**NETWORK MONITORING METHODS**



Class: Cyber Security

Prepared by: Rickardo Brown, St Patrick Currey

Date: 18/08/2023

Network Monitoring Methods

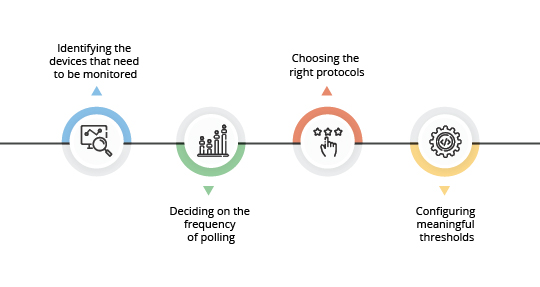
Introduction

Network monitoring methods are a crucial aspect of maintaining the security and optimal performance of modern networks. In today's interconnected world, networks play a pivotal role in enabling seamless communication and data exchange. However, with the increasing complexity and scale of networks, ensuring their security and efficiency has become a challenging task. In this presentation, we will delve into the essential concept of network monitoring, the tools used to discover normal network behavior, and the two primary methods for capturing network traffic.

Understanding Network Monitoring

The day-to-day operation of a network involves common patterns of traffic flow, bandwidth utilization, and resource access. These patterns collectively define the baseline of normal network behavior. Security analysts rely on understanding normal behavior to identify and address abnormal network activities that may indicate security breaches or performance issues.

Network Monitoring Steps:



The Need for Network Monitoring

Abnormal network behavior often signifies potential problems, such as security breaches or performance bottlenecks. Network monitoring is essential to proactively detect and respond to these issues before they escalate. Monitoring helps organizations maintain a robust security posture and provide uninterrupted services to users.

Tools for Discovering Normal Network Behavior

- Various tools are utilized to uncover patterns of normal network behavior:

- Intrusion Detection Systems (IDS): These tools identify suspicious activities and potential security breaches by analyzing network traffic for known attack patterns.

- AIDE: The Advanced Intrusion Detection Environment (AIDE) is an open-source host-based intrusion detection system (HIDS) for Unix, Linux, and Mac OS. This specialized tool focuses on the very important niche of checking file integrity, but does not offer any broader malware or attack detection.

Pros:

Open source

Runs on MacOS and \*nix systems

Verifies the integrity of files

Can target specific directories for monitoring or exclude certain files

Integrates with other tools

- BluVector: Formerly known as Cortex and now owned by Comcast, BluVector’s advanced threat detection solution uses artificial intelligence (AI) to complement an existing security stack. The AI detects fileless malware and zero-day threats and is designed to become more powerful the longer it sits in the environment.

Pros:

On premise

Collects logs

Builds off of trusted Suricata and Zeek technology

Integrates with other tools

Open platform – data is easily available

Takes in data from multiple intel feeds and sandboxes

Proprietary machine learning algorithm adds to capabilities

Broad MITRE ATT&CK coverage, does not use signature technology

Built-in tuning assistant to reduce false positives easily

- Packet Analyzers: Also known as packet sniffers, these tools capture and analyze individual data packets to diagnose network issues and assess application performance.

- Wireshark

- Solar Winds

- Network Miner

- Simple Network Management Protocol (SNMP): SNMP allows for centralized monitoring and management of network devices and their performance metrics.

- NetFlow: NetFlow collects and analyzes network traffic data to provide insights into traffic patterns, application usage, and potential anomalies.

Capturing Network Traffic: Overview

- Capturing network traffic is essential for effective network monitoring.

- Two primary methods for capturing traffic are network taps and traffic mirroring.

Network Taps (Test Access Points)

- Network taps are hardware devices that provide a passive way to monitor network traffic.

- They are inserted into the network between devices, copying the traffic and sending it to monitoring devices.

- Network taps are non-intrusive, ensuring that network performance is not impacted by the monitoring process.

- They are particularly useful for critical networks where performance is of utmost importance.

