FANSHAWE

INFO-6003

O/S & Application Security

Week 07

Agenda

- Windows Services
- Sysinternals - Process Explorer
- Service Security
- Session Isolation
- Protected Processes

Windows Services

Windows Services

- Services provide a communication function between clients and servers either local or remote
- All windows computers run both workstation and server services by default
- Workstation Service
  - Used for **Outbound** connections
- Server Service
  - Used for **Inbound** connections

Windows Services

- Workstation & Server services
  - Run on both client computers and servers
  - Workstations use server services for file sharing
- Services use protocols such as SMB & RPC to communicate
  - Used by many Windows services such as Net Login, Group policy, Print Spooler, etc.
    - RPC-Remote Procedure Calls
    - SMB-Server Message Block
      - A file transfer service in Windows

Windows Services

- Many services are activated and run by the OS on start up before a user even logs on
- The service account will run under a predefined user logon account
  - The service/process becomes a security principal
- Most services are loaded as DLLs or .EXEs from the %SYSTEMROOT%\system32 folder

Windows Services

- The operating system creates long complicated passwords for these accounts
- Password is changed regularly by the O/S
- Virtually impossible to logon to a computer using these service logon accounts

Windows Services

- Some examples of these that may run before any local user logs on include:
  - IIS
  - SSH
  - Telnet
  - FTP
- IIS and SQL Server are some of the most commonly attacked Windows Services

Windows Services

- Services generally run on their default ports which makes them easier to enumerate
  - IIS port 80
  - FTP port 21
  - SSH port 22
  - Telnet port 23
  - SQL Server port 1433

Disable Unused Services

- FTP port 20 & 21 TCP
- DNS port 53 TCP/UDP
- Telnet port 23
- TFTP port 69 UDP
- NNTP port 119 TCP
- NetBIOS ports 135 TCP/UDP, 137-138 UDP, 139 TCP
- RPC ports 1025 – 1039 TCP/UDP

This will help reduce the attack surface

Service Control Manager

- Services are managed with, and by, the Service Control Manager (SCM)
- The SCM allows services to log on and access resources without needing the administrator or a user to logon first
  - Service must have the “Log-on As A Service” right
  - SCM starts the services defined as auto start

Services Active Database

- The SCM reads information from the SCM database located in the registry at:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services

- The database contains values for all services and drivers needed to boot the operating system
  - Although you shouldn't go into the registry to set the values such as auto-start, this is where they are actually located

Services Active Database in Windows 10

Registry Editor

File Edit View Favorites Help

- Computer
  - HKEY_CLASSES_ROOT
  - HKEY_CURRENT_USER
  - HKEY_LOCAL_MACHINE
    - BCD00000000
    - DRIVERS
    - HARDWARE
    - SAM
    - SECURITY
    - SOFTWARE
    - SYSTEM
      - ActivationBroker
      - ControlSet001
      - CurrentControlSet
        - Control
        - Enum
        - Hardware Profiles
        - Policies
        - Services
          - .NET CLR Data
          - .NET CLR Networking
          - .NET CLR Networking 4.0.0.0
          - .NET Data Provider for Oracle
          - .NET Data Provider for SqlServer
          - .NET Memory Cache 4.0
          - .NETFramework
          - {4B64CF94-013F-4501-809D-1EFE26E94
          - {4E214F9A-9D2E-45AB-B8A5-4FEA9A03
          - {B736A063-A4DD-4763-95E2-2085821D
          - {DE85FFF7-FB0E-485F-AF76-ABEE9F4C
          - {E864F68D-5CC3-4FD1-924D-62BA3ED8
          - 1394ohci
          - 3ware
          - ACPI
          - acpiex
          - acpipagr
          - AcpiPmi
          - acpitime
          - AdobeARMservice
          - AdobeFlashPlayerUpdateSvc
          - ADOVMPPackage

Name	Type	Data
(Default)	REG_SZ	(value not set)
Description	REG_SZ	This service keeps your Adobe Flash Player installation up to date with the latest en...
DisplayName	REG_SZ	Adobe Flash Player Update Service
ErrorControl	REG_DWORD	0x00000001 (1)
ImagePath	REG_EXPAND_SZ	C:\Windows\SysWOW64\Macromed\Flash\FlashPlayerUpdateService.exe
ObjectName	REG_SZ	LocalSystem
Start	REG_DWORD	0x00000003 (3)
Type	REG_DWORD	0x00000010 (16)
WOW64	REG_DWORD	0x00000001 (1)

