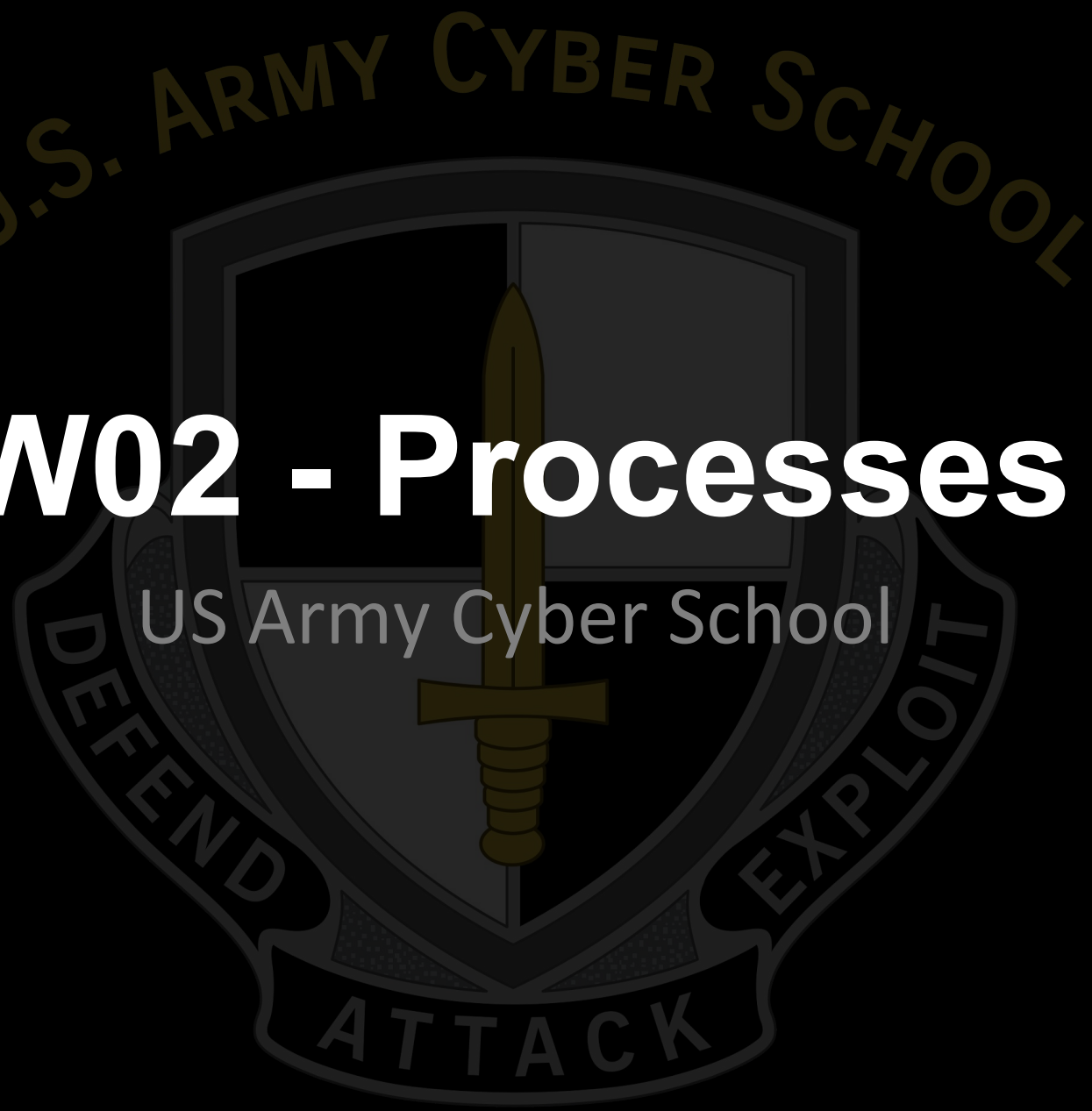


W02 - Processes

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 2 - Processes

- SKILL CCWE05: Define the Windows pre-boot process
- SKILL CCWE06: Define the Windows boot process
- SKILL CCWE07: Define the Windows logon process
- SKILL CCWE08: Identify Windows processes
  - CCWE08.01 - Explain how to find the current status of Windows processes
  - CCWE08.02 - Explain the process states and identify why they are important
  - CCWE08.03 - Explain process threads and handles
  - CCWE08.04 - Describe the thread states
  - CCWE08.05 - Discuss the differences between processes, threads, and handles
  - CCWE08.06 - Describe system processes

