Chapter 4

Tools of the Trade

Episode 4.01

Episode title: **Touring the Command-Line Interface**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Quick Review

- Windows offers both the standard Command shell as well as the more robust PowerShell
- macOS uses Terminal as the command-line interface (CLI)
- Linux CLIs are often referred to as the terminal, shell, console, or prompt
- ping queries other systems on a TCP/IP network to determine connectivity
- ipconfig (Windows) and ifconfig (Mac/Linux) show the current status of the network settings for a host system

Episode 4.02

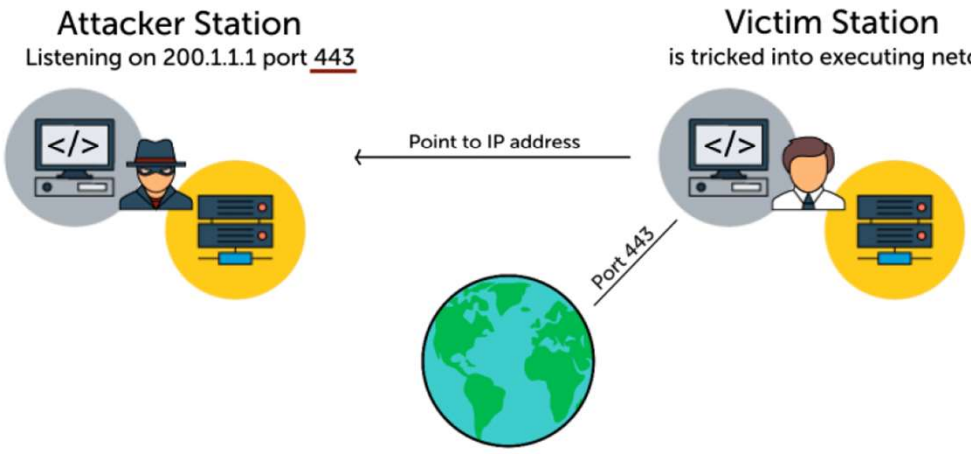
Episode title: **Shells**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Command-Line Environments

- Windows command line
- Microsoft PowerShell
- Linux shells
- Python
- Benefits
  - Automation via scripts

Netcat Reverse Shell



Reverse Shells

- Attackers often try to get a reverse shell (backdoor)
- Advanced persistent threat (APT)
  - Attacker has a way into the system repeatedly
- Tools
  - netcat (nc)
  - Metasploit framework
  - Cobalt Strike

Quick Review

- Command-line environments include the Windows command prompt, Microsoft PowerShell, Linux shells, and Python scripts
- Reverse shells involve victims' stations contacting attacker stations listening for connections
- Reverse shells can be used as an advanced persistent threat (APT)

Episode 4.03

Episode title: **The Windows Command Line**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Windows Command Line

- cmd.exe
- May need to run with elevated privileges
- Demo Windows commands
  - whoami
  - set (for env vars)
  - regedit
  - powershell.exe
- Batch file scripts (.BAT)

Quick Review

- The Windows command prompt is spawned from cmd.exe
- Batch file scripts have a .BAT extension
- Common Windows commands include whoami, ipconfig, and powershell

Episode 4.04

Episode title: **Microsoft PowerShell**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Microsoft PowerShell

- Can run in Windows, Linux, macOS
- Powershell.exe
- Object-oriented
- May need to run with elevated privileges
- PowerShell scripts (.PS1)

Microsoft PowerShell

- Demo PowerShell
  - get-command *physicaldisk*
  - get-help get-physicaldisk
  - get-physicaldisk | fl
  - get-physicaldisk | select friendlyname, mediatype, size
  - get-service
- Show PowerShell ISE

Quick Review

- PowerShell is an object-oriented command-line tool
- PowerShell works on Windows, Linux, and the macOS
- PowerShell cmdlets take the form of verb-noun (get-service)

Episode 4.05

Episode title: **Linux Shells**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Linux Shells

