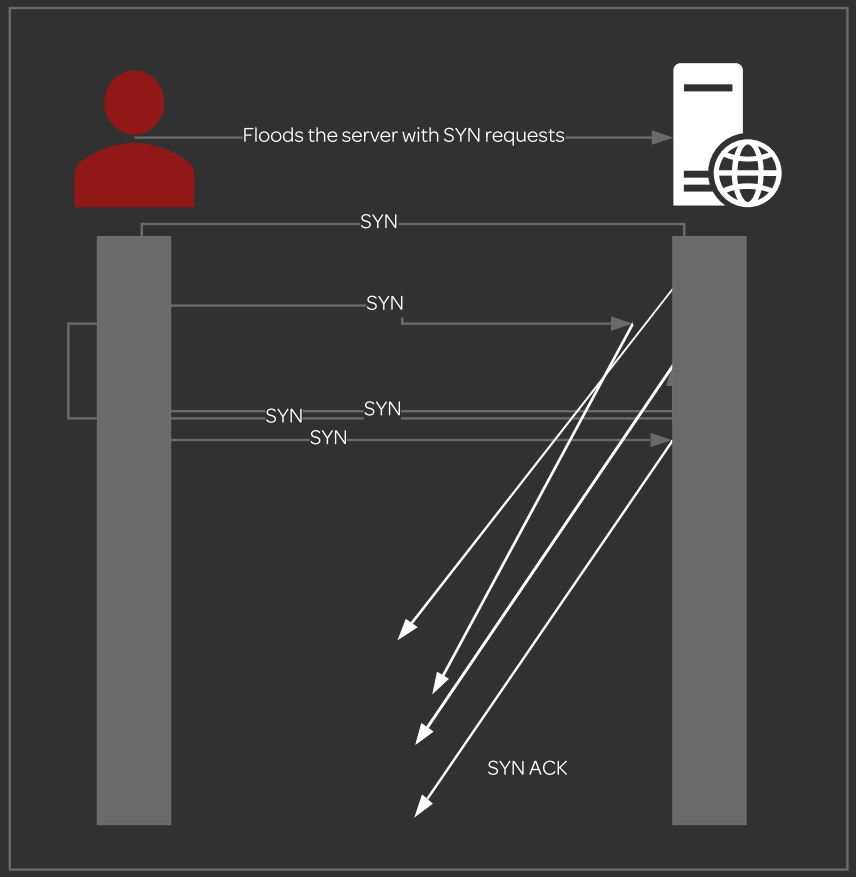
SYN FLOOD ATTACK

SYN flood attack is an attack in which the attacker takes advantage of the flaw that exists in the TCP three-way handshake.

In this attack, the attacker sends a huge number of SYN requests with fake source IPs. The target responds with a SYN ACK packet and waits for the sender to send back an ACK packet.

However, because the source IP is fake, the target never receives the expected ACK packet, leaving the connection to remain incomplete.

With so many incomplete connections, the system eventually becomes unable to respond to legitimate requests.



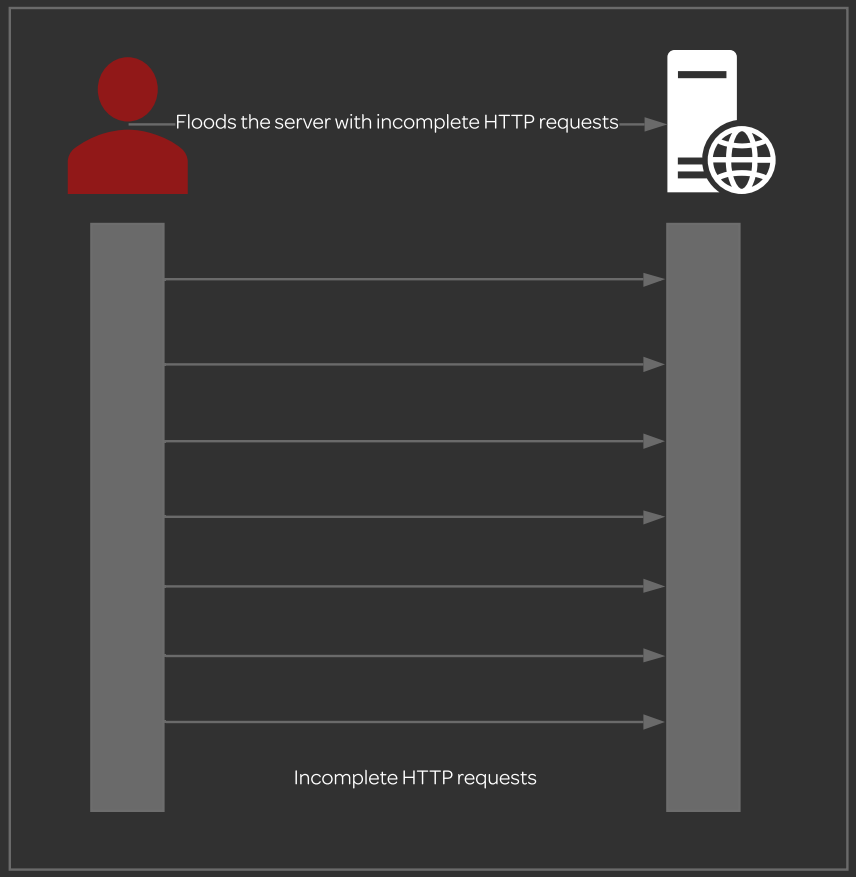
Hacking Web Servers and Web Applications

