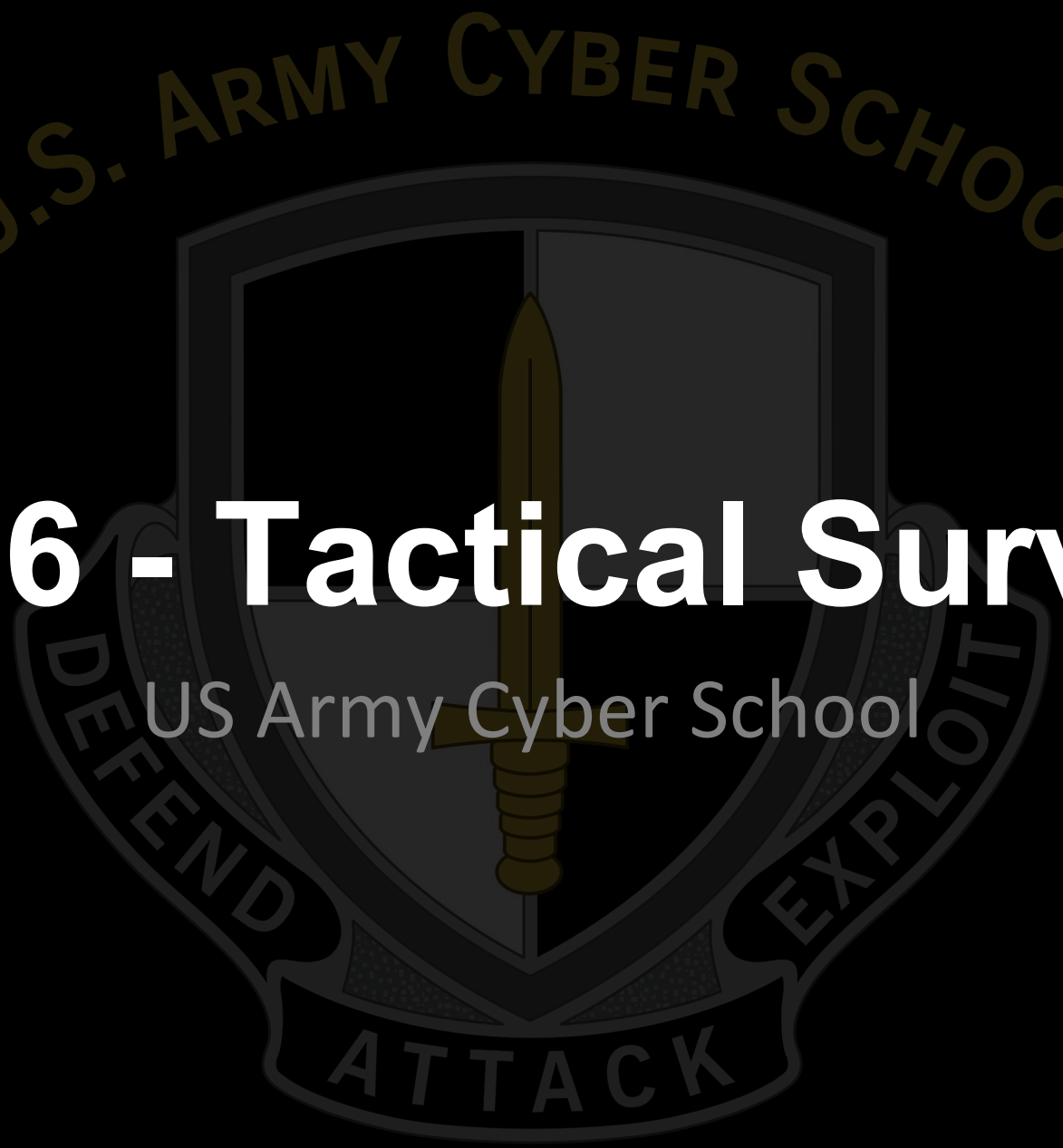

W06 - Tactical Survey

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 6 - Tactical Survey

- **SKILL CCWE29: Describe the phases of Incident Response**
  - CCWE29.01 - Identify what occurs in the Preparation phase of Incident Response
  - CCWE29.02 - Identify what occurs in the Identification phase of Incident Response
  - CCWE29.03 - Identify what occurs in the Containment phase of Incident Response
  - CCWE29.04 - Identify what occurs in the Investigation phase of Incident Response
  - CCWE29.05 - Identify what occurs in the Eradication phase of Incident Response
  - CCWE29.06 - Identify what occurs in the Recovery phase of Incident Response
- **SKILL CCWE30: Describe Order of Volatility**
  - CCWE30.01 - Discuss the factors involved when considering order of volatility
  - CCWE26.02 - Assess the order of volatility during an incident