- Syntax is case-sensitive
- Various types of shells
  - C shell
  - Korn shell
  - Bourne again shell (bash)
- Shell scripts (.sh)
  - Must be flagged as executable

Linux Shells

- Don’t sign in with the root account
- sudo command prefix
  - Runs commands with elevated privileges
  - User must be listed in sudoers
- Remotely accessible via Secure Shell (SSH) over TCP port 22

SSH Public Key Authentication

- ssh-keygen -t rsa
  - Creates ~/.ssh/id_rsa (private key)
  - Creates ~/.ssh/id_rsa.pub (public key)
- ssh-copy-id -i ~/.ssh/id_rsa.pub user@host
- ssh -i ~/.ssh/id_rsa user@host

Linux Shells

- Demo PuTTY SSH connection to bash
  - ls
  - whoami
  - sudo
  - ifconfig
  - mount

Quick Review

- Linux shells are case-sensitive
- Linux shells are not object-oriented
- Linux shell scripts normally end with .sh and must be flagged as executable
- The sudo command prefix runs with elevated privileges

Episode 4.06

Episode title: **Python Scripts**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Python

- Multi-platform
- Supports more complex needs than shell scripts
- Syntax is case-sensitive
- Python scripts (.py)

Python

- Show and run Python script in Linux
- #!/usr/bin/env python
- kmh = int(raw_input("Enter km/h: "))
- mph = 0.6214 * kmh
- print "Speed:", kmh, "KM/H = ", mph, "MPH"

Quick Review

- Python scripts run on any platform with a Python interpreter installed
- Python is case-sensitive and is generally more powerful than Linux shell scripts

Episode 4.07

Episode title: **Windows Command-Line Tools**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Windows Command-Line Tools

- ping
  - Tests whether remote node responds
  - Based on Internet Control Message Protocol (ICMP) (blocked by most firewalls)
- ipconfig
  - View TCP/IP settings
  - Perform basic tasks (Eg: DHCP renewal)

Windows Command-Line Tools

- arp
  - Address resolution protocol (ARP)
  - Converts IP address to NIC MAC address mapping
  - Shows arp table in memory
- netstat
  - View TCP/IP network statistics and connection states
- route
  - View and manage IP routes

Windows Command-Line Tools

- tracert
  - Track each router (hop) on the way to a target IP address
- pathping
  - Combines ping with tracert
- nslookup
  - Name server lookup
  - Test and troubleshoot DNS name resolution
  - Can be used for reconnaissance
- dig
- icacls
  - Manage NTFS file system permissions

Quick Review

- ping tests connectivity while tracert shows each hop in the path; pathping combines both
- Network commands include ipconfig, arp, netstat, and route
- nslookup is used to test DNS name resolution
- icacls manages NTFS file system permissions

Episode 4.08

Episode title: **Linux Command-Line Tools**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Linux Command-Line Tools

- Linux commands are case-sensitive
- cat
  - View the contents of a text file
- grep
  - Line filtering tool

Linux Command-Line Tools

- head/tail
  - Show beginning/ending number of lines
- logger
  - Writes entries to the Linux system log

Linux Command-Line Tools

- ifconfig
  - View network interface configurations
- ip
  - Supersedes ifconfig
- traceroute
  - Show each router (hop) to target IP
- dig
  - Test DNS name resolution

Linux Command-Line Tools

- chmod
  - Manage Linux filesystem permissions

Read - 4
Write - 2
Execute - 1

chmod 740 myfile.txt

File owner gets 7 (rwx)
File group gets 4 (r)
Other gets 0 ()

Quick Review

- Linux commands are case-sensitive
- Text manipulation commands include cat, grep, head, and tail
- logger writes to the system log
- chmod manages file system permissions
- Network commands include ifconfig, ip tracert, and dig

Episode 4.09

Episode title: **Network Scanners**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

