Cybersecurity Lab Portfolio - Alen Guner

Lab: Ransomware Simulation & Incident Response Report

Objective:

Simulate a ransomware attack in a controlled virtual environment, analyze the behavior, and write a professional incident report including IOCs, impact assessment, and remediation steps.

Tools Used:

- Windows 10 VM (isolated)
- Fake ransomware sample (e.g., from MalwareBazaar or test script)
- Wireshark
- Sysinternals Tools (Process Monitor, Autoruns)
- Optional: Red Canary Atomic Red Team

Steps Taken:

1. Lab Setup:

- Deployed isolated Windows 10 VM with snapshots enabled.
- Disabled internet access to prevent any real-world spread.

2. Ransomware Simulation:

- Executed fake ransomware sample or Red Canary simulation script.
- Observed file encryption, ransom note creation, and file renaming patterns.

3. IOC Collection:

- Used Process Monitor and Autoruns to track registry keys, new processes, and file activity.
- Captured hashes of modified/encrypted files and memory strings from the ransom note.

4. Network Monitoring:

- Used Wireshark to monitor for potential C2 communication attempts.
- Identified spikes in traffic and DNS lookups triggered by ransomware.

5. Reporting:

- Compiled full incident timeline: execution -> encryption -> ransom demand.
- Created an incident response report including containment and remediation steps.

Outcome / What I Learned:

- Simulated ransomware behavior safely in a controlled environment.
- Identified IOCs including ransom notes, file extensions, and encryption activity.
- Developed practical experience in IR documentation and analysis tools.
- Built a reusable IR report template for future malware incidents.

Keywords:

Cybersecurity Lab Portfolio - Alen Guner

Ransomware, Incident Response, IOCs, Windows VM, Wireshark, Sysinternals, Atomic Red Team, IR Report, Malware Analysis