**Day 5 - Applied Forensics & Response (24.6.)**

**1. End-to-End Incident Simulation (Case Walk-through)**

**Topics**

* Full-scope incident simulation with focus on:
  + **Initial detection**
  + **Forensic evidence acquisition**
  + **Timeline reconstruction**
  + **Root cause identification**
* Team-based analysis workflow (IR lead, forensic analyst, SOC responder)
* Case-based learning (e.g., ransomware in enterprise, insider data exfiltration)

**Required Infrastructure & Components**

* Simulated incident case (PCAP, memory image, disk image, SIEM logs)
* Collaboration environment (shared drive, Google Docs, Miro, etc.)
* Chain of custody templates, analyst notebook
* MITRE ATT&CK & Timeline reference matrix

**To-Dos & Steps**

1. Review and organize evidence from a simulated breach
2. Reconstruct the attacker’s steps (Initial Access → Persistence → Exfiltration)
3. Identify key indicators of compromise (IOCs) and TTPs
4. Assign tasks and responsibilities in team roles
5. Document assumptions, gaps, and detection improvements

**1. End-to-End Incident Simulation (Case Walk-through)**

**Webinars**:

* [Webcast: Incident Response Hands-on Walkthrough](https://www.youtube.com/watch?v=2BOOl8_nwjQ) – 00:12
* [Recorded Future Webinar: Real-World Incident Response Case Study](https://www.youtube.com/watch?v=-TOZuNYPi40) – 00:32

**YouTube**:

* [Incident Response Lifecycle](https://www.youtube.com/watch?v=IRSQEO0koYY) – 00:19
* [Ransomware Attack Full Analysis](https://www.youtube.com/watch?v=1VEQcuuNDJc) – 00:09

**Reading Material**:

* [NIST Computer Security Incident Handling Guide (SP 800-61r2)](https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf)
* [MITRE ATT&CK Navigator](https://mitre-attack.github.io/attack-navigator/)

**2. Timeline & Root Cause Analysis**

**Topics**

* Creating incident timelines from heterogeneous sources (logs, PCAP, images)
* Identifying dwell time, lateral movement, and data staging
* Root cause determination using forensic evidence
* Mapping attack techniques to MITRE ATT&CK framework
* Categorizing findings by severity and response priority

**Required Infrastructure & Components**

* Timeline builder tools (Excel, log2timeline, Timesketch)
* MITRE ATT&CK Navigator
* Event logs, user activity records, malware samples (simulated)
* Incident log template or ticketing system (Jira, TheHive optional)

**To-Dos & Steps**

1. Build a chronological view of attacker behavior
2. Map key actions to ATT&CK tactics and techniques
3. Identify delays, misdetections, or blind spots
4. Link forensic artifacts to specific phases (e.g., persistence via registry keys)
5. Highlight the root cause and recommend corrective actions

**Webinars**:

* [Google DFIR: Timeline Analysis Using Timesketch](https://medium.com/@ozan.unal/analysis-of-log-files-using-timesketch-fb68330ea67f) *(Walkthrough by Timesketch team)*
* [Magnet Forensics Webinar: Timeline Reconstruction and Forensics](https://www.youtube.com/watch?v=9BwB33nBZtw) – 00:32

**YouTube**:

* [Intro to Timeline Analysis in Incident Response | DFIR Science](https://www.youtube.com/watch?v=C4jNfXZ90fw) – 02:13
* [Building Attack Timelines with log2timeline](https://www.youtube.com/watch?v=hI4MGelYjHk) – 00:27

**Reading Material**:

* [Timesketch Open Source Timeline Analysis Tool](https://timesketch.org/)
* [Plaso (log2timeline) Documentation](https://plaso.readthedocs.io/en/latest/)
* [How to Perform Root Cause Analysis in Cybersecurity (SANS Whitepaper)](https://www.sans.org/media/score/504-incident-response-cycle.pdf)

**3. Investigation Report & Lessons Learned**

**Topics**

* Writing structured incident reports:
  + Executive summary
  + Technical findings
  + Timeline visualization
  + Recommendations
* Reporting best practices (clarity, completeness, evidence-based)
* Conducting a post-incident review ("hot wash")
* Metrics: MTTR, dwell time, impact cost estimation

**Required Infrastructure & Components**

* Incident report template (PDF or markdown)
* Case notes from simulation
* Peer review worksheet
* Optional: Threat intelligence enrichment (VirusTotal, Shodan, AbuseIPDB)

**To-Dos & Steps**

1. Write a complete incident report based on simulation findings
2. Summarize findings for both technical and non-technical audiences
3. Include visual timeline and evidence snapshots
4. Conduct team retrospective: what worked, what failed
5. Deliver a 5-min team presentation on key takeaways

**Webinars**:

* [SANS Webcast: Writing Effective Incident Reports](https://www.youtube.com/watch?v=vwKlNZ6mxak) – 00:37
* [Security Incident Response](https://www.youtube.com/watch?v=2I1BpZOW4HU) – 00:58

**YouTube**:

* [How to Write a Good Incident Response Report](https://www.youtube.com/watch?v=LXMvHkTDVHE) – 00:04
* [Digital Forensics and Incident Response](https://www.youtube.com/watch?v=9h0UvuRVQTQ) – 00:42

**Reading Material**:

* [SANS Incident Handler’s Handbook](https://dl.icdst.org/pdfs/files3/d60a0c473353813ed1f32c4faefedbd6.pdf) – 20 pages
* [Incident Management Overview](https://www.first.org/resources/papers/aa-dec2021/Incident-Response-Training-Presented-by-SEI-CERTCC-Angel-Slides.pdf)
* [CISA Incident Reporting Guide](https://www.cisa.gov/topics/cyber-threats-and-advisories/information-sharing/cyber-incident-reporting-critical-infrastructure-act-2022-circia)

**Afternoon Lab: TryHackMe or BTLO**

* **TryHackMe: Threat Hunting** → Perform IR on provided systems
* Optional: **BTLO CTF challenges** for real-world blue team exercises
* Combine memory, network & disk forensics with report writing
* Compete in small teams for investigation completeness & accuracy
* [TryHackMe: Threat Hunting Room *(Great for correlating forensic evidence in IR)*](https://tryhackme.com/)
* [TryHackMe: IR and Forensics Challenges *(Hands-on labs for disk, memory, network analysis)*](https://tryhackme.com/)
* [Blue Team Labs Online (BTLO)](https://blueteamlabs.online/) *(Free and premium CTFs focused on real-world blue team skills)*

**🎯 End-of-Day Goal**

Participants should be able to:

* Perform a structured incident analysis from end to end
* Use forensic data to build timelines and identify root cause
* Integrate detection, investigation, and documentation into a coherent response
* Communicate findings clearly in a report and team debrief
* Apply all core skills of IR, forensics, and reporting in a real-world scenario