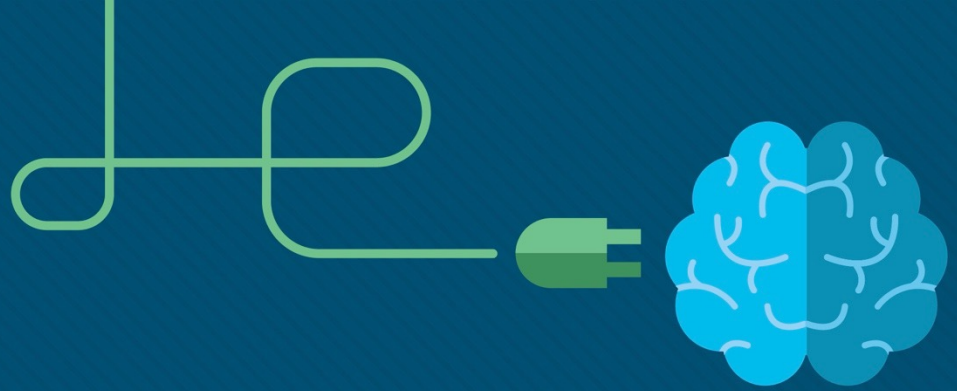


Chapter 6: Network Attacks: A Deeper Look

Information Security

Dr. Ayman Aljarbouh

6.1 Network Monitoring and Tools

Module Objectives

Module Title: Network Monitoring and Tools

Module Objective: Explain network traffic monitoring.

Topic Title	Topic Objective
Introduction to Network Monitoring	Explain the importance of network monitoring.
Introduction to Network Monitoring Tools	Explain how network monitoring is conducted.

Network Security Topology

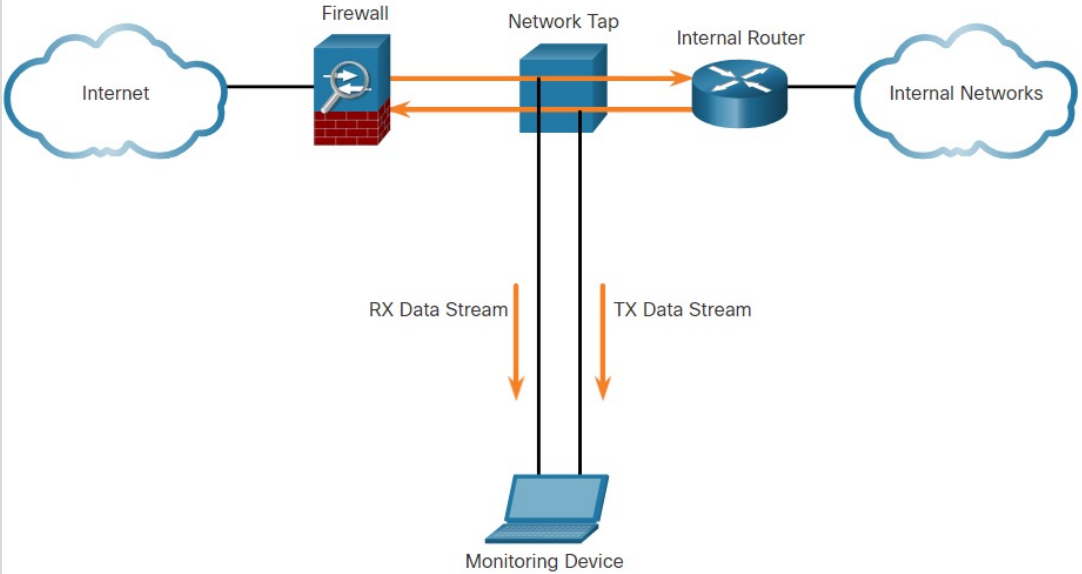
- Network requires a security infrastructure consisting of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and endpoint security software to protect.
- These methods and technologies are used to introduce automated monitoring, creating security alerts, or automatically blocking offensive devices.
- Devices such as firewalls and IPS operate based on pre-configured rules and monitor traffic and compare it against the configured rules.
- An important part of the cybersecurity analyst is to review all alerts generated by network devices and determine the validity of the alerts.

