https://certifications.tcm-sec.com/

TCM SECURITY

MUST-HAVE TOOLS FOR SOC ANALYSTS

Andrew Prince

TCM Blue Team Expert

Based off a blog post by Andrew Prince, the creator of the **Practical SOC Analyst Associate (PSAA) cert** and the **SOC 101** and soon to be released **SOC 201** course.

Find the blog post here: https://tcm-sec.com/soc-analyst-tools/

Get certified here: https://certifications.tcm-sec.com/psaa/

Try the course: https://academy.tcm-sec.com/p/security-operations-soc-101

NETWORK TRAFFIC TOOLS

SOC analysts require visibility into the traffic flowing into the networks they're responsible for; network artifacts and evidence found within packet captures provide the SOC with valuable insights into network activity and help answer investigative questions related to traffic patterns, anomalies, and potential indicators of compromise.

To analyze network traffic, we need to capture it first. That's where **Network Traffic Tools** enter the picture. These tools capture raw network traffic and subsequently write it to disk, often in the form of PCAP (packet capture) files. These files contain a detailed record of the packets transmitted over the network.

NETWORK TRAFFIC TOOLS

Some popular **network traffic** tools include:

Tcpdump

This is a popular command-line tool that captures network packets in real time. It’s lightweight, ubiquitous (as it’s found on most systems), and can handle very high network throughput. It also allows for filtering and capturing only the traffic of interest, making it useful for high-traffic environments.

Wireshark

Wireshark is a more graphic-based and feature-rich tool that allows users to capture and analyze packets in great detail. While it is not as lightweight as tcpdump (and unsuitable for high throughput environments), its user-friendly interface makes it one of the most popular choices for network traffic-related tasks. However, rather than traffic *acquisition*, it’s more often used for in-depth *inspection* of individual packets, conversations, and protocols.

NETWORK TRAFFIC ANALYSIS TOOLS

Network traffic analysis tools help analysts sift through large amounts of acquired traffic data to identify interesting artifacts, summarize statistics, or dig into protocols and packet data. Additionally, these tools often allow for deep inspection and correlation of network traffic, which can be a very useful way to retrace an attack timeline.

NETWORK TRAFFIC ANALYSIS TOOLS

Popular **network traffic analysis** tools include:

Wireshark, again!

This is one of the most widely used network protocol analyzers. It provides a graphical interface and several statistical features for analyzing network packets, conversations, and packet contents in detail.

Zeek (formerly Bro)

Unlike packet-based tools like Wireshark, Zeek focuses on analyzing high-level network events, including traffic flow, DNS queries, and HTTP requests. It's great for identifying patterns in traffic flows that can also be used as a network intrusion detection system.

NETWORK DETECTION TOOLS

Network detection tools focus on identifying and flagging suspicious or malicious behavior based on traffic patterns and flow data. Having and maintaining a network detection solution is an important part of a SOC’s monitoring capability, as it allows for real-time identification of potential intrusions.

Popular **network detection tools** include:

Snort

Snort is an open-source intrusion detection system (IDS) that can also function as an intrusion prevention system (IPS). It analyzes network traffic in real time and matches it against a configurable signature database to identify known attack patterns.

NETWORK DETECTION TOOLS

Suricata

Suricata is an additional network IDS/IPS that can perform real-time traffic analysis and intrusion detection. Like Snort, it matches network traffic to known attack signatures and offers additional advanced features such as multi-threading and flow capture.

Real Intelligence Threat Analytics (RITA)

Developed by Active Countermeasures, RITA is an open-source framework for network traffic analysis that can ingest Zeek logs directly, with a specialized focus on detecting command and control (C2) communication.

SYSTEMS-RELATED EVIDENCE

A complement to network visibility is system-related evidence, which is a broad category of data that provides important context for investigations and is often necessary to uncover the full scope of an attack timeline. This category of evidence includes operating system logs, authentication logs, and various other system-level artifacts that give us insight into what's happening on individual endpoints within the network.

Windows Event Logs

These capture a wide range of system activities and security events on Windows endpoints. By analyzing the security event logs, for example, analysts can piece together timeline events that may confirm or deny unauthorized access attempts, group membership additions, privilege escalations, or other unusual system behaviors that warrant further investigation.

SYSTEMS-RELATED EVIDENCE

Sysmon Logs

Sysmon enhances the verbosity of system monitoring. With a good Sysmon configuration, we can gain access to much more detailed visibility into the happenings on a Windows system, specifically around process creations, network connections, API calls, and changes to file creation timestamps. Sysmon configurations and exclusions are highly customizable and provide SOCs invaluable evidence for tracking an attacker's actions within an environment.

