W04 - System Hardening, Auditing, & Logs

US Army Cyber School

CCTC Windows Module Layout

- **CCTC - Windows Module**
  - **W01 - Command Line Tools**
  - **W02 - Processes**
  - **W03 - Registry**
  - **W04 - System Hardening / Auditing Logs**
  - **W05 - Windows Networking**
  - **W06 - Tactical Survey**

Windows Section 4 - System Hardening, Auditing, & Logs

- **SKILL CCWE16: Identify basic Windows Firewall concepts**
  - CCWE16.01 - Enable Windows Firewall settings with the graphical user interface and command line tools
  - CCWE16.02 - Describe the different components of Windows Firewall
- **SKILL CCWE17: Identify components of the New Technology File System (NTFS)**
  - CCWE17.01 - Describe basic file and folder permissions
  - CCWE17.02 - Modify permissions based on users and groups
  - CCWE17.03 - Apply permissions based on users and groups
- **SKILL CCWE18: Define Windows Resource Protection**
  - CCWE18.01 - Describe Windows Resource Protection
  - CCWE18.02 - Identify files that are protected by Windows Resource Protection
  - CCWE18.03 - Discuss the security implications of Windows Resource Protection on a compromised system

UNCLASSIFIED // FOUO

Windows Section 4 - System Hardening, Auditing, & Logs

- **SKILL CCWE19: Define User Account Control (UAC)**
  - CCWE19.01 - Identify the purpose of User Account Control (UAC)
  - CCWE19.02 - Employ user interface privilege isolation
- **SKILL CCWE20: Analyze Windows system security posture**
  - CCWE20.01 - Discuss Information assurance and information security policies
- **SKILL CCWE21: Identify Security Products**
  - CCWE21.01 - Identify host-based security products
  - CCWE21.02 - Identify network security products
  - CCWE21.03 - Discuss signature based detection
  - CCWE21.04 - Discuss heuristic based detection

Windows Section 4 - System Hardening, Auditing, & Logs

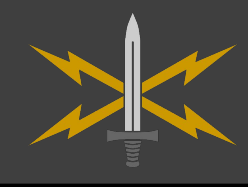
- **SKILL CCWE22: Define Windows Auditing**
  - CCWE22.01 - Explain why audit policies are important
  - CCWE22.02 - Explain the functionality of the main logs
  - CCWE22.03 - Discuss audit policy settings
  - CCWE22.04 - Identify the kinds of events that get audited and what they mean
- **SKILL CCWE23: Configure the audit policy for anomalous activity**
  - CCWE23.01 - Use GUI tools to view policy settings
  - CCWE23.02 - Use command line tools to view policy settings
- **SKILL CCWE24: Analyze event logs for anomalous activity**
  - CCWE24.01 - Identify events that would be audited and why
  - CCWE24.02 - Identify the location of logs on the Windows system
  - CCWE24.03 - Employ command line tools to view event logs

UNCLASSIFIED // FOUO

Day 8

Firewall Definition

A Firewall blocks network traffic based on rules.



The Windows Firewall

Enable Windows Firewall settings:

```
wf.msc
```

- Control Panel GUI

```
netsh advfirewall ?
netsh advfirewall show currentprofile
```

- Native CLI

```
wmic /namespace:\\Root\StandardCimv2 path
MSFT_NetFirewallRule WHERE 'DisplayName LIKE "%ICMP%"' get
DisplayName,Enabled,Profiles
```

- WMIC

```
Get-NetFirewallRule | Select Name, Enabled, Direction,
Description | Format -list
```

- Powershell

Windows Firewall Components

Windows Firewall Service

- HKLM\SYSTEM\CurrentControlSet\services\MpsSvc
- Executable hosting the service is svchost.exe
- The hosted DLL is mpssvc.dll

Profiles

- Private
- Public
- Work / Domain

Multiple profiles can be active on one interface at the same time

Log settings are per profile

New Technology File System (NTFS)

Each file in NTFS has a security descriptor

The security descriptor can include:

