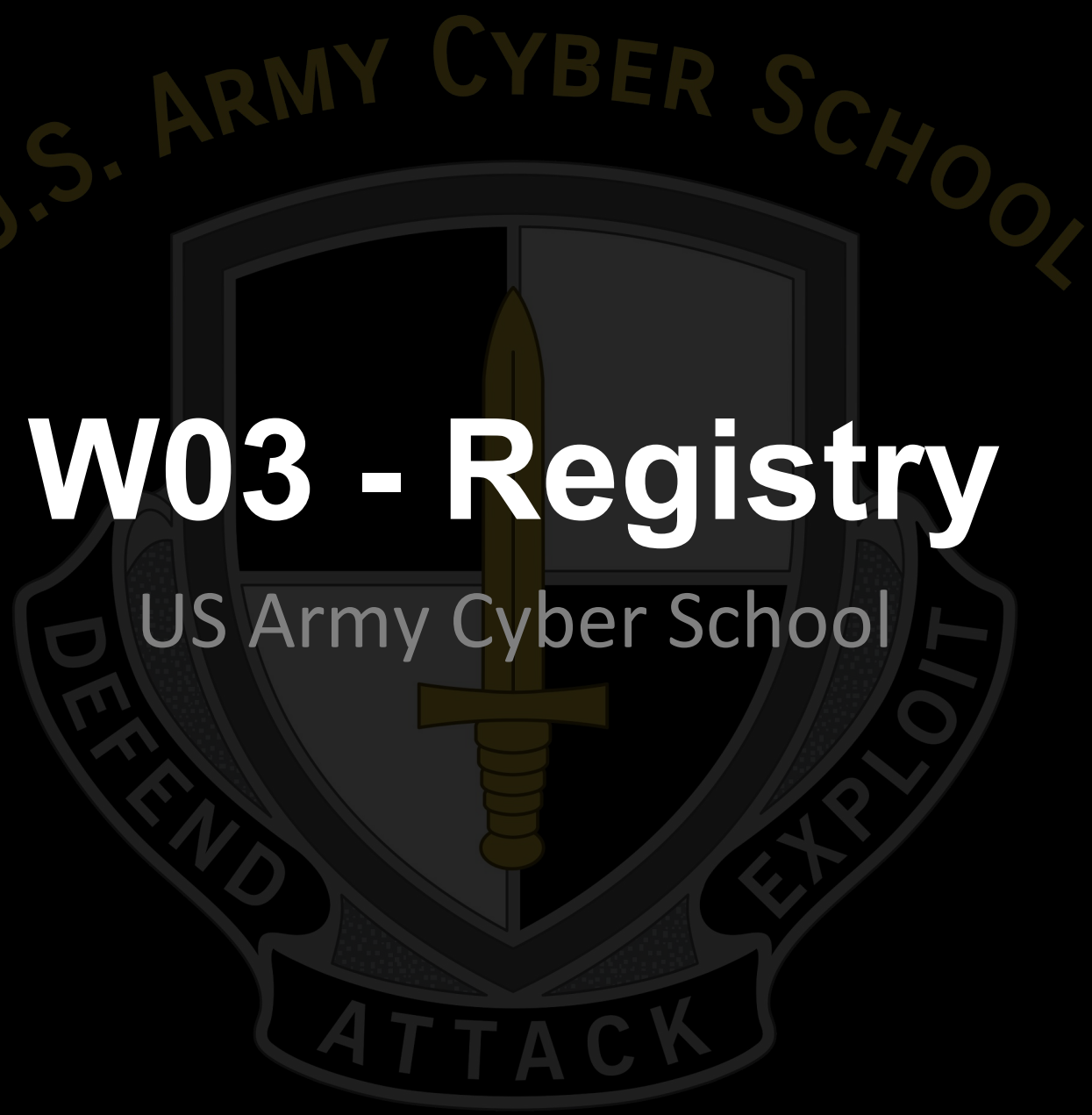

W03 - Registry

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 3 - Registry

- **SKILL CCWE13: Explain the Purpose of Window Registry**
  - CCWE13.01 - Explain the purpose and role of Windows Registry and its major functions
  - CCWE13.02 - Describe Registry hierarchy organization and primary components
- **SKILL CCWE14: Employ Windows Registry Tools**
  - CCWE14.01 - Identify parts of the Registry using GUI-based tools
  - CCWE14.02 - Use command line syntax to query, view, analyze, modify and create Registry values
  - CCWE14.03 - Explain when and how changes to the Registry are expected to take effect
- **SKILL CCWE15: Analyze Windows Registry for Suspicious Activity**
  - CCWE15.01 - Identify Registry locations that contain forensically relevant information
  - CCWE15.02 - Identify Registry locations that can be utilized for persistence
  - CCWE15.03 - Perform basic analysis on a Windows system with compromised Registry

UNCLASSIFIED // FOUO

Day 7

WE13.01

Purpose and Role of the Registry

What *IS* the Registry?

- Hierarchical database of critical system configuration
- Registry is the configuration and control mechanism for the Windows Operating system
- Contains system-wide and per-user settings

What is the role of the Registry?

- During initial boot process (pre-kernel)
  - List of boot device drivers to load before kernel
- During kernel boot process
  - Loads device drivers and system element configuration
- During logon
  - Reads per-user preferences and settings
- During application startup and execution
  - Licensing data, installed component, software settings/configuration
- Random reads and writes during application use

UNCLASSIFIED // FOUO

Registry Hives

WE13.02

A Registry Hive is a group of keys, subkeys, and values in the registry that has a set of supporting files that contain backups of its data.

