FOR577: **LINUX Incident Response and Threat Hunting™**

6 Day Program	36 CPEs	Laptop Required

You Will Be Able To

- Use the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries and to remediate incidents
- Hunt through and perform incident response on Linux systems using the SIFT Workstation
- Identify and track malware beaconing outbound to its command and control (C2) channel via analytical techniques.
- Determine how the breach occurred by identifying the beachhead and spear phishing attack mechanisms
- Track user and attacker activity second-by-second on the system you are analyzing through in-depth timeline and super-timeline analysis
- Identify lateral movement and pivots within your enterprise, showing how attackers transition from system to system without detection.
- Track data movement as the attackers collect critical data and shift those data to exfiltration collection points
- Recover and analyze archives and archive files (.rar, .tar, etc.) used by APT-like attackers to exfiltrate sensitive data from the enterprise network
- Use collected data to perform effective remediation across the entire enterprise.

Course Topics

- Advanced use of a wide range of best-of-breed open-source tools in the SIFT Workstation to perform incident response and digital forensics
- Hunting and responding to advanced adversaries such as nation-state actors, organized crime, and hacktivists
- Threat hunting techniques that will aid in quicker identification of breaches
- Rapid incident response analysis and breach assessment
- An incident response and intrusion forensics methodology
- Evidence collection, including disk and memory, during incident response and threat hunting
- Internal lateral movement analysis and detection
- Rapid and deep-dive timeline creation and analysis
- Adversary threat intelligence development, indicators of compromise, and usage
- Cyber-kill chain strategies
- Step-by-step tactics and procedures to respond to and investigate intrusion cases

FOR577: Linux Threat Hunting & Incident Response provides responders and threat hunting teams with advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including advanced persistent threat (APT) nation-state adversaries, organized crime syndicates, and hactivism. Constantly updated, the course addresses today's incidents by teaching the hands-on incident response and threat hunting tactics and techniques that elite responders and hunters are successfully using to combat real-world breach cases.

FOR577 teaches the skills needed to identify, analyze, and respond to attacks on Linux platforms and how to use threat hunting techniques to find the stealthy attackers who can bypass existing controls. The concepts taught are built on common foundations in that we gather evidence, analyze it, and make decisions based on this analysis, all the while focusing on the specifics of the Linux platform. By using the tools built into the SANS SIFT Workstation, the course provides an all-inclusive solution that enables responders to quickly and effectively react to sophisticated intrusions.

During the course you will work through a number of exercises culminating in a final capstone, challenge built around a realistic attack with endpoint evidence, log data, and other artifacts you will encounter during day-to-day incident response activities. You will uncover evidence of an advanced threat actor working through a multiple-phase attack, going from reconnaissance to initial intrusion, then moving laterally throughout the organization's network. During the capstone you will bring together everything you have learned during the course and present your findings and recommendations on how security can be improved.

Business Takeaways

- Understand attacker tradecraft in order to perform proactive compromise assessments
- Upgrade detection capabilities by having a better understanding of novel attack techniques and available forensic artifacts, and by focusing on critical attack paths
- Develop threat intelligence to track targeted adversaries and prepare for future intrusion events
- Build advanced forensics skills to counter anti-forensics and data hiding from technical subjects for use in both internal and external investigations

Author Statement

"Linux is a mainstream operating system found in almost every enterprise. It is used to host critical services and store sensitive personal and financial data, and it powers the underlying infrastructure we use on a day-to-day basis, making it a high-value target for our adversaries. Additionally, there is often a perception that Linux is 'more secure' than other operating systems, which results in less thorough security tool coverage. These two elements combine to make Linux intrusions both increasingly common and harder for our Security Operations Center/Incident Response teams to fully respond to. In one recent incident, attackers installed a persistence mechanism in a company's firewall that remained undiscovered during Windows-focused response and remediation activities.

"All cybersecurity defenders need to have the knowledge to deal with attacks on every platform in our environments. This means it is essential to understand how to collect and analyze digital evidence from Linux systems to determine the extent of the damage and identify the root cause of an incident. By analyzing the digital evidence, defenders can identify indicators of compromise and determine the tools, techniques, and processes used by the attacker. This information can be used to develop countermeasures and prevent similar attacks from occurring in the future."

—Taz Wake

Section Descriptions

SECTION 1: LINUX Incident Response and Analysis

Incident responders and threat hunters should be armed with the latest tools, techniques, and processes (TTPs) to identify, track, and contain advanced adversaries and to remediate incidents. It is important that our DFIR knowledge includes our own TTPs and those used by our adversaries. Section 1 introduces the fundamentals of incident response and then looks at the specific needs to carry out our duties in a Linux environment. The section starts by examining the reasons why we need incident response and presents SANS' six-step incident response methodology as it applies to an enterprise's response to a targeted attack. This section will also introduce the Stark Skunkworks intrusion scenario, which sets the stage for our lab exercises and capstone challenge. This is followed by looking at how, as incident responders, we can use the Linux command line to our advantage and analyze common activity such as installing specific software packages. We finish the section by looking at the importance of developing cyber threat intelligence to impact the adversaries' kill chain. We'll demonstrate forensic live response techniques and tactics that can be applied both to single systems and across the entire enterprise.

