

Try Hack Me

✓ likelihood
and severity
of the impact
potential for
damage

↓
weakness
that others
threat to
cause damage

↓
what
can cause
damage

Offensive Intro → aims to identify and exploit system vulnerabilities to enhance security measures, exploiting software bugs, leveraging insecure setups, taking advantage of unenforced access control policies
find hidden URLs
red team penetration testers specialize in these offensive techniques.

"dirb" → brute force

URL BASE - BASE we scanned → dirb http://---

WORDLIST FILES → /kullandigimiz common.txt

+ --- } URL's dirb found
+ --- }

Defensive Intro → ① Prevent intrusion from occurring ② Detect when occur and respond

- User Cyber Sec. Awareness : insolen bilinçlidir.
- Documenting and Managing assets : know the system and devices
- Updating and Patching
- Setting up preventative security devices : Firewall, IPS → intrusion prevention system
- " " logging monitoring devices

SOC → security operation Center → Threat Intelligence

Digital Forensics and Incident Response (DFIR) → Malware analysis

SOC

- Vulnerabilities , policy violations , auth. activity , Network intrusions
 ✓ necessary to fix with update or patch
 one direct sunlu ipidegi
 ↴
 si kullanan
 Confidential
 Sıfır yükleme!
- Network intrusions
 ↓
 Galitsi usernezi
 false detect etmeli
- malicious links

- Threat Intelligence : info about enemies , (TI) collects info to help the company better prepare against potential adversaries . Diff comp have diff adversaries → differ

meat
net
ceuk
ge
ce
e

- Digital forensic

application of science to investigate crime

forensic → low-copy
image vers. of image

telefon kartı gibi Digital branch ortaya atılmış

- o File Systems : bu digital ayak izini 'itemek storage' in boyası bilgi alanı silemeye us.

- o System Memory : disk kaydedmeden memory'de rastlamış olabilir virusi MEM. ayak izine bok.

- o System Logs : some traces will remain

- o Network logs

- Incident Response → Data breach or Cyber attack

aim → reduce damage , recovery shortest time

- ① Preparation
- ② Detection or Analysis
- ③ Containment, Eradication Recovery

team

- ④ Post Incident Activity

stop before affecting
other systems

143.110.280.149 part 22

- Malware analysis

↓
malicious

software → programs, documents etc.

- o Virus : piece of code attaches itself to a program spread from one computer to another

- o Trojan Horse : program that shows one desirable function but hides a malicious function underneath

- o Ransomware : is a malicious program that encrypt's user's files. attacker wants ransom for the decryption password

- o Static Analysis : without running the malicious program

- o Dynamic " " : run malware in a controlled environment

Abuse IPDB → malicious IPs

- Info Sec

→ *hack the box*

List of vuln and threat

↓
severity
and
likelihood
of the
impact

↓
whether
that
allows
threat

↓ what
damages

CIA
Model

[principles]

- Confidentiality : info is accessible to only authorized, implemented through encryption
- Integrity : lifecycle of data'nın authorized digital signatures + tamammalılığı. implemented through hashing
- Availability : when needed data should be available, implemented redundancy
- Non-repudiation : ensures that party cannot deny the authenticity
 - e-commerce, legal context
 - implemented through digital signatures
- Authentication : verifies the identity of a user, process or device implemented passphrase
- Privacy : handling of sensitive info
 - implemented through data minimization, consent, anonymization, merging

[purpose]

- protect business, sensitive data
- yeni teknolojileri şirketlerin
görsel rehberliği, ile tüketicileri sc̄ebenek

[Processes that ensure CIA]

① Risk assessment : identifies, evaluates potential vuln./Determines potential impact of security breaches / helps prioritize sec. efforts.

② Security Planning : strategies to address risks -- .

③ Imp. of sec controls : puts sec. plans into action

④ Monitoring Detection

⑤ Incident Response : includes steps like isolation, eradication, recovery

⑥ Disaster Recovery

⑦ Continuous improvement

- Tools in info sec.

- Firewalls: Controls incoming - outgoing network traffic
- IDS / IPS: Intrusion Detection / Prevention systems → monitor - block suspicious
- SIEM: Sec. info and event management → collect analyze sec. event. data
- Vulnerability scanners
- Penetration testing tools: Metasploit, Burp suite
- Encryption Tools: protect confidentiality and integrity
- Access control systems: Manage user permissions and authentications
- Sec. awareness training platforms

- INFOSEC DOMAINS -

- Network sec.

