Network Traffic Analysis

Mohd Akram Khan, GCIH
Scientist 'B'

Network Traffic Analysis

- The process of capturing network traffic information and inspecting it closely to determine communication patterns and network activities

Network Traffic Analysis

- Network monitoring
- Network planning, Performance analysis and improvement
- Security analysis
  - Detect any anomalous traffic

Traffic

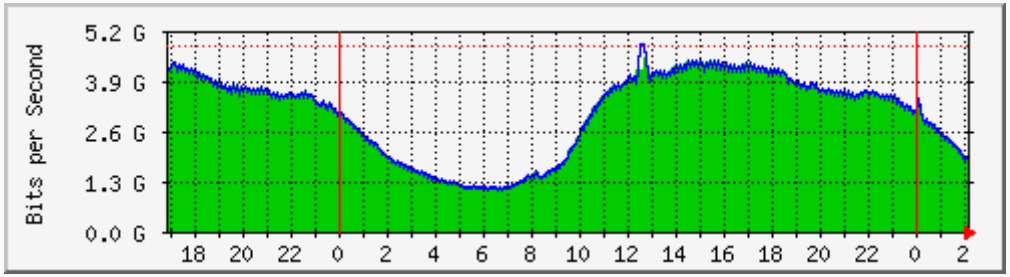
- Packet
  - Header + Payload
  - Header
    - TCP/UDP, IP Header
  - Payload
    - Application Layer Data
- Logs
  - System
  - Application

Traffic Analysis Approaches

- Active – relies upon data gathered from probe packets injected into the network.
  - E.g. SNMP based
- Passive – relies upon data gathered from active network traffic.
  - Network Header Based Analysis
    - E.g. Netflow based
  - Deep Packet Inspection
    - E.g. capture Header + Payload

SNMP Based Traffic Analysis

- Multi-Router Traffic Grapher (MRTG)
  - Is a tool for monitoring traffic loads on a network link. MRTG generates HTML pages that provide a live, visual representation of the network traffic.
  - It can be used to monitor any SNMP MIB.



	Max	Average	Current
In	4480.3 Mb/s	3042.4 Mb/s	1800.3 Mb/s
Out	4804.3 Mb/s	3046.5 Mb/s	1808.9 Mb/s

Network Header Based Analysis

Each packet can be examined for a set of IP packet attributes. These attributes are the IP packet identity or fingerprint of the packet and determine if the packet is unique or similar to other packets.

Some of the most important attributes of a TCP/IP packet:

- The protocol records the following attributes of a TCP/IP packet:
- Source address, i.e. the origin
- Destination address, i.e. the destination
- Source port, i.e. the application
- Destination port, the application
- Layer 3 protocol type
- Type of service, i.e. priority of the traffic

Network Header Based Analysis

Protocol Based Traffic Analysis

- Identify the traffic distribution based on different protocols
- Application based
  - HTTP
  - SMTP
  - DNS
- Transport Protocol based
  - TCP
  - UDP

Application Based Traffic Analysis

- Different application traffic have different pattern
- Web , DNS, FTP , P2P
- Conventional methods uses port numbers in packet header to identify the application
- - Eg : por t 80 for HTTP, 25 for SMTP etc

Network Header Based Analysis

Host Based Traffic Analysis

- Identify the distribution traffic based on IP address
- More useful for detailed understanding of the Host behavior
- Traffic pattern of critical hosts like web server, mail server and DNS server are important
- Useful for detecting abnormal behaviour of a worm, botnet , malware a ected host

Security Analysis

- Signature Based
  - Patterns of known attacks
- Anomaly Based
  - Based on the unusual behavior on a network , host , application etc.
  - Flood based attacks, Scanning etc.