Given the volume of logs and events generated across all of an organization's systems (especially when using a monitoring utility like Sysmon), it's important to centralize log collection and analysis for proper monitoring, scalability, and availability. Security Information and Event Management (SIEM) systems allow teams to aggregate, store, and correlate these logs from various sources and give analysts a central view of the organization's events as they occur.

SYSTEMS-RELATED EVIDENCE

Many system utilities have been developed that aid forensic investigations and threat hunting, as they help analysts gain detailed insights into the behavior, state, and configuration of a system. Analysts should know how to effectively use these tools to interpret the data they provide in the context of security incidents.

Sysinternals Suite

The Sysinternals Suite is a powerful collection of system utilities developed by Microsoft, often used to investigate and analyze Windows-based systems. Various tools from this suite can provide us with real-time insights into system activity, processes, file systems, registry changes, and network activity. Check out the examples on the next page.

SYSTEMS-RELATED EVIDENCE

Process Explorer

This tool provides detailed information about running processes, including their memory usage, handles, and associated binaries. It is useful for identifying suspicious or unknown processes running on a system, identifying process parent-child relationships, and correlating them to additional activity occurring over the network.

Autoruns

Oftentimes, attackers will implant persistence mechanisms on compromised systems to maintain access or continue executing malware after initial detection. The Autoruns utility effectively identifies what programs are set to run automatically when a system starts through common registry locations, services, scheduled tasks, and more. The baseline detection capabilities can hint at potential persistence mechanisms or malicious configurations that aren’t usually present and warrant further investigation.

DISK-RELATED EVIDENCE

Effective SOC Analysts should be comfortable with collecting and analyzing disk-related artifacts for incident investigations. Disk-based evidence gives us much more endpoint-level visibility and can provide deeper insights into indicators of malicious activity on individual systems.

Although, in some cases, this type of acquisition and analysis would be performed by specialized forensic analysts or incident responders, SOC Analysts should still have a foundational understanding of disk-related evidence and the tools necessary to collect, preserve, and analyze this data.

DISK IMAGE ACQUISTION TOOLS

Popular **disk image acquisition** tools include:

FTK Imager

FTK Imager is one of the most commonly used acquisition tools in forensic investigations. It creates exact disk images in a forensically sound manner, supports different formats, and captures the data without altering the original media. It also provides capabilities for previewing files, carving deleted data, and generating hashes for verifying integrity.

dd

dd is a command-line tool widely used in Unix-based environments that allows for raw disk cloning. dd is often used in incident response scenarios due to its lightweight nature and ability to perform raw cloning at scale. However, it comes with fewer safeguards compared to more specialized tools like FTK Imager.

DISK IMAGE ANALYSIS TOOLS

After acquiring a disk image, the next step is analysis. Disk analysis tools allow us to examine the contents of the disk image, potentially recover deleted files, analyze metadata, and identify leftover artifacts of compromise.

For example, Autopsy is a digital forensics utility that provides comprehensive disk analysis capabilities. It supports the examination of file systems, extraction of deleted files, and examination of system artifacts such as event logs, browser history, and registry entries.

LIVE TRIAGE TOOLS

In some cases, evidence data needs to be acquired from live systems instead of, or in addition to, disk images. Live triage tools enable the quick collection of artifacts from systems that are still running. These tools allow analysts to prioritize and triage key evidence to gain immediate insights into suspicious activity while a full disk image is being created.

For example, KAPE (Kroll Artifact Parser and Extractor) is a quick utility for collecting key artifacts from live systems, enabling analysts to quickly gather important data such as event logs, browser history, and system configuration files. KAPE is extremely customizable, Allowing it to be adapted for various types of incident data collection.

MEMORY-RELATED EVIDENCE

Memory-related evidence also plays an increasing role in modern incident response and forensic investigations. Volatile memory, or RAM, contains artifacts about the state of a system at any given time, including running processes, open network connections, user activity, volatile configurations, and more. Unlike persistent disk-based evidence, which typically remains on a system even after a reboot, memory evidence is often lost once a system is powered off.

Similar to disk-based forensic artifacts, specialized memory forensics might fall under the purview of incident responders or forensic teams. However, SOC Analysts should still understand how to extract and leverage memory artifacts as part of their broader investigative toolkit. It’s important to remember that while many other tools or evidence sources can often answer investigative questions quicker than memory-related evidence can, some questions can only be answered through memory analysis.

