

12.3.10 Monitoring Data and Metadata Facts

This lesson covers the following topics:

- Bandwidth monitors
- Metadata
- Data analyzers

Bandwidth Monitors

Today's bandwidth monitors provide a broader array of functions than simply monitoring the volume and speed of internet traffic. Bandwidth monitors can help you understand network usage, the protocols being used, users who consume a lot of bandwidth, and who is communicating on the network. When you use a bandwidth monitor, you will:

- Establish and update baselines. Baselines provide a reference for normal and abnormal activity.
- Create data points. To be useful and accurate, a baseline requires thousands of data points. Data points are customizable. You can set connectivity, file activity, and access attempts and failures.
- Set intervals. You can set intervals in minutes, hours, days, weeks, months, or a year. Longer monitor runs equal more data points.

Metadata

Metadata is produced by almost all network activity. Server requests, applications, and email are some examples of where metadata can be found. In the context of bandwidth monitors, metadata is used to investigate security related concerns or incidents. The following table describes three types of metadata.

Type	Description
Email metadata	Email provides metadata that is used to trace email. All emails come with a header that contains information about both the sender and recipient. Parts of the headers can be spoofed giving investigators false information. However, there are security devices that put X-headers throughout an email's header. These provide the originating email account and IP address not the spoofed one.
Mobile metadata	Tablets, laptops, smart phones, smart watches, and any other device that connects to the internet and can be moved around produces mobile metadata. These devices send emails, text-messages, and use apps. All of these produce metadata that can be used to identify people, places, times, and even deleted data. Pictures can be timestamped and geolocation stamped. Much of this metadata also reveals origination of the data and the sender.
Web metadata	Websites produce many types of metadata. The metadata on a user's machine versus the server can be very different. The data on both sides of the transmission can help fill in gaps and corroborate findings. Metadata includes IP addresses, user requests, user downloads, time spent on the site, and even attempts to gain unauthorized access. Web metadata includes cookies, browser history, and cached pages. Many times malicious actors will attempt to obfuscate their metadata. However, there are ways of finding the real metadata, especially for trained forensic investigators.

Data Analyzers

Network admins should always looking for a way to examine what is happening inside the network. There are a number of tools to help sift through the tremendous amounts of data generated by network activity. The following table describes some of these tools.

Tool	Description
NetFlow	NetFlow is a feature on Cisco routers. It works at layers 2 – 4. It can examine each data flow that comes through the network or it be set to sample sessions at certain intervals.
sFlow	sFlow is a packet sampling technology that works on layers 2 – 7 of the stack. Unlike NetFlow, sFlow only can be used in sampling mode. This is a stateless packet sampling that provides information on various layers and does it quickly and efficiently.
IPfix	IPfix directly integrates data that normally goes to Syslog or SNMP. This eliminates additional services collecting data from each network device. IPfix has provisions for fields that are variable length, meaning that there are no ID number restrictions. IPfix addresses the need for a standardized protocol for internal protocol flows. This data comes from routers, servers, and other network appliances that are mediation systems. The data is formatted, sent to an exporter, and then sent to a collector. IPfix, like NetFlow, looks at flow and the number of packets being sent and received during a given session.

Copyright © 2022 TestOut Corporation All rights reserved.