Introduction

Sophisticated cybercriminals understand the techniques and tools that they need to employ to move undetected throughout a victim network until they are able to find their intended targets. From their initial point of entry through to their privilege escalation and finally to exfiltrating their bounty, attackers know how to blend their activity in with legitimate traffic.

In their wake, organizations are left performing incident response and forensic investigations to understand how the attack unfolded. And, today, any investigation is going to involve a network traffic analysis component. Without it, it is just like the police failing to look at security camera footage to track down a criminal. In other words, if one knows where and how to search, network traffic often provides a unique view into the incident: providing evidence, uncovering the footprint of attackers and identifying the extent of the damage that was caused.

Network traffic analysis and incident response

Previously, when networks spanned multiple physical locations and connected dozens, if not hundreds of hosts, enterprises were able to easily examine and analyze data travelling between them without much of a challenge. Today, networks have grown to such a scale that identifying which endpoints are vulnerable, which connections are questionable and which activity is threatening has become so complex that an entire discipline was born: network traffic analysis.

As attacks have evolved, so too has network traffic analysis, forming its own key role among incident response and investigative activities and bringing with it a suite of commercial and open source tools. An enterprise's ability to use the data from all kinds of network devices and these tools — to identify attacks, piece together evidence of a breach, and identify the vector and possibly even the criminal — is key to being able to address the threats of today.

From brazen "script kiddie" attacks to organized, advanced persistent threats, network logs and network traffic analysis remains the key place where the incident response takes place.

Facets of network traffic analysis

There are three main areas where network traffic analysis supports cybersecurity and incident response: threat detection, breach analysis and remediation prioritization.

Threat detection

The fingerprints of an attacker can almost always be found if one just knows where to look. The problem, however, is that it can be almost impossible to monitor, log, analyze and act on all of the data flowing through a network in enough time to mitigate damage without the help of automated systems and tools.

Fortunately, these tools use algorithms, heuristics and event-based triggers to alert security professionals toward anomalies or intrusions and provide the captured data from compromised systems, traffic between internal and external devices, list systems that were probed, accounts utilized and data sets that were accessed and

exfiltrated. Of course, all of this relies upon an organization having not only a means to capture and record network traffic, but also a baseline from which to compare activity to identify such anomalies.

While there are hundreds of network protocols that may be used in an enterprise network, there are three groups where security professionals should know their “typical” behavior to compare it against any logged anomalies, which may suggest nefarious activities. Commercial tools can help with this process, but one of the most popular is Wireshark, an open-source traffic analysis tool that filters and displays data in a more user-friendly format.

Armed with a network traffic analyzer, an analyst can hunt for the following types of anomalies:

- **Protocol-based:** Unusual instances of DNS tunneling or suspicious HTTP headers, unrecognized TCP or UDP connections or suspicious TLS certificates
- **Traffic-based:** Suspicious traffic in a network such as port scans, invalid logins, remote file execution, web shell initiation, proxy bypasses and resource spikes
- **Host-based:** Abnormal behavior by system hosts, including upload/download volume, unusual activity time periods, new lateral movement and port profile changes

With these types of data in hand, security professionals can then diagnose system health, confirm with a breach has in-fact occurred and what to do next.

Breach analysis

Next, in the wake of a cyberattack, performing network traffic analysis can help organizations forensically recreate a blueprint of an attack and how the attacker moved through and accessed the network. Network traffic analysis will be able to reveal timestamps, port numbers, IP addresses, hosts, malicious packets and exfiltrated files, among other data. With this information, security professionals can better understand the scope of the breach, the mechanics of the initial exploitation and the potential damage caused by the breach.

Network traffic analysis will provide an organization with when and how traffic traversed your perimeter and moved laterally through its network, as well as the hosts and tools used. Paired with logs of communication between local, cloud and external systems, an inventory of compromised systems and datasets can be captured so vulnerabilities can be patched and remediation can begin.

Remediation prioritization

As the incident response cycle continues, network traffic analysis is able to inform an organization as it makes decisions on how and when to mitigate risk to their network. While an attacker may have used zero-day exploits, VPN connections and encrypted traffic, network analysis will still review to analysts the machines or hosts used as well as the IP address and ports processing the network traffic.

Armed with this amount of information and knowledge of exploited databases, an organization can begin to deploy responses to stop the attack, mitigate damage and close any security gaps that may have enabled the breach.

Learn Network Traffic Analysis for Incident Response

Conclusion: Bringing it all together

Network traffic analysis is both an ongoing discipline and a key part of incident response and forensics in the wake of a cyberattack. Network traffic analysis and the tools that enable it provides organizations with the ability to sort through countless amounts of data, drill down to key protocols, hosts and actions, and recreate and trace an attack back to its original source.

Armed with this information, organizations can help to prevent future attacks by closing vulnerabilities and introducing additional data that can be used in predictive modeling to hopefully prevent it from happening again.

Sources

. Wireshark, Wireshark Foundation

. A Summary of Network Traffic Monitoring and Analysis Techniques, Alisha Cecil

. Network Situational Awareness, Carnegie Mellon University