- several key elements that work together to form a protection strategy

firewalls, IDS/IPS, VPNs, Access control mech., Encryption tech.

it does not provide full protection

virtual private network
(over public networks)

include authent. and auth. auth.

with the increase of adoption of cloud IoT and remote work arrangements attacks expected significantly

chief e. CISO, penetration tester, ethical hackers, IT, CIO, security analyst, risk management teams, network administrators.
sec. officer day to day

- Application sec

→ against CIA triad

→ SQL injection, cross site scripting XSS, buffer overflows

approaches → Sec. by design = while designing from beginning

- ↳ × threat modeling: potential risks early on
- ↳ × Secure code reviews: check
 - ↳ × Servers and DBs: tunnel seyler sunlu giderse sifren
 - ↳ × authen & auth: kim yetkili

App. devs., sec. archs., IT ^{manag}, App sec. manager, CISO, security tester, penetration tester

Operational Security

- lifecycle. maintain secure envi for orgs. day-to-day operations sensitive info to be confid., intact, available, authorised

DG portinde esydekk vor örenli genel rehberlig ile portini veren

seguity plan yapası

critical
which items
are most imp.

prevent these
threats - aday
kilitle

who gets to enter
the room

① Assets identification ② Threat ident. ③ Vuln. Ident. ④ Access Control

⑤ Monitoring

items
that
need
extra protection

what could
go wrong?

password
badges etc.

who can access
sensitive data

asset management: up-date inventory of all info assets hardware etc.

change " : changes to their systems and processes w controlled manner w spec sec. auor. train.

CISO, IT, HR testing → inside sec. teams or outside consultants

Disaster Recovery and Business Continuity

depres felan sile olur devamlılık min date los.

DR → includes backing up data, replicating systems, cloud envin.

Yapınır Yeqdinya bi eventte sensiyet DR ; BC de öncesinde yapınır yeqdinya
diye düşünip içeri alınma fikri felan. Tutarla olsun show must go on

For companies BC means figuring out how to maintain operations during and after disruption

Business Contin. Manager, IT, operations, exec. leadership to DR/BC plans

RTO & RPO
time point

penetration tester

Cloud Security

shared responsibility model → you protect your own data sec.
cloud comp protects the infrastructure (building)

data breach, insecure APIs, misconfigured cloud storage, account hijacking
improper settings expose data

Key Areas

- Data Protection → like using strong lock
- IAM (Identity and Access Management) → only authorized can enter. personalized key
- Network sec.

Compliance, government meta mes for everyone

Responsibility

You, Cloud Service Providers, Sec. teams.

Physical Security

it's like installing sturdy locks on doors

protection of actual hardware

primary goal → deter, detect, delay and respond to potential physical threats
defense in depth

if one sec measure fails others are available

CISO HR IT

facilities management team → given it's name

IT sec. team hardware network equip.

All employees

✗ Red team penetration tester

Mobile Sec.

primary goal of mobile sec is to safeguard the sensitive info stored and transmitted by mobile devices.

- Device Protection

- Device sec. → Data sec. → Network sec. → Appli. sec.
- lock Biometric
 authorized access
- pen test
- ?
- some apps might be harmful
 permission management

IT depart, CISO, Sec. teams, IT sec. managers

IoT Sec

Internet of things

limited power and memory

CISO, IoT manager

Device manuf.: secure design → minimize unnecessary features.

Network admins.: network of IoT securage

App. Devs.: software interact w IoT is secure, proper authn else

- THREATS -

- Distributed Denial of Service (DDoS)

to interrupt normal functioning w flood of internet trafff.

DDoS attack comes from multiple sources simultaneously.

unlike
DoS → Denial of Service
Single source

often compromised comps or infected devices
tautiz
botnet

3 main components

- ① Attacker
person or group aim to attack
- ② Botnet
network of compromised devices
- ③ Victim
the targeted server etc.