Here the AdobeFlashPlayerUpdateSvc has it's subkey value set to 3

Services Active Database Values

https://support.microsoft.com/en-us/kb/103000

START TYPE	LOADER	MEANING
0x0 (Boot)	Kernel	Represents a part of the driver stack for the boot (startup) volume and must therefore be loaded by the Boot Loader.
0x1 (System)	I/O subsystem	Represents a driver to be loaded at Kernel initialization.
0x2 (Auto load)	Service Control Manager	To be loaded or started automatically for all startups, regardless of service type.
0x3 (Load on demand)	Service Control Manager	Available, regardless of type, but will not be started until the user starts it (for example, by using the Devices icon in Control Panel).
0x4 (disabled)	Service Control Manager	NOT TO BE STARTED UNDER ANY CONDITIONS.

Service Control Manager

- Once the database has been read, then the SCM does the following:
  - Logs the service on with the credentials listed
  - Loads the services user profile
  - Starts the service
  - Finds any dependencies and starts those if needed

Service Logon Accounts

- Windows has 3 Logon Accounts used by services
- **Local System**
  - Is a powerful account that can do anything the operating system can do
- **Local Service**
  - Has limited access to local computer
  - Privileges similar to a logged on user
- **Network Service**
  - Access to network with a local computer account for authorization
  - Limited access to local computer

Service Logon Accounts

- For access to network resources
- **Local System**
  - Has the security context of the local computer the account is created on
- **Local Service**
  - Connects to the network resource as null session (anonymous account)
- **Network Service**
  - Security token contains the Everyone & Authenticated user SID

Service Logon Accounts

- The **Local System** account has the most default privileges enabled followed by
  - **Administrators group**
  - **Local Service**
  - **Network Service**
  - **Standard users**
- Some privileges listed for the Local System account are disabled by default but the service can enable any listed privileges

Windows Services

- A service is a security principal and has a security token
  - Sometimes called a process token
  - Privileges of the service are listed in the token

Windows Services

- For Windows NT and 2000 ALL default built-in services started in Local System
  - Buffer overflow in one of these default systems would give a hacker system access
- WinXP & Win2003 server moved some Local System services to Local Service & Network Service (more limited accounts)
- Current versions of Windows have moved even more services out of the Local System context

Windows Services

- Since Vista and Server 2008 Microsoft committed to the Principle of Least Privilege to determine the exact rights and privileges required by each service
- The service logon account now has a list of default privileges and optional privileges
- If a privilege granted by the default log on account is not required for that particular service then the privilege is removed when that service starts

Windows Services

- Example of changes: DHCP
  - DHCP client runs under Local System context in WinXP
  - With Vista the DHCP client runs under the Local Service context
    - Has fewer privileges when run than actually assigned to the Local Service logon account
    - This is a good example of the principle of least privilege

Windows Service Tools

- When Windows starts up it can run services without needing a user to be logged on
  - Use Task Manager to see the services and which account a service is running under
- Any account can be used as a service account if it is given the Log on as a Service Right
  - Required to interact with Service Control Manager and be set for auto start

Task Manager

- Windows Task Manager will show the services that are running and the owner of the services
  - System (Local System)
  - Local Service
  - Network Service
  - Administrator
  - User account name

