



Lecture 26 — Threat Intelligence & Vulnerability Assessment

1) What is Threat Intelligence (TI)?

Definition: Threat intelligence is organized information about *who* is attacking, *why* they attack, and *how* they do it. TI helps security teams anticipate, detect, and respond to attacks faster — it turns raw data into actionable decisions.

TI's job in an organization: collect signals about malicious IPs/domains, malware hashes, attacker tactics, and relevant vulnerabilities — then feed that into detection and response (firewalls, IDS, patching, security policy).

Key outcome: Reduce risk by blocking known bad actors, hardening systems where attackers focus, and prioritising defensive actions.

2) Who/What do we gather info about? (Targets & Indicators)

- **Potential threat sources:** disgruntled employees, competitors, criminal gangs, state-sponsored groups, hacktivists.
 - **Technical indicators to track:** malware hashes, blacklisted IPs, malicious domains/URLs, CVE IDs, suspicious email senders, command-and-control servers.
 - **Why gather this:** to block, triage, or investigate — e.g., if an IP is blacklisted or a file hash matches malware, raise the alert level.
-

3) Useful public tools & how to use them (practical tips)

I'll explain each tool, why it's useful, and one practical use-case you can run in your study lab.

VirusTotal — file / URL / IP aggregator

What it is: A service that scans files and URLs with many antivirus engines, and stores metadata and historical sightings. Security teams use it to check

suspicious files/URLs and to see if a sample is already known malicious. [Tom's Hardware](#)

How to use (practical):

- Upload suspicious .exe/.zip or paste a URL → see which AV engines flag it and get related metadata (file hashes, network indicators).
- Use the **hash** (MD5/SHA256) to correlate across logs (SIEM) or to block on endpoints.

Why: Quick way to confirm if a sample has been seen before; helpful for triage.

ANY.RUN — interactive malware sandbox

What it is: An interactive (browser-based) malware sandbox where you run a suspicious file and watch its behavior in real time (processes, network calls).

Good for dynamic analysis. [any.run](#)

How to use (practical):

- Upload a sample (in a safe lab account) and observe what domains/IPs it contacts, registry changes, child processes — capture IOC list for blocking.
- Use screenshots and network events as evidence in reports.

Why: Dynamic behaviors often reveal C2 domains or dropped files that static scan misses.

Shodan — search engine for internet-connected devices

What it is: A search engine that indexes banners and metadata from devices/services exposed on the internet (cameras, routers, web servers).

Useful for mapping an organization's exposed attack surface. [help.shodan.io](#)

How to use (practical):

- Search your organisation domain / IP range to find exposed services (e.g., SSH, RDP, outdated web servers).
- Filter by product or port to find vulnerable versions and prioritize remediation.

Why: Attackers use Shodan to discover poorly secured IoT/servers — defenders can use it to find and fix exposures first.

Exploit-DB (Exploit Database) — PoC & CVE research

What it is: A public archive of proof-of-concepts (PoCs) and public exploits mapped to vulnerabilities (CVE). It's used by pentesters and defenders to see how a vulnerability can be exploited. exploit-db.com

How to use (practical):

- Look up a CVE to find PoC code or exploit details — helps estimate risk and urgency.
- Use searchsploit (Kali) offline to search exploits quickly.

Why: Knowing exploit availability changes how urgently you patch a CVE.

Nessus (Tenable) — vulnerability scanner

What it is: Nessus is a leading vulnerability scanner used to discover missing patches, misconfigurations and known vulnerabilities across systems. There is a free edition (Nessus Essentials) limited to 16 IPs — great for labs. [Tenable®](https://tenable.com)

How to use (practical):

- Install Nessus Essentials, register for the activation code, then run a scan of your lab IPs to find CVEs and severity ratings.
- Export scan results (CSV/PDF) and prioritize fixes by criticality.

Why: Automated scanning helps you find and quantify risks quickly.

Other quick resources (short uses)

- **DNSdumpster** — DNS reconnaissance for subdomains and host mapping (use for recon before a pen-test). [DNSDumpster.com](https://dnsdumpster.com)
- **Have I Been Pwned** — check emails or domains against known breaches (see if credentials leaked). [Have I Been Pwned](https://haveibeenpwned.com)
- **FireHOL IP Lists** — curated blocklists and reputation feeds to feed firewalls/IDS. [FireHOL IP Lists](https://firehol.net)

- **HackerTarget** — simple online tools (HTTP header checks, online Nmap) for quick external checks. [HackerTarget.com+1](https://hackertarget.com)

4) Threat actors & their motivations 🧑🔥

Common actor types and why they attack:

- **Cybercriminals (profit-driven)** — steal data, ransomware, banking fraud. Motivated by money.
- **Nation-states (political/geopolitical)** — espionage, disruption, sabotage; target government, critical infra.
- **Insiders (disgruntled employees)** — sabotage, data theft, leak sensitive info; motivation: revenge or financial gain.
- **Hactivists (ideological)** — defacement, data exposure to support a cause.
- **Script kiddies / thrill-seekers** — opportunistic; motivations: reputation, practice.

Why classify? Different actors use different tools and TTPs (tactics, techniques, procedures). TI helps tailor defenses to the relevant actor profile.