- Security identifiers (SIDs) for the owner
- A Discretionary Access Control List (DACL) that specifies the access rights (read, write, execute, delete) allowed or denied to particular users or groups
- A System Access Control List (SACL) that specifies the types of access attempts that generate audit records for the object

Modifying Permissions

WE17.02

```
Right Click -> Properties -> Security
```
- GUI - Explorer.exe

```
icacls C:\Windows\System32\notepad.exe
```
- Command Line

```
Get-Acl C:\Windows\System32\notepad.exe | Format-List
```
- Powershell

```
accesschk C:\Windows\System32\notepad.exe
```
- Sysinternals

Windows Resource Protection

Previously Windows File Protection (WFP) in Windows XP

- Watched for system file overwrite attempts
- Checked file signature against known good
- If bad, replaced with a copy from system32/dllcache folder

Windows Resource Protection provides the same capability

- Additionally, it will now keep the protected files from being installed to begin with, rather than just overwriting them.
- Protected Resources can only be modified by Windows Module Installer service (TrustedInstaller.exe)
- Also can protect system registry keys

Windows Resource Protection

What Resources specifically are protected? CLICK ME!

WRP protects critical files that are installed by the OS with the following extensions:

.acm, .ade, .adp, .app, .asa, .asp, .aspx, .ax, .bas, .bat, .bin,
.cer, .chm, .clb, .cmd, .cnt, .cnv, .com, .cpl, .cpx, .crt, .csh,
.dll, .drv, .dtd, .exe, .fxp, .grp, .h1s, .hlp, .hta, .ime, .inf,
.ins, .isp, .its, .js, .jse, .ksh, .lnk, .mad, .maf, .mag, .mam,
.man, .maq, .mar, .mas, .mat, .mau, .mav, .maw, .mda, .mdb, .mde,
.mdt, .mdw, .mdz, .msc, .msi, .msp, .mst, .mui, .nls, .ocx, .ops,
.pal, .pcd, .pif, .prf, .prg, .pst, .reg, .scf, .scr, .sct, .shb,
.shs, .sys, .tlb, .tsp, .url, .vb, .vbe, .vbs, .vsmacros, .vss,
.vst, .vsw, .ws, .wsc, .wsf, .wsh, .xsd, and .xsl.

Backups are kept in the %Windir%\winsxs\Backup folder

WRP Security Implications

Unable to overwrite protected files while Windows is running

Still able to mount drive into another OS, and overwrite them

Look for drivers installed by 3rd Party to compromise

With Administrator privilege, can alter the configuration to allow modification

User Account Control (UAC)

UAC limits the privileges of user run applications, even when run as Administrator, to prevent the modification of system files, resources, or settings. Requesting elevated privileges requires explicit acknowledgement from the user.

Some Windows executables can "auto elevate" without a prompt

User Interface Privilege Isolation (UIPI)

WE19.02

UIPI is part of UAC. Each process is given a privilege level

Higher integrity level can send messages to lower level integrity

Lower can only read from higher

UIPI can be bypassed by signed and trusted applications with the UIaccess manifest setting

Information Assurance (IA)

- Is the practice of assuring information and managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes.
- Includes protection of the integrity, availability, authenticity, non-repudiation and confidentiality of user data.
- Concerned with the business as a whole.
- Designed to cover more than just electronic information (paper, verbal)
- Multi-discipline approach to protecting the business as a whole
- Uses all available security mechanisms (technology, organisational, human-oriented, legal)
- Decision making takes place at the management level

Information Security

- Preservation of confidentiality, integrity and availability of information.
  Note: In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved. ~ ISO27000

