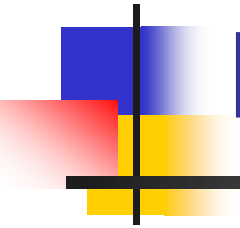


Network Forensics

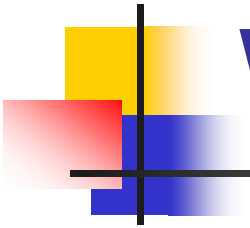
Collecting Network-based Evidence

Prof. Zaheed Shaikh

Department of Computer Engineering

Network Forensics

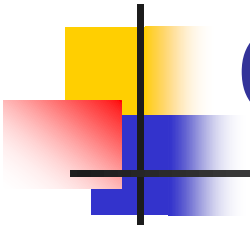
Network based Attacks, Prevention & Allied Tools



Why

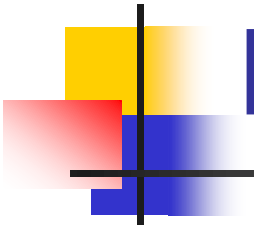
Surveillance

- to confirm suspicion,
- to accumulate evidence,
- to identify co-conspiritors.



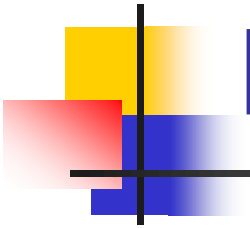
Goals

- Examine suspicion of incident.
- Accumulate additional evidence.
- Verify scope of compromise.
- Identify additional parties involved.
- Determine a timeline.



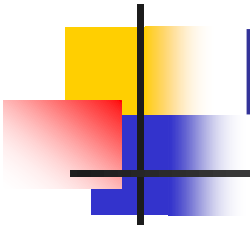
Network Monitoring

- Based on intrusiveness we distinguish:
  - Event Monitoring
    - Looks for certain types of packets representing events.
  - Trap-and-Trace Monitoring
    - Non-content monitoring.
    - Date, Time, Protocol, Source, Destination
  - Full-Content Monitoring
    - Get complete packages.



Network Monitoring System

- Match technologies and capabilities to the situation.
  - Goals of network surveillance.
  - Ensure proper legal standing.
  - Acquire proper hardware and software.
  - Ensure the security of the platform.
  - Evaluate the network monitor.



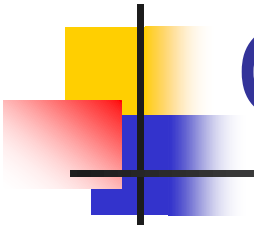
Network Monitoring Goals

- Watch traffic to and from a specific host.
- Monitor traffic to and from a specific network.
- Monitor a specific person's actions.
- Verify intrusion attempts.
- Look for specific attack signatures.
- Focus on a specific protocol.

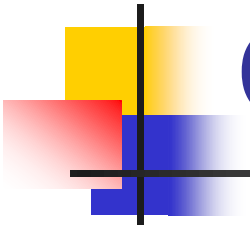
Network Monitoring Tools

- Match hardware power to the task.
  - T3 need 1GHz processor, 1GB RAM
  - Implement proper chain of custody for backup storage.
- Match software properties to the task.
  - OS
  - Remote access?
  - Silent Sniffer?
  - Capture files in portable format?
  - Technical skills needed for monitor.
  - Amount of data

Capturing Data on a Network



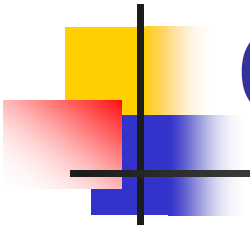
- Develop a threat model before deploying Network Security Monitoring
  - Internal / External Attacker
  - Wireless / Wired / …
- Develop Monitoring zoning
  - Demilitarized zone
  - Wireless zone
  - Intranet zones



Capturing Data on a Network

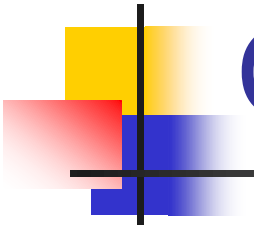
- Wired monitoring
  - Hubs
  - SPAN ports
  - Taps
  - Inline devices

Capturing Data on a Network

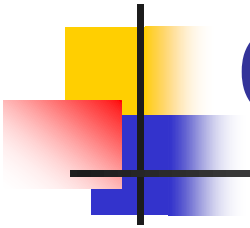


- Hubs
  - Broadcasts incoming data on all interfaces.
  - Be careful about NIC capacity (10/100/1000 Mb/sec)
  - Be careful about hub quality
- Are inexpensive, but can introduce collisions on the links where the hub sits.

