CSF 432: Intro to Network and System Security

Week 10 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes

Process Monitoring

Process Monitoring

Log management

- Very diverse log sources
  - And quite large
- Usually sent via syslog
  - Stored in a large drive array
- Massive storage requirement
  - There's never enough
- Data rollup becomes important
  - Take samples every minute
  - Keep 5-minute samples for 30 days
  - After 30 days, rollup to 1 hour sample times

Process Monitoring

Data graphing

- Many different data sources
  - Raw logs
  - Summarized metadata
- Usually managed through a SIEM
  - Turn raw data into something visual
- Graphing can require extensive resource utilization
  - Churn through terabytes of data
- Can use built-in graphs
  - Or build custom reports

Process Monitoring

Port scanning

- Nmap - Network mapper
  - Find and learn more about network devices
- Port scan
  - Find devices and identify open ports
- Operating system scan
  - Discover the OS without logging in to a device
- Service scan
  - What service is available on a device? Name, version, details
- Additional scripts
  - Nmap Scripting Engine (NSE) - extend capabilities, vulnerability scans

Process Monitoring

Vulnerability scanning

- Usually minimally invasive
  - Unlike a penetration test
- Run a vulnerability scanner
  - Poke around and see what's open
- Identify systems and security devices
- Test from the outside and inside
  - Don't dismiss insider threats
- Gather as much information as possible
  - We'll separate wheat from chaff later

Process Monitoring

Vulnerability scan results

- Lack of security controls
  - No firewall, no anti-virus, no anti-spyware
- Misconfigurations
  - Open shares, guest access
- Real vulnerabilities
  - Especially newer ones
  - Occasionally the old ones

Process Monitoring

Patch management

- Incredibly important
  - System stability, security fixes
- Service packs - All at once
- Monthly updates
  - Incremental (and important)
- Emergency out-of-band updates
  - Zero-day and important security discoveries

Process Monitoring

Protocol analyzers

- Solve complex application issues
  - Get into the details
- Gathers packets on the network
  - Or in the air
  - Sometimes built into the device
- View traffic patterns
  - Identify unknown traffic
  - Verify packet filtering and security controls
- Large scale storage
  - Big data analytics

Event Management

Event Management

Interface monitoring

- Up or down
  - The most important statistic
  - No special rights or permissions required
  - Green is good, red is bad
- Alarming and alerting
  - Notification should an interface fail to report
  - Email, SMS
- Short-term and long-term reporting
  - View availability over time
- Not focused on additional details
  - Additional monitoring may require SNMP

Event Management

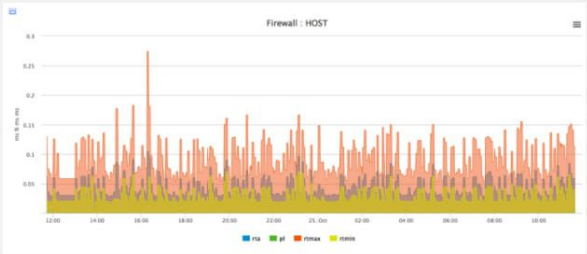
SIEM

- Security Information and Event Management
  - Security events and information
- Security alerts
  - Real-time information
- Log aggregation and long-term storage
  - Usually includes advanced reporting features
- Data correlation
  - Link diverse data types
- Forensic analysis
  - Gather details after an event

Event Management

Syslog

- Standard for message logging
  - Diverse systems, consolidated log
- Usually a central logging receiver
  - Integrated into the SIEM
- You're going to need a lot of disk space



Event Management

SNMP

- Simple Network Management Protocol
  - A database of data (MIB) Management Information Base
- SNMP v1 - The original
  - Structured tables, in-the-clear
- SNMP v2 – A good step ahead
  - Data type enhancements, bulk transfers, still in-the-clear
- SNMP v3 - The new standard
  - Message integrity, authentication, encryption
- SNMP information can be very detailed
  - Access should be very limited

