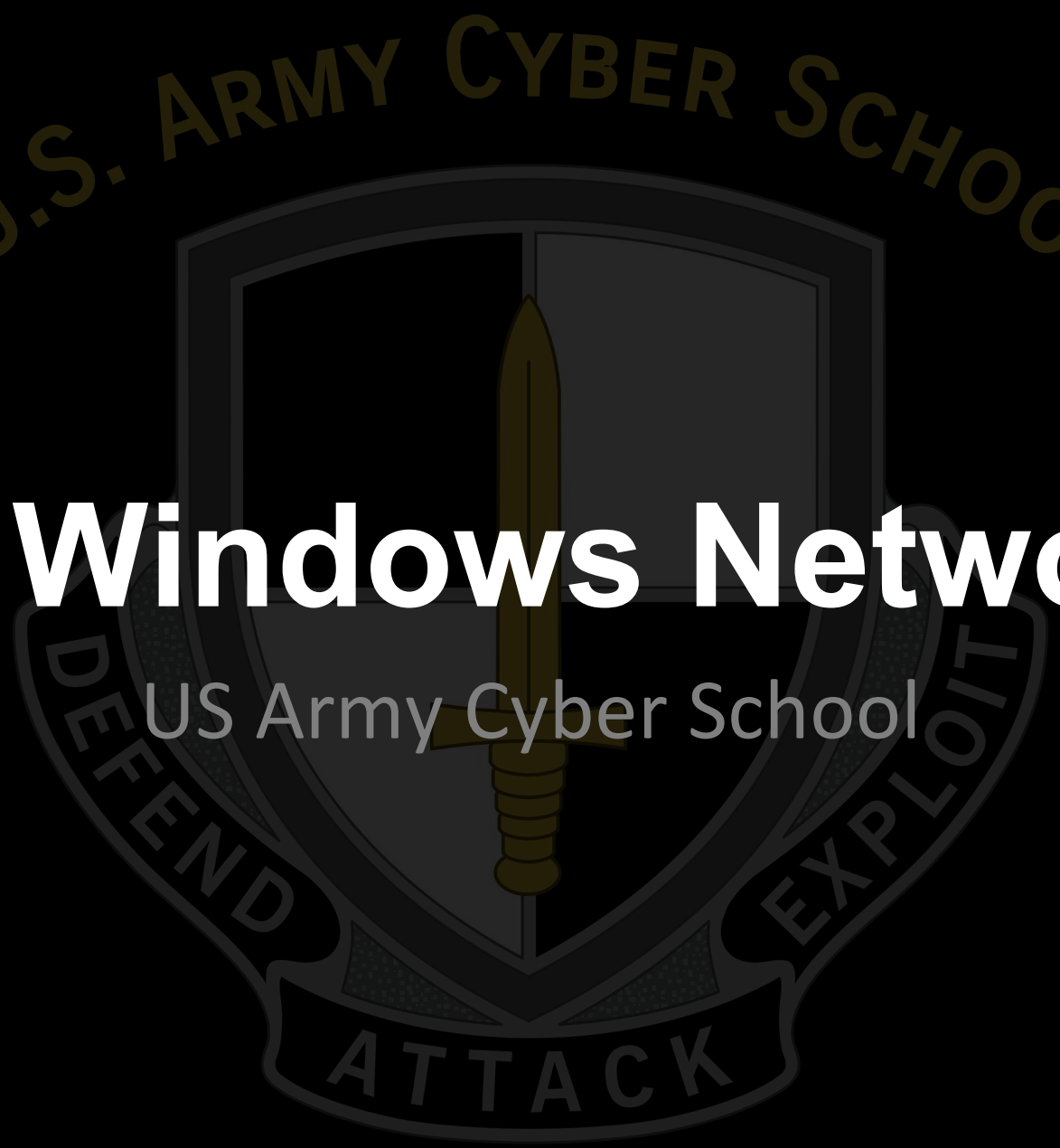

W05 - Windows Networking

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 5 - Windows Networking

- **SKILL CCWE25: Identify Windows Networking Features**
  - CCWE25.01 - Describe Server Message Block (SMB)
  - CCWE25.02 - Explain the purpose of mailslots
  - CCWE25.03 - Describe NetBIOS
  - CCWE25.04 - Distinguish hostnames from NetBIOS names
  - CCWE25.05 - Explain Windows network naming schemes
  - CCWE25.06 - Define host name resolution
  - CCWE25.07 - Define Remote Procedure Call (RPC)
  - CCWE25.08 - Describe Group Policy Objects
  - CCWE25.09 - Perform Group Policy Object queries through command line
  - CCWE25.10 - Modify Group Policy Objects
- **SKILL CCWE26: Perform Basic Network Analysis on a Windows Machine**
  - CCWE26.01 - Perform basic network analysis using built-in tools
  - CCWE26.02 - Describe sockets
  - CCWE26.03 - Identify services associated with listening ports
  - CCWE26.04 - Assess security implications of listening ports and established connections

UNCLASSIFIED // FOUO

Windows Section 5 - Windows Networking

- **SKILL CCWE27: Analyze Security Identifiers**
  - CCWE27.01 - Identify the purpose of security system components
  - CCWE27.02 - Explain how access tokens are important for security
  - CCWE27.03 - Explain security identifiers and how they are generated
  - CCWE27.04 - Locate a SID in the Windows Registry and associate it with a user profile
  - CCWE27.05 - Identify built-in Windows user accounts
  - CCWE27.06 - Identify the differences between local and domain accounts
  - CCWE27.07 - Describe common user rights and the rights assigned to built-in groups
- **SKILL CCWE28: Identify Active Directory Basics**
  - CCWE28.01 - Identify the Active Directory Schema and Global Catalog
  - CCWE28.02 - Describe the features of Active Directory
  - CCWE28.03 - Explain the logical and physical structure of Active Directory
  - CCWE28.04 - Describe functions of the resources associated with Active Directory
  - CCWE28.05 - Employ command line tools to gain information about a system or network