Windows Section 2 - Processes

- SKILL CCWE09: Analyze the validity of Windows processes
  - CCWE09.01 - Identify the importance of the output of command line tools
  - CCWE09.02 - Determine the abnormal activities that are taking place on a system based on a process list
- SKILL CCWE10: Identify Different Types of Malware
  - CCWE10.01 - Distinguish between types of malware
  - CCWE10.02 - Discuss the purpose and methodology of bots and botnets
- SKILL CCWE11: Identify aspects of virtualization
  - CCWE11.01 - Discuss the importance of virtual machines
- SKILL CCWE12: Identify the importance of situational awareness
  - CCWE12.01 - Explain the situational awareness process
  - CCWE12.02 - List ways to gain situational awareness on a remote system
  - CCWE12.03 - Explain potential reasons for heightened situational awareness

Day 4

Pre-Boot, Boot, Logon - Windows XP

BIOS

Pre-Boot	-	Power On Self Test (POST)
MBR	-	Loads boot code
Bootcode	-	Searches partition table for boot sector and loads NTLDR
NTLDR	-	Reads in boot.ini for OS choices, runs NTDETECT.com to query hardware
	-	Stored data from NTDETECT.com in HKLM\Hardware registry key
	-	Starts NTOSKRNL.exe and HAL.dll
NTOSKRNL.exe	-	starts SMSS.exe
SMSS.exe	-	Launches Winlogon.exe and CSRSS
Winlogon	-	starts LSASS, loads MSGINA, starts SCM, starts logonui.exe

Pre-Boot, Boot, Logon - Windows XP

WE07

MSGINA.dll	- Graphical Identification and Authorization (GINA) dll library - Activates the user shell - Customizable identification and authentication procedures - Logon dialog
Winlogon	- Receives credentials from MSGINA and passes them to LSASS
LSASS	- Checks creds against LSA database cache then NTLM or Kerberos if not found - Sends user token back to Winlogon
Winlogon	- Starts userinit in user context
Userinit	- Loads user profile, runs startup programs, starts explorer.exe

Pre-Boot - Windows 7

There are two different types of pre-boot processes

BIOS

- **Power on Self Test (POST)**
- **MBR**
  - First 512 byte sector on hard disk
  - Reads and loads Volume Boot Record
- **VBR**
  - Loads bootmgr into memory
- **Bootmgr**
  - Reads Boot Config Database (BCD)
  - Boot menu and memtest
  - Calls winload (fresh boot)
  - Calls winresume
- **Winload**
  - **Loads NTOSKRNL.exe**
  - **Loads dependencies**
  - **Loads device drivers**

EFI / UEFI

- **Power on Self Test (POST)**
- **Runs Bootloader (from NVRAM)**
  - Loads BCD (also in NVRAM)
- **Bootloader detects hardware**
- **EFI boot manager gives OS boot menu**
- **Winload.efi: EFI version of winload**
- **Requires EFI system partition**
  - Formatted as FAT
  - Up to 1GB in size

