The Analysis Process

Network Traffic Analysis is a dynamic process that can change depending on the tools we have on hand, permissions given to us by the organization, and our network's visibility. Our goal is to provide a repeatable process we can begin to utilize when performing traffic analysis.

Traffic Analysis is a `detailed examination of an event or process`, determining its origin and impact, which can be used to trigger specific precautions and/or actions to support or prevent future occurrences. With network traffic, this means breaking down the data into understandable chunks, examining it for anything that deviates from regular network traffic, for potentially malicious traffic such as unauthorized remote communications from the internet over RDP, SSH, or Telnet, or unique instances preceding network issues. While performing our analysis, we are also looking to see what the trends look like within the traffic and determine if it matches a baseline of typical operational traffic.

Traffic analysis is a highly versatile and essential tool to have in our defensive toolbox. Without the ability to monitor traffic, we are working with a massive piece of the puzzle missing. Analytics on network usage, top-talking hosts and servers, and internal communications are all crucial pieces that provide us, the administrators and defenders, a way to see and correct issues before or soon after they happen. Visibility is probably the most beneficial thing it provides. With this visibility, we can capture traffic over different periods to set a baseline for our environment. This baseline makes it easier to see when a change has occurred. In more advanced implementations for NTA that include other tools like IDS/IPS, firewalls, host and network logs, and additional information being fed into Tools like Splunk or ELK Stack, having the ability to monitor traffic is invaluable. The tools help us quickly alert on malicious actions happening. Many defensive tools have signatures built for most of the common attacks and toolkits.

Having proper defensive capabilities is vital for everyone, but what about daily operations? How can NTA help us? Watching network traffic live can make it easy to troubleshoot a connection issue or determine if our infrastructure and the corresponding protocols are functioning correctly. If we can see where the traffic is going, we can determine if there is an issue.

Lastly, this is a dynamic skill, and using automated tools to aid us is perfectly fine. Just do not rely on them solely. Utilize the skills you have and perform manual checks as well. This will help us by putting eyes on our network. We will have checks and balances between ourselves and the tools since the tools can be beaten. Malicious actors are finding ways to bypass security measures all the time. The human eye is still our best resource for finding the bad.

Analysis Dependencies

Traffic capturing and analysis can be performed in two different ways, `active` or `passive`. Each has its dependencies. With passive, we are just copying data that we can see without directly interacting with the packets. For active traffic capture and analysis, the needs are a bit different. Active capture requires us to take a more hands-on approach. This process can also be referred to as `in-line` traffic captures. With both, how we analyze the data is up to us. We can perform the capture and analysis once done, or we can perform analysis in real-time while the traffic is live. The table below lays out the dependencies for each.

Traffic Capture Dependencies

Dependencies	Passive	Active	Description
`Permission`	☑	☑	Depending on the organization we are working in, capturing data can be against policy or even against the law in some sensitive areas like healthcare or banking. Be sure always to obtain permission in writing from someone with the proper authority to grant it to you. We may style ourselves as hackers, but we want to stay in the light legally and ethically.

My Workstation

OFFLINE

Start Instance

∞ / 1 spawns left

Mirrored Port	☑	☐	A switch or router network interface configured to copy data from other sources to that specific interface, along with the capability to place your NIC into promiscuous mode. Having packets copied to our port allows us to inspect any traffic destined to the other links we could normally not have visibility over. Since VLANs and switch ports will not forward traffic outside of their broadcast domain, we have to be connected to the segment or have that traffic copied to our specific port. When dealing with wireless, passive can be a bit more complicated. We must be connected to the SSID we wish to capture traffic off of. Just passively listening to the airwaves around us will present us with many SSID broadcast advertisements, but not much else.
Capture Tool	☑	☑	A way to ingest the traffic. A computer with access to tools like TCPDump, Wireshark, Netminer, or others is sufficient. Keep in mind that when dealing with PCAP data, these files can get pretty large quickly. Each time we apply a filter to it in tools like Wireshark, it causes the application to parse that data again. This can be a resource-intensive process, so make sure the host has abundant resources.
In-line Placement	☐	☑	Placing a Tap in-line requires a topology change for the network you are working in. The source and destination hosts will not notice a difference in the traffic, but for the sake of routing and switching, it will be an invisible next hop the traffic passes through on its way to the destination.
Network Tap or Host With Multiple NIC's	☐	☑	A computer with two NIC's, or a device such as a Network Tap is required to allow the data we are inspecting to flow still. Think of it as adding another router in the middle of a link. To actively capture the traffic, we will be duplicating data directly from the sources. The best placement for a tap is in a layer three link between switched segments. It allows for the capture of any traffic routing outside of the local network. A switched port or VLAN segmentation does not filter our view here.
Storage and Processing Power	☑	☑	You will need plenty of storage space and processing power for traffic capture off a tap. Much more traffic is traversing a layer three link than just inside a switched LAN. Think of it like this; When we passively capture traffic inside a LAN, it's like pouring water into a cup from a water fountain. It's a steady stream but manageable. Actively grabbing traffic from a routed link is more like using a water hose to fill up a teacup. There is a lot more pressure behind the flow, and it can be a lot for the host to process and store.

The last dependency is more of a recommendation than a requirement, but we feel it is necessary to mention it. Having an understanding of how day-to-day traffic flows is critical to being successful. It is possible to perform traffic analysis without one, but it will be much harder and time-consuming. The baseline will enable us to quickly filter out common traffic for that network while performing our analysis. Doing so can speed our process up and help spot the outliers or issues much sooner. Let us look at this scenario for a second:

> ⓘ You are a network administrator for a large corporation with several thousand employees on campus. It has been brought to your attention that a segment of your network is having connectivity issues. Several of those hosts are reporting extremely high latency, along with new files appearing on their desktops. To start getting a picture of what is happening, you attach a computer to that segment and start a capture. After a few minutes have passed, you stop the capture and start your analysis.

Now consider this. Without a baseline of our daily network traffic, how do we know what is typical for that network? We grabbed a ton of information during the capture timeframe, and we need to clear some of it away. This process can take a lot of time since we will have to examine every conversation to ensure it is ok, determine if the hosts we see belong on the network or are rogue assets, among much more. This process quickly became a daunting task, right?

With this scenario and access to a network baseline, we can quickly strip away known-good communications. Utilizing data analysis tools such as the top talkers' module in Wireshark can help identify hosts that may be sending a large amount of data. We can check this against the host's normal baseline to determine if it is out of character. Another way could be to look at connections between internal hosts or common and uncommon ports. Since we could clear our view, we can now see that several user hosts connect on ports 8080 and 445. The ports themselves are not weird, but the fact that it is two user PCs talking to each other over these ports is. Web traffic usually flows from a host to a hosted web server or an intranet web server hosting business applications. The same can be said for SMB traffic. It is very suspicious to see two hosts talking to each other over this port. With what we now know, we can quickly send up a trouble ticket looking for help handling a potential breach now.

When talking about network intrusions, the faster we can get visibility, the less potential damage to our network. Be sure to clearly understand how traffic flows in our networks and how protocols commonly act.