Endpoint Telemetry & Analysis - Overview

Brian Olliff

Defensive Engineering Instructor

Key Concepts

+ Host and endpoint data
+ Endpoint analysis
+ Endpoint security

MAJOR TOPICS

- Host data and telemetry
- Analysis of Windows endpoints
- Analysis of Linux-based systems
- Endpoint security

LEARNING OUTCOMES

- Understand where logging data can be found on endpoints and in network traffic
- Be familiar with methods to investigate running processes on Windows and Linux
- Be able to explain how Linux permissions are structured and configured
- Understand the fundamentals of endpoint security techniques

PREREQUISITES

- Basic network and IT knowledge
- Basic understanding of cybersecurity fundamentals
- Fundamental Windows and Linux administration

Let’s Get Started!

Endpoint Telemetry & Analysis

+ Aligned with Cisco CyberOps Associate
+ Starting with general endpoint/host telemetry information
+ Windows and Linux permissions and logs

Endpoint Logs

User Endpoints

- Endpoint types
  - Workstations (desktop and laptop)
    - On prem and remote
  - Mobile devices (tablets and phones)
- Important information to log/monitor
  - Network info - IP, DNS, VLAN, etc
  - User info - usernames, login/out times
  - Application logs
  - Running processes
- Log collection level depends on many factors

Log Methods

- Windows event logs
  - Provided by Event Logging Service
  - Information depends on system configuration/application settings
    - Highly configurable
  - Application, Security, System
- Application logs
- Linux system
  - Built-in logging locations (var/log, etc)
  - Syslog messages
- Centralized logging, typically with SIEM

Network Ports

Network Port

- Messages associated with protocols use both TCP and UDP
  - Both use port numbers to identify specific destination process for message
- 1 - 65,535
  - Well-known ports 1 - 1024
    - Many have assigned and/or standardized uses
- Any port can be used for any application/purpose*
  - Frequent tactic for attackers to evade detection or bypass security controls
  - System administrators to “hide” listening port

Standard Ports

Port Number(s)	Application (Protocol)
TCP 20 & 21	FTP
TCP 22	SSH
TCP 23	Telnet
TCP 25	SMTP
TCP/UDP 53	DNS
TCP 80 and 443	HTTP/S
UDP 161 & 162	SNMP

Identifying Listening Ports

- Locally on host
  - netstat (Windows/Linux)
  - lsof (Linux)
  - Router/switch commands
    - *`show control-plane host open-ports`*
- Remote port scanner
  - nmap - most popular
  - Most vulnerability scanners
- Recommended to periodically do internal checks on network
- Various security controls to manage filter traffic to open ports

Logged-In Accounts

User Access

- Least privilege
- Two methods to login to systems
  - Locally
  - Remotely
    - Windows - RDP, VNC (other clients)
    - Linux - SSH, VNC and others
    - Malicious connections through RAT or remote shell
- Identifying logged in users assists with compromise detection
  - Gaining access and persistence is early phase of attack
  - Goal of privilege escalation

Identifying Accounts

- Event logs, centralized logging and monitoring (SIEM)
- Windows
  - RDP management tools
  - PsTools - PsLoggedOn
  - PowerShell modules (Get-ActiveUser)
- Linux
  - *w* - logged in users
  - *who* - similar to w, less information shown
  - *users* - only list of users
  - *last* - currently logged in users and last logged in time
  - *lastlog* - information on all users (logged in or not)

Processes & Applications

Running Processes

- Instance of program/application currently being executed
- Can be viewed directly on host, or remotely
  - Also evaluated based on port/protocols
- Multiple purposes
  - Identify source of resource consumption
  - Configure and tune security controls/policies
  - Configure QoS settings
  - Identify rogue processes or malware
    - Requires additional analysis

Viewing Running Processes

- Windows Task Manager
  - Shows processes and resource usage in graphic interface
- *tasklist* command
  - Similar to Task Manager, but command line
- Linux
  - *ps* command (multiple useful flags)
    - -e, -aux
  - *ps -u* <username>
- Network port identification
  - Doesn't show specific process, but can help with identification

Identifying Applications

- Same tools method to view running processes can be used
  - Windows Task Manager
  - Command line tools
  - macOS Activity Monitor tool
- nmap flags and scripts
- Cisco options
  - Classification engine in IOS - NBAR (Network-based Application Recognition)
  - WSA (Web Security Appliance)
  - NetFlow with Stealthwatch Flow Sensor
  - Firepower Management Console (FMC)