Capturing Data on a Network

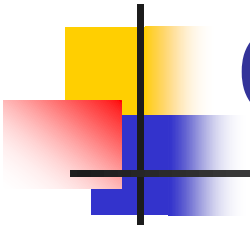


- Switched Port Analyzer (SPAN)
  - A.k.a. Port mirroring, Port monitoring.
  - SPAN port located on enterprise class switches.
  - Copy traffic between certain ports to SPAN port.
  - Configurable
- Easy access to traffic.
- Can make mistakes with configuration.
- Under heavy load, SPAN port might not get all traffic.
- SPAN only allows monitoring of a single switch.



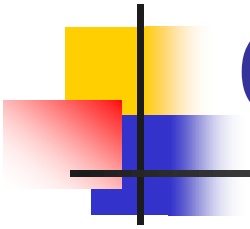
Capturing Data on a Network

- Test Access Port (TAP)
  - Networking device specifically designed for monitoring applications.
  - Typically four ports:
    - Router
    - Firewall
    - Monitor traffic on remaining ports.
      - One port sees incoming, the other outgoing traffic.
- Moderately high costs.



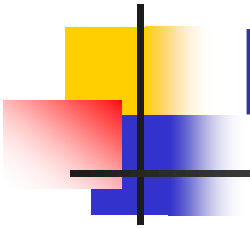
Capturing Data on a Network

- Specialized inline devices:
  - Server or hardware device
    - Filtering bridges
      - E.g. server with OpenBSD and two NICs



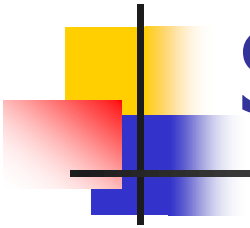
OS for Sniffing

- Requirements:
  - Robust implementation of TCP/IP.
  - SSH for remote access.
  - Simple to disable services.
  - Simple to run local firewall.



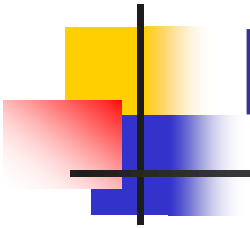
Remote Access

- Network connection.
  - Network adapter.
  - VLAN
  - SSH
  - Firewall restricts IP addresses.
- Modem /”Out of Band” communications
  - User ID / password
  - Calls from specific phone numbers.



Silent Sniffing

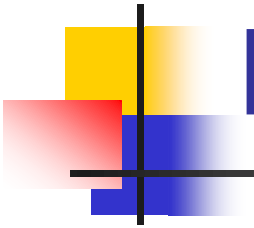
- Sniffing can be detected:
  - Test for cards in promiscuous mode.
  - Sniffers providing name-lookup make DNS queries.
  - Sniffing machines have a higher response rate if the network is flooded.
  - Incorrect implemented TCP/IP stacks react to packets with correct IP address but wrong ethernet address.
- Physically disable traffic from the card.



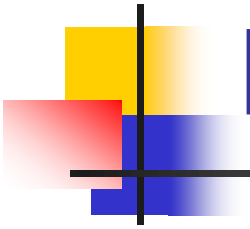
Data File Formats

- Captured traffic goes into a data file.
- Capture files have different formats.
- Proprietary formats can lock you in.
- We will use windump and ethereal.
  - Free
  - Work well.
  - Runs on most platforms.

Deploying the Network Monitor

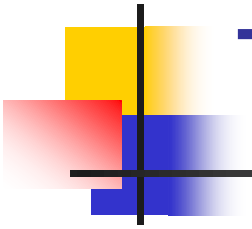


- Physical Security
  - Physical Access => Logical Access.
  - Chain of Custody: Capture files need to be authenticated.



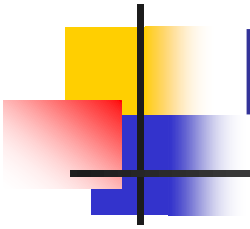
Evaluating the Monitor

- Check Load.
- Check File System.



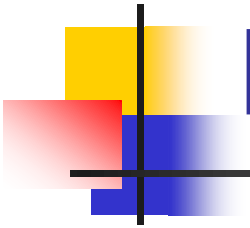
Trap-And-Trace

- Monitors only IP header and TCP header, but no content.
- Legal Issues:
  - Without user supplied data, less privacy violation for corporate users.
  - Without user supplied data, less need for a warrant.
- Tcpdump to screen protects private data.



Full-Content-Monitoring

- Sniffers can capture complete packages.
- Use a filter to block out noise.
- Protect capture files to maintain chain of custody. (file naming, scripting, md5)



Network-Based Logs

Most network traffic leaves an audit trail.

- Routers, firewalls, servers, … maintain logs
- DHCP log IP leases
- Firewalls offer logging.
- IDS can capture part of an attack.
- Host-based sensors detect alteration of libraries
- Login attempts are logged.