DYN → Mirai

Ransomware

WannaCry attack → 200k computer, 180 country Hospitals in UK

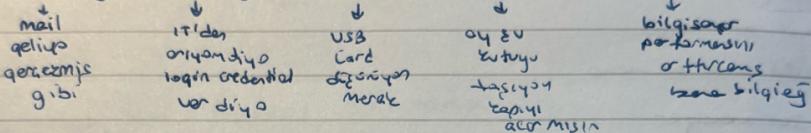
Step by step

phishing emails. then encrypting files

Social Engineering

psychological manipulation.

o Phishing, Pretexting, Baiting, Tailgating, Social Probing



Insiders Threat

• by knowing or not knowing

◦ Malicious insiders → intentionally

◦ Negligent " → not intentionally due to lack of knowledge or carelessness

◦ Compromised " → exterior hacker gets login info from an insider through various means

Insider threat kill chain → ① Motivations ② Preparation ③ Planning ④ Execution ⑤ Concealment

GDPR → general data protection Regulation

HIPAA → Health Insurance Portability and Accountability Act

Orgs have complex landscape of legal and regulatory requirements designed to protect sensitive info. Failure to comply with these mandates has severe consequences

Payment Card Industry Data Sec. Standard (PCI DSS) → can lead to penalties and loss of accreditation

Legal ramifications → might add legal issues

Advanced Persistent Threats → one of the most dangerous and damaging

sophisticated continuous cyberattack, intruder remain undetected
sometimes stealthy. long term access
widespread econ. damage -

In 2020 SolarWind → once inside, not immediate attack but wait
install malware → when update come

- Cyber Sec Teams -

Threat Actors → people who attacks bottlers

- scout, lockpicker, getaway driver, exfiltration specialist, leader
+ temitleyici extracts data or deploy malware

Red Team

CISO makes sure implementation also physical sec.

Blue Team

- security Analyst, SOC, threat hunters, incident responders
- Security Engineers
 - hidden threats or vulnerabilities

Purple Team

direct interaction b/w both red and blue

diff b/w SOC and Security Analyst is that

- ↑
 - 7/24 monitor
 - general
- ↓
 - specific monitoring for a specific topic
 - more analytic monitoring

-Jobs-

CISO → belediye başkanı guard backbone of cybersec. strategy of org.
multi faceted approach

SOC Manager, SOC Analyst

- ↑
 - Coordinates activities
 - exec. operational
 - Security monitoring
- ↑
 - monitoring glorist

Bug Bounty Hunter

operate independently to uncover vuln. in various digital assets belonging to orgs.

gönnüllü random gelip Bug Bounty Programla hizmetlerin bisei bulursa, ödüller veriler

- END OF INFOSEC -

④ Digital Forensic → CIA 'sı olur

Cyber Security Careers

① Security Analyst → CIA 'sı olur

security measures. security plan, analyze & explore evaluate company networks
review stakeholders

• compile ongoing reports, documenting sec. issue

• develop security plans

• güzel güvenliği reports, security plan hazırla, tarama hazırla

• yeni solduruları tarihi güncel tut.

② Security Engineer → CIA 'sı olur

• develop, implement security solutions using threats, vulnerabilities

• The ultimate goal security measure sağlığı sağlayıp kaybı min netwerk

• testing, screening sec. measures across software

• identify and implement systems needed for optimal sec.

• Monitor network and reports to update systems

③ IR

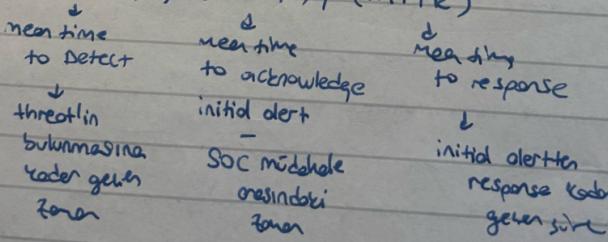
real time, during data breach

metrics : (MTTR) mean time to repair

③ IR

real time , during data breach

metrics : (MTTD) , (MTTA) , (MTTR)



④ Malware Analyst

analyses suspicious programs , discovering what they do and writing reports about their findings.

- reverse engineering (low level to compiled language)
- strong programming background (assembly , C)
- Static , dynamic analysis

Ü

↔

⑤ Penetration Tester

ethical Hacking

test system software of company to uncover vulnerabilities

confidentiality

info sec is important

Integrity

Availability

⑥ Red Teamer

similar to pen tester more targeted job role

Quiz → Incident Responder

