FOR572: Advanced Network Forensics: Threat Hunting, Analysis, and Incident Response

GNFA
Network Forensic Analyst
giac.org/gnfa

6 Day Program | 36 CPEs | Laptop Required

You Will Be Able To

- Extract files from network packet captures and proxy cache files, allowing follow-on malware analysis or definitive data loss determinations
- Use historical NetFlow data to identify relevant past network occurrences, allowing accurate incident scoping
- Reverse engineer custom network protocols to identify an attacker's command-and-control abilities and actions
- Decrypt captured SSL/TLS traffic to identify attackers' actions and what data they extracted from the victim
- Use data from typical network protocols to increase the fidelity of the investigation's findings
- Identify opportunities to collect additional evidence based on the existing systems and platforms within a network architecture
- Examine traffic using common network protocols to identify patterns of activity or specific actions that warrant further investigation
- Incorporate log data into a comprehensive analytic process, filling knowledge gaps that may be far in the past
- Learn how attackers leverage meddler-in-the-middle tools to intercept seemingly secure communications
- Examine proprietary network protocols to determine what actions occurred on the endpoint systems
- Analyze wireless network traffic to find evidence of malicious activity
- Learn how to modify configuration on typical network devices such as firewalls and intrusion detection systems to increase the intelligence value of their logs and alerts during an investigation
- Apply the knowledge you acquire during the week in a full-day capstone lab, modeled after real-world nation-state intrusions and threat actors

Take your system-based forensic knowledge onto the wire. Incorporate network evidence into your investigations, provide better findings, and get the job done faster.

It is exceedingly rare to work any forensic investigation that doesn't have a network component. Endpoint forensics will always be a critical and foundational skill for this career but overlooking their network communications is akin to ignoring security camera footage of a crime as it was committed. Whether you handle an intrusion incident, data theft case, employee misuse scenario, or are engaged in proactive adversary discovery, the network often provides an unparalleled view of the incident. Its evidence can provide the proof necessary to show intent, uncover attackers that have been active for months or longer, or may even prove useful in definitively proving a crime actually occurred.

FOR572 was designed to cover the most critical skills needed for the increased focus on network communications and artifacts in today's investigative work, including numerous use cases. Many investigative teams are incorporating proactive threat hunting to their skills, in which existing evidence is used with newly-acquired threat intelligence to uncover evidence of previously-unidentified incidents. Others focus on post-incident investigations and reporting. Still others engage with an adversary in real time, seeking to contain and eradicate the attacker from the victim's environment. In these situations and more, the artifacts left behind from attackers' communications can provide an invaluable view into their intent, capabilities, successes, and failures.

In FOR572, we focus on the knowledge necessary to examine and characterize communications that have occurred in the past or continue to occur. Even if the most skilled remote attacker compromised a system with an undetectable exploit, the system still has to communicate over the network. Without command-and-control and data extraction channels, the value of a compromised computer system drops to almost zero. Put another way: Bad guys are talking – we'll teach you to listen.

This course covers the tools, technology, and processes required to integrate network evidence sources into your investigations, with a focus on efficiency and effectiveness. You will leave this week with a well-stocked toolbox and the knowledge to use it on your first day back on the job. We will cover the full spectrum of network evidence, including high--evel NetFlow analysis, low-level pcap-based dissection, ancillary network log examination, and more. We cover how to leverage existing infrastructure devices that may contain months or years of valuable evidence as well as how to place new collection platforms while an incident is underway.

Whether you are a consultant responding to a client's site, a law enforcement professional assisting cybercrime victims and seeking prosecution of those responsible, an on-staff forensic practitioner, or a member of the growing ranks of threat hunters, this course offers hands-on experience with real-world scenarios that will help take your work to the next level. Previous SANS SEC curriculum students and other network defenders will benefit from the FOR572 perspective on security operations as they take on more incident response and investigative responsibilities. SANS DFIR alumni can take their existing operating system or device knowledge and apply it directly to the network-based attacks that occur daily. In FOR572, we solve the same caliber of real-world problems without the use of disk or memory images.

FOR572 is an advanced course – we hit the ground running on day one. Bring your entire bag of skills: forensic techniques and methodologies, full-stack networking knowledge (from the wire all the way up to user-facing services), Linux shell utilities, and everything in between. They will all benefit you throughout the course material as you FIGHT CRIME. UNRAVEL INCIDENTS...ONE BYTE (OR PACKET) AT A TIME

Section Descriptions

SECTION 1: Off the Disk and Onto the Wire

Today you will learn how to apply what you already know about digital forensics and incident response to network-based evidence. You will also become acclimated to the basic tools of the trade. The Linux SIFT Workstation virtual machine, which has been loaded with network forensic tools, will be your primary toolkit for the week.

TOPICS: Web Proxy Server Examination; Foundational Network Forensics Tools: tcpdump and Wireshark; Network Evidence Acquisition; Network Architectural Challenges and Opportunities

"First course I've taken that gives insight into the forensic mindset required for investigating incidents."