Network Monitoring Methods

- Tools used to help discover normal network behavior include IDS, packet analyzers, SNMP, NetFlow, and others.
- Traffic information capture methods:
  - **Network TAPs** – Network test access points that forward all traffic including physical layer errors to an analysis device.
  - **Port mirroring** – enables a switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.

Network Taps

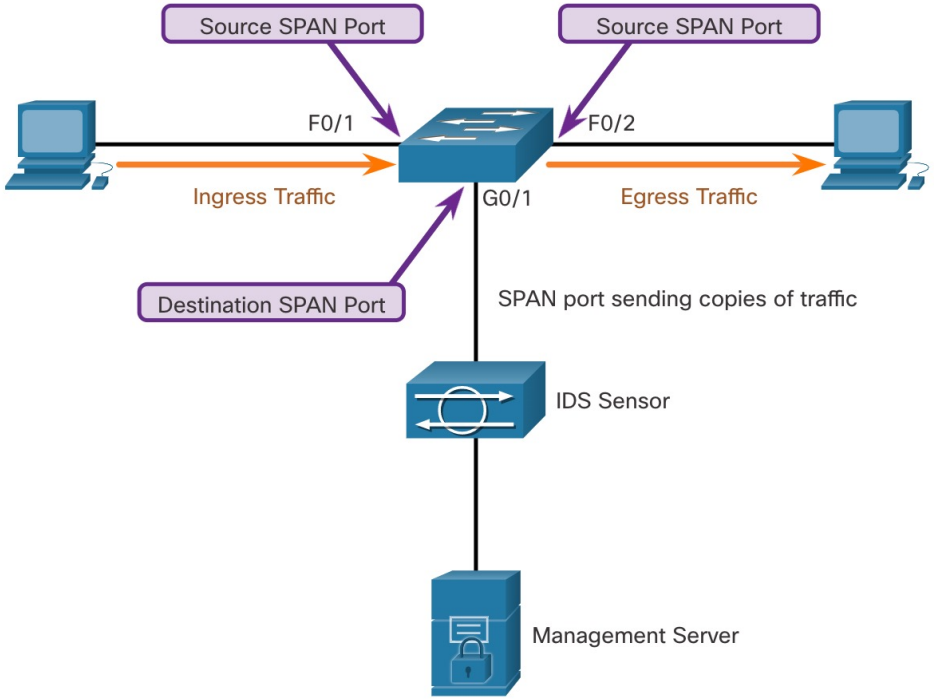
- A network tap is typically a passive splitting device implemented inline between a device of interest and the network. A tap forwards all traffic including physical layer errors to an analysis device.
- Taps are also typically fail-safe, which means if it fails or loses power, traffic between the firewall and internal router is not affected.



Implementing a TAP in a Sample Network

Traffic Mirroring and SPAN

- Special techniques such as port mirroring must be employed to bypass network segmentation imposed by network switches.
- Port mirroring enables the switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.
- In the figure, the switch will forward ingress traffic on F0/1 and egress traffic on F0/2 to the destination SPAN port G0/1 connecting to an IDS.
- The association between source ports and a destination port is called a SPAN session. In a single session, one or multiple ports can be monitored.



Switch interconnecting two hosts and mirroring traffic to an IDS and Network Management Server