WE06

Boot - Windows 7

NTOSKRNL
- SYSTEM
- Prepares for running native system
- Runs SMSS

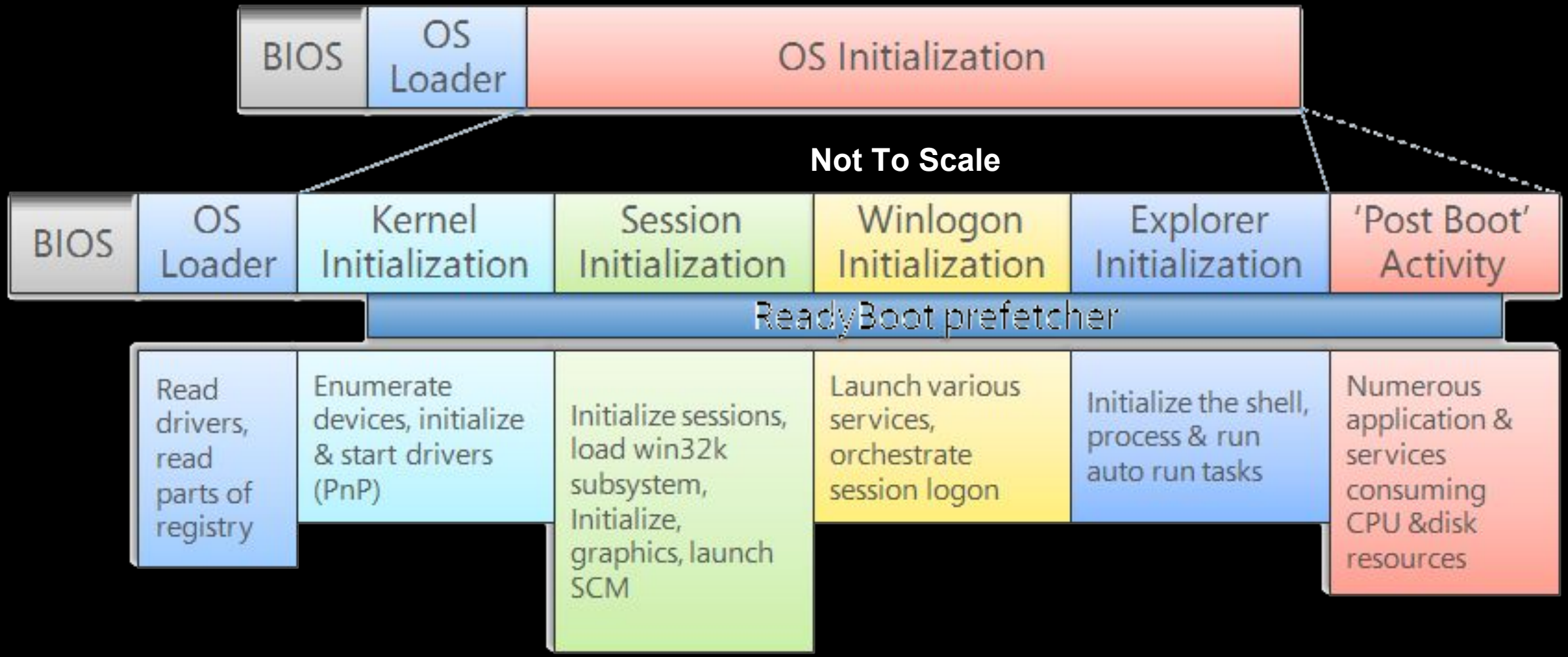
HAL.dll
- Hardware Abstraction Layer (HAL)
- Interfaces driver to kernel

SMSS
- Session manager
- Session 0 loads Win32k.sys (kernel subsystem)
- Runs WININIT

WININIT
- Starts Service Control Manager (SCM)
- Starts Local Security Authority SubSystem (LSASS)
- Starts Local Session Manager (LSM)

CSRSS
- Client/Server Runtime SubSystem
- Client side of the win32 subsystem process
- Thread creation

Boot - Windows 7



Logon- Windows 7

Winlogon	-	Coordinates logon and useractivity - Launches logonui
Logonui	-	Interactive logon dialog box
Services	-	Loads auto-start drivers and services

NOTE: Main difference between local logon and domain logon is WHERE the user is authenticating.

- Local Logon - authenticates locally with the Security Account Manager (SAM)
- Domain Logon - authenticates with the Domain Controller (DC)

ACTIVITY: Monitor the Boot Process in PROCMON

CLICK ME FOR ACTIVITY PROMPT!