SLOWLORIS ATTACK

Slowloris is an attack tool used by attackers to take down web infrastructures. In this attack, the attacker sends a huge number of incomplete HTTP requests to the target server.

The server receives the requests, opens a connection for each received request, and waits for the received requests to complete.

Since the requests never complete and with so many open connections, the server eventually becomes unable to receive new connections.



Hacking Web Servers and Web Applications

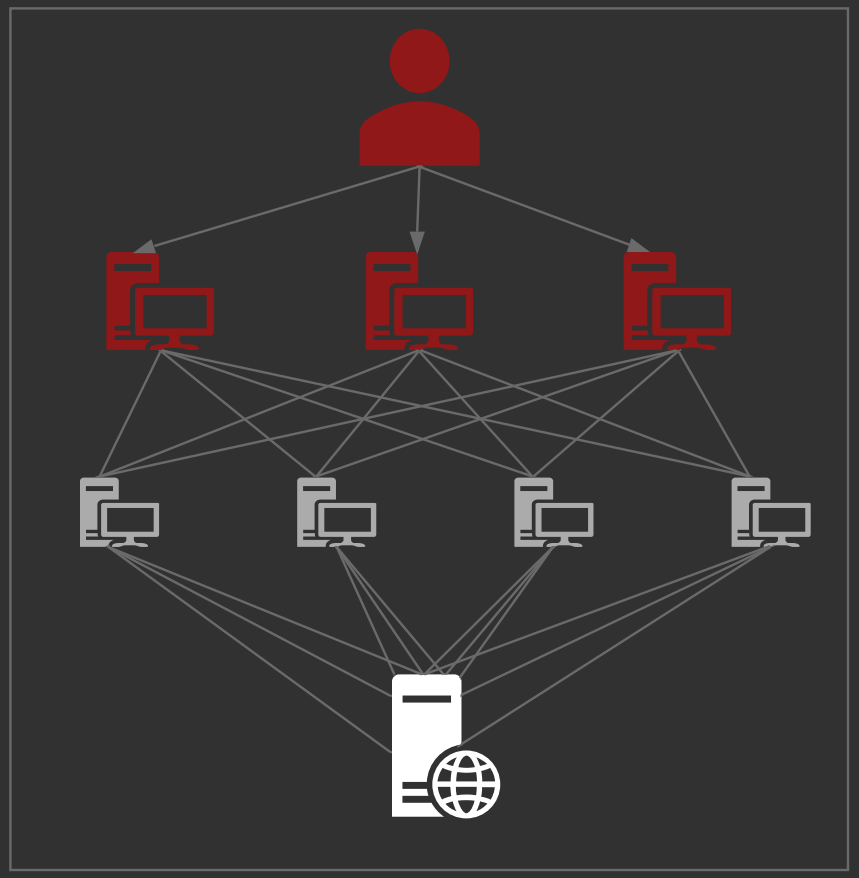
DRDOS ATTACK

Distributed reflection DoS attack is an attack in which the attacker uses two sets of machines to carry out an attack.

One set consists of zombies called intermediary machines, and the other set consists of uncompromised machines called secondary machines.

The attacker instructs the intermediary machines to send a number of packets to secondary machines. The packets sent contain the target's IP address as the source address. Once the secondary machines receive the requests, they respond and try to connect to the target.

With a huge number of secondary machines sending so many requests repeatedly (because they are being discarded by the target), the target eventually becomes overwhelmed and unable to function properly.



