**Linux Review**

persistence

enumeration of a network

sysV: cron, running config (acts like registry)

sysD: init, timing, wants & requires of services, profiles

commands

w (whos logged in)

which ls (where ls comes from)

whatis ls (one line manual page)

find

locate (searches everything)

grep

sed (alter the output text, doesnt change actual data)

awk

apropos ls

hier

\*netstat -ano

linux boot process

BIG MIKE GOT KILLED IN RUSSIA

**BIOS MBR Grub Kernel Init Runlevel**

dmesg | tail (show last 10 logs, head=first 10)

systemV: service --status-all (running +, not running - services)

systemD: systemctl list-units (List all unit files that systemd has listed as active)

\*temp directory- any user is able to create temp file (less restrictive)

\*proc- pseudo file system shows everything running

look for fd (file directory) directory, pipe\* indicator

permissions

SUID (bit set to run EUID becomes the one who is running it)

ex: sudo

GUID (permission set if two diff groups it distinguishes the two)

ex: user-group-other, rwerwerwe, 421421421, chmod 777

SGID (directory permissions)

Sticky bit (drwxrwxrwt) s or t

syscall

fork() - (creates new process by duplicating existing process) from kthreadd

exec() - (new process takes over parent space, used to bypass certain permissions)

For user-space processes /sbin/init ( PID = 1 )

For kernel-space processes [kthreadd] ( PID = 2 )

kill -l > SIGTERM

orphan (a parent process dies and child process gets adopted by /sbin/init with PID 1)

zombie (completed execution but hasnt been reaped by its parent process, cannot be killed However, they do take up PIDs in the process table which is a finite resource. Zombie entries can be removed from the process table by killing its parent process)

jobs

cron jobs

controlled by /etc/crontab

stored in /var/spool/cron/crontabs/

touch (creates empty file)

Auditing and logging

Syslog stores its logs as human-readable text documents within **/var/log**. It is configured using files in **/etc/rsyslog/**

wtmp- history file for utmp (keeps track of login) /var/log/wtmp and /var/run/utmp

\*last command (ascii representation of binary)

/var/run/btmp (bad logins)

last -f /var/log/btmp

cat /var/run/utmp -currently logged in)

**Powershell Review**

Registry

Scheduled Tasks

Profiles

Basic cmdlet

Get-Verb, Get-Command, Get-Help cmdlet, \***Get-Member**, Get-Localuser,

Pipe

| Select-Object Name, ID, path

| Where-Object {$\_.ID -lt ‘1000’}

Methods

A method is an action that can be taken on an item. "Revoke"

Properties

Placeholder for something about a cmdlet ex: Status, Name, and DisplayName

Powershell profile

Create powershell profile

New-Item -ItemType File -Path $profile -Force

$profile | Get-Member -Type NoteProperty

# Displays the profile values of Names, MemberType, and Paths.

$Profile | get-member -type noteproperty | ft -wrap

# Displays the same results but completed in case it was cut off '...'

$PROFILE | Get-Member -MemberType noteproperty | select name

# Narrowed results to display only Names

Test-Path -Path $profile.currentUsercurrentHost

Test-Path -Path $profile.currentUserAllHosts

Test-Path -Path $profile.AllUsersAllHosts

Test-Path -Path $profile.AllUserscurrentHost

CIM class (template for instance running eg process, service)

ciminstance

Get-Cimclass \*

# Lists all CIM Classes

Get-CimInstance –Namespace root\securitycenter2 –ClassName antispywareproduct

# Lists the antispywareproduct class from the root/security instance

Get-CimInstance -ClassName Win32\_LogicalDisk -Filter “DriveType=3” | gm

# Shows properties and methods for this Instance

Get-WmiObject -Class Win32\_LogicalDisk -Filter “DriveType=3”

# Using the Windows Management Instrumentation method

Bootloader

On Windows only ONE boot manager, multiple boot loaders

BCDedit

Network

netstat -ano

alias (list all aliases)

UAC Bypass