UNCLASSIFIED // FOUO

Day 10

Remote Procedure Call (RPC)

- Applications load a DLL containing stub procedures for remote functions.
- The stub then calls RPC run-time procedures to locate where the remote procedure resides
- The stub negotiates a transport mechanism
- It then calls the procedure on the remote system with the parameters
- Reverse happens to return data

Mailslots

- One-way Interprocess Communication
- Implemented in Kernel32.dll and msfs.sys
- Acts as a file kept in memory
- Useful for a single process sending broadcasts to multiple processes
- Max single message size of 424 bytes

SMB/CIFS & NetBIOS

- Server Message Block (SMB)
  - Primary remote file-access protocol on Windows Clients and Servers
- Also known as Common Internet File System (CIFS)
- Hostnames vs NETBIOS names
- `nbtstat` command

Windows Network Naming Schemes

- Relative Distinguished Name (RDN)
  - Hostname or computer name
- DNS domain hierarchy location
- The combination of these form the FQDN for the system

Network Analysis Using Built-in Tools

Device network configuration (using CLI)

- `ipconfig` - IP
- `nbtstat` - NetBIOS Statistics
- `route` - Routing table
- `arp` - MAC addressing info
- `netstat` - Network statistics

Network Analysis Using Built-in Tools

`ipconfig /?`	- help for network settings
`ipconfig`	- No MAC addresses
`ipconfig /all`	- More robust, includes MAC addresses
`ipconfig /displaydns`	- Shows DNS resolver cache
`netstat`	- Network statistics
`arp /?`	- arp help
`arp -a`	- displays ARP table

Network Analysis Using Built-in Tools

`netstat /?`	-	help for network connections/listeners
`netstat`	-	Only active connections
`netstat -ano`	-	Connections and open ports
`netstat -anb`	-	Shows PIDs tied to activity, needs priv
`netstat -s`	-	Network statistics
`netstat -r`	-	show routing table
`route /?`	-	help with adding routes
`route print`	-	show routing table (like netstat -r)

Sockets

A Socket is one endpoint of a two-way communication link between two programs running on a network. An endpoint consists of an IP address and a port number.