UNCLASSIFIED // FOUO

Windows Section 6 - Tactical Survey

- **SKILL CCWE31: Analyze the Enumeration Process**
  - CCWE31.01 - Identify baseline knowledge on a machine
  - CCWE31.02 - Gather baseline knowledge on a machine
  - CCWE31.03 - Discuss the differences between malicious and normal activity
  - CCWE31.04 - Characterize system features through enumeration
  - CCWE31.05 - Identify scheduled tasks that may affect the purpose or activity on a machine
  - CCWE31.06 - Explain what should be assessed during enumeration of the environment
  - CCWE31.07 - Describe how to detect and enumerate malware
- **SKILL CCWE32: Discuss the Documentation Involved in a Tactical Survey**
  - CCWE32.01 - Identify the importance of Operational Notes (Op Notes)
  - CCWE32.02 - Discuss the components of a report
- **SKILL CCWE33: Use Enumeration Information to Analyze Courses of Action**
  - CCWE33.01 - Discuss the primary factors for recommending a course of action based on enumeration
  - CCWE33.02 - Identify the common vulnerabilities that could change the course of a mission
  - CCWE33.03 - Discuss the development of courses of action

UNCLASSIFIED // FOUO

Day 12

WE29

The 6 Phases of Incident Response

1. Preparation
2. Identification
3. Containment
4. Investigation
5. Eradication
6. Recovery

REMEMBER!

Be P.I.C.I.E.R. about your Incident response practices!

1. Preparation

BEFORE AN INCIDENT OCCURS

- Packing List
- Update tools
- Training
- Documentation
  - SOP
  - Policies and Procedures
- Network Diagrams
- Incident Response Team
- Enable NTP

2. Identification

DETERMINE IF WORKING WITH AN ADVERSE EVENT OR AN INCIDENT

- EVENT: Any observable occurrence in a system or network.
- ADVERSE EVENT: Event with a negative consequence, such as:
  - Unauthorized use of system privileges
  - Unauthorized access to sensitive data
  - Execution of malware that destroys data
- INCIDENT: Event that violates an organization's security or privacy policies:
  - Unusual Activity/Configs Outside Baseline
  - Unknown Connections
  - Unknown User Accounts
  - Unusual User Privileges
  - External devices
  - High Traffic Volumes
  - Unusual Logons

WE29.03

3. Containment

LIMIT DAMAGE CAUSED TO SYSTEMS AND PREVENT ANY FURTHER DAMAGE FROM OCCURRING.

- Cordon and Clear (VLANs)
- Remove from Network (when feasible)
- Quarantine
- Sandbox
- Patch / Hotfix
- Add Firewalls

UNCLASSIFIED // FOUO

4. Investigation

- **DETERMINE THE PRIORITY, SCOPE, AND ROOT CAUSE OF AN INCIDENT.**
- **Attribution**
- **Avenue of Approach**
- **Indicators of Compromise (IOCs)**
- **Vulnerability Assessment**
- **Forensic Analysis**
  - **Static Analysis**
  - **Dynamic Analysis**

5. Eradication

REMOVE THE INFECTION

- From the investigation you should know what you have to remove (malware analysis, playbook)
- Reimage
- Key Rotation
- Clean (and monitor)

6. Recovery

DETERMINE WHEN TO BRING THE SYSTEM BACK INTO PRODUCTION AND HOW LONG WE MONITOR THE SYSTEM FOR ANY SIGNS OF ABNORMAL ACTIVITY.