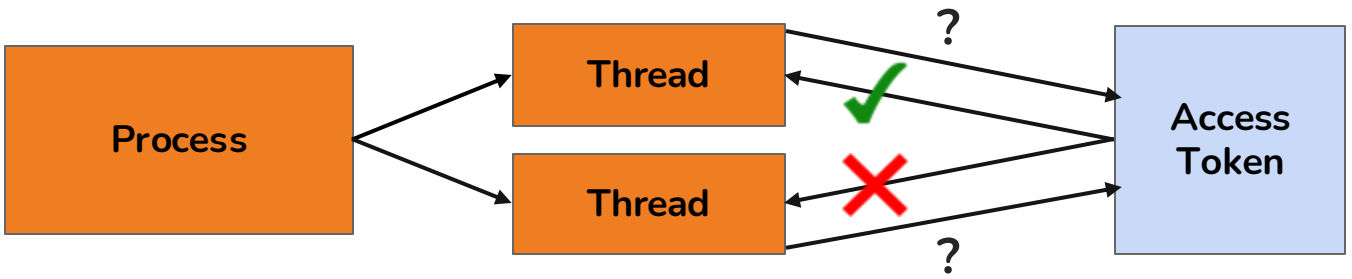
Windows Processes & Handles

Processes and Threads

- Process
  - Program running on system, contains all resources needed to execute
- Thread
  - Basic unit that OS allocates processor time to
- Job
  - Grouped processes managed as a unit
- Thread pool
  - Group of worker threads to increase efficiency of execution
- Fiber
  - Single unit of execution, manually scheduled by application

Process Security

- Processes must have permission to run
  - Permissions based on access control tied to user rights
- Windows uses tokens to identify security context for processes
  - *CreateProcessWithTokenW* function
- Authenticated users assigned authorization for specific levels of access
  - Auth data stored in token



Processes and Memory

- Processes function in *virtual address space*
  - Private for each process
  - Other processes cannot access without specific sharing
- Page table maintained to reference virtual space to physical address
- *Working set*
  - Subset of virtual address space of an active process
- Paging
  - Used when thread attempts to use more memory than available
  - Some memory content written to disk - *page (paging) file*

Handles

- Abstract reference value to a resource
  - Identifies resource for process to work with, using Win32 APIs
- Hide real memory address from API
  - Allow system to reorganize memory - transparent to program
- Can identify value and associate access rights to value
  - ex: process requesting read/write access to a file
- *Handle leak*
  - Process requests handle, but does not free after finished using
  - Can result in handles marked “in use” and being unavailable
  - May cause performance issues or crashes

Windows Management Instrumentation (WMI)

WMI

- System management infrastructure (Windows only)
- Preinstalled on most versions of Windows
  - Older versions may not include, but available to install
- Used for remote/local management and information sharing
  - Requires other programs or scripts
- Access should be restricted if not absolutely necessary
  - Can be used by malware
  - Can limit remote access and local permissions

WMI Capabilities

- Provide information about local or other remote computers
- Configure security and system settings
- Modify permissions for users/groups
- Manipulate hardware configurations
- Run applications and processes
- Configure and view event logs

Windows
Event Logs

Event Logs

- Logging system built-in Windows
  - Runs as a service (Windows event logging service)
- Logging capabilities for operating system and various applications
  - Microsoft applications (SQL server, IIS, etc)
  - Non-Microsoft applications
- Can be viewed using Windows Event Viewer
- 3 common event log types
  - Application
  - Security
  - System

Common Event Types

- Error
  - Indicate significant problem (data/functionality loss)
- Warning
  - Less significant issue, but may cause issues
- Information
  - Routine information, usually successful operations
- Success Audit
  - Audited successful security events
- Failure Audit
  - Audited failed security events