Processes and Threads

`Tasklist`	- cmd.exe : loaded modules, services, owner
`Pslist`	- sysinternals : detailed information
`WMIC PROCESS list full`	- WMIC : executable path for process
`Get-process`	- powershell
`Get-wmiobject -class win32_process`	- powershell
`Task Manager`	- GUI

RESEARCH ACTIVITY:
Process States

Process States

New/Created	- Open file (.exe) - Create initial thread - Pass to kernel32.dll to check permissions - Pass to csrss, build structure, spawns first sub-thread, inserts into windows subsystem-wide proc list - Starts execution of initial thread - For real-time systems, processes may be held in “New State” to avoid contention, otherwise moved to “Ready State”
Running	- Process currently being executed (one or more threads executing)
Ready	- Process ready to execute when given the opportunity (CPU Time)
Waiting	- Process can’t execute until some event occurs (I/O Read)
Terminated/Exit	- Termination of a process due to a halt or abort

Paging

Pages

- Memory is allocated to process in distinct chunks

Page Size

- Smallest unit of protection at the hardware level
- 4KB for small page, 2MB for large page

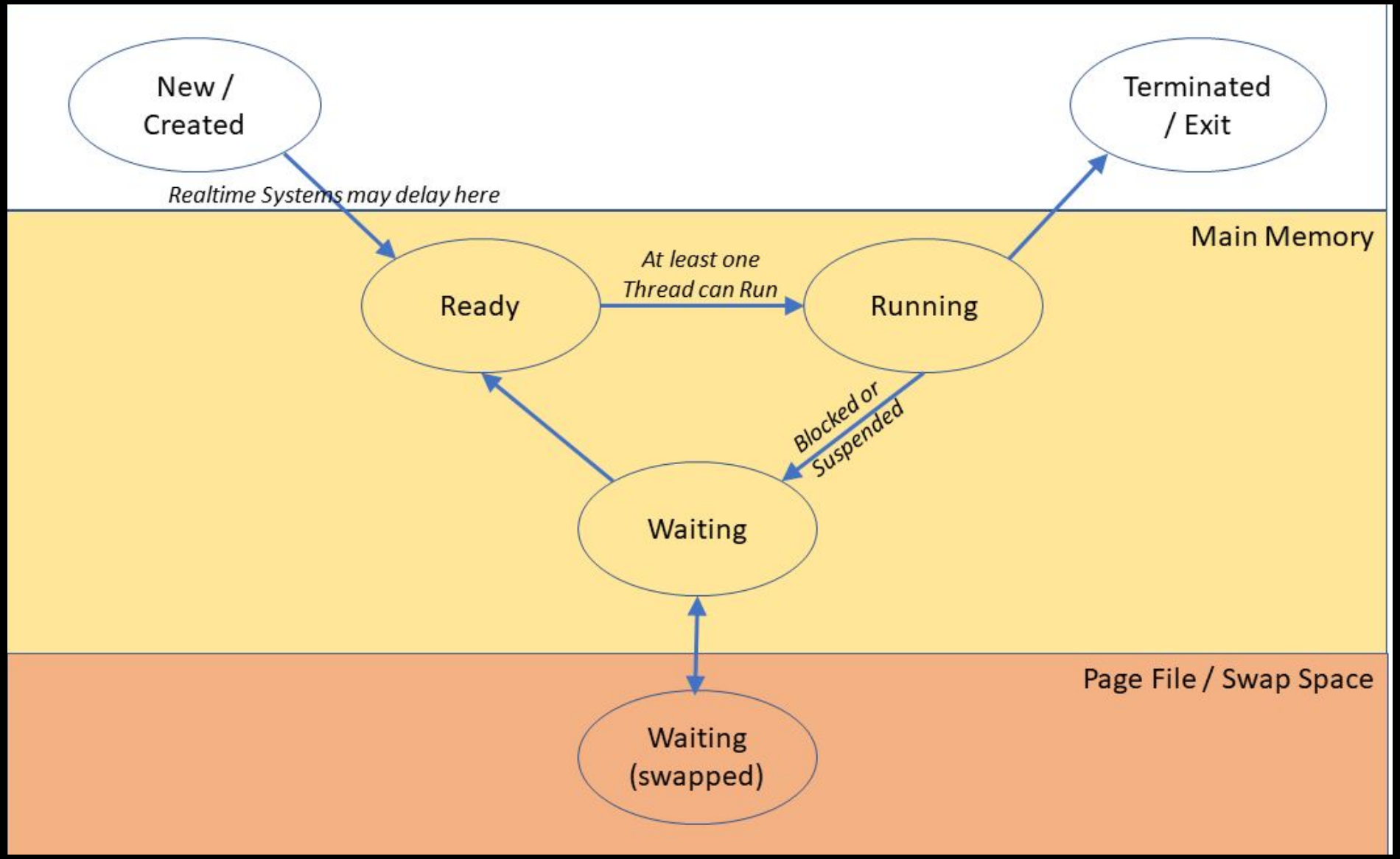
Overcommitted

- Physical memory becomes overcommitted (threads try to use more memory than available) pages are written to the page file on disk

Page Fault

- Occurs when a thread references an invalid page
- if page is on disk in the page file, it can be brought back into memory

Process States



Day 5

Windows Services

What are Windows Services?