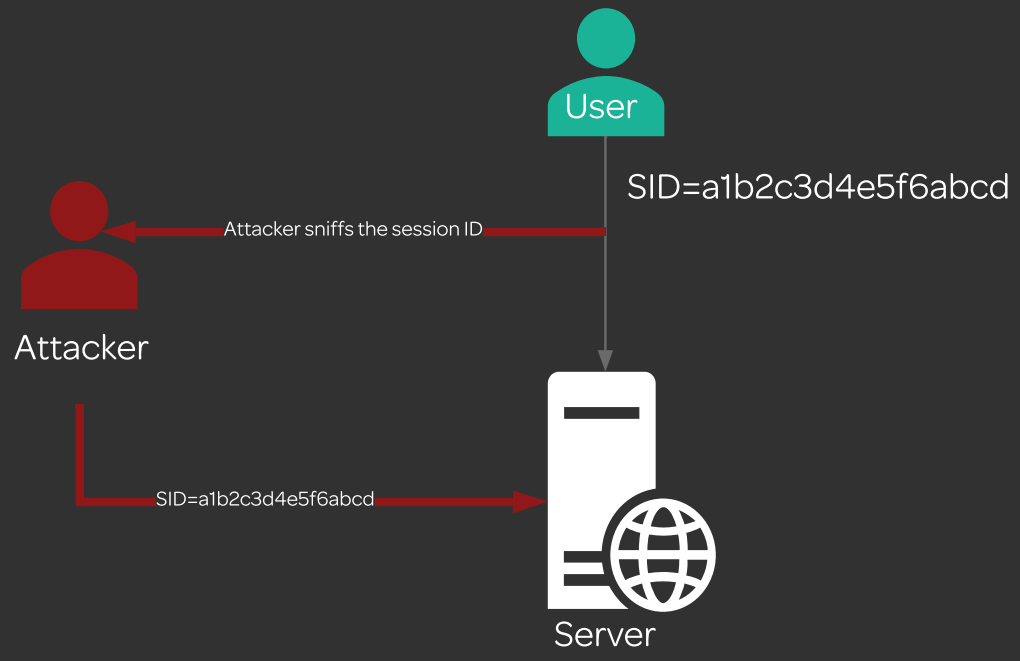
SESSION HIJACKING

Session hijacking is an attack in which the attacker targets a session between two machines in order to gain access to the target machine.

Passive Session Hijacking	Passive session hijacking refers to observing the traffic on the network and not interfering with the communication.	Network Level Session Hijacking	Application level session hijacking is an attack in which the attacker targets a legitimate session and attempts to either predict or steal the session ID and thus gain access to the server.
Active Session Hijacking	Active session hijacking refers to the attacker interfering with the session and becoming a participant in the communication with the target server.	Application Level Session Hijacking	Network level session hijacking is an attack in which the attacker intercepts the packets transmitted between the client and the server.

SESSION SNIFFING

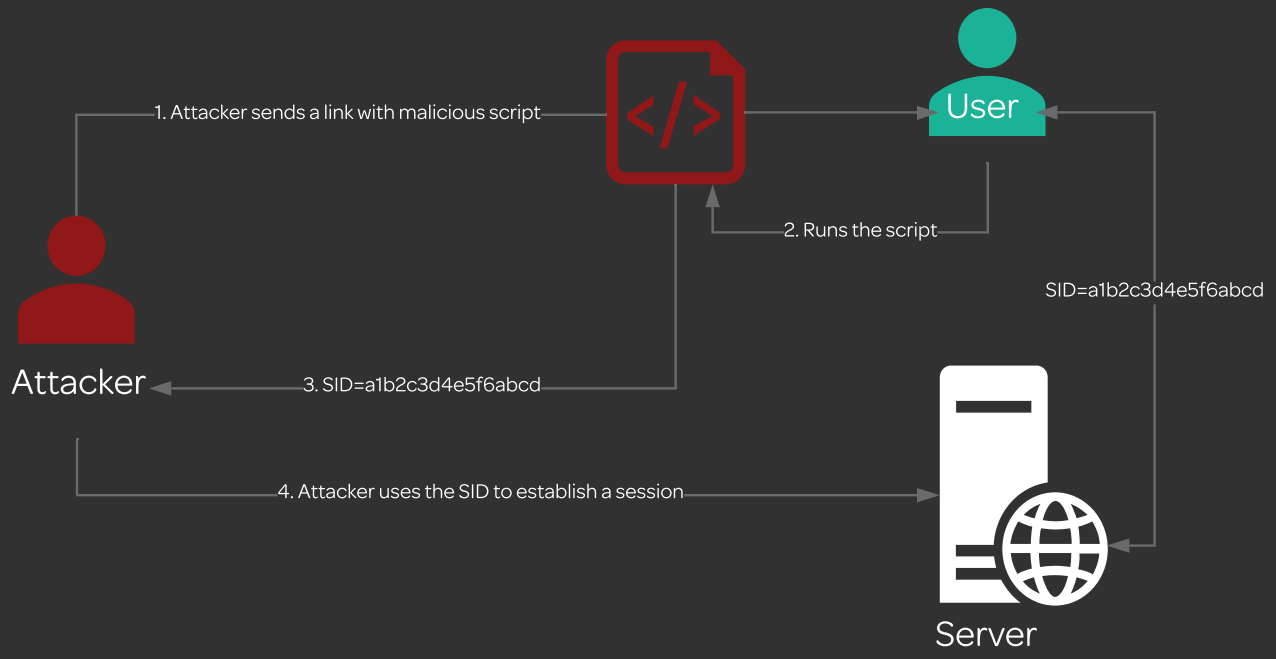
Session sniffing attack is an attack in which the attacker uses sniffers to capture packets and then analyzes them to determine the session token. Once the attacker acquires the session token, they are able to gain access to the server.