Network Flow

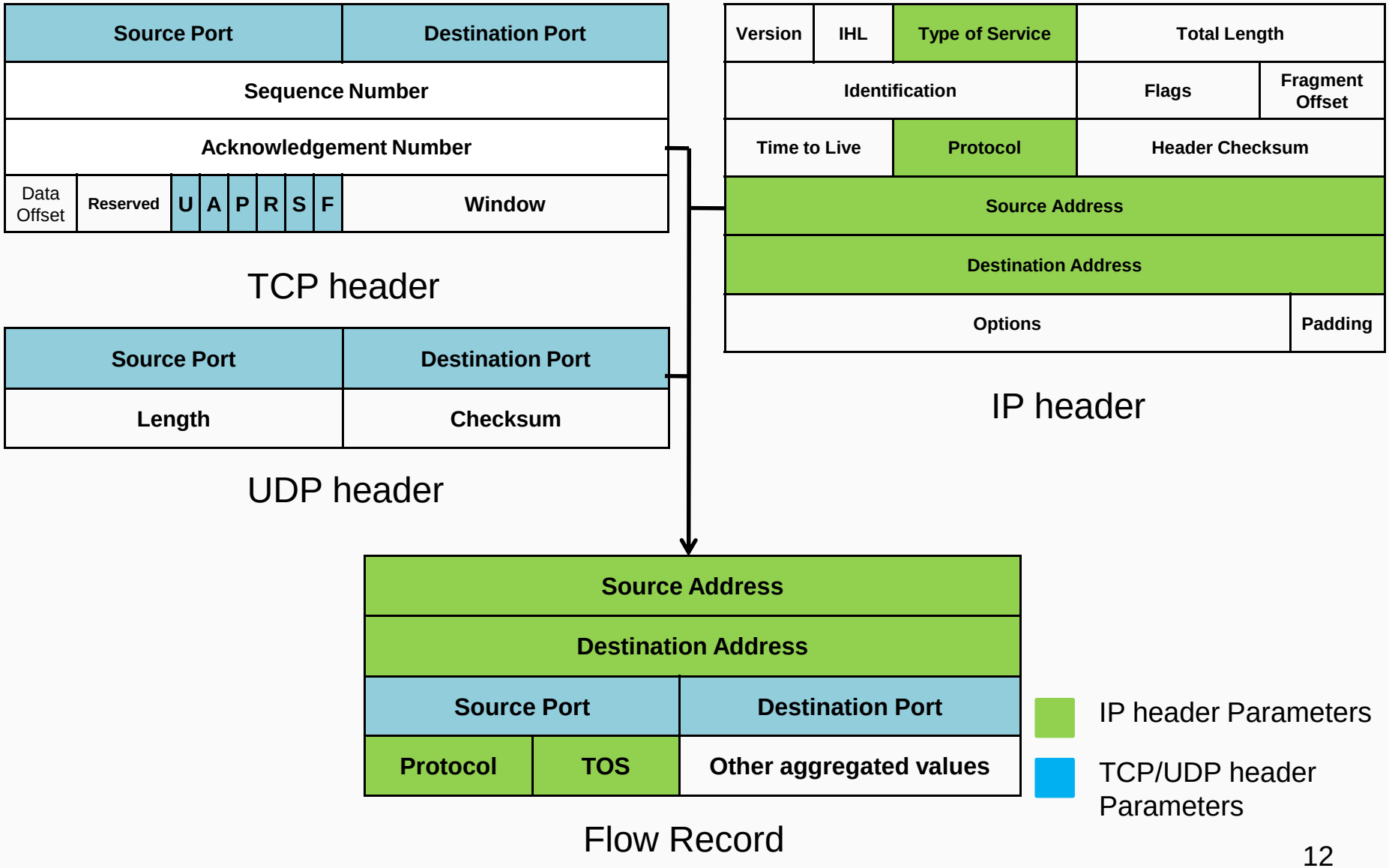
Flow is a unidirectional series of IP packets of a given protocol traveling between a source and a destination (IP, port) pair within a certain period of time.

- Aggregate information from different packets in to a flow
- Different levels of analysis can be possible
- Compared to packet based analysis , volume of data is very less
- Suitable for high speed traffic analysis