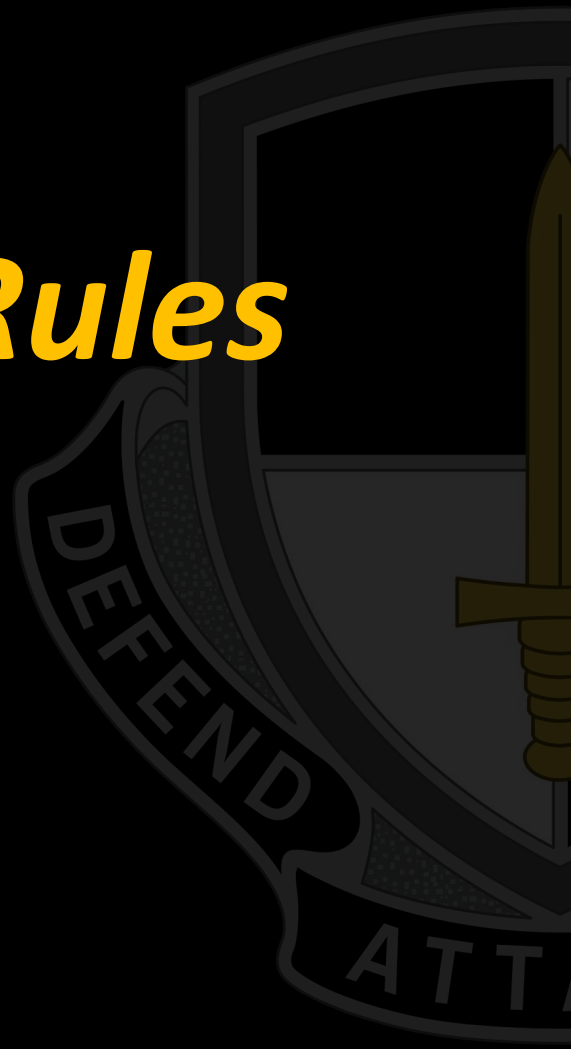
- CIA Triad is the basis for InfoSec, but it has been greatly expanded upon since the 1970's when first introduced to include a wide-range of 'Security Goals'

- Primary focus is on technical security mechanisms

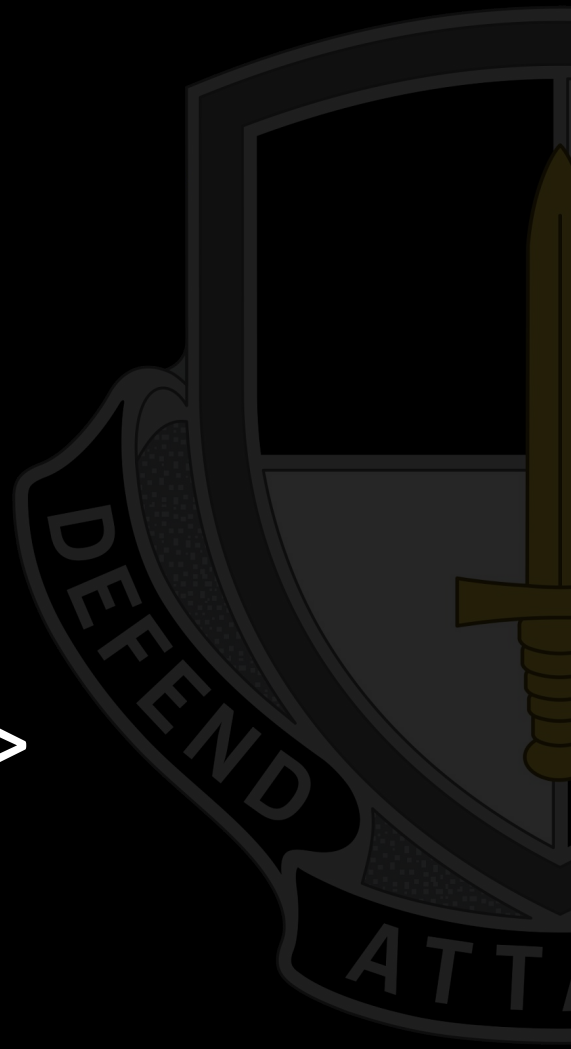
- Crafted by technical employees rather than management

ACTIVITY: Make Firewall Rules

CLICK ME FOR ACTIVITY PROMPT!