Hacking Web Servers and Web Applications

CROSS-SITE SCRIPTING ATTACK

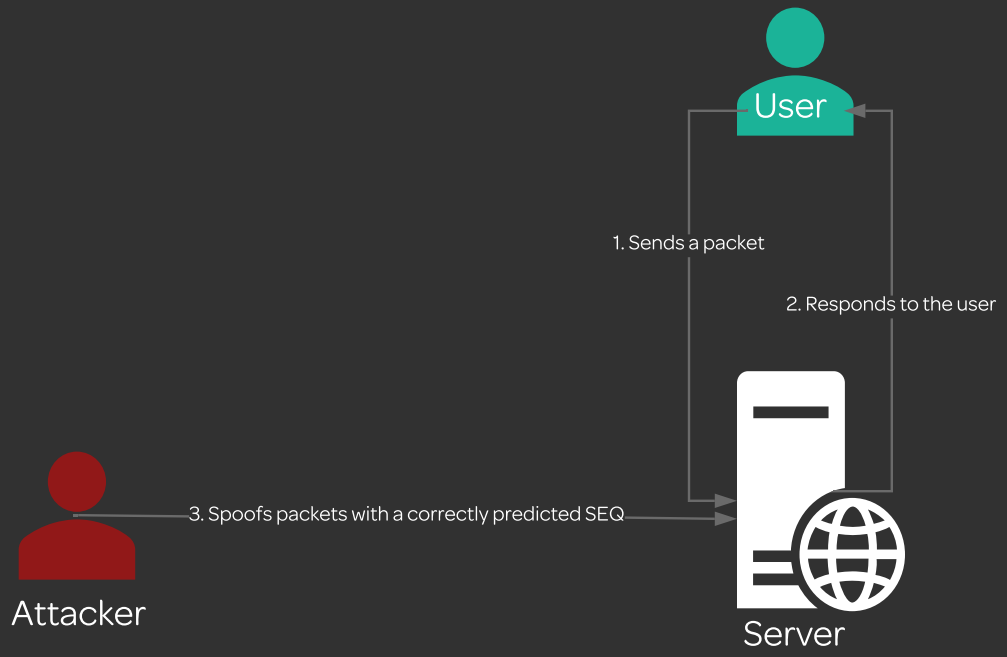
Cross-Site Scripting or XSS attack is an attack in which the attacker injects scripts into web pages which are executed on the target's system. Attackers use this attack to obtain the target's session ID.