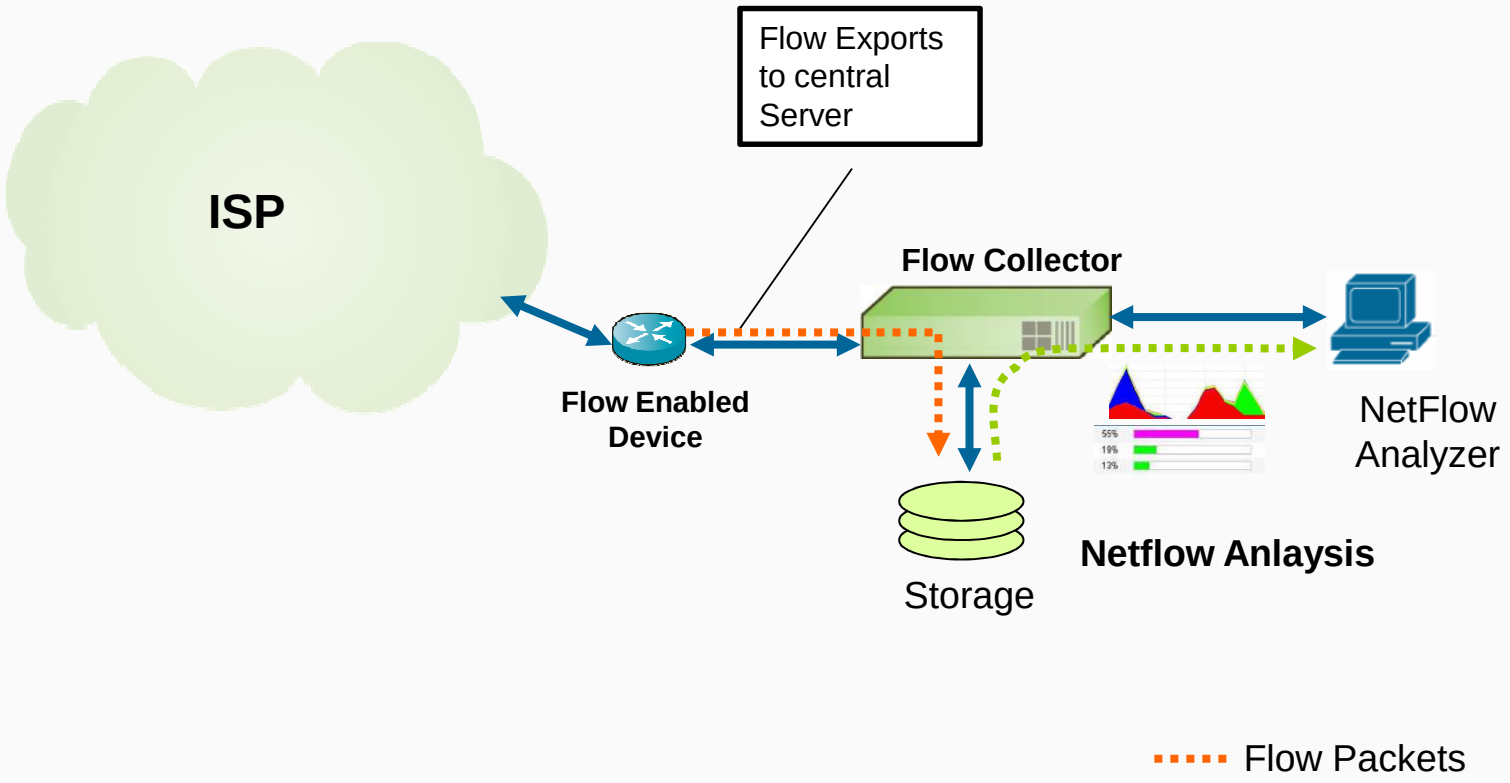
Flow Technologies

- Different vendor specific flow definitions and exporting mechanisms are available
  - Netflow from Cisco
  - Sflow from Inmon
  - Jflow from Juniper
  - NetStream from Huawei
  - Cflowd from Alcatel-Lucent

Flow Record



Network Traffic Flow Collection



Network Traffic Flow Analysis

The network traffic flow data could be used for studying network behaviour, security anomalies and vulnerabilities in a network as given below:

- Rate-Based Anomaly Detection
- Behavioral Anomaly Detection
- Fingerprint Detection
  - Malicious Code Detection

Rate-Based Anomaly Detection

- Baseline Traffic
  - Normal pattern of traffic in the network
  - Maximum and Minimum traffic
  - Traffic volumes for different applications
    - at different points in the network
    - across a span of time to detect a security event
- Distributed Denial-of-Service (DDoS) / Denial-of-Service (DoS) attacks.

