Common THREAT ACTORS and MOTIVATION

D2

ACTORS :

- Nation state — (well-resourced) ⟶ APT threat actors = specialized teams
- unskilled attacker - (limited resources) = no experience
- hacktivist (driven by ideological...) promotes causes
- insider
  - organized crime (well-resourced)* ⟶ steal confidential trade secrets for the benefit of a competing company!
  - shadow IT (insider without a malicious intent) = without authorization, bypassing official IT protocols!

Motivations :

- data exfiltration (stealing data) = steal and sell it on the black market.
- espionage (gathering information for intelligence) [ex. disrupt critical infrastructure]
- Service disruption (DDOS)
- Blackmail (extorting using compromising information) = unless a substantial sum of money is paid
- Financial gain = money*
- Revenge
- War (cyberwarfare or military conflict)

- operational capacity = Resources/funding
  - Nation state (USA, ITA...)
  - organized crime...

→ define the ACTORS and then the MOTIVATIONS, or the opposite.

Explain common threat vectors and attack surfaces

(B2)

Message-based:
- email = phishing, malicious attachments
- SMS = text based scams, malicious links, and Smishing (= SMS phishing)
- Instant Messaging = chat based phishing, malware distribution and social engineering

(and To end encryption)

Image based: malware hidden, steganography

File-based:
- malicious files
- Trojans
- ransomware

Unsecure Networks:
- Wireless
- Wired
- Bluetooth - exploiting device connections

Open service ports: exploiting open ports for unauthorized access.

Supply chain: attacks on linked third-party providers
- Managed Service Providers (MSPs) - "a breach"
- Vendors
- Suppliers = attacking through the supply chain network.

Human vectors / Social Engineering

-> exploit the vulnerabilities of human psychology to breach digital defences.

- phishing = attackers send emails that seem to come from a legitimate authority.
- Spear phishing = is a more targeted variant: it involves attacks directed at specific groups.
  - due to the frequent occurence of these attacks, many companies will conduct phishing campaign simulations.
- Smishing (SMS phishing)
- impersonation
  - business email compromise;
  - pretexting = an attacker might pose as a tech support agent, convincing you to share sensitive data under the guise of resolving an issue.
- watering hole attack: - compromise legitimate websites by implanting malicious code
- brand impersonation = imitating valuable brands.
- Typosquatting: it exploits typing errors. Similar domains and so on, such as misspelling errors.

Zero-day Vulnerabilities

- it's a secret passage in a computer software (vuln.? exploit) that hackers find before the software's creators do.

⟶ zero-day vuln.s are not know, there are no patches & sec. tools (firewall..) that can detect them.

SOLUTION CHAPTER 7/28:

1) if a certificate is compromised ⟶ it must be added (by admin) To the Certificate Revocation List (CRL)

2) a VM sprawl attack (rogue VM connected To the network) ⟶ HOW TO PREVENT:
- craft explicit guidelines for using VMs
- Automating the process (less error prone) of creating, add to the network ... VMs.

3) what's the greatest risk when outsourcing the develop of a third-party service which will hold sensitive information? (ex TIMENEXT in Leonardo & Q) ⟶ • Weak configurations: (default passwords, inadequate encryptions, or overly permissive access control.)

4) In a sec. ~~incident~~ breaches, ~~or DDOS~~ we got some sensitive data lost
What proactive measure can we adopt to minimize the data breaches in The future? ⟶ implement Data Loss Prev. (DLP)

5) a "VM escape" ⟶ it's a breach where an attacker gains unauthorized access To the host system within a VM.

Explain various types of vulnerabilities

Application vulnerabilities:

- memory injection: unauthorized code inserted into a program's memory space.
- buffer overflow: data exceeding allocated memory, leading to potential exploits.
- race conditions: conflicts arise when multiple processes access shared resources.
- TOC/TOU: timing mismatches exploited during checks and usage.
- malicious update: attackers introducing harmful code through software updates.

Web-based vulnerabilities:

- SQLi: attackers manipulating input to exploit database vulnerabilities (SQL queries executed)
  - ↳ the website's backend uses "user input directly in constructing SQL queries" without proper validation or sanitization.

- XSS: malicious scripts injected into web pages.

  XSS can use the <script> and </script> HTML TAGS and can include Javascript in between

  ex. A user can post comments on a web site like

```
html
<script>
  alert('XSS attack!');
</script>
```

  → When other users visit the page and view the comments, the malicious script gets executed in their browsers.
  → The script's attacker could steal cookies, hijack sessions, other malicious actions.