TOPICS: Why Incident Response is Needed; The Incident Response Process; SRL Skunkworks; Introduction to Linux; Package Management; Threat Intelligence and Host-based Threat Hunting

SECTION 2: Disk Analysis and Evidence Collection

Disk evidence collection and analysis skills are crucial for incident responders, forensic investigators, and threat hunters because they allow for identifying the source and scope of a security breach. Digital forensic experts need to collect and preserve data from disk storage devices such as hard drives, solid-state drives, and USB drives in order to determine how an attack occurred, what data was accessed or stolen, and who was responsible. Without this critical evidence, it is challenging to reconstruct the events leading up to the breach and determine the necessary steps to prevent similar incidents from happening in the future. Moreover, disk analysis skills help responders and investigators identify the type of malware or malicious code used in the attack. This information is essential to determine the tactics, techniques, and procedures used by the attackers and their motivations. By analyzing the data stored on disks, responders and investigators can identify suspicious files, unusual network traffic patterns, and other indicators of compromise. They can then use this information to develop countermeasures to mitigate the risk of further attacks.

TOPICS: The Sleuth Kit; Linux File Systems; Disk Evidence Collection; Image Mounting; Operating System File Structures; File System Artifacts

Who Should Attend

- Incident response team members
- Threat hunters
- Experienced digital forensic analysts
- Experienced security operations center analysts
- Information security professionals
- Federal agents and law enforcement professionals
- Red Team members
- Penetration testers
- Exploit developers
- SANS SEC401, SEC450, SEC504 and SEC500 graduates looking to take their skills to the next level
- SANS SEC508 graduates looking to learn how to adapt their skills to a different operating system

SECTION 3: LINUX Logging and Log Analysis

Section 3 looks at how to use the data logged by the operating system to profile the device and analyze boot sequences, kernel activity, logins and user events. The section covers default log data, Auditd (although this isn't enabled by default on all Linux distros, you should definitely consider turning it on) and the Operating System Journal. Log data is a fundamental evidence source for incident response and threat hunting. It allows investigators to understand what happened and when it happened. Using built-in capabilities, we can peel back the actions of our adversaries and, with well-configured logging, make it almost impossible for an attacker to completely hide from our investigation. Unfortunately, Linux logging can be significantly different from what we are used to—especially if we have come from a Windows DFIR background. Significant issues faced by investigators include the different ways Linux distro's log data and a mix between UTC and local timestamps. This section will look at strategies you can implement to manage and mitigate these issues.

TOPICS: Device Profiling; Linux Logs; Auditd; The Operating System Journal

SECTION 4: Live Response and Volatile Data

Section 4 expands on the knowledge we have built so far and introduces tools and techniques to respond to intrusions in larger enterprises. The section starts by looking at how to scale your response and some of the tools that can assist with this. This topic is then developed further as we move into Endpoint Detection and Response (EDR) solutions for the Linux environment and introduce two alternatives to expensive commercial EDR tools—OSSEC and Velociraptor. We'll cover how to configure and deploy both tools, enabling you to make sure that all your Linux devices have good quality monitoring and response capabilities. Finally, this section looks at Linux memory structures and how to collect volatile data for analysis. Given that this can be a complex process, and that analytical tools today are still not what they should be, we also look at using live response techniques to view this data on a target system. This has the added benefit of being something we can leverage through EDR tools, reducing the time and bandwidth required to capture memory from systems where the installed RAM could be running in the hundreds of gigabytes.

TOPICS: Enterprise Response; Endpoint Deteciton and Response (EDR); Linux Memory and DFIR; Live Memory Analysis

SECTION 5: Advanced Incident Response Techniques

This course section builds on the previous sections by looking at how we can use our increased knowledge to enhance our incident response work. We start by looking at triage, which is essential for any modern incident response, especially in large enterprises. We introduce the concept of rapidly assessing systems to make quick decisions about which devices need further investigation. This approach allows us to quickly work through large environments and focus our investigative efforts where they provide maximum value. We'll also look at freely available tools that help facilitate triage and improve response times. The section then moves to looking at timeline generation. Timelines are arguably an incident responder's superpower, allowing you to uncover some of the deepest secrets about an attack. We will look at two basic methods for building timelines and how to analyze them effectively. Once we understand the timelines, we will look at how attackers try to defeat them, then examine the most common anti-forensic techniques and how incident responders can minimize their impact on the investigation. We close the section with a broad discussion on how to make incident response in Linux better.

TOPICS: Triage and DFIR Tools; Timelines; Anti-Forensics; Improving Incident Response

SECTION 6: The APT Incident Response Challenge

This incredibly rich and realistic Intrusion Forensic Challenge is based on a real-world advanced persistent threat (APT) group. It brings together techniques learned throughout the course and tests your newly acquired skills in a case that simulates an attack by an advanced adversary. The challenge is based on a real intrusion into a Linux enterprise environment. You will be asked to uncover how the systems were compromised in the initial intrusion, find other systems the adversary moved to laterally, and identify intellectual property stolen via data exfiltration. This capstone exercise will enable you to leave the course with hands-on experience investigating realistic attacks, curated by a cadre of instructors with decades of experience fighting advanced threats from attackers ranging from nation-states to financial crime syndicates and hactivist groups.

TOPICS: Work in incident response teams to analyze multiple systems in an enterprise network; Learn to identify and track attacker actions across a multi-device environment finding initial exploitation, reconnaissance, persistence, privilege escalation, lateral movement, and data theft/exfiltration; Witness and participate in a team-based approach to incident response; Discover evidence of some of the most common and sophisticated attacks in the wild, including custom nation-state malware; Each team will be asked to answer key questions, just as they would during a real breach in their organizations, in critical areas