Log Management

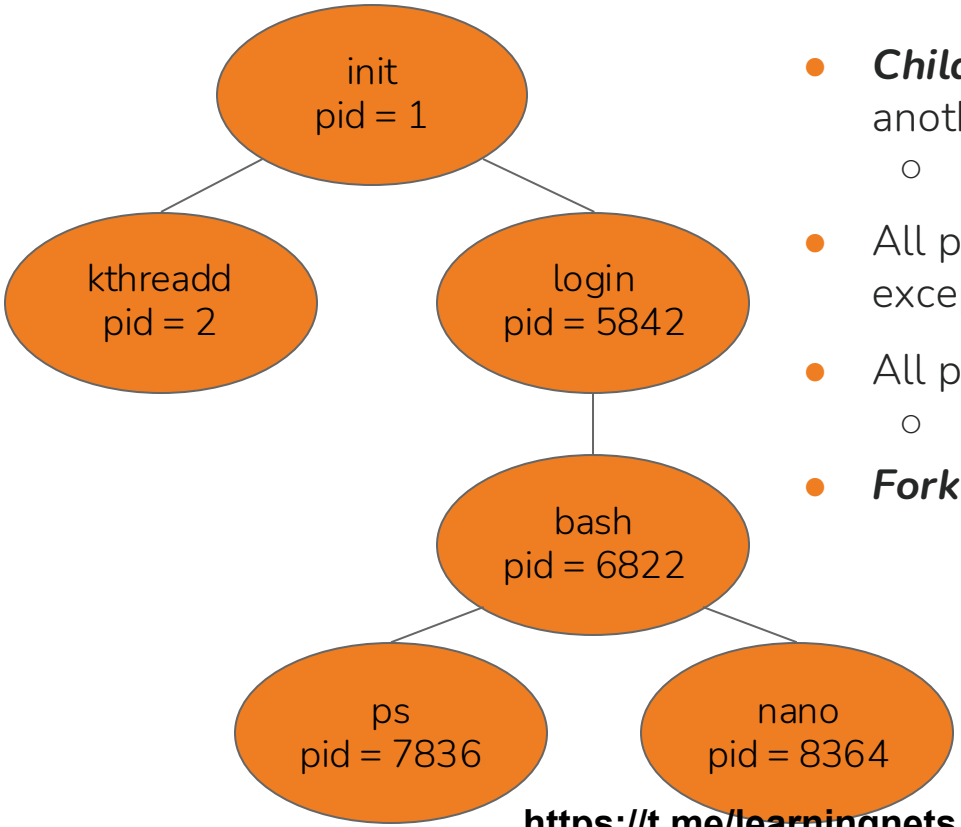
- Logs can consume significant amount of storage
  - By default, old logs deleted as new logs created
- Ideally exported to a centralized logging system (SIEM)
  - Allows longer log retention
  - One location to view logs from multiple systems
  - Easier to read format for many types of logs (log parser)
- Log data should be protected
  - Critical piece for incident response and forensic investigations
  - Threat actors frequently attempt to delete or alter logs

Linux Processes

Running Processes

- Processes can run in foreground or background
  - Foreground - visible on screen, interactive, shell is occupied (if using shell)
  - Background - usually not visible, shell allows other commands
    - Run using **&** after command (**`./script.sh &`**)
- Multiple types of processes
  - Init, Child, Orphan, Zombie, Daemon
- Processes start in **ready** state, then move to **running** state
  - *Process scheduling*
- Preemptive scheduling
  - OS determines process has higher priority, interrupts other running process
- Nonpreemptive scheduling
  - Runs when CPU has available cycles

Parent and Child



- ***Child process*** - process created by another process at runtime
  - ***Parent process***
- All processes have parent process except ***init***
- All processes assigned an ID when ran
  - process ID or ***pid***
- ***Fork*** - parent creates child process

Orphans and Zombies

- Many reasons a process can terminate
- Orphan process
  - Parent process terminates, child process allowed to continue running
  - Becomes child of ***init*** process - but labeled as orphan
- Zombie process
  - Parent process terminates child process
  - Time between child process ending, and status being returned to parent
    - Resources released
    - Process still listed in process table
    - Listed as ***zombie process***

Daemons

- Processes running in the background
  - Not controlled by active user
  - Many start automatically at boot
- Typically created by init process
  - Permissions can vary depending on what is provided to process
- Not all are started automatically
  - Some start only when user or event triggers them
- Can be controlled like any other process
  - Terminated, started, restarted, etc

Linux Permissions

File Permissions

- Three basic permissions can be applied to files or directories
  - Read (r)
  - Write (w)
  - Execute (x)

```
drwxrwxr-x 9 brian brian     4096 Jun 21 13:10 vitality-goes
-rw-rw-r-- 1 brian brian  8942848 Oct  1  2023 wazuh-agent.deb
drwxrwxr-x 9 brian brian     4096 May  5 15:58 websites
```

- Permissions can be modified using ***chmod*** command
- Owner modified using ***chown*** command
- Group ownership modified using ***chgrp*** command

chmod

- Command can be used two ways
  - Symbolic method (text)
  - Numeric method
- Symbolic
  - **u** - user who owns file
  - **g** - group file belongs to
  - **o** - all other users
  - **a** - all of the above (instead of **ugo**)
  - **+/-** - add or remove permission

```
brian@ubuntu:~$ ls -l wazuh-agent.deb
-rw-rw-r-- 1 brian brian 8942848 Oct  1  2023 wazuh-agent.deb
brian@ubuntu:~$ chmod a+x wazuh-agent.deb
brian@ubuntu:~$ ls -l wazuh-agent.deb
-rwxrwxr-x 1 brian brian 8942848 Oct  1  2023 wazuh-agent.deb
```

chmod Numeric

- Three-digit number specifies permissions
  - Each digit 0 - 7
  - First digit applies to owner
  - Second digit applies to group
  - Third digit applies to all other users

r	w	x
1	0	1

0 0 0 = 0	1 0 0 = 4
0 0 1 = 1	1 0 1 = 5
0 1 0 = 2	1 1 0 = 6
0 1 1 = 3	1 1 1 = 7

Symlink

- File that contains reference to another file or directory
  - Absolute or relative path
  - Contains name of another file/directory, but not the data
- Created using ln command
  - *ln -s reference_file link_file*
- Removing symlink does not affect original file
- Removing original file creates ***orphan symlink***