Task Manager Server 2008

Windows Task Manager

File Options View Help

Applications | Processes | Services | Performance | Networking | Users

Name	PID	Description	Status	Group
netprofm	944	Network List Service	Running	LocalService
lltdsvc		Link-Layer Topology Discovery...	Stopped	LocalService
FontCache	944	Windows Font Cache Service	Running	LocalService
fdPHost		Function Discovery Provider H...	Stopped	LocalService
EventSystem	944	COM+ Event System	Running	LocalService
upnphost		UPnP Device Host	Stopped	LocalServiceAndNoImpersonation
TBS		TPM Base Services	Stopped	LocalServiceAndNoImpersonation
SSDPSRV		SSDP Discovery	Stopped	LocalServiceAndNoImpersonation
SCardSvr		Smart Card	Stopped	LocalServiceAndNoImpersonation
FDResPub		Function Discovery Resource ...	Stopped	LocalServiceAndNoImpersonation
AppIDSvc		Application Identity	Stopped	LocalServiceAndNoImpersonation
lmhosts	820	TCP/IP NetBIOS Helper	Running	LocalServiceNetworkRestricted
FCRegSvc		Microsoft Fibre Channel Platfo...	Stopped	LocalServiceNetworkRestricted
eventlog	820	Windows Event Log	Running	LocalServiceNetworkRestricted
Dhcp	820	DHCP Client	Running	LocalServiceNetworkRestricted
AudioSrv	820	Windows Audio	Running	LocalServiceNetworkRestricted
pla		Performance Logs & Alerts	Stopped	LocalServiceNoNetwork
MpsSvc	1076	Windows Firewall	Running	LocalServiceNoNetwork
DPS	1076	Diagnostic Policy Service	Running	LocalServiceNoNetwork
BFE	1076	Base Filtering Engine	Running	LocalServiceNoNetwork
wudfsvc		Windows Driver Foundation - ...	Stopped	LocalSystemNetworkRestricted
WPDBusEnum		Portable Device Enumerator S...	Stopped	LocalSystemNetworkRestricted
WdiSystemHost		Diagnostic System Host	Stopped	LocalSystemNetworkRestricted

Services...

Processes: 45 | CPU Usage: 0% | Physical Memory: 24%

Task Manager Windows 10

Task Manager

File Options View

Processes | Performance | App history | Startup | Users | Details | Services

Name	PID	Description	Status	Group
FontCache	1268	Windows Font Cache Service	Running	LocalService
fdPHost	1268	Function Discovery Provider Host	Running	LocalService
EventSystem	1268	COM+ Event System	Running	LocalService
CDPSvc		Connected Device Platform Service	Stopped	LocalService
bthserv		Bluetooth Support Service	Stopped	LocalService
AJRouter		AllJoyn Router Service	Stopped	LocalService
wcncsvc		Windows Connect Now - Config Registrar	Stopped	LocalServiceAndNoImpersonation
upnphost		UPnP Device Host	Stopped	LocalServiceAndNoImpersonation
TimeBroker	1172	Time Broker	Running	LocalServiceAndNoImpersonation
SSDPSRV	1172	SSDP Discovery	Running	LocalServiceAndNoImpersonation
SensrSvc		Sensor Monitoring Service	Stopped	LocalServiceAndNoImpersonation
SCardSvr		Smart Card	Stopped	LocalServiceAndNoImpersonation
QWAVE		Quality Windows Audio Video Experience	Stopped	LocalServiceAndNoImpersonation
FDResPub	1172	Function Discovery Resource Publication	Running	LocalServiceAndNoImpersonation
BthHFSrv		Bluetooth Handsfree Service	Stopped	LocalServiceAndNoImpersonation
wscsvc	1180	Security Center	Running	LocalServiceNetworkRestricted
Wcmsvc	1180	Windows Connection Manager	Running	LocalServiceNetworkRestricted
vmictimesync		Hyper-V Time Synchronization Service	Stopped	LocalServiceNetworkRestricted
NgcCtnrSvc		Microsoft Passport Container	Stopped	LocalServiceNetworkRestricted
lmhosts	1180	TCP/IP NetBIOS Helper	Running	LocalServiceNetworkRestricted
icssvc		Windows Mobile Hotspot Service	Stopped	LocalServiceNetworkRestricted
HomeGroupProvider	1180	HomeGroup Provider	Running	LocalServiceNetworkRestricted
EventLog	1180	Windows Event Log	Running	LocalServiceNetworkRestricted
Dhcp	1180	DHCP Client	Running	LocalServiceNetworkRestricted
Audiosrv	1180	Windows Audio	Running	LocalServiceNetworkRestricted
AppIDSvc		Application Identity	Stopped	LocalServiceNetworkRestricted
WwanSvc		WWAN AutoConfig	Stopped	LocalServiceNoNetwork
pla		Performance Logs & Alerts	Stopped	LocalServiceNoNetwork

Fewer details | Open Services

Services.msc

- A complete list of services can be found with the services.msc command
- Double clicking on a listed service will show the properties of the service and allow configuration changes
  - Path to find executable
  - Service start up type
    - Automatic, Automatic(Delayed), Manual, Disabled
  - Service Status and Controls
    - Start, stop, pause, resume

Services.msc in Windows 10

Services

File Action View Help

Services (Local)

Services (Local)

Select an item to view its description.