Performance Metrics

Performance Metrics

Monitoring the interface

- Often your first sign of trouble
  - The local problems are easy to attack
- Can sometimes indicate a bigger issue
  - Problem with a switch or congestion in the network
- View in the operating system
  - Interface details
- Monitor with SNMP
  - Remote monitoring of all devices
  - Most metrics are in MIB-II

Performance Metrics

Interface monitoring

- Link status - link up, or link down?
  - May be a problem on the other end of the cable
- Error rate
  - Problems with the signal - CRC error, runt, giant
- Utilization
  - Per-interface network usage
  - Run bandwidth tests to view throughput
- Discards, packet drops
  - No errors in the packet, but system could not process
- Interface resets
  - Packets are queued, but aren't sent
  - Connection is good, but line protocols aren't talking
  - Reset and hope for the best
- Speed and duplex
  - These should match on both sides
  - Auto speed and auto duplex isn't always the best option
  - Check for expected throughput

Remote Access

Remote Access

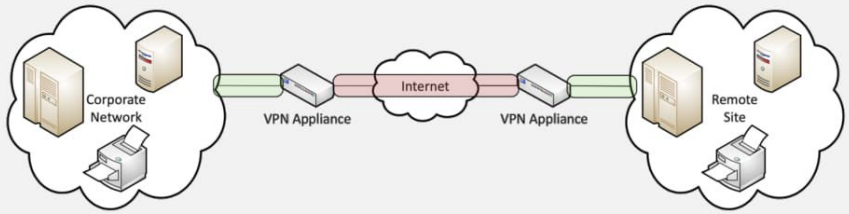
IPSec (Internet Protocol Security)

- Security for OSI Layer 3
  - Authentication and encryption for every packet
- Confidentiality and integrity/anti-replay
  - Encryption and packet signing
- Very standardized
  - Common to use multi-vendor implementations
- Two core IPSec protocols
  - Authentication Header (AH)
  - Encapsulation Security Payload (ESP)

Remote Access

Site-to-Site VPNs

- Encrypt traffic between sites
  - Through the public Internet
- Use existing Internet connection
  - No additional circuits or costs



Remote Access

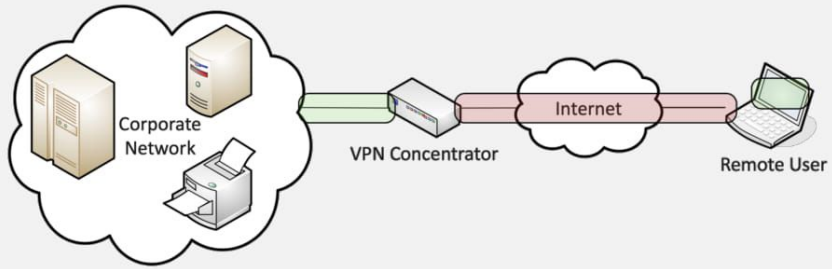
SSL VPN (Secure Sockets Layer VPN)

- Uses common SSL/TLS protocol (tcp/443)
  - Avoids running into most firewall issues
- No big VPN clients
  - Usually remote access communication
- Authenticate users
  - No requirement for digital certificates or shared passwords (like IPSec)
- Can be run from a browser or from a light VPN client
  - Across many operating systems

Remote Access

Host-to-Site VPNs

- Also called “remote access VPN”
- Requires software on the user device
  - May be built-in to existing operating system



Remote Access

DTLS VPN

- Datagram Transport Layer Security
  - The security of SSL/TLS, the speed of datagrams
  - Transport using UDP instead of TCP
- TCP brings some great features
  - Packet reordering
  - Retransmission of lost/dropped data
- TCP sometimes gets in the way
  - Streaming, VoIP
  - When you lose a packet, it’s too late to recover it