EXERCISE:
Malicious Registry



Blackboard -> Windows Section 3: Registry ->
Exercise: Malicious Registry

Day 9

Host-based Security Products

- Runs local on the machine, only concerned with that machine. OS dependent, version dependent. Some install as a service. Many new versions are cloud based.
- System Firewalls
- Process monitoring, kernel calls
- Directory monitoring
- System Setting/Registry monitoring
- Log monitoring
- Authentication, Authorization, Accounting (AAA)
- Application Whitelisting

Network Security Products

- Monitors traffic across the wire.
  - Can be inline or passive.
  - Inline often modifies traffic between destination and source.
- Network Firewalls
- Intrusion Detection System(IDS) / Intrusion Prevention System (IPS)
- Web/Application Proxy
- VPN Concentrator

Signature Based Detection

- Device/Software maintains a database of previously identified attack signatures. Compares activities and binaries to this database to determine if they are a match.
- Only capable of catching previously identified attacks
- Signatures require constant updating
- Small changes to a binary could bypass the signature

Heuristic Based Detection

- Device/Software develops a baseline of the system, then looks for anomalous activity
- Has potential to catch 0-day attacks (Good Luck)
- Larger number of false positives vs detection based (Job Security)

Windows Auditing

- Why are audit policies important?
  - Maintain a record of access to secure objects

- What is the functionality of the main logs?
  - At startup (or on config changes), LSASS sends the system audit policy to the Security Reference Monitor (SRM).
  - When an object is accessed, SRM generates auditing messages and sends them to LSASS.
  - LSASS sends the event log messages on to the Event Logger.

Windows Event Logs

Application	Contains events logged by applications.
Security	Contains events such as valid and invalid logon attempts, as well as events related to resource use such as creating, opening, or deleting files or other objects.
System	Contains events logged by system components, such as the failure of a driver or other system component to load during startup.
CustomLog	Contains events logged by applications that create a custom log. Using a custom log enables an application to control the size of the log or attach ACLs for security purposes without affecting other applications.

Windows Auditing

- Audit Policy Settings
  - Auditing settings are contained in the System Access Control List (SACL)
    - Object -access ACE:
      - Audit settings defined on a per object basis
  - Global Audit Policy - SACL
    - Global policy to setup auditing on all objects of one type:
      - File system objects
      - Registry keys
  - Local Security Policy must also be enabled for auditing to be logged