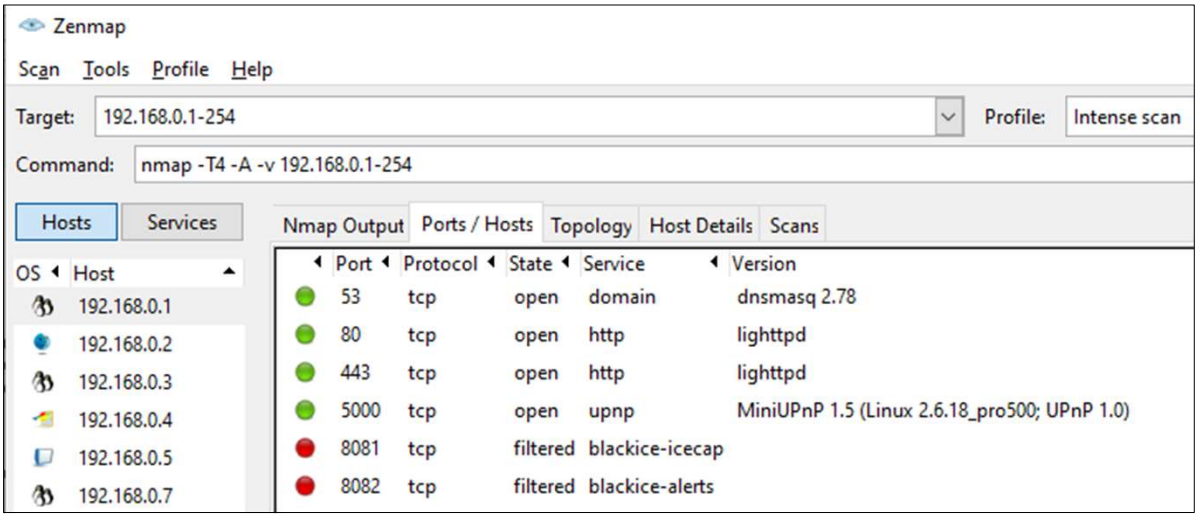
Network Scanners

- Attackers use this for reconnaissance
- Very loud on the network (easily detected)
- Scan network nodes and show
  - IP address
  - MAC address
  - Operating system
  - Open ports

Network Scanners

- Periodic scans
  - Identify differences (rogue systems, new listening ports)
- Nmap
  - Network mapper
  - https://nmap.org
  - Zenmap frontend GUI

Zenmap GUI


Zenmap
Scan Tools Profile Help
Target: 192.168.0.1-254
Profile: Intense scan
Command: nmap -T4 -A -v 192.168.0.1-254
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
192.168.0.1
192.168.0.2
192.168.0.3
192.168.0.4
192.168.0.5
192.168.0.7
Port
Protocol
State
Service
Version
53 tcp open domain dnsmasq 2.78
80 tcp open http lighttpd
443 tcp open http lighttpd
5000 tcp open upnp MiniUPnP 1.5 (Linux 2.6.18_pro500; UPnP 1.0)
8081 tcp filtered blackice-icecap
8082 tcp filtered blackice-alerts

Quick Review

- Nmap is a network scanner that identifies nodes, IP addresses, MAC addresses, OS, and port number details
- Periodic scans allow comparing to previous scans to identify changes

Episode 4.10

Episode title: **Network Scanning with Nmap**

Objective: **4.1 Given a scenario, use the appropriate tool to assess organizational security.**

Nmap

- Demo Nmap/Zenmap GUI
  - Show how to start scan
  - Open existing scan file

Quick Review

- Zenmap is a frontend GUI to Nmap
- Nmap can be used at the command line
- Nmap scans can be saved as .XML files

Episode 4.11

Episode title: **Network Protocol Analyzers**

Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Network Protocol Analyzers

- Capture network traffic
  - Network placement is crucial
  - Hardware device or software
  - Network switch port analyzer (SPAN) copies all VLAN traffic to one switch port

Network Protocol Analyzers

- Wired and wireless capturing
- Captures can be saved
- Packets are easily forged with free tools such as hping3