MEMORY ACQUISITION TOOLS

While far from an exhaustive list, some popular memory acquisition tools include:

WinPMEM

As the name suggests, WinPMEM is a widely used tool for acquiring live memory on Windows systems. As with all memory capture tools, it creates a memory dump file, which can be analyzed later to identify artifacts related to processes, network activity, and other evidence, all of which are handy when building an attack timeline.

https://certifications.tcm-sec.com/

TCM SECURITY

MEMORY ACQUISITION TOOLS

FTK Imager

While primarily known for its disk imaging capabilities, FTK Imager also has memory acquisition functionality. It can capture memory from live Windows systems and save the data in a forensically sound way.

LiME (Linux Memory Extractor)

For Linux-based systems, LiME is a popular tool for acquiring memory images. It supports both full and partial memory captures.

MEMORY ACQUISITION TOOLS

LiME (Linux Memory Extractor)

For Linux-based systems, LiME is a popular tool for acquiring memory images. It supports both full and partial memory captures.

MEMORY ANALYSIS TOOLS

Once memory has been acquired, it can be analyzed for relevant evidence of malicious activity, baseline anomalies, or other indicators of compromise similar to disk images.

Popular memory analysis tools are included on the next page.

https://certifications.tcm-sec.com/

MEMORY ANALYSIS TOOLS

Volatility

Volatility is, by far, one of the most widely used open-source memory forensics frameworks. It allows analysts to perform deep analysis of previously captured memory dumps. Through a large repository of prebuilt and user-created plugins, Volatility allows analysts to extract detailed information about running processes, network connections, registry configurations, open files and binaries, loaded drivers, and much more.

https://certifications.tcm-sec.com/

MEMORY ANALYSIS TOOLS

Rekall

Similar to Volatility, Rekall is another powerful command-line tool for examining the contents of memory dumps. Rekall also supports a variety of investigative features, including process and network enumeration, file system analysis, and more. Choosing between these tools often comes down to personal preference.

Redline

Developed by FireEye, Redline is a GUI-based memory and host forensic tool that can analyze memory dumps, disk images, and system information.

THREAT INTELLIGENCE-RELATED EVIDENCE

Lastly, the most effective evidence sources aren't limited to only what is inside our networks. Threat intelligence-related evidence is extremely useful in helping SOC Analysts detect, investigate, and better understand threats by providing context on the nature of the attack. Threat intelligence includes information about the tactics, techniques, and procedures (TTPs) used by attackers, as well as data about indicators of compromise (IOCs) from documented attacks, such as IP addresses, domains, URLs, and email addresses.

Often, this intelligence comes in the form of threat intelligence feeds, which need to be sourced, collected, and integrated into the SOC's current tooling. However, analysts often use reputation and aggregation tools ad-hoc to verify if certain indicators are associated with malicious activities during investigations.

REPUTATION TOOLS

One of the most crucial aspects of threat intelligence is understanding the reputation of certain entities within the network. Reputation tools help assess the trustworthiness of file or network elements, such as domains, IP addresses, URLs, and email addresses by checking their historical involvement in malicious activity.
Some **popular reputation tools** include:

VirusTotal

As essentially the Swiss army knife for any analyst, VirusTotal is a widely used tool that aggregates results from multiple antivirus engines and scanning tools to analyze files, URLs, and IP addresses for potential threats. It helps analysts quickly assess the disposition of a given file, hash value, or link by providing a comprehensive report of how different security vendors classify it.

https://certifications.tcm-sec.com/

REPUTATION TOOLS

Cisco Talos

In a similar realm, Cisco Talos is a leading provider of threat intelligence that offers insights into domains, IP addresses, URLs, and other indicators of compromise (IOCs).

DomainTools

DomainTools is a powerful tool for domain and IP address research. It provides historical and real-time data about domain ownership, registration details, and network associations, which can help analysts uncover suspicious activity or malicious dispositions tied to specific domains or IP addresses.

MxToolbox

MxToolbox offers a range of network and email diagnostic tools, including checks for DNS records, blacklists, and email headers. It is commonly used for investigating suspicious domains, email activity, and verifying if an entity is listed on blacklists.

URLScan

URLScan is a tool that scans and analyzes URLs to assess their security risk. It is commonly used to identify malicious websites, phishing attempts, and suspicious links.