- Remove VLANs
- Return network to normal
- Lessons Learned
- Update SOP, AAR
- Continually Monitor (leaving sensors behind to be accessed remotely)

Volatility

- VOLATILITY IS A MEASURE OF HOW PERISHABLE ELECTRONICALLY STORED DATA IS (WHEN ELECTRICAL POWER IS TURNED OFF OR FAILS)

1. Order of Volatility
    1. registers, cache
    2. routing table, arp cache, process table, kernel statistics, memory
    3. temporary file systems
    4. disk and other storage media
    5. remote logging and monitoring data that is relevant to the system in question
    6. physical configuration, network topology
    7. archival media

- During an Incident
    - Gather baseline information
    - Cursory review of baseline information
    - Preliminary dig through system for indicators of compromise and symptoms
    - Trace indicators to source
    - Targeted analysis of suspicious information in baseline information
    - Crawl system for malicious items
    - Consolidate information

RESEARCH ACTIVITY:
Enumeration VS. Baseline

DISCUSSION: Enumeration VS Baseline

- Research and develop a short brief for the class, explaining the difference between a baseline and an enumeration.
- Items for discussion:
  - Difference between baselining a SERVER or a user WORKSTATION
  - How OFTEN should you baseline
  - Does it make sense to baseline the entire REGISTRY
- Other things you could baseline
- STATIC baselines
- DYNAMIC baselines

Baseline Knowledge

- How and When to baseline
- Items to consider
  - Local User Accounts
  - Running Processes
  - Services (installed and autostart)
  - Autorun locations (startup folder, registry locations (Run, RunOnce, Explorer shell extensions)
  - Scheduled tasks
  - Drivers and system files (file hash)
  - Network communications (established and listening. Also, is there a configured IPv6 connection on an IPv4 network or vice versa.)
  - Loaded modules (DLLs)
  - Installed applications and user context (who's running with elevated privileges?)
  - Group policy objects

What are some ways to use native Windows and SysInternals to gain awareness?

Malicious VS Normal Activity

- Normal activity
  - System that operates within security policies and in the way that it was intended.
- Normal behavior
- Malicious activity
  - Persistent Access

Scheduled Tasks for Malicious Actions

- Enumerate scheduled tasks
  - A scheduled task may be used to launch malicious activity, or to maintain persistence on a compromised system
  - How could this be mitigated

Enumeration: What Should be Assessed?

Report needs to cover the 5 W's (and an H)

- ❑ WHO is behind the attack?
- ❑ WHERE did it originate?
- ❑ WHAT did the attacker do on the compromised system?
- ❑ WHEN did the attacker gain access?
- ❑ HOW did the attacker gain access?
- ❑ WHY did the attacker choose this system?

- ❑ Based on those questions, use a SYSTEMATIC, ITERATIVE process to approach enumerating a suspected system.
  - ❑ Design initial FORENSIC HYPOTHESIS based on SOPs and suspect system behavior.
  - ❑ Design SYSTEM ENUMERATION to confirm or deny the hypothesis and provide supporting information
  - ❑ ANALYZE the results of the enumeration
  - ❑ Based on those results, REFINE or REFORMULATE the hypothesis, or expand the search and start over

Detect and Enumerate Malware

Some ways to detect and enumerate malware include:

- Comparison with a known good baseline
- Look for anomalous behavior
- Scanning for vulnerabilities
- Anti-malware scanners
  - Signature based
  - Heuristic
- Log files
- Sandboxing
- Packet sniffing
- Event correlation

Day 13

Identify the Importance of Operations Notes

- Your Op Notes will feed into your report depending whether the report is an executive or technical summary.
  - Offensive and Defensive
  - Offensive Op Notes are as detailed as possible.
  - Included in these Op Notes are Time Stamps, programs/tools that are executed, outputs,
- Why is this important?

Identify the Importance of Operations Notes

- What is reporting
- Sections of a report
  - Executive summary
  - The body
  - Technical Summary

Discuss the Primary Factors for a COA

- Factors that will influence courses of action on an offensive mission are:
  - Commander's intent
  - Antivirus or security products on target
  - Risk analysis (Do the ends justify the means) Ex: Is it worth risking a million dollar exploit to acquire a word document from the computer of a low-level terrorist?
  - Duration of effects and intent (deny, destroy, disrupt)
  - Second and third order effects
  - As always, the tools at your disposal will guide your COA

Changes to Course of a Mission

- Offense:
  - If new vulnerabilities are discovered
- Defense:
  - Threat Actor presence
  - Mitigate the vulnerabilities

WE33.03

Development of Courses of Action

- Receipt of mission
- Analysis of mission
- COA Development
- COA comparison
- COA approval
- Conduct mission
- AAR / Lessons learned

DISCUSSION: Covering Your Tracks

What is the purpose of covering your tracks?

Exercise: Enumerate Baseline

Blackboard -> Windows Section 6: Tactical Survey ->
Exercise: Enumeration Baseline