Behavioral Anomaly Detection

- Relationships among hosts on the network
  - to pinpoint security threats that may blossom in a very short period of time. e.g. ***a worm, spyware or some other malicious behavior.***

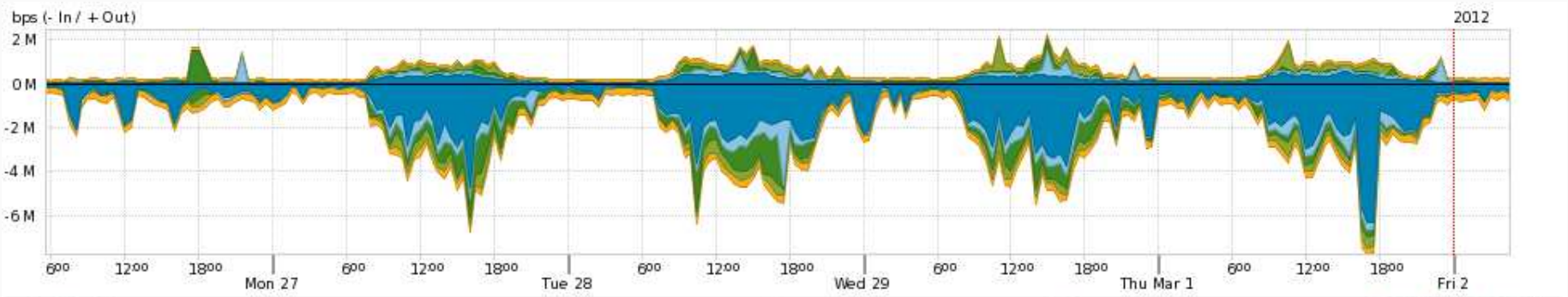
- Anomalous traffic
  - any deviation from the normal traffic pattern which can occur due to different attacks
  - attacks which are not detected by signature based detection techniques

- Inappropriate Usage
  - Free data/one click hosting site access
  - Remote Desktop Access

Fingerprint Detection

- Identifies any traffic that violates a behavioral fingerprint, e.g.
  - Malware
  - inappropriate usage & policy violations
  - Network Scans
    - **low scans, fast scans, “stealth” scans and host sweeps.**

Network Traffic Flow Analysis



Application	In	Out	Total (In + Out)
http	1.19 Mbps	161.89 Kbps	1.35 Mbps
dns	285.96 Kbps	131.16 Kbps	417.13 Kbps
other	281.05 Kbps	82.41 Kbps	363.46 Kbps
ssl	199.16 Kbps	76.82 Kbps	275.97 Kbps
smtp	167.24 Kbps	93.84 Kbps	261.07 Kbps

Network Traffic Flow Analysis

Tools

- NTOP
  - (http://www.ntop.org/netflow.html)
- NfSen and NFDUMP
  - (http://nfdump.sourceforge.net/)
  - (http://nfsen.sourceforge.net/)
- SiLk (System for Internet Level Knowledge) tool kit
  - (http://silktools.sourceforge.net/)
- Flow-Tools and FlowScan
  - (http://www.splintered.net/sw/flow-tools/)
  - (http://net.doit.wisc.edu/~plonka/FlowScan/)
- NetSA Aggregated Flow toolchain
  - (http://aircert.sourceforge.net/naf/)