HW vulnerabilities:

- ~~Firmware~~: low level sw controlling hw. — TRUSTED BOOT = validate + signed firmware
- End of life: security gaps due to discontinued hw support. (a system is no longer manufactured).
- Legacy: Older hw with outdated security measures, that are still in use.

Virtualization vulnerabilities:

- VM escape: unauthorized breakout from a VM to the host system: Hypervisor can unintentionally create a path for lateral movement.
- VM sprawl: unmanaged VMs installed on your network: uncontrolled and excessive creation of VMs within a virtualized environment.
- Resource reuse: Overuse of shared resources, leading to vulnerabilities: impact the performance and so on
  - ↳ use encryption

Cloud-specific vulnerabilities

- Risk of shared tenancy: multiple customers sharing the same physical infrastructure. if the customer does not secure its data properly, then that could lead to a side-channel attack. (isolation mechanisms not working correctly).
- inadequate configuration management
- identity and access management flaws: misconfigured user permissions, compromise credentials...
- CASB (Cloud Access Security Broker): Unlike traditional group policy, CASB assumes the crucial role of overseeing all cloud clients, ensuring their security and that all devices are patched.

Supply chain vulnerabilities

- service provider → data breaches, service disruptions and unauthorized access.
- hw provider: hw forms the backbone of IT infrastructure.
- SW provider: (ex third-party code libraries).

Mobile device vulnerabilities

- side loading: installing a/ps from unofficial sources -> APK → Android
- Jailbreaking: bypassing iOS restrictions, compromising device security → iOS

Cryptographic Vulnerabilities

- CA compromise: the digital world relies on CAs to issue digital certificates.
- Key compromise: crypto systems are only as strong as their keys: H/T, weak generation, poor key management..

- Certificate Revocation Lists (CRLs) and the Online Certificate Status Protocol (OCSP): these are vital tools to maintain the integrity of the Trust infrastructure.
  - CRLs verify current validity of digital certificates
  - OCSP (which is the faster) enables real-time certificate validation by querying CAs for up-to-the-minute status information.

- Secure Key Management → storing them in a HW Security Module (HSM)
- SSL/TLS downgrade: SSL traffic is intercepted by a server pretending to have an older, less secure browser, to communicate with that server, SSL switches to a weaker encryption method, and it is then easy for hackers to see private data. (Ex. Poodle MiTM attack → Padding Oracle On Downgraded Legacy Encryption.)

D2

Indicators of malicious activity

malware = malicious SW -> SANDBOX (ex. CUCKOO)

- Potentially Unwanted Program (PUPs) — inside other programs you download
  - Ransomware
  - Trojans (backdoor)
    - PE (portable exec. file) that usually requires User Account Control (UAC) to give permission?
    - RATs - Remote Access Trojans
- Worms = self-propagates (movement to and from LAN/WAN)
- Spyware = tracks user activities by using tracking cookies and then sending it.
- Bloatware = "programs garbage": non possono eliminare, sono presenti dalla fabbrica.

+Polymorphic Viruses → able to modify their code, signature-based detection methods become less effective.

- Keylogger = Keyboard
- Logic bomb = trigger
- Rootkit = root/kernel level access: is able to intercepts system level function calls, event...

NETWORK ATTACKS

- most are called Server-side attack as they target an organization's servers such as domain controller*, which hold user accounts, SQL DB servers... customer data.
- First step is always PIVOTING attack = Network Mapper tool like nmap → open ports, services running... all hosts.

- DoS - Traffic comes from one single IP Adress
- DDoS - ← ← from multiple IP addresses (flooded with a massive volume of traffic)
  - Amplified: ICMP ("ping") = small request that triggers much larger response.
  - Reflected: attacker obtains the victim's IP address and craft a packet seemingly from the victim.
- ARP Poisoning (Layer 2 = LAN) attack ——— MAC address fool the router/switches.
- DNS cache Poisoning: cache because is stored on the local machine and that's the first step of DNS name resolution process. It's a prime target for attackers...

  On Windows, > ipconfig /displaydns

  cache = C:\Windows\System32\drivers\etc.

  redirects the victim from a legitimate to a fraudulent website.

Wireless attack:

- Rogue access point
- Evil Twine = impersonate a real network and also intercepts communications. → duplicate (SSID)

like DNS or ARP poisoning attack, these are "On-path"/MiTM attack!

Replay Attack is on-path that intercepts data but "replay" the data.
(Ex. Kerberos prevents Replay attack using unique seq. numbers and timestamp)

1. credential replay attacks ——— Wireshark or tcpdump (sniffer)
   - telnet (NO) → use SSH
   - legacy NT LAN Manager (NTLM) authentication (NO) → use Active Directory (which uses Kerberos)

2. credential stuffing → usando le credenziali che rubo su altri siti!