Linux Logging

Syslog

- Most common type of logging for Linux-based systems
- Runs as a daemon (background process)
  - Configuration in ***/etc/rsyslog.conf*** (by default)
  - Syslog-ng - open source option (***/etc/syslog-ng/syslog-ng.conf***)
- Logs stored in **/var/log**

Syslog Facilities

- Application or process that submits log message

auth	Authorization activity on system
authpriv	Same as auth, but sent to more secure location
cron	System scheduler messages
daemon	Catchall logging for daemons
mail	Mail-related system messages
user	Standard user processes

Syslog Priorities

emerg	Emergency condition, system unusable
alert	Should be dealt with immediately
crit	Critical condition, may not direct affect system stability
err	Standard errors
warning	Standard warnings
notice	Attention needed, but not an error
info	General informational message, standard behavior
debug	Used for debugging system errors or applications
none	Do not log

Log Types

- Transaction logs
  - Records all transactions that occur (ex: database transaction log)
- Session logs
  - Track changes made during web-based system management session
- Alert logs
  - Record error messages (startup, shutdown, disk/swap space, etc)
- Threat logs
  - Triggered when action matches defined security rule

Web Server Logging

- Apache
  - By default stored in **/var/log/apache2**
  - Errors and diagnostic info sent to **error.log**
  - Server requests/responses sent to **access.log**
  - Uses combined log format
    - access, agent, referrer
- NGINX
  - Stored in **/var/log/nginx** by default

```
brian@ubuntu:~$ cat /var/log/apache2/access.log
192.168.1.98 - - [10/Oct/2024:11:49:22 +0000] "GET /Current-Weather HTTP/1.1" 200 1096 "-" "Mozilla/5.0 (
Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/18.0 Safari/605.1.15"
-rw-r----- 1 root adm    0 Jun 21 00:00 /var/log/apache2/other_vhosts_access.log
```

Endpoint Security

Endpoint Protection

- Anti-virus is most basic form of protection
- Host-based firewalls (personal firewall)
  - Basic functionality, provides L3/4 filtering
- HIPS - host-based intrusion prevention system
  - More advanced protection - spyware, virus, worms, ransomware, etc
- Advanced malware protection systems
  - Cisco AMP (now called Cisco Secure Endpoint)

Encryption

- Email encryption
  - Connection between client and server
  - Email messages themselves
  - Archived messages
- Data/file encryption
  - Data at rest & data in transit (in motion)
  - Windows BitLocker
  - macOS FileVault
  - Many third-party options

Application Filtering

- Whitelist
  - List of entities that are permitted to run or be installed
  - Challenging to properly manage
- Blacklist
  - List of entities that are not permitted
  - Will never be a complete list
- Graylist
  - List of objects that have not yet been determined harmful or safe
- Cisco Firepower
  - Features to assist using intelligence from Cisco Talos
  - IPS and NGFW to assist with network filtering

Sandboxing

- Isolated location for software to run without affecting system
  - Can prevent malware from accessing/modifying data
- System-based sandboxing
  - Google Chromium
  - JVM
  - HTML5 “sandbox” attribute with iframes
- Incident response activities
  - Used for analysis of malware or suspicious files
  - Include software/processes to monitor behavior of applications

Endpoint Telemetry & Analysis - Summary

Key Concepts - Recap

+ Host and endpoint data
+ Endpoint analysis
+ Endpoint security

Learning Outcomes Recap

+ Understand where logging data can be found on endpoints and in network traffic
+ Be familiar with methods to investigate running processes on Windows and Linux
+ Be able to explain how Linux permissions are structured and configured
+ Understand the fundamentals of endpoint security techniques

Next Steps

- Additional Resources: Skill Dive labs for endpoint investigation and analysis
- Continue the Cisco CyberOps Associate learning path
- Dive deeper into endpoint telemetry and analysis with additional INE courses

Thank you!

Endpoint Telemetry & Analysis

- Aligned with Cisco CyberOps Associate
- Thank you for your time!

EXPERTS AT MAKING YOU AN EXPERT