Remote Access

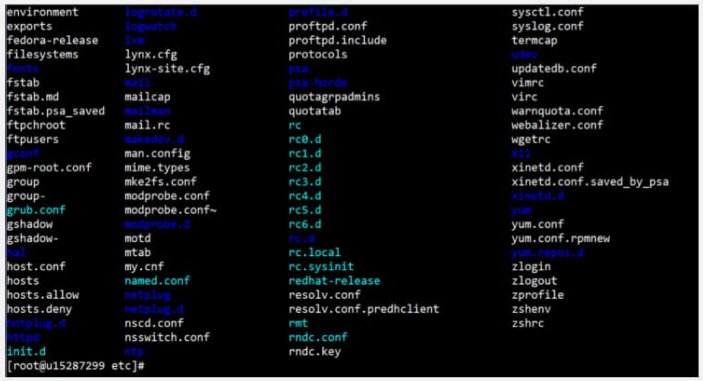
Remote desktop access

- Share a desktop from a remote location
  - It’s like you’re right there
- RDP (Microsoft Remote Desktop Protocol)
  - Clients for Mac OS, Linux, and others as well
- VNC (Virtual Network Computing)
  - Remote Frame Buffer (RFB) protocol
  - Clients for many operating systems
- Commonly used for technical support - and for scammers

Remote Access

SSH (Secure Shell)

- Encrypted console communication - tcp/22
- Looks and acts the same as Telnet - tcp/23



Remote Access

Web-based management console

- Your browser
  - The universal client
- Manage a device from an encrypted web-based front-end
  - Connect to the HTTPS URL and login
- The important features are in the browser
  - You may need the CLI for the detailed operations

Remote Access

Transferring files

- FTP – File Transfer Protocol
  - Transfers files between systems
  - Authenticates with a username and password
  - Full-featured functionality (list, add, delete, etc.)
- FTPS
  - FTP over SSL (FTP-SSL)
  - File Transfer Protocol Secure
  - This is not SFTP
- SFTP
  - SSH File Transfer Protocol
  - Provides file system functionality
  - Resuming interrupted transfers, directory listings, remote file removal
- TFTP – Trivial File Transfer Protocol
  - Very simple file transfer application
  - Read files and write files
  - No authentication
  - May be used to download configurations
  - VoIP phones

Remote Access

Out-of-band management

- The network isn't available
  - Or the device isn't accessible from the network
- Most devices have a separate management interface
  - Usually a serial connection / USB
- Connect a modem
  - Dial-in to manage the device
- Console router / comm server
  - Out-of-band access for multiple devices
  - Connect to the console router, then choose where you want to go

Policies and Best Practices

Policies and Best Practices

Privileged user agreement

- Network/system administrators have access to almost everything
  - With great power comes great responsibility
- Expectations
  - Use other non-privileged methods when appropriate
- Limitations
  - Use privileged access only for assigned job duties
- Signed agreement
  - Everyone understands the policies

Policies and Best Practices

Password policies

- Written policy
  - All passwords should expire every 30 days, 60 days, 90 days, etc.
- Critical systems might change more frequently
  - Every 15 days or every week
- The recovery process should not be trivial!
  - Some organizations have a very formal process

Policies and Best Practices

On-boarding

- Bring a new person into the organization
  - New hires or transfers
- IT agreements need to be signed
  - May be part of the employee handbook or a separate AUP
- Create accounts
  - Associate the user with the proper groups and departments
- Provide required IT hardware
  - Laptops, tablets, etc.
  - Preconfigured and ready to go

Policies and Best Practices

Off-boarding

- All good things...
  - But you knew this day would come
- This process should be pre-planned
  - You don't want to decide how to do things at this point
- What happens to the hardware and the data?
- Account information is usually deactivated
  - But not always deleted

Policies and Best Practices

Licensing restrictions

- So many licenses
  - Operating systems, applications, hardware appliances
  - And they all use different methods to apply the license
- Availability
  - Everything works great when the license is valid
  - Meeting the expiration date may cause problems
  - Application may stop working completely
- Integrity
  - Data and applications must be accurate and complete
  - A missing/bad license may cause problems with data integrity

