AbdelRahman Mohamed Hassan

Junior Cyber Security Specialist

AbdelrahmanMHasssan@gmail.com 01098857028 Cairo, Egypt

SUMMARY

I am a passionate Junior Cyber Security professional with hands-on experience in Incident Response and Threat Hunting. I specialize in tracking down attackers by analyzing network traffic, Windows event logs, and memory dumps. I am eager to bring my investigative mindset, solid foundation in TCP/IP, and practical triage skills to a fast-paced SOC team.

PROJECTS

Enterprise Incident Response Capstone

- *Reconstructed a complete APT killchain across Network, RAM, Disk, and Event Logs.*
- *Proved in-memory credential theft (LSASS dumping) by tracking Sysmon Event ID 10.*
- *Detected rootkit persistence by parsing offline SYSTEM registry hives for malicious boot-start drivers*

Endpoint Forensics & Threat Hunting Scenarios

- Tracked attacker lateral movement and data exfiltration using Prefetch, Shellbags, and LNK analysis.
- Mathematically proved deliberate timestomping by correlating NTFS $MFT timestamp discrepancies.
- Hunted advanced fileless malware by dissecting Sysmon IDs 19-21 to uncover encoded PowerShell payloads hiding in WMI.

Memory & Network Forensics

- Utilized Volatility to extract injected code, VAD hooks, and hidden DLLs from raw memory dumps (e.g., Stuxnet triage).
- Conducted PCAP analysis using Wireshark to isolate malware beacons and extract malicious payloads from HTTP streams

Biometric Employee Access Scanner

Developed a biometric attendance/access prototype connecting hardware flow with software tracking.

TECHNICAL SKILLS

Endpoint Forensics
NTFS $MFT, Prefetch, Shellbags, LNK Jumplists

Threat Hunting
Sysmon, Hayabusa, Event Log Triage

Malware Tactics
WMI Persistence, Registry Hives, Timestomping Detection

Memory & Network
Sysmon, Hayabusa, Event Log Triage

DFIR Tooling
KAPE, Eric Zimmerman Tools (EZTools), Timeline Explorer

EDUCATION

Higher Technological Institute (HTI) | Computer Science - In Progress