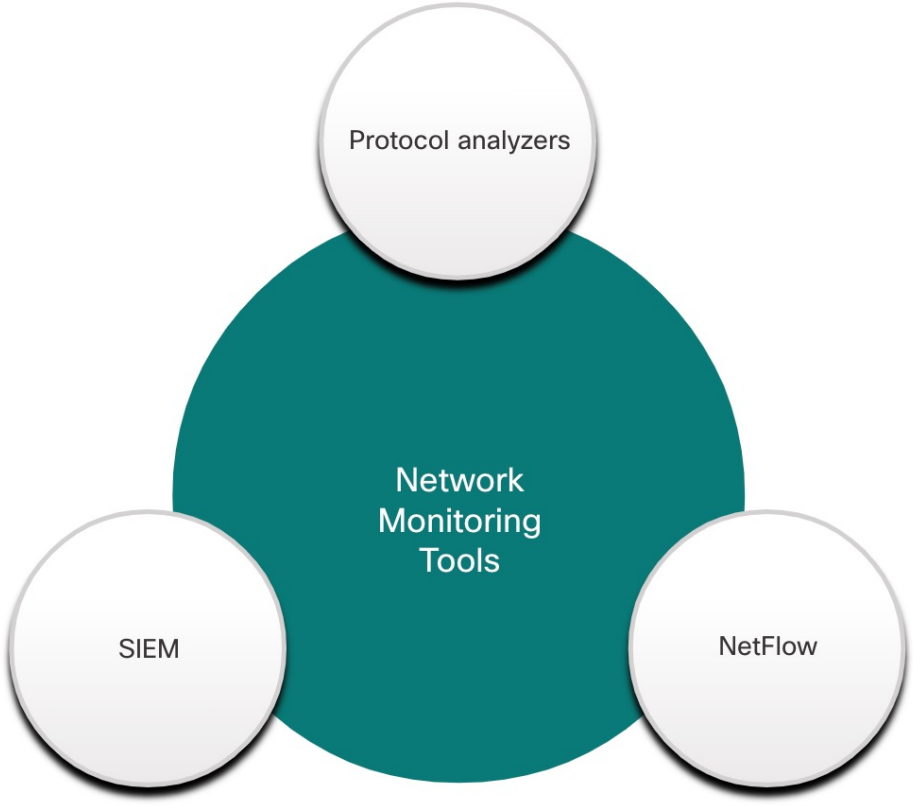
Traffic Mirroring and SPAN

- Special techniques such as port mirroring must be employed to bypass network segmentation imposed by network switches.
- Port mirroring enables the switch to copy frames of one or more ports to a Switch Port Analyzer (SPAN) port connected to an analysis device.
- In the figure, the switch will forward ingress traffic on F0/1 and egress traffic on F0/2 to the destination SPAN port G0/1 connecting to an IDS.
- The association between source ports and a destination port is called a SPAN session. In a single session, one or multiple ports can be monitored.

SPAN Term	Description
Ingress traffic	Traffic that enters the switch
Egress traffic	Traffic that leaves the switch.
Source (SPAN) port	Source ports are monitored as traffic entering them is replicated (mirrored) to the destination ports.
Destination (SPAN) port	A port that mirrors source ports. Destination SPAN ports often connect to analysis devices such as a packet analyzer or an IDS.

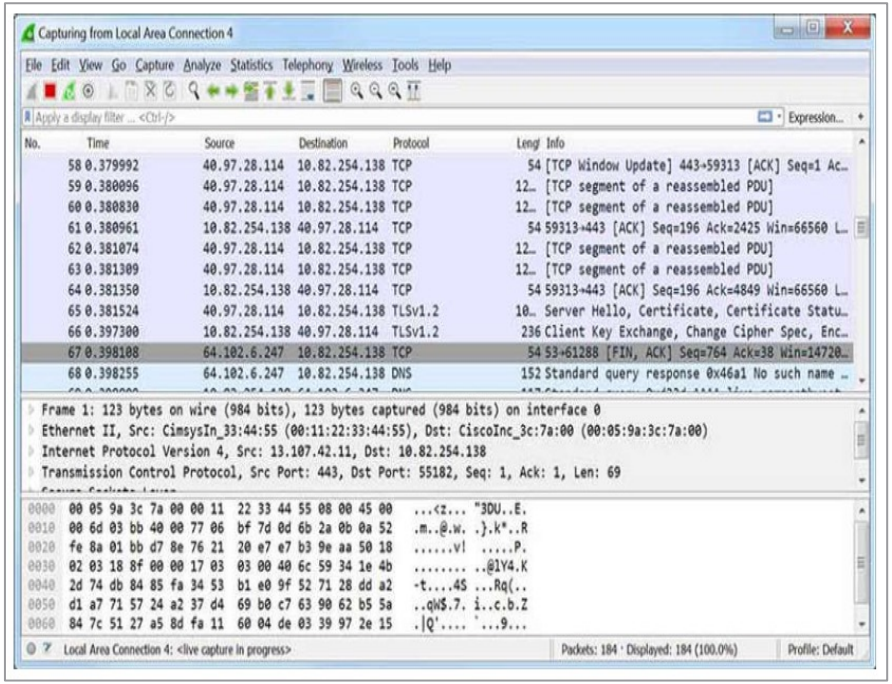
Network Security Monitoring Tools

- Common tools that are used for network security monitoring include:
  - Network protocol analyzers such as Wireshark and Tcpdump
  - NetFlow
  - Security Information and Event Management Systems (SIEM)
- It is common for security analysts to rely on log files and Simple Network Management Protocol (SNMP) for network behavior discovery.