Application attack

- injection attack
- Buffer Overflow: Windows use Data Execution Prevention (DEP) to mitigate marking memory pages as non-executable.
- privilege escalations
- Forgery attacks
  - Cross-Site Request Forgery (CSRF): users are tricked into performing actions without their consent
  - Server-Side (SSRF): vulnerability that allows to send unauthorized requests from a server

use Secure coding + input validation

- Directory Traversal → /etc/passwd user info
  /etc/shadow encrypted password hashes
  (ex. ../../../../ or %2f..%2f..%2f or ..2f..2f..2f) is a Traversal attack

CRYPTOG. ATTACKS

- SSL/TLS downgrade attack: it does not intercept, it's focused on DOWNGRADING the security protocol
- SSL stripping: intercepts a secure HTTPS and downgrade to an unsecured HTTP.
- Password SPRAYING = focus on common usernames and passwords → - strong passw policies - MFA

credential
- STUFFING: attackers use stolen credentials to gain access
- HARVESTING: attackers collecting credentials! (gathering)

Mitigations used to secure the enterprise

(52)

SEGMENTATION

- creating isolated environment/segments that restrict the "lateral movement" of potential attackers.
- VLANs = virtual = logical network segments with a single SWITCH.
- Subnetting = divides an IP network into smaller subnets, each with a subnet mask.

Compliance requirements: - PCI DSS (Payment Card)
- HIPAA (Health insurance..) → protect PHI (Health Information of individual).

ACL { organization's data, applications, network, cloud } policies

In general, ACLs — network → used by ROUTERS and FIREWALL *
— system → file/folder access (rwx)

- least privilege principle.

* newly FW will contain only "deny all" rule by default → Allow List = Whitelist
→ Block List (deny list) [ex. Microsoft's AppLocker]

MONITORING

- SIEM - Sec. Inform. and Event Mng.:
  Can correlate LOGS from multiple sources (servers...) and analyze them to detect and respond to security incidents in real time. — capturing network traffic —

- SOAR - Sec. Orchestration, Automation and Response:
  works in real time to tackle threats. → automate incident response processes!

- EDR - Endpoint Detection and Response
  designed for individual endpoints → it's able to detect threats and prevent similar malware infections in the future.
  ← threat intelligence feeds = Indicators of Compromise (IoC) - known malware signature -

- Vulnerability Scanner (ex. Nessus)
  Can scan enterprise network for vulnerabilities, including missing patches and SW flaws.

Host-level protection — something that runs on individual devices

- Host-based Intrusion Prevention System (HIPS): unauthorized access, malicious activities...

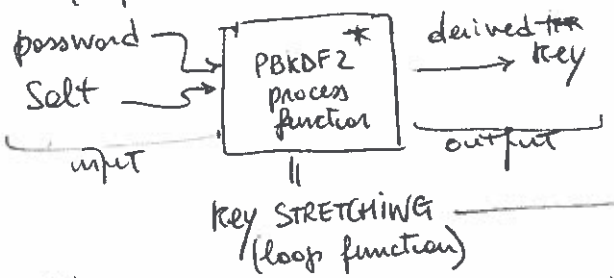
Windows Defender:
- SmartScreen = cloud-based anti-phishing and malware
- FW*
- malware scanning

(On MAC (Apple) there's a built-in "Defender")

- Host-based Firewall* = monitors incoming/outgoing network traffic (it's SW)

- **Disabling Ports/Protocols** — reduce attack surface
  - no longer use Telnet (TCP p23) as plaintext → SSH (port 23)
  - NETBIOS (p. 137-139) = legacy file and print services → SMB protocol (Server Message Block) (p. 445)
    - now, it's → Samba in Linux
    - Windows Services: Server (ID = LanmanServer) + Workstation (ID = LanmanWorkstation).
      ↓ it uses NTLM or KERBEROS protocols for authentication

PBKDF2, in cryptography (Password-based Key Derivation Function)
- used to reduce vulnerability to brute force attacks.
- published in 2017 for password hashing



The added computational work* makes password cracking much more difficult.

Salt reduces RainbowTable attack (precomputed hashes) → NIST recommends a salt length = 128 bits

** derived key (final) = PBKDF2(PRF, Password, Salt, c, dkLen)
- derived key (final) → stored on DB
- PRF: function (ex. XOR)
- c: iterations
- dkLen: desired bit length of derived key

For example, WPA2 uses:

DK = PBKDF2(HMAC-SHA1, passphrase, ssid, 4096, 256)