Policies and Best Practices

International export controls

- Equipment, information, data
  - Country-specific laws controlling export
- Not only shipment of physical items
  - Includes the transfer of software or information
  - Protect PII
- Dual-use software can be controlled
  - Dual-use for both civilian and military use
  - Security software, malware, hacking tools
- Check with legal team - don't ship unless you're sure

Policies and Best Practices

Data Loss Prevention (DLP)

- Where's your data?
  - Social Security numbers, credit card numbers, medical records
- Detailed policies needed to define what is allowed
  - How is sensitive data transferred?
  - Is the data encrypted? How?
- DLP solutions can watch and alert on policy violations
  - Often requires multiple solutions in different places

Policies and Best Practices

Remote access policies

- Easy to control internal communication
  - More difficult when people leave the building
- Policy for everyone
  - Including third-party access
- Specific technical requirements
  - Encrypted connection, confidential credentials, use of network, hardware and software requirements

Policies and Best Practices

Security incidents

- User clicks an email attachment and executes malware
  - Malware then communicates with external servers
- DDoS
  - Botnet attack
- Confidential information is stolen
  - Thief wants money or it goes public
- User installs peer-to-peer software and allows external access to internal servers

Policies and Best Practices

Incident response policies

- How is an incident identified?
  - Automated monitoring, personal account
- How is the incident categorized?
  - Email issue, brute force attack, DDoS, etc.
- Who responds to an incident?
  - Large list of predefined contacts
- What process is followed?
  - Formal process needs to be created prior to the incident

Policies and Best Practices

BYOD

- Bring Your Own Device or Bring Your Own Technology
- Employee owns the device
  - Need to meet the company's requirements
- Difficult to secure
  - It's both a home device and a work device
  - How is data protected?
  - What happens to the data when a device is sold or traded in?

Policies and Best Practices

Acceptable use policies (AUP)

- What is acceptable use of company assets?
  - Detailed documentation
  - May be documented in the Rules of Behavior
- Covers many topics
  - Internet use, telephones, computers, mobile devices, etc.
- Used by an organization to limit legal liability
  - If someone is dismissed, these are the well-documented reasons why

Policies and Best Practices

Non-disclosure agreement

- NDA (Non-disclosure agreement)
  - Confidentiality agreement / Legal contract
  - Prevents the use and dissemination of confidential information
- Internal
  - Protect the organization's private and confidential information
  - Part of employee security policies
- External
  - Two parties can't disclose private information or company secrets about the other party

Policies and Best Practices

System life cycle

- Managing asset disposal
  - Desktops, laptops, tablets, mobile devices
- Disposal becomes a legal issue
  - Some information must not be destroyed
  - Consider offsite storage
- You don't want critical information in the trash
  - People really do dumpster dive
  - Recycling can be a security concern

Policies and Best Practices

Physical destruction

- Shredder / pulverizer
  - Heavy machinery - complete destruction
- Drill / Hammer
  - Quick and easy - platters, all the way through
- Electromagnetic (degaussing)
  - Remove the magnetic field
  - Destroys the drive data and the electronics
- Incineration

Policies and Best Practices

Safety procedures and policies

- Equipment safety
  - Electrical safety policies
- Personal safety
  - Jewelry policy, lifting techniques, fire safety, cable management, safety goggles, etc.
- Handling of toxic waste
  - Batteries, toner
  - Refer to the MSDS (Material Safety Data Sheet)
- Local government regulations
  - Safety laws, building codes, environmental regulations

CSF 432: Intro to Network and System Security

Week 10 - Review

Michael Conti

Department of Computer Science and Statistics
University of Rhode Island

Fall 2020

Sources: Professor Messer's CompTIA N10-007 Network+ Course Notes