ProcessID of 4

**system**

Which file format is used for holding multiple codes and procedures for a windows program?

**DLL**

These apps typically start when the computer is booted and run equity in the background until it is shut down

**services**

These are instances of executable code running on a system

**process**

This system level process will be associated with each session listed from the GetProcess cmmand

**csrss**

Which is not a way to examine process

**get-processes**

Which command will show the path of a service

**get-ciminstance Win32\_serive | select name, process id, path**

which will not show scheduled task

autotask

which will not show network connectivity

**get**-**netstat**

which parameter will show process (executable involved)

-b

UAC stands for?

**user account control**

UAC is used to limit privileges of running application

TRUE

Any object within a computer system that contains data or evidence that something is a **ARTIFACT**

Artifacts can be associated with an user. What command does not associate with SID user

get -usersettings | select name,sid

Which is not relevant about artifacts

randomly sprinkled

Get-ComputerInfo

—

command used by systemD to configure units

**systemctl**

a zombie process os

**a completed child process waiting for its parent**

An orphan process is

**adopted by init after its parent dies**

A zombie process is also known as

**A defunct process**

When is this cron job running: 12 4 \* \* \* /usr/bin/backup

**4:12 AM**

What is this cron job doing 12 \* \* \* /usr/bin/backup

**running every hour on the 15 min mark on Sunday**

What identifies a kernel mode process on a ps output?

**[brackets] or PPID of 2 (kthreads)**

A daemon process:

**will always be an orphan**

Cron jobs located

**/etc/crontab or /etc/cron.d**

Defines the access rights for process

**EUID**

Define which user can kill and send signals to a process

**RUID**

Copies a parent process before making a child process for a new program

**fork()**

What is the ancestor process of all user mode process

**sbin/init**

Sets users crontab file to the contents of a listed file

**crontab -u [user] file**

Displays the user’s crontab contents

**crontab -l -u [user]**

Removes the user’s crontab content

**crontab -r -u [user]**

Edit user’s crontab

**crontab -e -u [user]**

—

Kernel’s job in boot process

**execute /sbin/init**

what does the BIOS do during linux boot?

**perform post and passes control to the boot loader program**

what is the correct order for the linux boot process

**BIOS MBR Grub Kernel Init Runlevel**

Big mike got killed in russia

What is partition?

**logical subdivision of physical media**

Maximum partitions can be created in MBR?

**4**

Each primary partition in the MBR consumes how many bytes?

**16**

Reads and executes the first sector on the boot disk to load to memory?

**BIOS**

Contains the bootloader, partition table and validity check?

**MBR**

Configurable bootloader sets default IS and kernel parameters

**GRUB**

Establishes memory management, drivers, mounts filesystem

**↳Kernel**

Configures the environment for the system.runs startup script

**INIT**

determines mode that the OS will run in

**RUNLEVEL**

Command to identify bootloader **display details about block devices**

**lsblk**

config file for /sbin/init

inittab

Location of the startup scripts (sysV)

/etc/init.d

Single user mode

**Runlevel 1**

Multi-user without networking

**Runlevel 2**

Multi-user with networking

**Runlevel 3**

Multi-user with networking + GUI

**Runlevel 5**

Config file for GRUB 2.x

**grub.cfg**

—

POST

Power of self test

This happens during the Hardware Initialization phase

Performs POST and loads firmware settings

For HAL.dll, HAL stands for

Hardware abstraction layer

Windows Boot Manager

Reads the file system and starts the OS

The First user mode process

smss.exe

Used to define the boot menu

BCD store (binary coded decimal)

This contains the disk partitions for BIOS

MBR master boot record

This process handles User authentication services

lsass.exe

How many boot managers are there?

1

Always had a process ID of 4

System

—