- Long running executable application that run in their own container (process)
- Can be started automatically at boot, on demand, or when requested
- Can be paused, stopped, or restarted
- Run in the background, normally without a user interface
- Provide a service such as HTTP, FTP, or RDP

Windows Services

How do we view services on a machine?

`Sc`	-	cmd.exe, querying and management
`Get-service`	-	powershell
`WMIC service`	-	WMIC

Examples

`Sc queryex eventlog`	-	info for eventlog service including PID
`Tasklist /FI “pid eq XXX” /v`	-	query tasklist for PID associated with eventlog
`Tasklist /FI “pid eq XXX” /svc`	-	query tasklist for svchost services
`Sc qdescription eventlog`	-	query eventlog service description
`Sc qc eventlog`	-	show the binary command that loads the service

NOTE: What if the service is R/W to someone it shouldn’t be? What context do services run as?

ACTIVITY: Service Enumeration

CLICK ME FOR ACTIVITY PROMPT!

Threads and Handles

Threads

- Basic unit to which the OS allocates processor time
- Can execute any part of the process code
  - Including parts currently being executed by another thread
- Share memory with each other as well as the process
- Deadlock is possible if the threads are waiting for each other's resources
- Synchronization (semaphores, mutexes) are used to control access to shared variables
- Client/Server Run-Time Subsystem (CSRSS) maintains a list of threads
- Threads are part of a execution priority pool 0-31 per processor, highest executes next