Hacking Web Servers and Web Applications

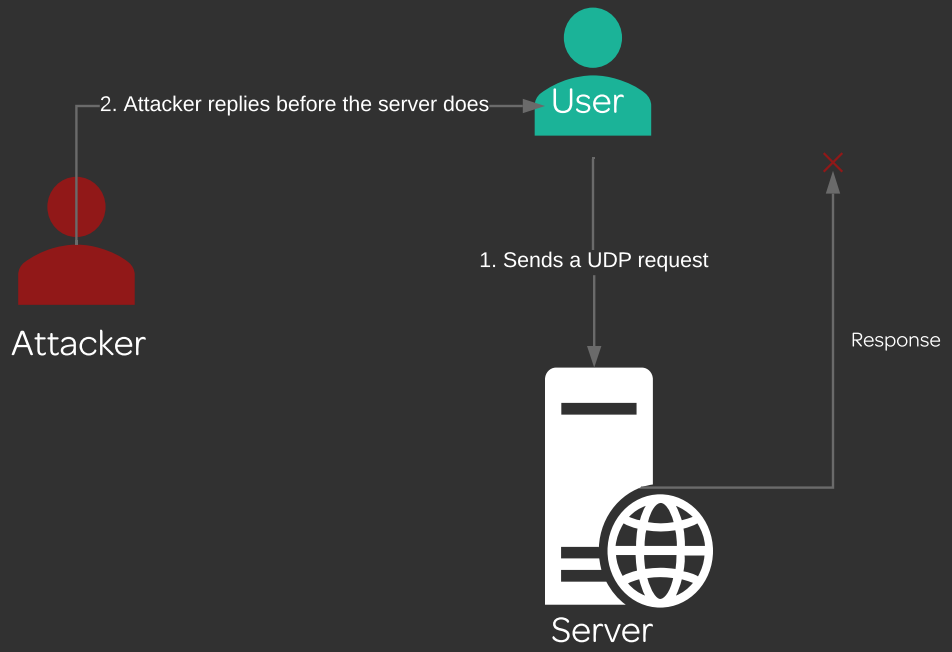
TCP/IP HIJACKING

TCP/IP hijacking is an attack in which the attacker uses spoofed packets to hijacks the target connection and then redirects the traffic to their computer. When this happens, the server continues the communication with the attacker, believing them to be a valid client.



UDP HIJACKING

UDP hijacking is an attack in which the attacker hijacks a UDP session, creates and sends a forged reply to the client making it look like it came from the server. This prevents the client to proceed its communication with the server.



SQL INJECTION

SQL Injection is an attack in which the attacker injects malicious SQL queries into the application. In this attack, the attacker targets vulnerable applications and attempts to either gain unauthorized access or retrieve data stored in the database.

Attackers use SQL injection to:

- Log onto the system without providing valid credentials
- Retrieve sensitive information stored in the database
- Modify the information stored in the database
- Delete the information stored in the database

SQL INJECTION METHODOLOGY

SQL Injection Methodology defines steps to be followed for a successful injection attack.

Information Gathering	SQL Injection	Advanced SQL Inection
		
Information gathering refers to the attacker collecting information about the target application and database including its structure, name, version, type, etc. The objective here is to identify vulnerabilities for SQL injection.	Proceed with the execution of different SQL injection attacks to extract information from the database including the database name, column names, and records.	The attacker uses advanced SQL injection attacks to compromise the target network and OS in two ways: • Reading/writing system files from the disk • Executing commands using a remote shell

SQL INJECTION TYPES

In-Band SQL Injection	In-band SQL injection is an injection attack in which the attacker uses one channel to inject malicious queries and retrieve results.
Blind SQL Injection	Blind SQL injection is an injection attack in which the attacker is unable to see the results of the injected queries, so they form queries to return true or false and based on that determine whether the application is vulnerable to SQL injection.
Out-of-Band SQL Injection	Out-of-band SQL injection is an injection attack in which the attacker uses more channels to inject malicious queries and retrieve results.

Cryptography

Cryptography

CRYPTOGRAPHY

Cryptography refers to the process of hiding information by converting the readable text into unreadable text using some sort of a key or encryption algorithm. Information protected using cryptography includes emails, files, and other sensitive data.

The objective of cryptography is to ensure the encrypted information retains its:

- confidentiality
- integrity
- authentication
- non-repudiation

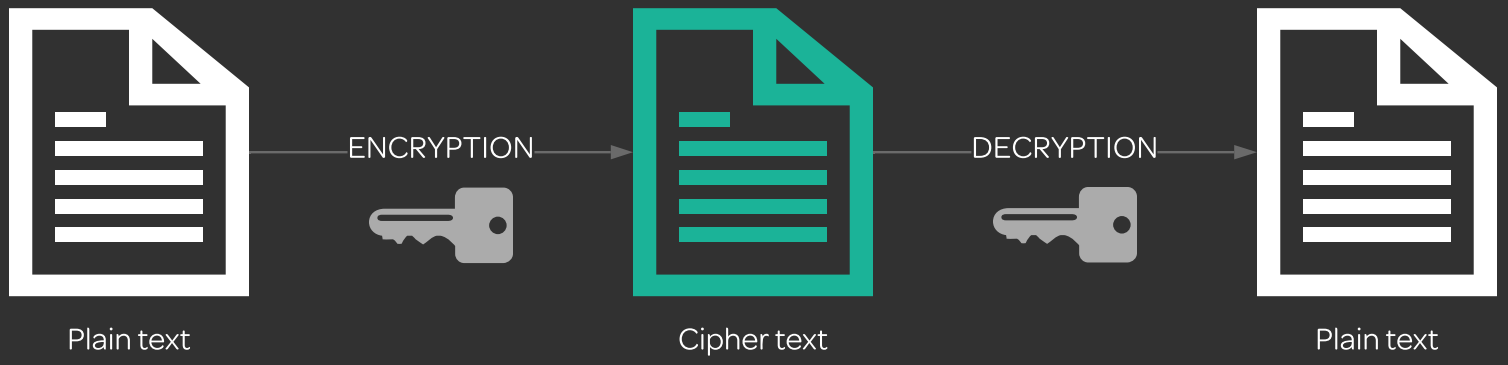
Cryptography

CRYPTOGRAPHY PROCESS

Cryptography

ENCRYPTION TYPES

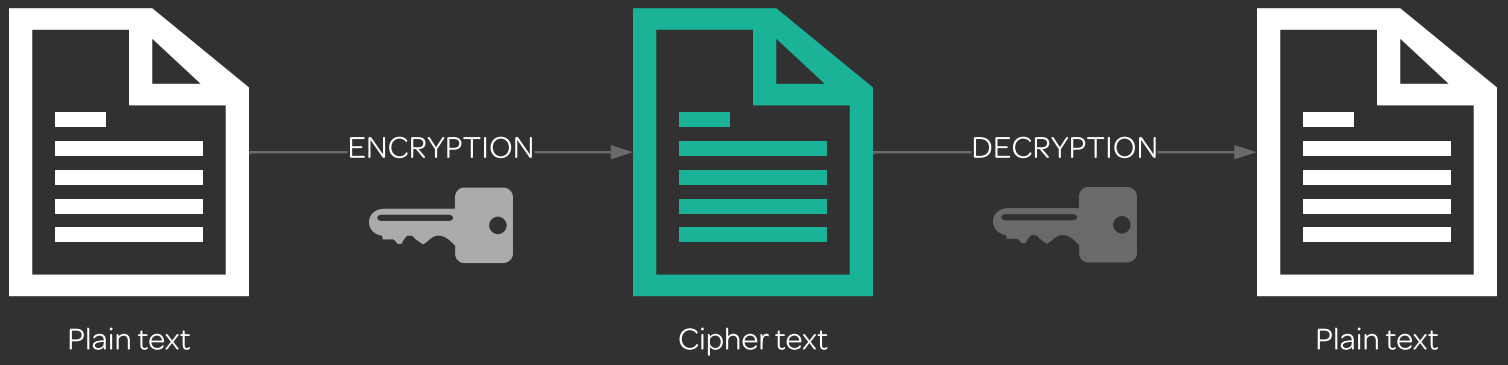
Symmetric encryption uses one key to encrypt and decrypt the information that is sent/received.



Cryptography

ENCRYPTION TYPES

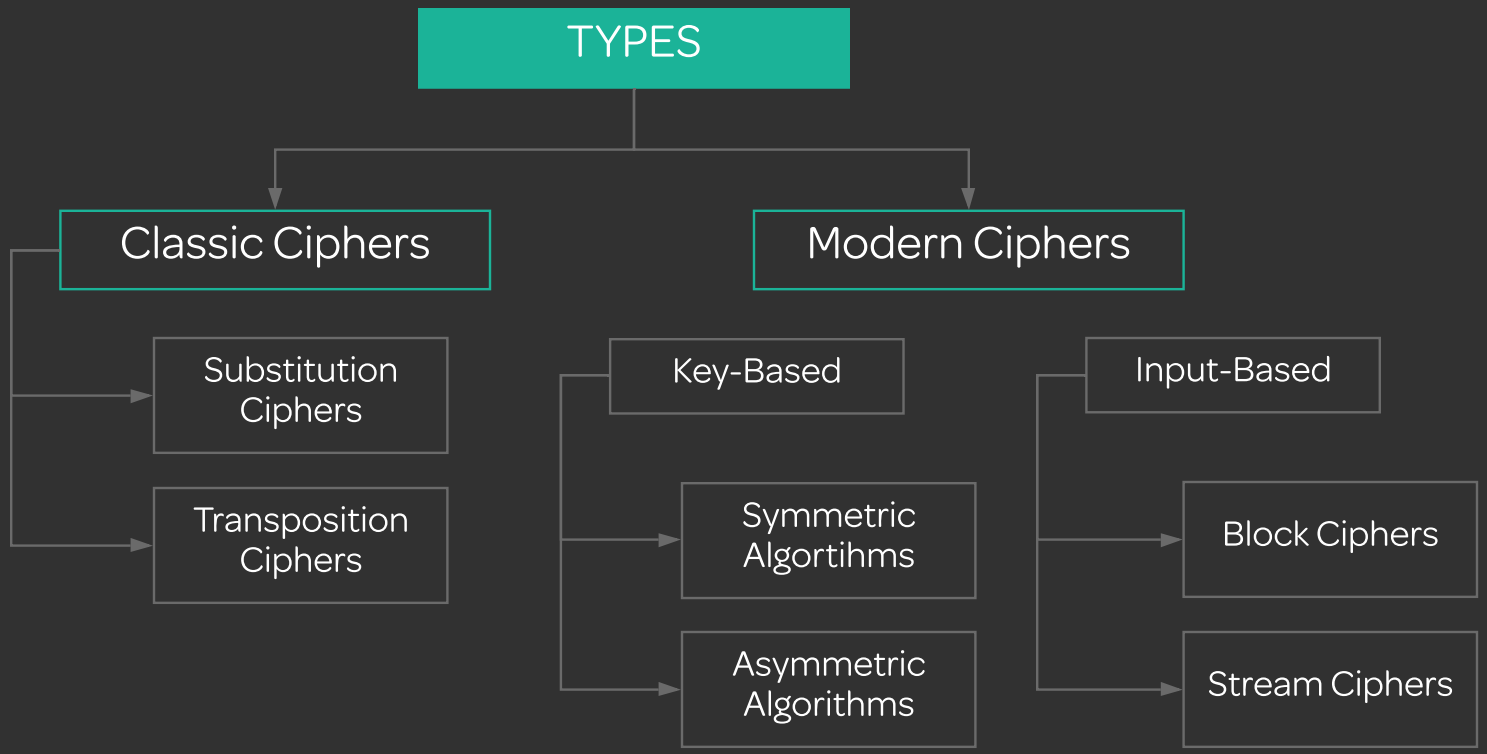
Asymmetric encryption uses two keys to encrypt and decrypt the information that is sent/received.