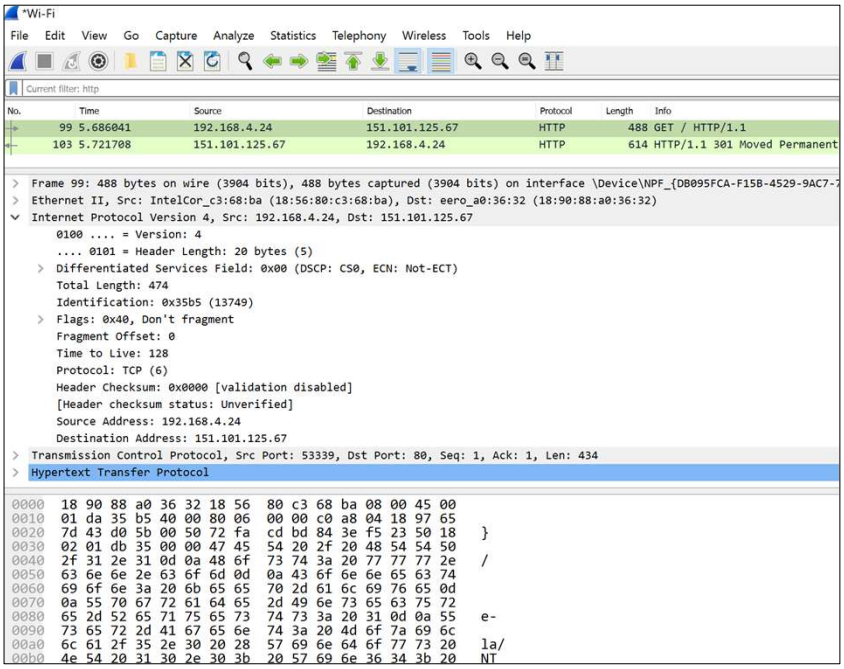
Network Protocol Analyzers

- Filter and analyze captured traffic
  - Capture and display filters
  - View packet headers (addressing)
  - View packet payload (data)
  - Analyze TCP streams

Network Protocol Analyzers

- tcpdump in Linux
- Cisco NetFlow
  - Capture IP traffic on routers
  - Similar to the sFlow standard
  - Superseded by IPFIX standard

Wireshark


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Current filter: http
No. Time Source Destination Protocol Length Info
99 5.686041 192.168.4.24 151.101.125.67 HTTP 488 GET / HTTP/1.1
103 5.721708 151.101.125.67 192.168.4.24 HTTP 614 HTTP/1.1 301 Moved Permanent
Frame 99: 488 bytes on wire (3904 bits), 488 bytes captured (3904 bits) on interface \Device\NPF_{DB095FCA-F15B-4529-9AC7-7
Ethernet II, Src: IntelCor_c3:68:ba (18:56:80:c3:68:ba), Dst: eero_a0:36:32 (18:90:88:a0:36:32)
Internet Protocol Version 4, Src: 192.168.4.24, Dst: 151.101.125.67
0100 .... = Version: 4
.... 0101 = Header Length: 20 bytes (5)
Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
Total Length: 474
Identification: 0x35b5 (13749)
Flags: 0x40, Don't fragment
Fragment Offset: 0
Time to Live: 128
Protocol: TCP (6)
Header Checksum: 0x0000 [validation disabled]
[Header checksum status: Unverified]
Source Address: 192.168.4.24
Destination Address: 151.101.125.67
Transmission Control Protocol, Src Port: 53339, Dst Port: 80, Seq: 1, Ack: 1, Len: 434
Hypertext Transfer Protocol
0000 18 90 88 a0 36 32 18 56 80 c3 68 ba 08 00 45 00
0010 01 da 35 b5 40 00 80 06 00 00 c0 a8 04 18 97 65
0020 7d 43 d0 5b 00 50 72 fa cd bd 84 3e f5 23 50 18 }
0030 02 01 db 35 00 00 47 45 54 20 2f 20 48 54 54 50
0040 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77 77 2e /
0050 63 6e 6e 2e 63 6f 6d 0d 0a 43 6f 6e 6e 65 63 74
0060 69 6f 6e 3a 20 6b 65 65 70 2d 61 6c 69 76 65 0d
0070 0a 55 70 67 72 61 64 65 2d 49 6e 73 65 63 75 72
0080 65 2d 52 65 71 75 65 73 74 73 3a 20 31 0d 0a 55 e-
0090 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f 7a 69 6c
00a0 6c 61 2f 35 2e 30 20 28 57 69 6e 64 6f 77 73 20 la/
00b0 4e 54 20 31 30 2e 30 3b 20 57 69 6e 36 34 3b 20 NT