- Scrutinizer
- Cisco Anomaly Detector
- Arbor PeakFlow SP CP

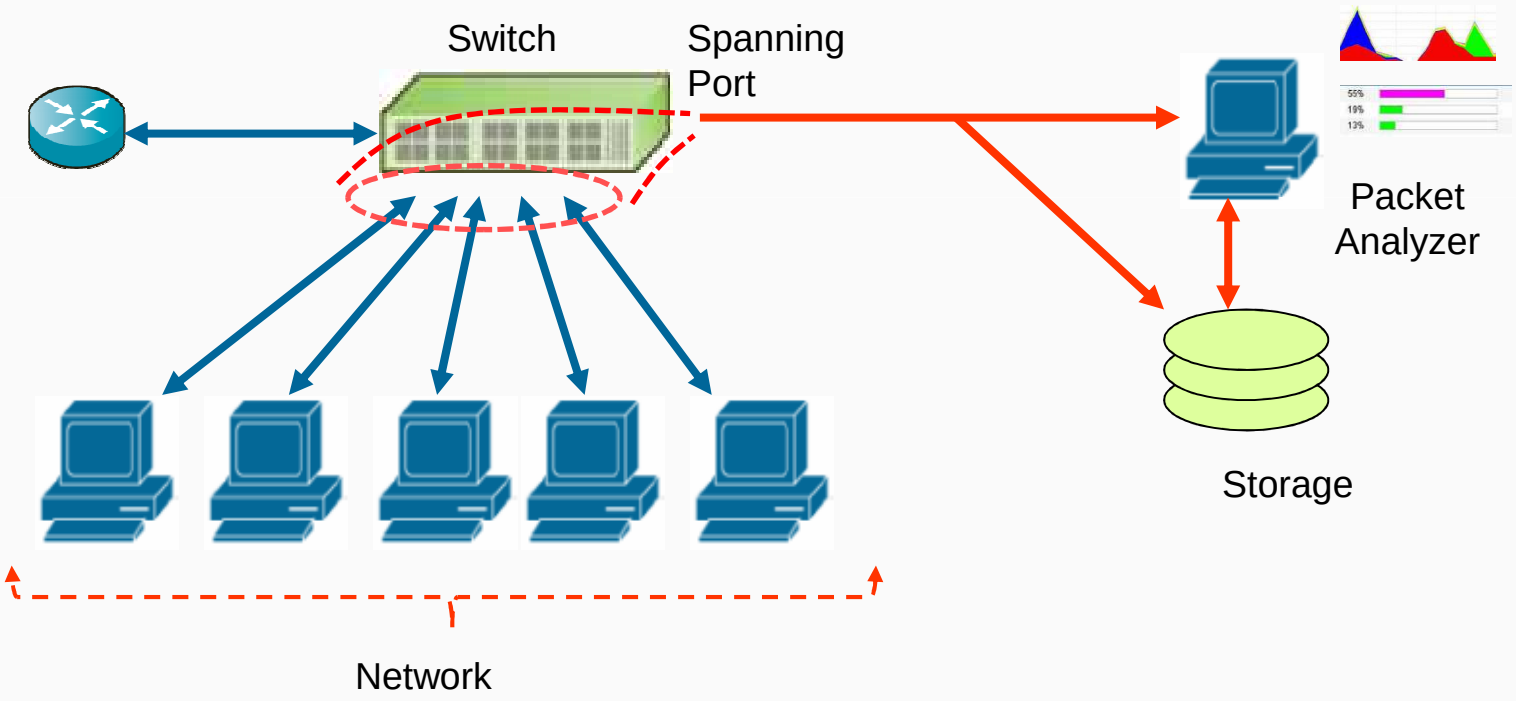
Inline Monitoring

- Capturing the full packet
  - Real time analysis
  - Storing it for forensics
  - Extracting only the metadata
    - for historical analysis