WE13.02

Primary Hive (Root) Keys

HKCU - **CURRENT USER : individual user settings**

HKU - **USERS : all accounts on machine, the root key containing the ntuser.dat hives for ALL users.**

HKCR - **CLASSES ROOT : file association and COM objects, backward compatibility, and file extension information**

HKLM - **LOCAL MACHINE : system related information, SAM, Critical boot/kernel functions, 3rd party software, hardware, BCD.dat**

HKCC - **CURRENT CONFIG : Current hardware profile, information that is gathered at runtime**

Remote Hive Keys

Only HKU and HKLM are available via remote tools

All the other Hive Keys are symbolic links for ease of access:

HKCU = HKU\<SID OF CURRENT USER>

HKCC = Can be located with value HKLM\SYSTEM\Select\Current

HKCR = Merged view of :

HKLM\Software\Classes and

HKCU\Software\Classes

The Hivelist

```
reg query hklm\system\currentcontrolset\control\hivelist
```

\REGISTRY\MACHINE\HARDWARE	-	Recreated every time the system starts
\REGISTRY\USER\<SID>	-	Specifies location of files that store the current user profile
\REGISTRY\MACHINE\SECURITY	-	Specifies location of files that store the HKLM\Security key
\REGISTRY\USER\.DEFAULT	-	Specifies location of files that store the HKU\.DEFAULT key
\REGISTRY\MACHINE\SYSTEM	-	Specifies location of files that store the HKLM\SYSTEM key
\REGISTRY\MACHINE\SOFTWARE	-	Specifies location of files that store the HKLM\SOFTWARE key
\REGISTRY\MACHINE\SAM	-	Specifies location of files that store the HKLM\SAM key

Components of the Registry

Registry contains KEYS and VALUES:

- KEYS contain other keys (AKA Sub-keys) and/or a collection of property/value pairs. Keys are a container object, much like a folder
- VALUES store data. Values are non-container object, much like a file

12 Data types are available, Most commonly used:

REG_SZ	REG_BINARY	REG_DWORD
REG_LINK	REG_MULTI_SZ	REG_QWORD

Registry Tools

GUI

- Regedit.exe
  - psexec -s -i regedit
  - psexec -s -i powershell

Command Line

- REG.exe

WMIC

- WMIC CLASS StdRegProv CALL <Method-Name)

Powershell

- Get-item
- Get-itemproperty
- Get-Childitem
- Set-itemproperty
- New-item
- New-itemproperty
- psdrive
- new-psdrive
  - Name: HKU
  - PSProvider: Registry
  - Root: HKEY_USERS

Query, Create, Modify, Delete

QUERY

- (CLI) reg query [\\Machine\] HKLM\SOFTWARE\TEST
- (PS) get-item -path "HKLM:\Software\Test"
- (WMIC) wmic class StdRegProv call EnumValues sSubKeyName=”Software\Test”

CREATE

- (CLI) reg add HKLM\software\test /v data /d “This is the data”
- (PS) new-itemproperty -path "HKLM:\Software\test" -name “data” -value “This is the data”
- (WMIC) wmic class StdRegProv call SetStringValue sSubKeyName=”software\test” sValueName=”data” sValue=”This is the data”

MODIFY

- (CLI) reg add HKLM\SOFTWARE\TEST /v data /d “This is modified” /f
- (PS) set-itemproperty -path "HKLM:\Software\test" -name “data” -value “This is modified”
- (WMIC) wmic class StdRegProv call SetStringValue sSubKeyName=”software\test” sValueName=”data” sValue=”This is modified”

DELETE

- (CLI) reg delete [\\Machine\]HKLM\SOFTWARE\TEST
- (PS) remove-item -path "HKLM:\Software\Test"
- (WMIC) wmic class StdRegProv call DeleteKey sSubKeyName=”software\test”

ACTIVITY: New Registry Key

CLICK ME FOR ACTIVITY PROMPT!

Registry Changes

- Changes to the Registry often require a restart, as many programs read the registry values upon load
- Whether the entire system needs to be restarted, or just a program, depends on the program that is reading the changes
- As a general rule:
  - Changes to Windows SYSTEM Settings require a reboot
  - Changes to Windows USER Settings require a logout/login
  - Changes to Windows POLICY Settings usually don't require a reboot
  - Changes to an APPLICATION require a restart
  - NOT ALWAYS true, but general rules/guidelines
- It is also important to note that some parts of the registry are always loaded into memory

Forensically Relevant Keys

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnce

HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows NT\CurrentVersion\Schedule\Taskcache\Tasks

HKLM\SYSTEM\CurrentControlSet\SERVICES\

HKLM\SYSTEM\CurrentControlSet\Enum\USBSTOR

HKU\<SID>\Software\Microsoft\Internet Explorer\TypedUrls

HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles\

Registry Keys for Persistence

WE15.02

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKU\<SID>\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\BCD00000000

HKLM\SAM\SAMs
```

Baselining the Registry

- What are some methods to determine if the registry has been compromised?
- Why is it important to baseline the Registry?
- How could we baseline the Registry?

ACTIVITY: Baseline Your Registry

CLICK ME FOR ACTIVITY PROMPT!