Risk includes vulnerability, threat
- Risk → likelyhood and severity of the impact potential for damage
- vulnerability → weakness that allows threat to cause damage
- threat → what can cause damage

TryHackme

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. red team, penetration testers specialize in these offensive techniques.

find hidden URLs
"dirb" → brute force

URL BASE_BASE we scaned → dirb http://- - - -

WORLLIST FILES → kullandığımız common.txt

+ - - -
+ - - -

} URL's dirb found

Defensive Intro

→ ① Prevent Intrusion from occuring ② Detect when occur and respond

- User Cyber Sec. Awareness : insanları bilinçlendir.
- 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, unauth. activity, Network intrusion
  - Vulnerabilities → necessary to fix with update or patch, ama direkt bunlar işi değil
  - policy violations → şi kullanıcı confidential şişi yüklenmeli
  - unauth. activity → çalıntı username'i fark detect etmeli
  - Network intrusion → malicious links

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

- Digital forensic
  - application of science to investigate crime

forensic → low-copy image
vers: of image

telefon zart zart gelizince Dijital branch ortaya cikmis

- File Systems : bu dijital ayak izini izlemek storage'in baya bilgi cikaryo silinenler us.
- System Memory : diske kaydetmeden memory'de runlamis olabilir virusu MEM. ayak izine bak
- System Logs : some traces will remain
- Network logs

- Incident Response → Data breach (→ steal company data) or Cyber attack

aim → reduce damage, recovery shortest time

① Preparation (team) ② Detection and Analysis ③ Containment, Eradication Recovery (stop before affecting other systems) ④ Post Incident Activity

143.110.250.149 part 22

- Malware analysis

malicious software → programs, documents etc.

- virus : piece of code attaches itself to a program spread from one computer to another
- Trojan Horse : program that shows one desirable function but hides a malicious function underneath
- Ransomware : is a malicious program that encrypt's user's files. attacker wants ransom for the encryption password
- Static Analysis : without running the malicious program
- Dynamic " : run malware in a controlled environment

AbuseIPDB → malicious IPs

- InfoSec → hack the box

Risk → vuln and threat

- severity and likelihood of the impact
- weakness that allows threat
- what damages

CIA triad

principles

- Confidentiality : info is accessible to only authorized, implemented through encryption
- Integrity : lifecycle de data'nın authorized digital signature tanımlaması işlemin. implemented through hashing
- Availability : when needed data should be available, implemented redundacy
- 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 passwords
- privacy : handling of sensitive info implemented through data minimi, consent token merge

Processes that ensures CIA

1. Risk assesment : identifies, evaluates potential vuln./Determines potential impact of security breeches / helps prioritize sec. effort.
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

purpose

-protect business, sensitive data ve yeni teknolojiler şirketlerin günlük rahatlığı ile kullanımını sağlanak

- Tools in info sec.
  - Firewalls : Controls incoming - outgoing network traffic
  - IDS / IPS : Intrusion Detection / prevention systems → monitor - block suspicious
  - SIEM : Sec. info and event mangement → 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 mechan., Encryption tech.

↓ It does not provide full protection

↓ virtual private Network (over public networks)

↓ include authent. and authoriz.

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

chief info sec. officer e- CISO, penetration tester, ethical hackers, IT, CIO, security analyst - risk mangent teams, network administrations.

security analyst → day to day

network administrations → day to day

- Application Sec

acele ise yilan konser → rowady corpories

- again CIA triad
- SQL injection, cross site scripting XSS, buffer overflows

approaches → Sec. by design = while desiging from beginning
- ↳ threat modeling : potential risks early on
- ↳ Secure code reviews : check
- ↳ Servers and DBs : temel seyler bunlar giderse sigorta
- ↳ authen & author : kim yetkili

App. devs., sec. orchs., IT (many many), App sec. meger, CISO, security tester, penetration tester

Operational Security

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

DG partinde eşyaların var önemli gönül rahatlığı ile partini vermeyi sağlıyo plan yapıyoz

① Assets identification (which items are most imp. → critical info assets; items that need extra protection)
② Threat iden. (what could go wrong? → vazo devrilmesi mi?)
③ Vuln. Ident. (prevent these threats - odayı kilitle; password badges etc.)
④ Access Control (who gets to enter the room; who can access sensitive data)
⑤ Monitoring

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

change " : changes to their systems and processes w controlled maner w opsec

sec. awar. train.

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

Disaster Recovery and Business Continuity

deprem falan bile olsa devamlılık min data los.