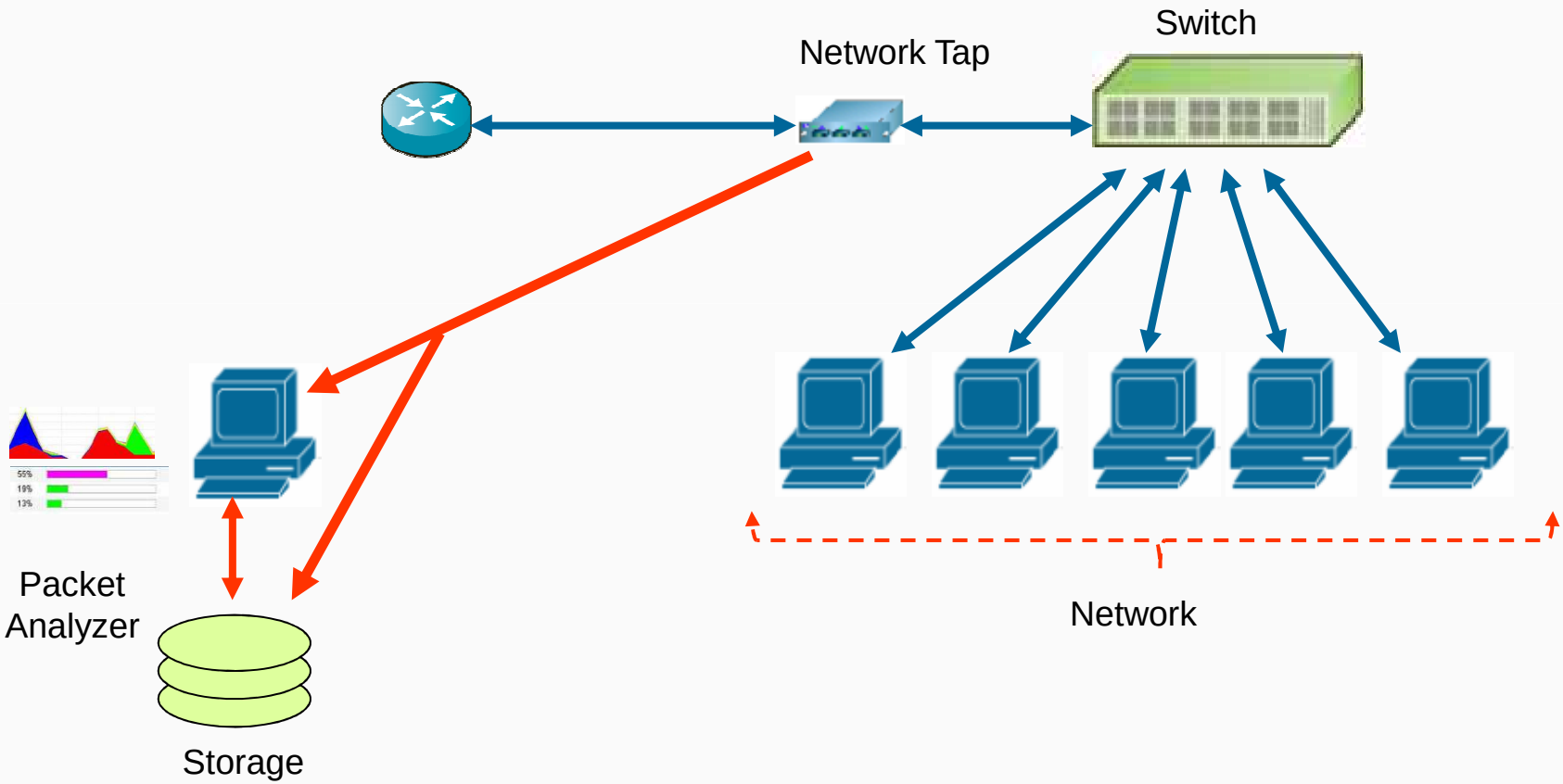
- Detection of Threats/Scans at all levels (Including Application Level threats e.g. “buffer overflow” attacks etc)
- Detection of Malicious code threats within the network
- Analysis of Malicious code behavior
- Forensic analysis of detected threats

- Methods:
  - Port spanning (i.e. mirroring) of the uplink of the switch to another interface so that the packet capture device can see the traffic.
  - In-line appliance to capture/forward the traffic onto multiple destinations. e.g. Network Tap etc.

Inline Monitoring: Port Spanning



Inline Monitoring: Network Tap



Tools

- TCPDump
- NetworkMiner
- Wireshark
- Niksun*
- Netwitness*
- Riverbed*

System/Application Logs

- Log contains critical event level information and can be used for
  - Detecting exploitation and intrusion attempts, e.g. scanning/probing or exploitation attempts, failed login attempts, data theft etc.
  - Forensic analysis of the incidents
- System Logs
  - System logs contain the local event logged by the system or host, e.g.
  - Windows event logs (Application Logs, Security Logs, System Logs)
  - Linux system logs (usually contained in /var/log, and can be centralized using syslog)
- Application Logs
  - Logs of individual server applications e.g.
  - Web Server Logs (IIS, Apache)
  - Mail Server Logs
  - FTP Server Logs
  - Database Server Logs (Oracle, SQL Server, MySQL etc.)
- Tools
  - LogParser, Sawmill, Webalizer, Notepad etc.

Thank You