— Tyler Whittington, **PWC**

SECTION 2: Core Protocols and Log Aggregation/Analysis

There are countless network protocols that may be in use in a production network environment. We will cover those that are most likely to benefit the forensicator in typical casework, as well as several that help demonstrate analysis methods useful when facing new, undocumented, or proprietary protocols. By learning the "typical" behaviors of these protocols, we can more readily identify anomalies that may suggest misuse of the protocol for nefarious purposes. These protocol artifacts and anomalies can be profiled through direct traffic analysis as well as through the log evidence created by systems that have control or visibility of that traffic. While this affords the investigator with vast opportunities to analyze the network traffic, efficient analysis of large quantities of source data generally requires tools and methods designed to scale.

TOPICS: Hypertext Transfer Protocol Part 1: Protocol; Hypertext Transfer Protocol Part 2: Logs; Domain Name Service (DNS): Protocol and Logs; Forensic Network Security Monitoring; Logging Protocol and Aggregation; Syslog; Microsoft Eventing; Log Data Collection, Aggregation, and Analysis; Elastic Stack and the SOF-ELK Platform; Basics and Pros/Cons of the Elastic Stack; SOF-ELK

SECTION 3: NetFlow and File Access Protocols

Network connection logging, commonly called NetFlow, may be the single most valuable source of evidence in network investigations. Many organizations have extensive archives of flow data due to its minimal storage requirements. Since NetFlow does not capture any content of the transmission, many legal issues with long-term retention are mitigated. Even without content, NetFlow provides an excellent means of guiding an investigation and characterizing an adversary's activities from pre-attack through operations. Whether within a victim's environment or for data exfiltration, adversaries must move their quarry around through the use of various file access protocols. By knowing some of the more common file access and transfer protocols, a forensicator can quickly identify an attacker's theft actions.

TOPICS: NetFlow Collection and Analysis; Open-Source Flow Tools; File Transfer Protocol; Microsoft Protocols

SECTION 4: Commercial Tools, Wireless, and Full-Packet Hunting

Commercial tools are a mainstay in the network forensicator's toolkit. We'll explore the various roles that commercial tools generally fill, as well as how they can be best integrated into an investigative workflow. With the runaway adoption of wireless networking, investigators must also be prepared to address the unique challenges this technology brings to the table. However, regardless of the protocol being examined or budget used to perform the analysis, having a means of exploring full-packet capture is a necessity, and having a toolkit to perform this at scale is critical.

TOPICS: Simple Mail Transfer Protocol; Object Extraction with NetworkMiner; Wireless Network Forensics; Automated Tools and Libraries; Full-Packet Hunting with Moloch

SECTION 5: Encryption, Protocol Reversing, OPSEC, and Intel

Advancements in common technology have made it easier to be a bad guy and harder for us to track them. Strong encryption methods are readily available and custom protocols are easy to develop and employ. Despite this, there are still weaknesses even in the most advanced adversaries' methods. As we learn what the attackers have deliberately hidden from us, we must operate carefully to avoid tipping our hats regarding the investigative progress – or the attacker can quickly pivot, nullifying our progress.

TOPICS: Encoding, Encryption, and SSL/TLS; Meddler-in-the-Middle; Network Protocol Reverse Engineering; Investigation OPSEC and Threat Intel

SECTION 6: Network Forensics Capstone Challenge

This section will combine all of what you have learned prior to and during this week. In groups, you will examine network evidence from a real-world compromise by an advanced attacker. Each group will independently analyze data, form and develop hypotheses, and present findings. No evidence from endpoint systems is available – only the network and its infrastructure.

TOPICS: Network Forensic Case

Who Should Attend

- Incident response team members and forensicators
- Hunt team members
- Law enforcement officers, federal agents, and detectives
- Security Operations Center personnel and information security practitioners
- Network defenders
- Information security managers
- Network engineers
- IT professionals
- Anyone interested in computer network intrusions and investigations

NICE Framework Work Roles

- Cyber Defense Incident Responder (OPM 531)
- Cyber Operator (OPM 321)
- Cyber Crime Investigator (OPM 221)
- Law Enforcement/CounterIntelligence Forensics Analyst (OPM 211)
- Cyber Defense Forensics Analyst (OPM 212)

GNFA
Network Forensic Analyst
giac.org/gnfa

GIAC Network Forensic Analyst

The GIAC Network Forensic Analyst (GNFA) certification validates a practitioner's ability to perform examinations employing network forensic artifact analysis. GNFA certification holders have demonstrated an understanding of the fundamentals of network forensics, normal and abnormal conditions for common network protocols, processes and tools used to examine device and system logs, and wireless communication and encrypted protocols.

- Network architecture, network protocols, and network protocol reverse engineering
- Encryption and encoding, NetFlow analysis and attack visualization, security event & incident logging
- Network analysis tools and usage, wireless network analysis, & open source network security proxies