Quick Review

- Protocol analyzers allow the capture and analysis of network traffic
- Network placement determines what traffic will be seen
- Captures can be saved
- Be aware that packets are easily forged

Episode 4.12

Episode title: **Using Wireshark to Analyze Network Traffic**

Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Using Wireshark to Analyze Network Traffic

- Demo Wireshark

Quick Review

- Wireshark is a free GUI tool
- Packet headers are used for addressing
- Packet payloads contain data
- Captures can be filtered by many attributes

Episode 4.13

Episode title: **Using tcpdump to Analyze Network Traffic**

Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Using tcpdump to Analyze Network Traffic

- Demo tcpdump

Quick Review

- tcpdump is a command-line utility built into Linux
- You can specify which interface to capture traffic from
- Captured files can be saved and analyzed at a later date

Episode 4.14

Episode title: **Log Files**

Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Log Files

- Network, host, and device monitoring
- Potential indicators of compromise (IoC)
- Must ensure log files are secure
  - Forward log entries to a centralized logging host

Log Tools

- Windows log tools
  - Event Viewer
  - PowerShell
    - get-eventlog
- Linux logs
  - /var/log
  - logger
  - journalctl
- Device logs
  - Network printer, wireless AP, etc

Windows Log Files

- Demo Event Viewer

Linux Log Files

- Demo viewing Linux logs

Quick Review

- Log files can be used for network, host, and device monitoring as well as detecting indicators of compromise (IoC)
- Log files must be kept secure
- Windows log tools include the Event Viewer and get-eventlog in PowerShell
- Linux logs can usually be found in /var/log or by using the logger command

Episode 4.15

Episode title: **Centralized Logging**

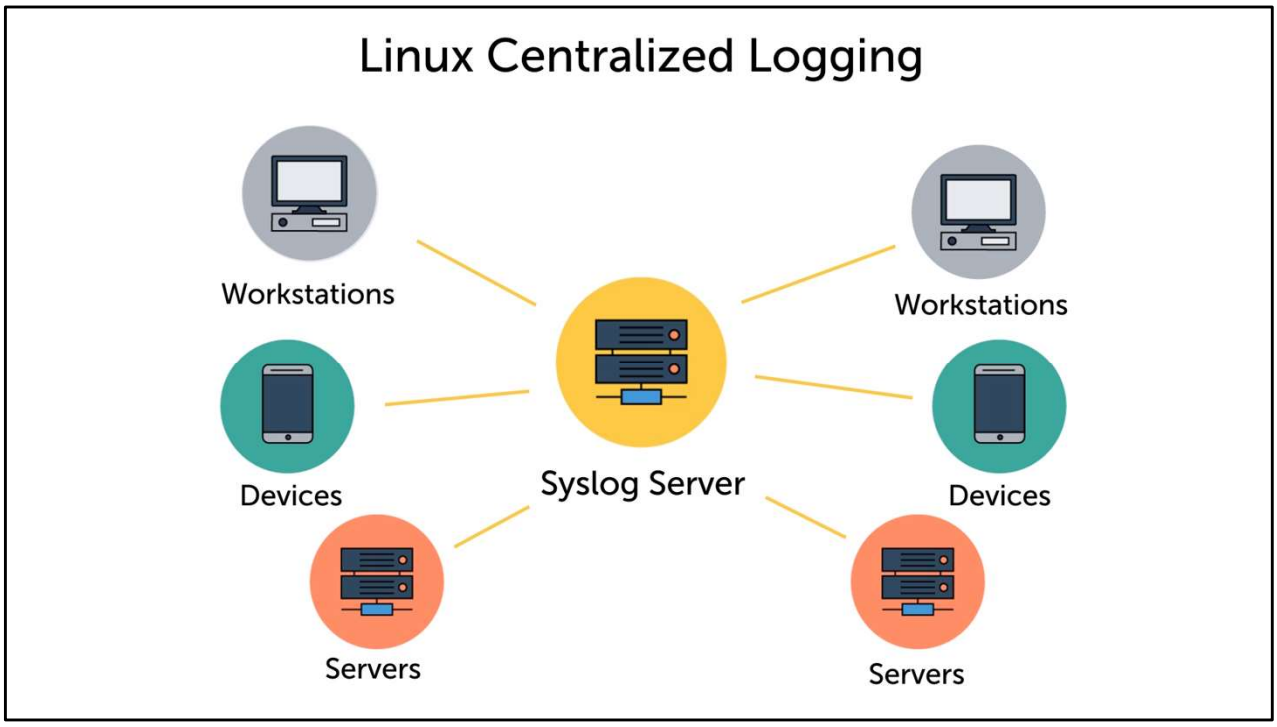
Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Centralized Logging

