**Theoretical Knowledge**

**1. Advanced Threat Analysis**

* **What to Learn:**
  + **Core Concepts:** Threat Modeling (using STRIDE), MITRE ATT&CK Framework, Advanced Attack Vectors (APTs, supply chain attacks, zero-day exploits).
  + **Key Objectives:** Model threats, map attacks to the ATT&CK framework, and understand sophisticated attack vectors.
* **How to Learn:**
  + Explore the MITRE ATT&CK website and use the ATT&CK Navigator.
  + Analyze reports on the SolarWinds breach.
  + Create STRIDE-based threat models using OWASP Threat Dragon.
  + Study zero-day exploits via Exploit-DB.

**2. Security Frameworks in Depth**

* **What to Learn:**
  + **Core Concepts:** NIST Cybersecurity Framework (CSF) and its five functions (Identify, Protect, Detect, Respond, Recover). ISO 27001 Controls and their application.
  + **Key Objectives:** Apply security frameworks to real-world scenarios, such as mitigating ransomware.
* **How to Learn:**
  + Review official NIST CSF guides.
  + Explore ISO 27001 checklists and map controls to a ransomware scenario.
  + Cross-reference CIS Controls with NIST CSF to identify overlaps.
  + Analyze the WannaCry ransomware case study.

**3. Incident Response Fundamentals**

* **What to Learn:**
  + **Incident Lifecycle:** Preparation, Detection, Containment, Eradication, Recovery.
  + **Key Components:** The role of playbooks, SOC workflows, and incident prioritization.
* **How to Learn:**
  + Study SANS Institute Incident Response papers.
  + Use Let's Defend for simulated incident response scenarios.

**4. Risk Management Advanced Concepts**

* **What to Learn:**
  + **Concepts:** Quantitative vs. qualitative risk assessment, Business Impact Analysis (BIA).
  + **Key Objectives:** Quantify risks and assess business impacts effectively.
* **How to Learn:**
  + Use FAIR Institute guides for risk quantification.
  + Calculate Annualized Loss Expectancy (ALE) using Google Sheets.

**Practical Application**

**1. Threat Hunting with Open-Source Tools**

* **Activities:**
  + **Tools:** Elastic Security, Security Onion, Sigma Rules.
  + **Task:** Ingest sample logs into Elastic Security and write a Sigma rule to detect suspicious PowerShell activity.
* **Enhanced Tasks:**
  + **Sigma Rule Creation:** Write a Sigma rule to detect PowerShell command execution.
  + **Test with harmless script:** powershell -Command "Write-Host test" in a Windows VM.
  + **Threat Hunting Query:** Query Elastic Security for Event ID 4688 to identify PowerShell events. Document in a Slack-friendly table:

|  |  |  |  |
| --- | --- | --- | --- |
| **Timestamp** | **Process** | **Command Line** | **Notes** |
| 2025-08-18 10:00:00 | powershell.exe | powershell -Command Write-Host | Suspicious execution |

**2. Malware Analysis Basics**

* **Activities:**
  + **Tools:** REMnux, Hybrid Analysis.
  + **Task:** Analyze a benign sample (e.g., calc.exe) in REMnux using strings and peframe.
* **Enhanced Tasks:**
  + **Static Analysis:** Run strings calc.exe > output.txt in REMnux and summarize 3 interesting strings in a 50-word report.
  + **Dynamic Analysis:** Submit calc.exe to Hybrid Analysis and compare behavior reports with REMnux findings.

**3. Build a Vulnerability Management Pipeline**

* **Activities:**
  + **Tools:** OpenVAS, DefectDojo.
  + **Task:** Scan a Metasploitable VM with OpenVAS and import results into DefectDojo.
* **Enhanced Tasks:**
  + **Vulnerability Scan:** Run an OpenVAS scan on Metasploitable2, export results, and import into DefectDojo. Prioritize 3 vulnerabilities.

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **CVSS Score** | **Description** |
| VSFTPD Backdoor | 7.5 | Allows remote access |

* **Remediation Plan:** Propose mitigation steps (e.g., for VSFTPD, patch or disable the service).

**4. Incident Response Simulation**

* **Activities:**
  + **Tools:** Velociraptor, MITRE Caldera.
  + **Task:** Simulate a phishing attack with Caldera and collect artifacts with Velociraptor.
* **Enhanced Tasks:**
  + **Phishing Simulation:** Deploy a mock phishing payload with Caldera on a Windows VM. Document the attack path in a 100-word summary.
  + **Artifact Collection:** Use Velociraptor to collect process and network artifacts (SELECT \* FROM processes; SELECT \* FROM netstat;). Save to CSV and analyze for IOCs.

**5. Network Defense with Open-Source Tools**

* **Activities:**
  + **Tools:** Suricata, Elastic SIEM, CrowdSec.
  + **Task:** Configure Suricata to block malicious IPs and map alerts to MITRE ATT&CK.
* **Enhanced Tasks:**
  + **Suricata Rule:** Create a rule to block a malicious IP (e.g., drop ip 192.168.1.100 any -> any any (msg:"Block Malicious IP"; sid:1000001;)).
  + **Test by pinging** from another VM.
  + **ATT&CK Mapping:** Map a Suricata alert to a MITRE ATT&CK technique.

|  |  |  |  |
| --- | --- | --- | --- |
| **Alert** | **Tactic** | **Technique** | **Notes** |
| Suspicious HTTP | Command and Control | T1071 | Outbound traffic to C2 |

**6. Risk Assessment Practice**

* **Activities:**
  + **Tool:** Google Sheets.
  + **Task:** Calculate ALE for a mock scenario.
* **Enhanced Tasks:**
  + **ALE Calculation:** Calculate ALE for a ransomware scenario (SLE = $10,000, ARO = 0.2) in Google Sheets. Document: ALE = SLE × ARO.
  + **Risk Matrix:** Create a 5x5 risk matrix (Likelihood vs. Impact) and score the ransomware scenario.

**7. Create an Incident Response Report**

* **Activities:**
  + **Tool:** SANS templates.
  + **Task:** Document an incident using SANS templates.
* **Enhanced Tasks:**
  + **Report Draft:** Write a report for a simulated phishing incident, including Executive Summary, Timeline, and Mitigation Steps.
  + **Flowchart Creation:** Diagram of the incident response process (Detection → Containment → Recovery).

**8. Capstone Project: Full Incident Response Cycle**

* **Activities:**
  + **Tools:** Metasploit, Wazuh, CrowdSec, Google Docs.
  + **Task:** Simulate an attack, detect, contain, and report.
* **Advanced Tasks:**
  + **Attack Simulation:** Exploit a Metasploitable2 vulnerability with Metasploit (e.g., vsftpd\_24\_backdoor).
  + **Detection:** Configure Wazuh to alert on the attack. Document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Timestamp** | **Source IP** | **Alert Description** | **MITRE Technique** |
| 2025-08-18 11:00:00 | 192.168.1.100 | VSFTPD exploit | T1190 |

* **Containment:** Block the attacker's IP with CrowdSec and verify with a ping test.
* **Reporting:** Write a 200-word report summarizing the incident, including findings, actions, and recommendations.

**Deadline and Submission**

* **Deadline:** Friday 4:30 PM
* **Submission:** Create a GitHub repository named cyart-red-teaming. In that repo, create a folder named Week 2. Add all documentation (PDFs, notes, screenshots), workflow steps, and code in subfolders or a README file. You will need to submit the Git repository link on Friday.