Cryptography

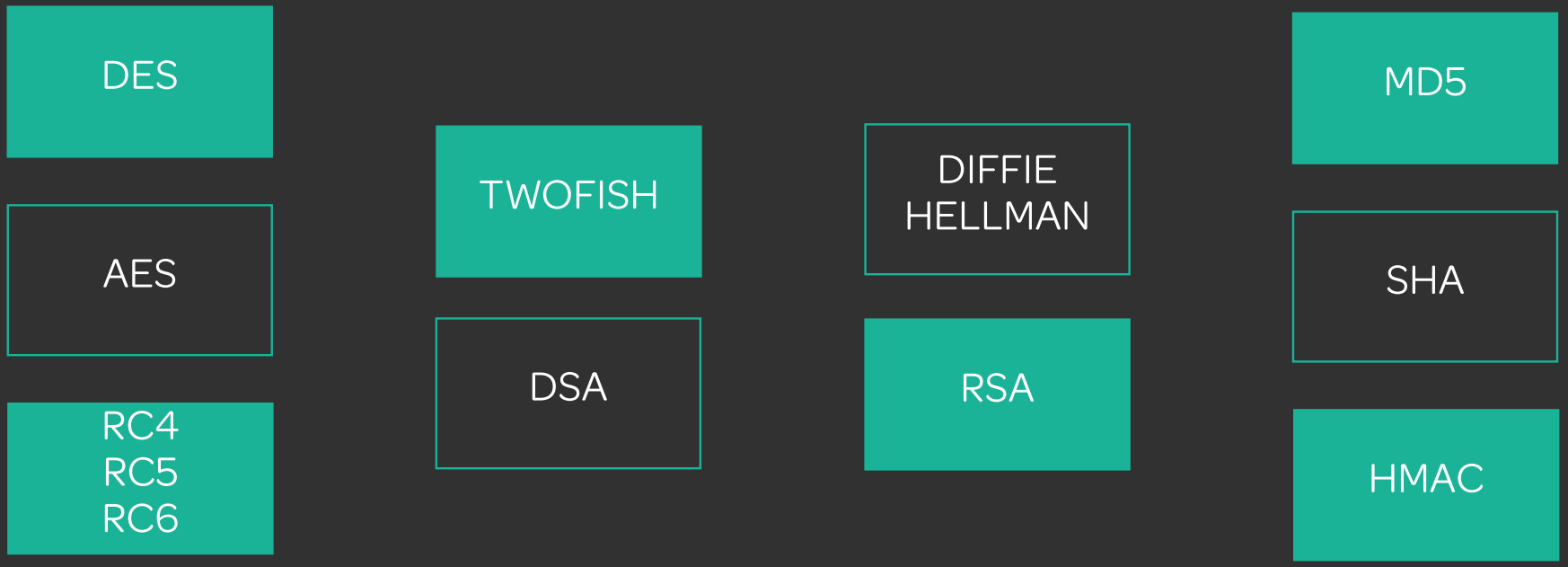
CIPHERS

Cipher refers to an algorithm which is used for encryption and decryption.