Threads and Handles

Handles

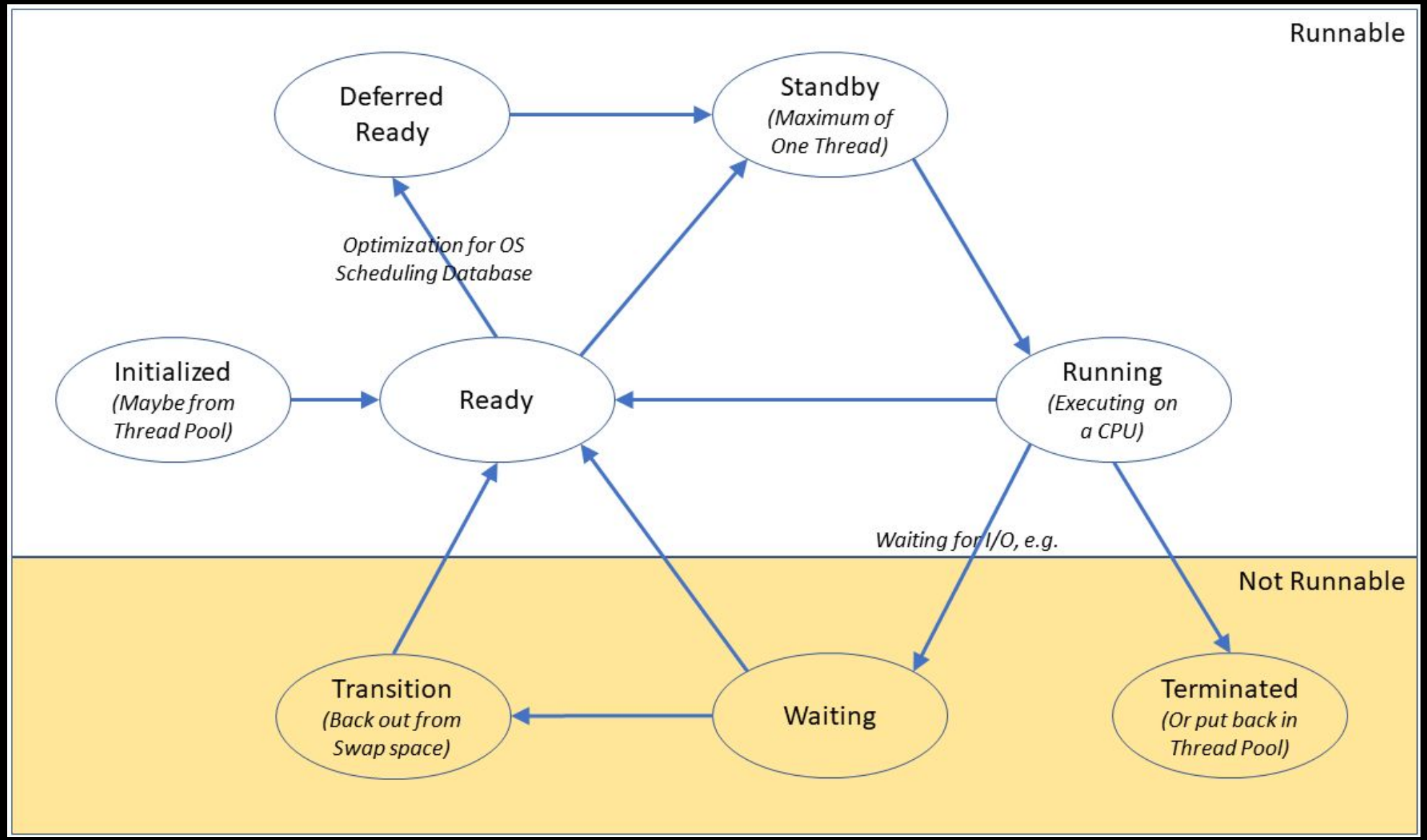
- Objects are data structures representing a system resource (file, thread, etc)
- Applications can't access objects directly, must obtain a handle
- Handles for each process are tracked in an internal table known as the Object Manager
- Handles allow a common interface to objects, regardless of underlying changes to the object
- Handles allow Windows to track ACLs for objects during handle creation time

RESEARCH ACTIVITY:
Thread States

The 8 Thread States

Ready	-	Waiting for Execution, in priority pool
Deferred Ready	-	Selected to run, but not yet executed. Optimization for scheduling database
Standby	-	Next thread to run, only one per processor per system
Running	-	A thread currently running on a processor
Waiting	-	A period of inactivity while waiting for an event
Transition	-	Ready for execution, but paging needed to bring back into memory
Terminated	-	Finished execution, heading for deallocation in most cases
Initialized	-	Thread is being created

Thread States



Processes VS. Threads VS. Handles

Process

- The primary container (memory structure) for a program being executed

Thread

- Represents sequential machine-code instructions that a processor executes

Handle

- Pointer to OS objects referenced within a process

System Processes

What are system processes?

- *processes owned by, and executed by the operating system*
- *required for the system to function*

What are the two types of system processes?