Traffic Mirroring using Switch Port Analyzer (SPAN)

- Switch Port Analyzer (SPAN) is a feature available on many network switches.

- SPAN allows network administrators to configure a switch to replicate specific traffic from one or more ports to a designated monitoring port.

- The replicated traffic can then be analyzed by monitoring tools.

- SPAN is flexible and cost-effective, as it uses existing network infrastructure.

Choosing the Right Method

- The choice between network taps and SPAN depends on factors such as network size, criticality, and monitoring goals.

- Network taps offer complete visibility but may involve additional hardware costs.

- SPAN is efficient and cost-effective but requires careful configuration to ensure relevant traffic is mirrored.

Best Practices for Effective Network Monitoring

- Regularly update and fine-tune monitoring tools to adapt to evolving network behavior.

- Establish a baseline of normal behavior to more effectively identify anomalies.

- Integrate network monitoring with incident response procedures for swift action.

- Ensure compliance with data privacy regulations when capturing and analyzing network data.

Conclusion

- Network monitoring is vital for maintaining security and performance in modern networks.

- Tools like IDS, packet analyzers, SNMP, and NetFlow help discover normal network behavior.

- Capturing network traffic can be achieved through network taps or traffic mirroring using SPAN.

- The choice between methods depends on network characteristics and monitoring objectives.

[What Is Network Monitoring? | @SolutionsReview Explores](https://www.youtube.com/watch?v=ppKqAjBB714&ab_channel=SolutionsReview)

ManageEngine OpManager

ManageEngine OpManager is a network monitoring tool that continuously monitors devices such as routers, switches, firewalls, load balancers, wireless LAN controllers, servers, VMs, printers, and storage devices. Manage Engine OpManager must be installed on-site, but it comes with pre-configured network monitor device templates for increased ease-of-use.

Key features include:

Real-time network monitoring

Physical and virtual server monitoring

Multi-level thresholds

Customizable dashboards

WAN Link monitoring

SNMP monitoring

Email and SMS alerts

Automatic discovery

Paessler PRTG Network Monitor

Paessler PRTG Network Monitor allows organizations to monitor all their systems, devices, traffic, and applications in their IT infrastructure without additional plugins. You can choose between a number of sensors that will monitor areas of your network, such as bandwidth monitoring sensors, hardware parameters sensors, SNMP sensors, VOIP and QoS sensors, and others.

Key features include:

Integrated Technologies (SNMP, WMI, SSH, HTTP requests, SQL, and more)

Live-status dashboards

Email, push, or HTTP request alerts

Threshold-based alert system

Reports system

Scan for devices by IP segment

Solarwinds NPM

While Solarwinds Network Performance Manager has performance in the name, it is still a valuable network security monitoring tool because of the tracking of network elements such as servers, switches, and applications. Solarwinds NPM can jump from SNMP monitoring to packet analysis to give your organization greater control over the segmentation monitoring of your network and increase network security.

Key features include:

Critical path visualization

Intelligent mapping

WiFi monitoring and heat maps

Advanced alerting

SNMP monitoring

Discovers connected devices automatically

Nagios

Nagios is a monitoring and alerting engine designed to run natively on Linux systems. The open-source model of Nagios provides the opportunity for organizations to customize and adapt the system to meet their needs. The tool breaks down statuses into three categories – Current Network Status, Host Status Totals, and Service Status Totals. Through the use of APIs, you can integrate other services for true flexibility.

Key features include:

Performance dashboard

API integration

Availability reports

Alerting

Extended add-ons

Upgrade capabilities for Nagios XI

WhatsUp Gold

WhatsUp Gold is a tool that pulls infrastructure management, application performance management, and network monitoring all into one tool. It’s a user-friendly tool based on features with customizable pricing packages to fit your organization’s exact structure and network security needs.

Key features include:

Hybrid cloud monitoring

Real-time performance monitoring

Automatic report generation

Network mapping

Easy-to-use monitoring dashboard