CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Using Network Flow Data to Profile Your Network and Reduce Vulnerabilities

Key Message: A network profile can help identify unintended points of entry, misconfigurations, and other weaknesses that may be visible to attackers.

Executive Summary

"A network profile is an inventory of all the assets on a network and their associated purpose. Such a profile can enable network administrators to better consider how decisions about configuration changes will affect the rest of the assets on the network. Security administrators can evaluate the profile for assets that violate policy and for any suspicious activity. Business administrators can use the profile to help guide long-term plans for network upgrades and staffing. As the profile changes over time, network operators and defenders can monitor for emerging concerns. This, in turn, can lead to policy changes and reallocation of network resources." [1] A network profile is developed by capturing and analyzing network flow data (traffic over ports, protocols, etc.) available at perimeter gateways.

In this podcast, Austin Whisnant and Sid Faber, members of CERT's Network Situational Awareness team, discuss how organizations can use network flow data to identify their top, public facing assets and services that generate the most network traffic, asset misconfigurations, and assets that they may not know about. This is important because a potential attacker can observe and take advantage of this information.

This podcast is based on an August 2012 report authored by Austin and Sid titled *Network Profiling Using Flow*.

PART 1: WHAT A NETWORK PROFILE CAN TELL YOU ABOUT YOUR NETWORK

Uses of a Network Profile

A network profile is a list of all of the assets on a network and their purpose. It can provide useful information for the following roles:

- system administrators: to know what is on their networks and thus what they need to defend
- business administrators: for purchasing and allocating network resources (systems, devices)
- operators: to know what is going on, on their networks

A network profile

- can be used as the basis for building a complete asset inventory
- identifies what assets are supposed to be doing (for example, which machines are servers and which are clients)
- identifies what assets are not supposed to be doing
- can be compared with other network monitoring reports to see if assets are behaving as intended
- helps network owners know what services are facing the outside world and learn everything an attacker might know, to be one step ahead
- helps identify misconfigurations that can then be corrected
- helps identify assets that owners didn't know were connected to their networks and find out if they should be

All of this information can help eliminate potential vulnerabilities and points of entry, including those that might allow an attacker to bypass organizational firewalls and access internal networks.

PART 2: SEVEN STEPS FOR BUILDING A NETWORK PROFILE

The steps are as follows:

1. gather available network information (network maps, equipment purchase orders)
2. select an initial data set (one day, one week depending on the size of the network)
3. identify the active, monitored address space (the entire network or a subnet)
4. catalog common services (Web, DNS, VPN, FTP)
5. catalog other services (SQL protocol)
6. catalog leftover assets (any IP addresses that haven't been captured)
7. maintain the profile (update at least once/month depending on network size and activity level)

This approach uses network flow data rather than packet capture or other approaches for creating a network inventory.

Resources to Build/Maintain a Network Profile

The time and effort required to build and maintain a network profile depends on the size of the network and how dynamic it is:

- small, more static network: create a profile in a few days or a week; update every six months or so
- large-scale, dynamic network: create a profile in a few weeks; update often

You can also start with a small subnet, or several, and then aggregate results as you go.

Gather Information; Select Initial Data Set

Often network information (network maps, lists of servers) is out of date. Once you have a network profile, you can update this information.

For the initial data set, you may want to concentrate on your outgoing traffic or a specific subnet.

Sensor Placement

Sensor placement for collecting netflow data is critical; different sensors may produce different results. Given you are most interested in what an outsider might see, place sensors around the perimeter (internet border, chokepoints, and gateways).

For many networks, the generation of netflow data is already built in, for example, via network routers. Enabling netflow data is a configuration option.

There are limitations on what routers can do. It is better if you have dedicated sensors but these are not required to get started.

Identify Active Address Space

This involves determining the IP addresses, hosts, assets, and services that are of greatest interest. First, look at all hosts that have active TCP connections. Then consider other protocols such as UDP and ICMP.

Once you have this information, determine if there are missing assets, for example, those that support backups.

Generate a list of IP addresses for these assets.

Catalog Services and Leftover Assets

During this step, pick a service such as Web traffic and find assets that are communicating Web traffic. Look for Web servers first to obtain port numbers, protocols, and other technical details. If the server is communicating on this port,

then it is most likely a Web server.

Do the same for other services such as DNS and VPN.

Next, identify IP addresses that are generating traffic and have not yet been profiled. Analyze the traffic that such IP addresses are producing, identify the highest volume services associated with that traffic, and associate the asset with those services.

Network Profile Data

Most netflow tools have a command line, text interface that reports netflow records. These records typically contain port numbers, protocols, IP addresses, flags, byte counts, and packet counts. Tools are available to sort this data as desired, to obtain statistics and other information of interest.

PART 3: NETFLOW ANALYSIS TOOLS; DETECT ANOMALIES BY TRACKING TRENDS

Netflow Analysis Tools

The primary tool used at CERT is SiLK – System for Internet-Level Knowledge. SiLK generates netflow data from packet captures, stores data, and analyzes data. SiLK is able to collect netflow data in very large network environments. SiLK is open source and free to download.

Other netflow analysis tools include Lancope (StealthWatch), Cisco (NetFlow), and Argus.

Collect Trends Over Time

Observing how netflow data changes over time can be extremely valuable, to confirm expected behavior (for example, weekend FTP uploads to refresh content, software updates and patches) and catch unexpected behavior for further analysis.

Trends can indicate how network bandwidth is being consumed and how new technologies (for example, streaming audio and video, bring your own device (BYOD) are affecting network performance.

Proactive Network Security

Attackers can use netflow data to observe your network footprint and your assets and services that are visible on the internet, including ones you may not know about.

Network profiling is a more proactive approach to network security. A profile allows you to better understand how your network behaves so you can better detect anomalies. However, anomalies can only be detected if you know what constitutes normal, expected behavior – and departures from normal.

Such anomalies are typically not detectable using traditional, signature-based methods such as antivirus, intrusion prevention, and intrusion detection.

Netflow data can enhance the knowledge of network and security analysts. They can then better understand network dynamics and how to react to unique threats.

Resources

[1] Whisnant, Austin & Faber, Sid. Network Profiling Using Flow (CMU/SEI-2012-TR-006). Software Engineering Institute, Carnegie Mellon University, August 2012.

CERT Network Situational Awareness website

FloCon conference website