- USER Mode
  - Runs in private virtual address space
  - Applications are isolated, one crash will not cause another to crash
- KERNEL Mode
  - All run in a single virtual address space
  - Not isolated from other processes

Process Validity

PID's Sequence	-	Out of order PIDs
Name	-	Unfamiliar process names, Duplicate processes, Spelled Incorrectly
Process Age	-	typical startup processes but launched more recently, (ex. smss.exe)
Priority Levels	-	Processes with higher or lower priority level than required/expected
Handles	-	Libraries or files the process has open

QUIZ: Which of the following processes has a legitimate name?

- Googleupdate.exe **VS.** Googleupdater.exe **VS.** Googleupdate.exe

ACTIVITY: Malware Research

CLICK ME FOR ACTIVITY PROMPT!

Types of Malware - Attacks

Virus	- Requires user interaction to replicate
Worm	- Does not require user interaction to replicate
Trojan	- Malware hidden within another legitimate program - Not usually self-replicating
Malicious Mobile Code	- Transmitted from remote host to local host - Executed without user instruction (i.e. Javascript, VBScript, etc)
Blended Attack	- Multiple infection/transmission methods used together

Types of Malware - Tools

Backdoor	- Malicious program that allows illegitimate access to a machine - User is unaware
Remote Access Tool (RAT)	- Malicious program that provides remote command and control
Rootkit	- Malicious program that is ONLY used to hide things - DOES NOT provide access or command and control alone
Keylogger	- Records keyboard usage
Botnet Client	- Remote administration/Command and Control of a botnet
Spyware	- Monitors behavior of user
Adware	- Paid for ads to infected users
Ransomware	- Blocks access to a resource, requires payment from victim

Bot Herders, Botnets, and Zombies

Bot Herder - Person in control of the botnet

Botnet - Multiple machines infected and controlled by a bot herder

Zombie - Individual machine infected and part of the botnet

Purpose

- *Bot herder can utilize the botnet to accomplish a task such as:*
  - *Attack (DDoS)*
  - *Computation (Password Cracking / Bitcoin Mining)*
  - *Infection of additional systems*
  - *Obfuscation of traffic*

Methodology

- *Payload is configured to infect the intended machines and delivered to the victim*
- *Victim executes the payload, infecting the machine, and joining the botnet*
- *Victim machine calls back to the bot herder's C&C server for additional instructions*

EXERCISE:
Windows Baseline Processes

Blackboard -> Windows Section 2: Processes ->
Exercise: Windows Baseline Processes

Day 6

Malware/Process Analysis

Static Analysis - Examine malware without executing it

- Strings
- IDA Pro, OLEDebug
- DLL's used/referenced in Strings output
- OSINT (Open Source Research)
    - Name/Hash check for existing information online

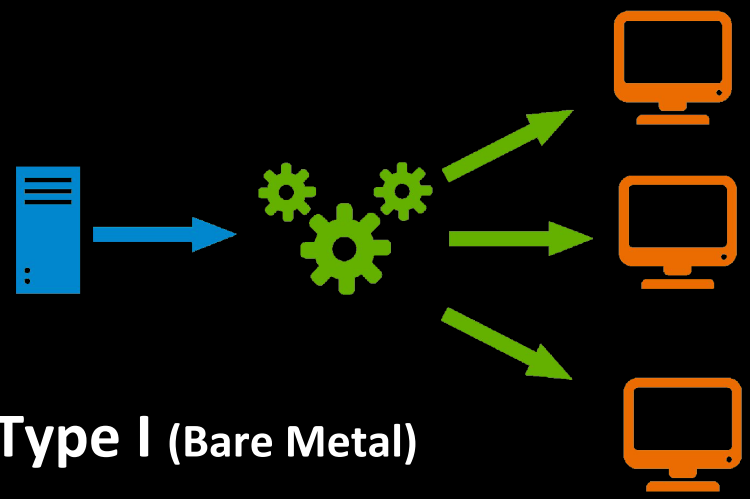
Dynamic Analysis - Examine malware while it is running