Configure the audit policy for anomalous activity

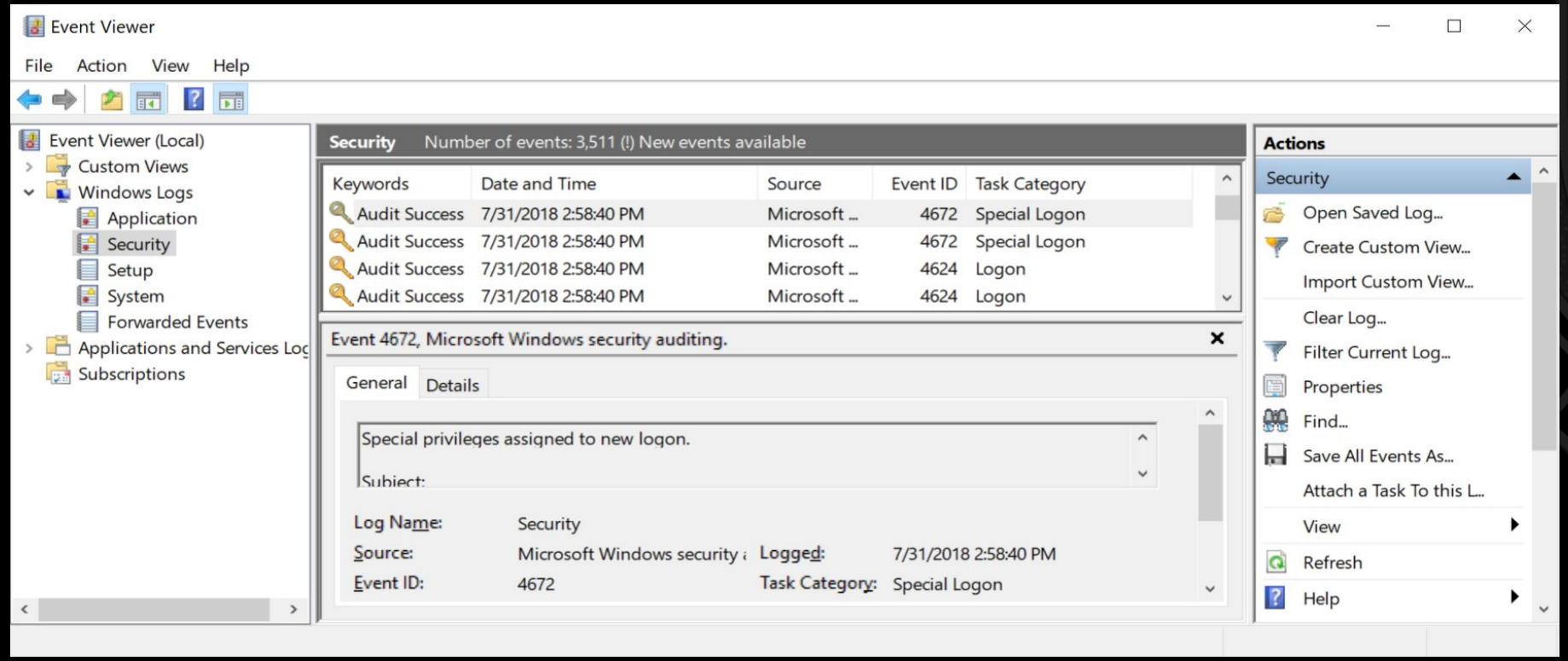
- Local Security Policy (GUI)
  - Advanced Audit Policy Configuration Settings
- Command Prompt
  - `auditpol /get /category:*`

```
auditpol /resourceSACL /type:File /view
auditpol /resourceSACL /type:Key /view
```

WE24.01
WE24.02

View/Analyze Event Logs - GUI

- `eventvwr`
  - Reads in C:\Windows\System32\Winevt folder.
  - Locations are configurable.



View/Analyze Event Logs - CLI

Command Prompt

```
wevtutil el
```
- show all logs

```
wevtutil gli security
```
- get security log info

```
wevtutil qe security /c:3
```
- get last 3 events from security log

Powershell

```
Get-EventLog -LogName System -Newest 10
```

```
PS C:\WINDOWS\system32> get-eventlog -LogName System -Newest 10

   Index Time          EntryType   Source                 InstanceID Message
   ----- ----          ---------   ------                 ---------- -------
     895 Jul 31 17:05  Information Service Control M...   1073748864 The start type of the Background Intelligent Tr...
     894 Jul 31 17:04  Information Service Control M...   1073748864 The start type of the Background Intelligent Tr...
     893 Jul 31 17:02  Information Service Control M...   1073748864 The start type of the Background Intelligent Tr...
     892 Jul 31 16:56  Error       DCOM                       10016 The description for Event ID '10016' in Source ...
     891 Jul 31 15:34  Information Microsoft-Windows...         16 The description for Event ID '16' in Source 'Mi...
     890 Jul 31 15:23  Error       DCOM                       10016 The description for Event ID '10016' in Source ...
     889 Jul 31 15:20  Information Microsoft-Windows...         19 Installation Successful: Windows successfully i...
     888 Jul 31 15:20  Information Microsoft-Windows...         43 Installation Started: Windows has started insta...
     887 Jul 31 15:20  Information Microsoft-Windows...         16 The description for Event ID '16' in Source 'Mi...
     886 Jul 31 15:20  Information Microsoft-Windows...         19 Installation Successful: Windows successfully i...
```

ACTIVITY: Modify Audit Policy and Firewall

CLICK ME FOR ACTIVITY PROMPT!

DISCUSSION: Discuss the Purpose of Covering Your Tracks

ACTIVITY: Cover Your Tracks

CLICK ME FOR ACTIVITY PROMPT!