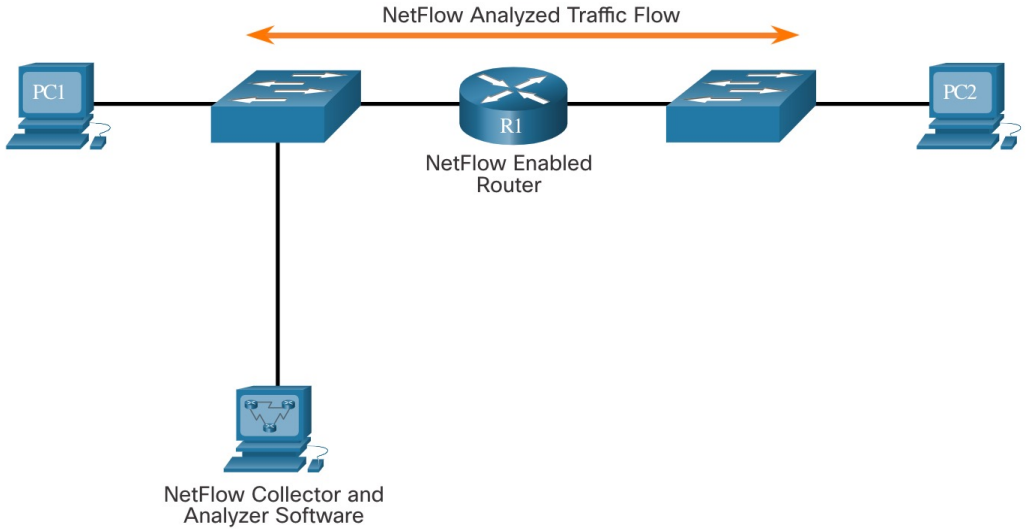
Network Protocol Analyzers

- Network protocol analyzers (or ‘packet sniffer’ applications) are programs used to capture traffic.
- Protocol analyzers display what is happening on the network through a graphical user interface.
- Network protocol analyzers are not only used for security analysis but also used for network troubleshooting, software and protocol development, and education.
- As shown in the figure, Wireshark is used in Windows, Linux, and Mac OS environments. It is a very useful tool for learning network protocol communications.



NetFlow

- NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets flowing through a Cisco router or multilayer switch.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis; however, it does not capture the content.
- NetFlow collectors like Cisco Stealthwatch can also perform advanced functions including:
  - **Flow stitching**: It groups individual entries into flows.
  - **Flow deduplication**: It filters duplicate incoming entries from multiple NetFlow clients.
  - **NAT stitching**: It simplifies flows with NAT entries.



PC1 connected to PC2 using HTTPS

SIEM

- Security Information Event Management (SIEM) systems provide real time reporting and long-term analysis of security events.
- SIEM includes the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources throughout the organization. It provides more complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Aggregation reduces the volume of event data by consolidating duplicate event records.
  - **Reporting** - Reporting presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM Systems

- Splunk is one of the more popular proprietary SIEM systems used by Security Operation Centers.
- As an open source option, this course uses the ELK suite for SIEM functionality. ELK is an acronym for three open source products from Elastic:
- **Elasticsearch** - Document oriented full text search engine
- **Logstash** - Pipeline processing system that connects "inputs" to "outputs" with optional "filters" in between
- **Kibana** - Browser based analytics and search dashboard for Elasticsearch

New Terms and Commands

• Wireshark • tcpdump • Simple Network Management Protocol (SNMP) • Security Information and Event Management Systems (SIEM)	• Intrusion Prevention Systems (IPS) • Switch Port Analyzer (SPAN) • Egress traffic • Ingress Traffic • Intrusion Detection Device (IDS)	• Test Access Points (TAPs) • Network Tap • Elastic Search Logstash Kibana (ELK) • NetFlow

Lab 22 - Logging Network Activity

In this lab, you will do the following:

- Intercept credentials using a sniffer device, while observing an FTP session. An exchange of Syslog messages will also be intercepted by a sniffer device.