- Simple Network Management Protocol (SNMP)
  - Bandwidth monitoring
  - Software agent or built into firmware
    - Management Information Base (MIB)
  - SNMP traps notify SNMP management stations
- NXLog
  - Open-source log collection tool

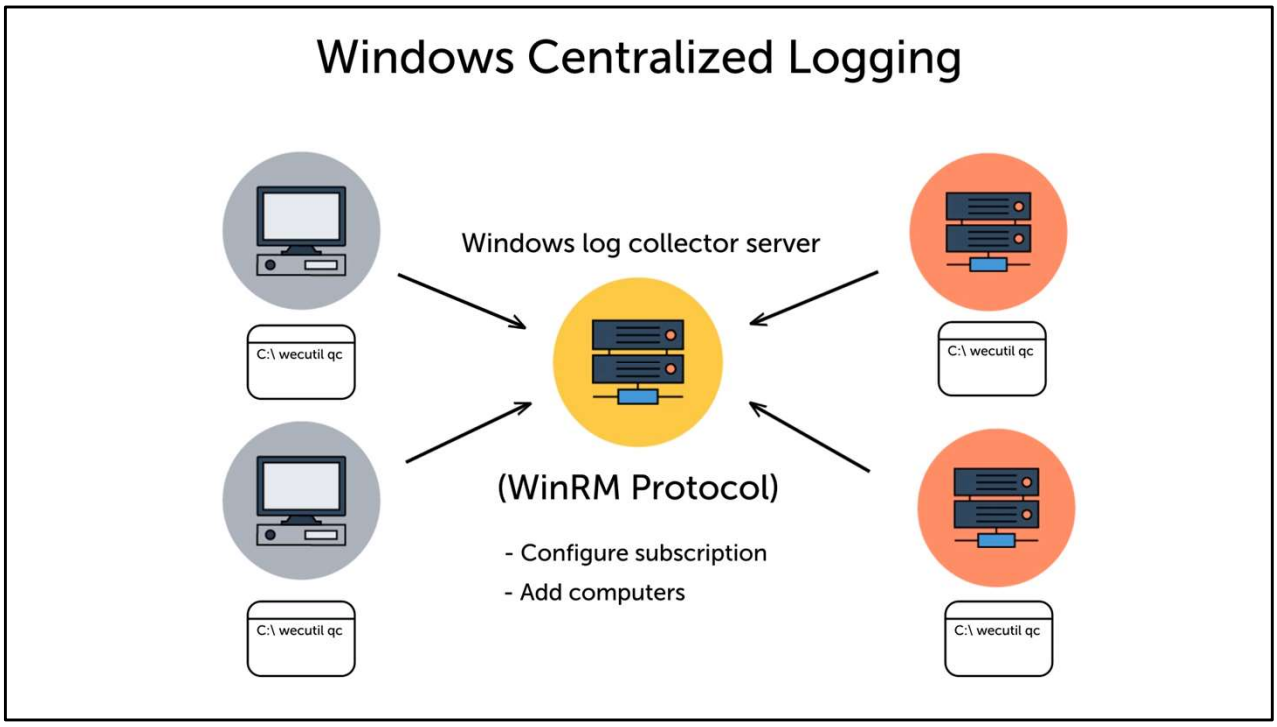
Linux Centralized Logging

- Syslog/rsyslog
- Normally uses UDP port 514
- Filter traffic that gets sent


Linux Centralized Logging
Workstations
Workstations
Devices
Syslog Server
Devices
Servers
Servers

Windows Centralized Logging

- Event Viewer subscriptions
  - Send local log data to a collector server over the WinRM protocol


Windows Centralized Logging
Windows log collector server
C:\ wecutil qc
C:\ wecutil qc
C:\ wecutil qc
C:\ wecutil qc
(WinRM Protocol)
- Configure subscription
- Add computers

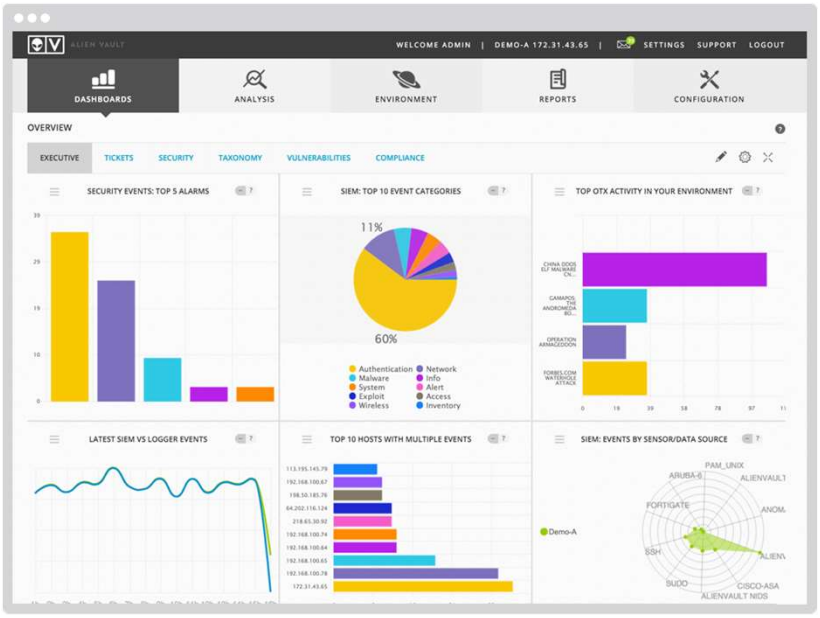
Security Information and Event Management (SIEM)

- Sensors/collectors
  - Logs, intrusion detection/ prevention system (IDS/IPS), packet captures, antivirus
- Enterprise-level centralized log ingestion service
- Dashboard visualizations
  - Alerts, packet captures, malware alerts, etc.
  - Identify trends and correlation

SIEM Process

- Data inputs
- Log aggregation
- Analysis
- Review reports

Alien vault SIEM dashboard



Quick Review

- Linux centralized logging can be done using syslog/rsyslog
- Windows centralized logging can be done using Event Viewer subscriptions
- Centralized logging and alerting for any type of device is done using a SIEM solution

Episode 4.16

Episode title: **Configuring Linux Log Forwarding**

Objective: **4.3 Given an incident, utilize appropriate data sources to support an investigation.**

Demo

- Configure Linux log forwarding using 2 Ubuntu Linux VMs

Quick Review

- Linux log forwarding can be achieved using rsyslog
- Source host logs continue to exist
- Filters control which events get forwarded