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

Yağmur Yağdıysa bi eventte şemsiye DR; BC de öncesinde yağmur yağarsa diye düşünüp içeri alınma fikri falan. olursa 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 authorised can enter, personalized key
- Network sec.

compliance, government mete rules for everyone

Responsibility

you, Cloude 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 normal

IT sec. team hardware, network equip.

All employees

✗ Red team penetration tester

Mobile Sec.

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

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

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

IoT sec

Internet of things

limited power and memo

CISO, IoT manager

Device manfuc.: secure design → minimize (unnecessary) features.

Network admins.: network of IoT securage

Appi. Devs. : software interact w IoT is secure, proper auten also

-THREATS-

- Distributed Denial of Service (DDoS)

to interrupt normal functioning. w flood of internet traff.

DDoS attack comes from multiple sources. simultaneously.

unlike

DoS → Denial of Service
single source

often compromised comps or infected devices
↓ tauiz
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, 150 country Hospitals in UK

Step by step

phishing emails. then encrypting files

Social Engineering

psychological manipulation.

- Phishing , Pretexting , Baiting , Tailgating , Quid Pro Quo

Phishing ↓ mail geliyo gerçekmiş gibi

Pretexting ↓ IT'den arıyorum diyo login credential ver diyo

Baiting ↓ USB Card düşürüyor merak

Tailgating ↓ oy ev kutuyu taşıyom kapıyı açar mısın

Quid Pro Quo ↓ bilgisayar performansını arttırcam bana bilgi ver

Insiders Threat

- by knowing or not knowing
  - Malicious Insiders → intentionally
  - Negligent " → not intentionally ama rahatlıklarından ilgisizlikten
  - Compromised " → exterior hacker gets login info from an insider

Insider threat kill chain → phases: ① motivation ② planning ③ preparation ④ execution ⑤ concealment → izleri yok et

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 mandatories has severe consequences

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

Legal ramification → müşteri adalet istiyo

Advaced Persistent Threats → one of the most dangerous and damaging

Sophisticated continuous cyberattack, intruder remain undetected

sometimes devletsel. long term access

widespread econ. damage.

In 2020 SolarWind → once inside, not imidiable attack but wait

install malware ↘ when updatecome

- Cyber Sec Teams -

Threat Actors → people do attacks kötüler

- scout, lockpicker, getaway driver, exfiltration specialist, leader
  - getaway driver ↓ temizleyici
  - exfiltration specialist ↓ extracts data or deploy ransomware

Red Team

CISO make sures implementation also physical sec.

Blue Team

- Security Analyst, SOC, threat hunters, incident responders
  Security engineers
  - threat hunters ↓ hidden threats or vulnerabilities

purple team

direct interaction btwn both red and blue

diff betwn SOC and Security Analyst is that

- SOC ↓ 7/24 monitor general
- Security Analyst ↓ specific monitoring for a specific topic more analytic monitoring

-Jobs-

CISO → belediye başkanı guard backbone of cybersec. strategy of org.

multifaceted approach

SOC Manager, SOC Analyst

- SOC Manager ↓ coordinates activities exec. operational security monitoring
- SOC Analyst ↓ monitoring alerst

Bug Bounty Hunter

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

gönüllü random gelip Bug Bounty Programla hacklıyosun biri bulursa ödül veiolor

— END OF INFOSEC —

④ Digital forensic → CIA 'sel olan

Cyber Security Careers

① Security Analyst → daha investigative

security measures. security plans, analysts explore evaluate company networks

- various stakeholders
- compile ongoing reports, documenting sec. issue
- develop security plans
  - güzel giden şeyleri raporla, security plan hazırla, takımı hazırla
  - yeni saldırılara karşı güncel kal.

② Security Engineer → daha mimarisel

- develop, implement security solutions using threats, vulnerabilities
- The ultimate goal security measure sürekliliği sağlayıp kayıtları minimum tutmak
  - 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 : (MTTD)

③ IR

real time, during data breach

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

- (MTTD) → mean time to detect → threat'in bulunmasına kadar geçen zaman
- (MTTA) → mean time to acknowledge initial alert → SOC müdahale arasındaki zaman
- (MTTR) → Mean time to response → initial alert'ten response kadar geçen süre

④ Malware Andlyst

analyses suspicious programms, 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

⑥ Penetration Tester

Info sec is important
- confidentiality
- Integrity
- Availability

ethical Hacking

test system software of company to uncover vulnerabilities

⑦ Red teamer

similar to pen tester more targeted job role

Quiz → Incident Responder