- Stream
  - Enable processes to communicate using TCP.
  - A stream socket provides a bidirectional, reliable, sequenced, and unduplicated flow of data with no record boundaries.
  - After the connection is established, data can be read from and written to these sockets as a byte stream.
- Datagram
  - Enable processes to use UDP to communicate.
  - A datagram socket supports a bidirectional flow of messages.
  - A process on a datagram socket might receive messages in a different order from the sending sequence.
  - A process on a datagram socket might receive duplicate messages.
  - Messages that are sent over a datagram socket might be dropped.
- Raw
  - Enable access to the underlying transport provider.
  - Can manipulate the underlying transport, so they can be used for malicious purposes that pose a security threat. Therefore, only members of the Administrators group can create sockets of type SOCK_RAW on Windows 2000 and later.

Host Name Resolution

1. Does the name belong to the local system?
2. Is it in the cache?
   - `ipconfig /flush dns` #flush the dns cache locally
3. Is the name in the host file?
   - `c:\Windows\System32\Drivers\etc\hosts`
4. Query configured DNS server?

Exercise: Identify Network Connections from Malware

Blackboard -> Windows Section 5: Windows Networking -> Exercise: Identify Network Connections from Malware

Day 11

Purpose of Security System Concepts

- Security Reference Monitor (SRM): Kernel Mode (ntoskrnl)
- Local Security Authority Subsystem (LSASS)
- LSASS policy database
- Security Accounts Manager (SAM)
- SAM database: HKLM\SAM
- Active Directory:
- Authentication Packages
- Interactive Logon Manager (Winlogon):
- Logon User Interface (LogonUI):
- Credential Providers (CP):
- Network Logon Service (Netlogon):
- Kernel Security Device Driver (KSecDD):

Access Tokens & Security Identifiers

- SID
  - S-1-5-21-547793982-3027706357-987482306-1003
- RID
  - S-1-5-21-547793982-3027706357-987482306-1003
  - 500 - Admin Account
  - 501 - Guest Account
  - 1000 - Beginning of User Accounts
- `psgetsid`
- `WMIC useraccount list brief`

Locate a SID in the Windows Registry

- CLI
  - `reg query HKU`
  - `reg query "hklm\software\microsoft\windows nt\currentversion\profilelist\{SID}"`
- WMIC
  - `wmic useraccount get name,sid,fullname`
  - `wmic useraccount where sid={sid} get name`
  - `wmic useraccount where name={name} get sid`
- Powershell
  - `Get-ChildItem Registry::\HKEY_USERS -ErrorAction SilentlyContinue`
  - `Get-ChildItem 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList\'`

RESEARCH ACTIVITY:
Built-in User Accounts

https://support.microsoft.com/en-us/help/243330/well-known-security-identifiers-in-windows-operating-systems

Local and Domain Accounts

- Built-In User Accounts
- Local Account SIDs
- Domain Accounts
- Logon
  - In a local logon
  - In a domain logon
  - Credential Providers

Active Directory Basics

- Active Directory Schema and Global Catalog
- Schema
  - Schema Class Object
  - Schema Attribute Object
- Global Catalog
  - Listing of all objects in the forest

Features of Active Directory

- Centralized Data Storage
- Scalability, Extensibility, Manageability
- Integration with DNS
- Client Configuration Management
- Policy-Based Administration
- Replication of Information
- Flexible, Secure Authentication and Authorization
- Security Integration
- Directory-enabled Applications and Infrastructure
- Interoperability with Directory Services
- Signed and Encrypted LDAP Traffic

Logical & Physical Structure of Active Directory

- Logical Structure
  - Domains
  - Organizational Units
  - Trees and Forest
- Physical Structure
  - Sites
  - Domain Controllers
  - Member Servers

Group Policy Objects

- `gpresult`
- DS Tools - A set of command line tools that began shipping natively with Windows Server 2003
  - DSADD - add specific types of objects to the directory
  - DSGET - display the selected properties of a specific object in the directory
  - DSMOD - modify existing objects in the directory
  - DSQUERY - query the directory according to specific criteria

ACTIVITY: Disorderly Domain

CLICK ME FOR ACTIVITY PROMPT!