Cryptography

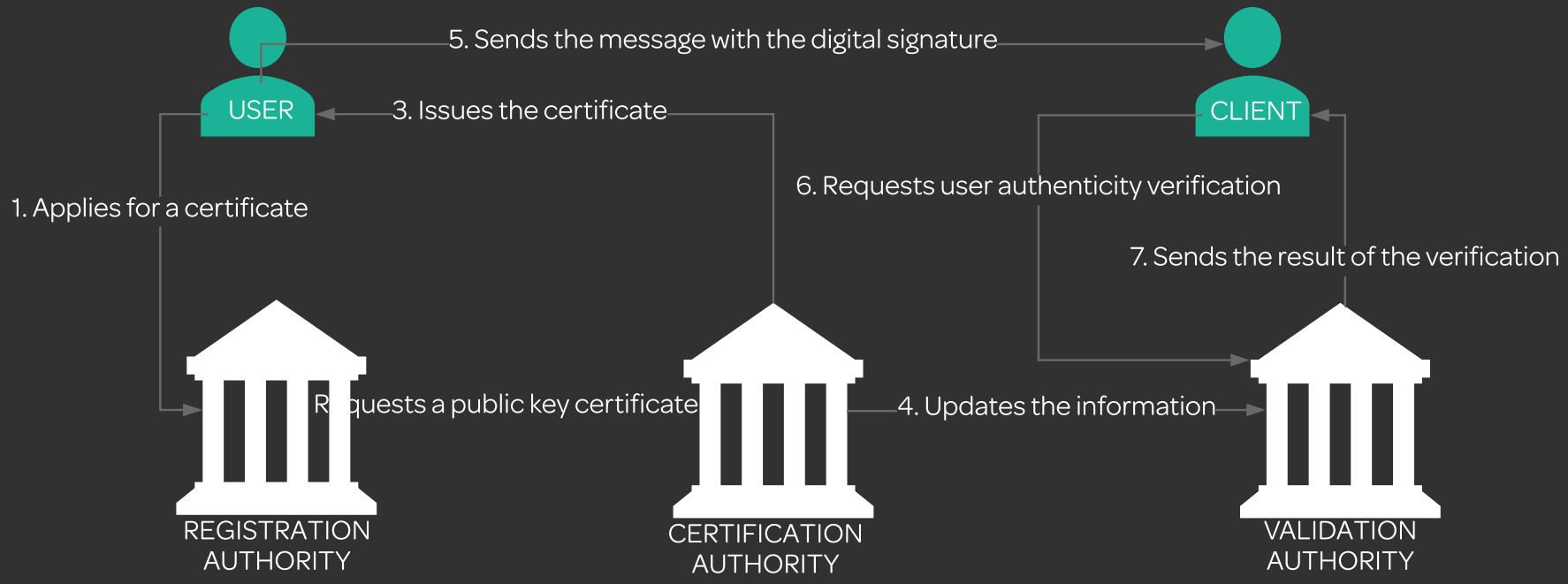
ENCRYPTION ALGORITHMS



Cryptography

PKI

Public Key Infrastructure or PKI refers to hardware, software, people, policies, and procedures that are required to manage digital certificates. It is a security architecture which was developed to increase the confidentiality of information that is being exchanged.



Cryptography

PKI

Signed Certificates

Signed certificate is a certificate issued by Certification Authorities (CA). It contains a public key and the owner's identity.

Self-Signed Certificates

Self-signed certificate is a certificate issued and signed by oneself. It is usually used for testing purposes and otherwise is not to be trusted.

CRYPTANALYSIS

Cryptanalysis refers to the process of decryption of ciphers and encrypted text. It is able to identify vulnerabilities in cryptosystems and thus extract plain text from the encrypted one.

Methods used in cryptanalysis are:

- Linear cryptanalysis is used on block ciphers
- Differential cryptanalysis is used on symmetric key algorithms
- Integral cryptanalysis is used on block ciphers

CODE-BREAKING TECHNIQUES

Brute Force Technique	Brute force technique tries every possible combination of characters to break the encryption
Frequency Analysis Technique	Frequency analysis technique analyzes the frequency at which certain symbols occur and based on that breaks the encryption
Trickery and Deceit	Trickery and deceit technique requires using social engineering techniques to extract the keys and break the encryption