5) Indicator of Compromise (IOC) — explained 🌱

IOC = Indicator of Compromise

These are observable artifacts that show a system has been breached or is compromised. Examples:

- File hashes (MD5/SHA256) of malware
- Malicious IP addresses or domains contacted by malware
- Unusual registry keys or scheduled tasks
- Suspicious process names or parent/child relationships
- Unusual outbound connections at odd times

Use: Match IOCs against logs (SIEM, EDR) to detect infections and trigger containment.

6) Three types of Threat Intelligence — tactical, operational, strategic (detailed) 🎯

1) Tactical TI (short-term, technical) ⚙️

- **What:** Raw, technical indicators (IOCs) — IPs, hashes, domains, YARA rules.
- **Who uses it:** SOC analysts, SIEM rules, firewall/IDS signatures.
- **Goal:** Immediate detection and blocking (e.g., add IP to firewall blocklist).
- **Example:** A new C2 domain appears — block on perimeter and add signature to IDS.

2) Operational TI (mid-term, campaign-level) 🕒

- **What:** Context about campaigns, attacker TTPs, infrastructure used (C2 hosts, malspam campaigns), replayable timelines.
- **Who uses it:** Incident response teams, threat hunters.
- **Goal:** Understand ongoing attacks and coordinate containment and hunting.
- **Example:** A phishing campaign targeting HR using specific lure messages — create targeted user awareness and hunt for compromise indicators.

3) Strategic TI (long-term, business-oriented) 🏛️

- **What:** High-level analysis for executives — threat trends, geopolitical risk, industry-specific risks, intelligence that informs policy and investment.
- **Who uses it:** CISOs, risk managers, board.
- **Goal:** Prioritize security strategy, budgeting, and risk acceptance decisions.
- **Example:** “Nation-state activity against our sector is increasing” → invest in hardened controls and monitoring.

Remember: Tactical → operational → strategic move from immediate technical items to big-picture business decisions.

7) Vulnerability Assessment — what it is & how to do it 🔍

Definition: A structured process to find, classify, and prioritize vulnerabilities on systems and applications.

Typical steps:

1. **Asset discovery** — enumerate hosts, apps, and services (use Nmap / Shodan).
2. **Scanning** — run vulnerability scanners (Nessus, OpenVAS) to detect missing patches, misconfigurations, and CVEs.
3. **Validation** — verify the scanner findings manually (false positives happen).
4. **Risk rating** — use CVSS or internal scoring to prioritize fixes.
5. **Remediation & patching** — apply patches, config changes, or compensating controls.
6. **Rescan & report** — confirm fixes and provide management reports.

Tool tip: Nessus Essentials (free) lets you scan up to 16 IPs — great for learning and small environments. [Tenable®](#)

8) Practical playbook: How to combine Threat Intelligence + Vulnerability Assessment 🧩

1. **Run a Nessus scan** on your public IPs → get list of CVEs. [Tenable®](#)
2. **Search Exploit-DB** for PoC/exploit availability for the highest-severity CVEs → if PoC exists, raise patch priority. [exploit-db.com](#)
3. **Query Shodan** for internet-exposed services and match them against vulnerable versions found in step 1 → remediate immediate exposures. [help.shodan.io](#)
4. **Use VirusTotal / ANY.RUN** on suspicious files found during triage to see if they're known malware and get IOCs (hashes, C2 domains). [Tom's Hardware+1](#)

5. **Feed IOCs into firewall/IDS** (or blocklists like FireHOL) and update detection rules. [FireHOL IP Lists](#)

9) Quick “how-to” cheat sheet (commands / steps you can try in a lab) 🧪

- **Nessus (basics):**
 1. Register Nessus Essentials, get activation code.
 2. Install and log in to the web UI.
 3. Create a scan → add target IP(s) → run scan → export results.
- **Shodan (basic queries):**
 - `org:"YourOrgName" port:22` → find exposed SSH boxes.
 - Search by product: `product:"Apache httpd"` → find servers.
- **VirusTotal (quick):**
 - Paste file hash or URL into VirusTotal → view AV detections & related IOCs.
- **ANY.RUN (quick):**
 - Upload sample (use a test VM account) → watch network calls and process tree → export IOCs.
- **Exploit-DB (quick):**
 - Search CVE or software name → read PoC to understand exploitability.

10) Common mistakes & tips ✅ ❌

- ❌ **Don't** blindly block everything flagged by one source — false positives exist.
 - ✅ **Do** cross-validate: check VirusTotal + sandbox + network logs before blocking wide ranges. [Tom's Hardware+1](#)
 - ✅ **Prioritize** fixes where an exploit is publicly available or the service is internet-exposed (high risk). [exploit-db.com+1](#)
-

11) Short glossary (quick reference) 📄

- **IOC:** Indicator of Compromise (hashes, IPs, domains).
 - **TTP:** Tactics, Techniques, Procedures (how attackers operate).
 - **CVE:** Common Vulnerabilities and Exposures (identifier for a vulnerability).
 - **CVSS:** Scoring system to rate vulnerability severity.
 - **PoC:** Proof of Concept (exploit code demonstrating vulnerability).
-

12) Final checklist (what to practice this week) ✅

- Install **Nessus Essentials** and run a 1–2 IP scan. [Tenable®](#)
- Upload a harmless sample to **VirusTotal** and read the analysis. [Tom's Hardware](#)
- Use **Shodan** to scan your own public IP and see what's exposed. help.shodan.io
- Search **Exploit-DB** for one CVE from your Nessus scan and read the PoC. exploit-db.com
- Try **ANY.RUN** on a sample (in safe lab account) to watch behavior. any.run