Skillmine
Technology • Consulting • Services

Approach Paper

Enterprise Incident Response

Skillmine Technology Consulting Pvt Ltd

Enterprise Incident Response

Attacks against computer systems are increasing in frequency and sophistication. In order to effectively defend data and intellectual property, organizations must have the ability to rapidly detect and respond to threats.

The below paper is an outline to the approach envisaged by Skillmine to suggest basic investigative techniques needed to respond to varied landscape of threat actors and intrusion scenarios. This is updated on a yearly basis to reflect the latest in forensics and intrusion techniques. The premise is to keep in mind, how to conduct rapid triage on a system to determine if it is compromised, uncover evidence of initial attack vectors, recognize persistence mechanisms, develop indicators of compromise to further scope an incident etc.

Process Overview:

- ✓ Detection and Analysis Identify mechanisms to detect threats, prioritizing and categorizing leads, the need to fully scope targeted attacks and methods to proactively hunt for signs of compromise
- ✓ Remediation The goal of remediation, when remediation is necessary, planning for remediation, and executing a remediation event
- ✓ Acquiring Forensic Evidence Most common forms of endpoint forensic evidence collection and different types of forensic imaging and file system access
- ✓ Live Response Acquisition Live data collection, the key evidence typically acquired during this process, guidelines for forensically sound acquisition, Explore any tools being used

Process Flow:

1. Windows Evidence

Investigate a compromised Windows system, including the NTFS file system, Prefetch, web browser history, event logs, the registry, memory etc

a. Prefetch Prefetch files can capture evidence of previously-executed applications and additional metadata

b. File System Analysis The behaviour of the NTFS file system and its key artefacts, including the Master File Table, timestamp behaviour, alternate data streams, recovery of deleted data, and directory index attributes

c. The Registry Acquire and parse its artefacts to analyse system & user specific evidence it contains

d. Event Logs Analysis of core system, security, and application event logs, as well as the Application and Services logs etc.

e. Memory Analysis Analyse basic sources of evidence in memory, including processes, handles, and memory sections; attack scenarios that typically require memory analysis, such as recovery of command history, process injection, and rootkit behaviour etc.

2. Persistence

a. Common Persistence Mechanisms Leverage Windows Services for persistence

b. Advanced Persistence Mechanisms DLL search order hijacking and binary modification

c. Alternative Remote Access Techniques Such as VPN compromise and web shells

3. Investigating Lateral Movement

Analysis of unwanted movement in a compromised Windows environment, the distinctions between network logons and interactive access, and the resulting sources of evidence on disk, in logs, and in the registry.

a. Reconnaissance Enumeration of domains, users, systems, shares, and other information in a Windows environment

b. Windows Credentials Understanding various forms of password attacks, including pass-the-hash and in-memory cleartext password recovery

c. Logon Events Analyse unwanted movement through system logs

d. Remote Command Execution Tracing remote execution

e. Interactive Session Artefacts File system and registry-based sources of evidence resulting from interactive / GUI access to a Windows system, including ShellBags, LNK files, and MRU keys

4. Hunting

Proactively investigate an entire environment for signs of compromise. Explore Task Scheduler, event log entries, Shim Cache and Windows Services. Techniques for efficient searching, stacking, and data reduction etc.

5. Investigating Web Application Attacks

Analyse web logs to recognize and interpret common attack techniques

a. Web Logs Common web log paths, GET vs. POST, content encoding and HTTP response codes.

b. Common Web Attacks Analysis of the log entries and evidence resulting from SQL injection and web shell attacks.

c. Obfuscation & Encoding Understand disguise of web attacks to evade automated security controls and inhibit log analysis

d. Log Analysis

Private and Confidential – If you are not an intended recipient of this document. Please immediately delete this document from your computer or any other electronic device if you are using an electronic copy and/or please immediately trash this document if you are using a printed copy.