- ProcMon
- TCPView
- IDA Pro, OLEDebug
- Reg Shot
- Wireshark

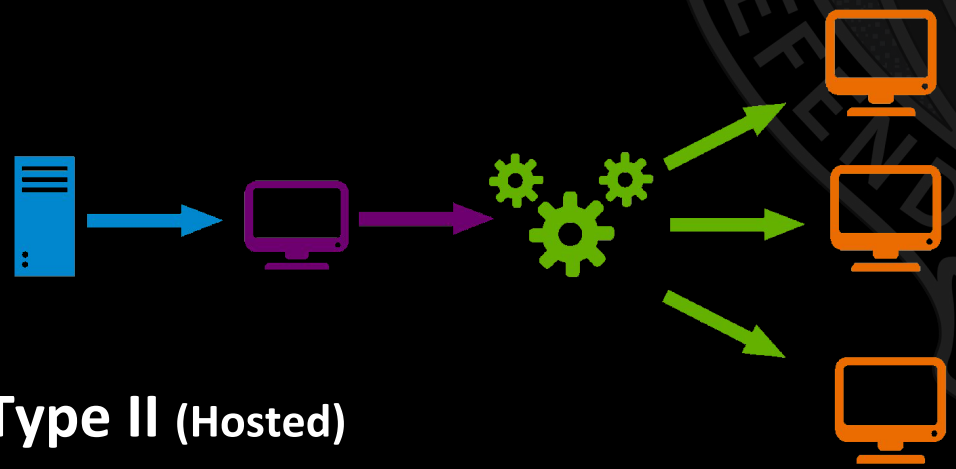
Virtualization

What is Virtualization?

- **Virtualization is technology that allows you to create multiple simulated environments or dedicated resources from a single, physical hardware system. Software called a HYPERVISOR connects directly to that hardware and allows you to split 1 system into separate, distinct, and secure environments known as VIRTUAL MACHINES (VMs).**



Type I (Bare Metal)



Type II (Hosted)

Virtualization - Benefits

- One set of Hardware -> Many virtual machines (VM)
- VMs can be dynamically created and allocated to users
- Baseline Image can be more rapidly updated
- VMs instances can easily be rolled back to undo changes
- Provide fault tolerance through redundant hardware and migration
- Could be used as a pivot point
- Could provide persistence if data store is compromised
- Lessens attribution
- Configurable software solution (OS, Services, Programs, etc)
- Useful for protected Malware Analysis (Malware Detonation Chamber)
- Quick restoration times
- Usable as Honey Pot or Tar Pit
- Difficult for malware to maintain persistence
- Easily manageable across enterprise

Virtualization - Risks

- Typically require more upfront planning and configuration
- In public cloud environments, lack of granularity in control of data at rest can lead to compliance issues (HIPPA, etc).
- Some functions may not work well in a VM, such as copy/paste, printers, netstat, without additional setup effort.
- Persistence can be lost if the target machine is restored
- Could end up in a honey pot or tar pit
- If the data store is compromised all new instances will also be compromised
- Planning and initial setup cost more with virtual networks.

Situational Awareness

What is situational awareness?

- A method of gaining an understanding of the current operating environment on the target machine
- It applies both defensively and offensively
- Allows you to get an idea of what the system is used for and what type of users use it
- Used to decide what courses of action are appropriate for the system

Situational Awareness

What is running on the system?

- Processes
- Services
- Scheduled Tasks
- Registry Keys
- Security Products (AV/Admin Tools)

Users

- Accounts
- Groups
- Domain

Networking

- System networking settings
- Local subnet
- Active Network Connections
- Routing
- Firewall settings

Logging and Auditing

- Windows event logs
- Windows auditing policies

Situational Awareness

What areas are the most important to be aware of?

- Running Processes
- Active Users
- Network Configuration
- Network Communications
- Logging
- Scheduled Jobs
- Aliases

What Easiest way to gain situational awareness on a machine?

- Using the CLI commands previously mentioned and more to come!