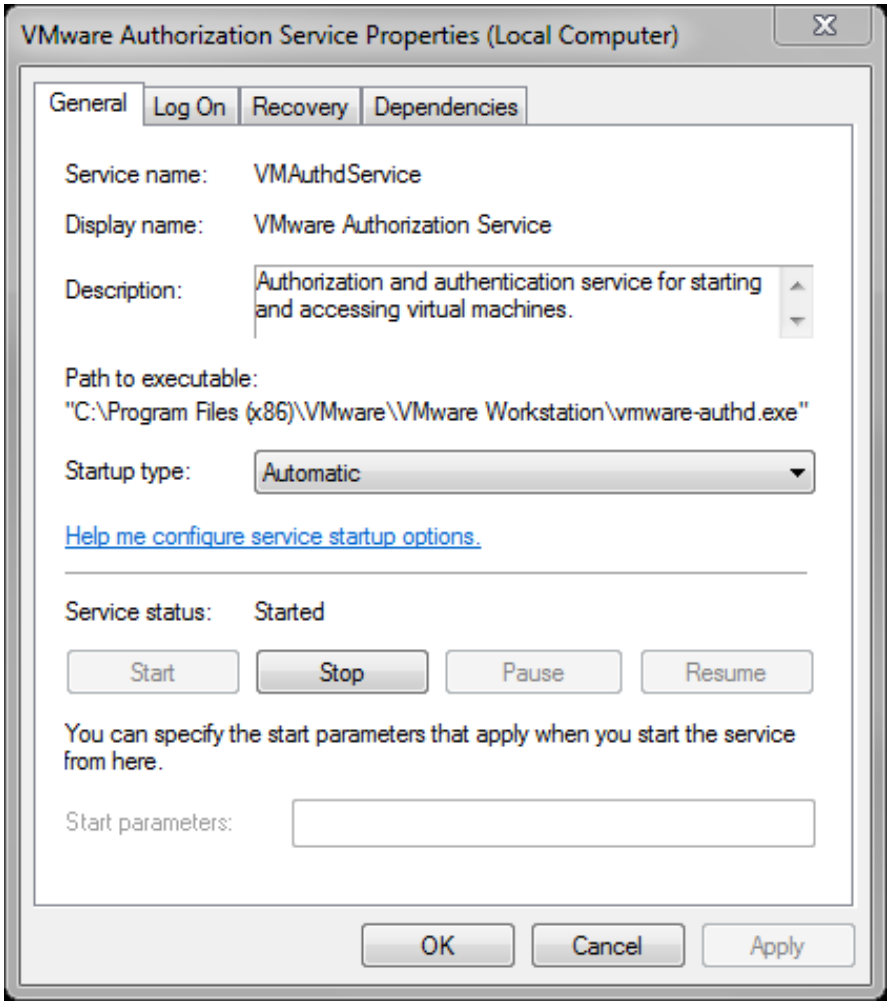
Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local System
Adobe Acrobat Update Service	Adobe Acro...	Running	Automatic	Local System
Adobe Flash Player Update Service	This service ...		Manual	Local System
AllJoyn Router Service	Routes AllJo...		Manual (Trigger Start)	Local Service
AMD External Events Utility		Running	Automatic	Local System
App Readiness	Gets apps re...		Manual	Local System
Application Host Helper Service	Provides ad...	Running	Automatic	Local System
Application Identity	Determines ...		Manual (Trigger Start)	Local Service
Application Information	Facilitates t...	Running	Manual (Trigger Start)	Local System
Application Layer Gateway Service	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local System
AppX Deployment Service (AppXSVC)	Provides inf...		Manual	Local System
ASP.NET State Service	Provides su...		Manual	Network Service
ASUS Com Service		Running	Automatic	Local System
ASUS System Control Service		Running	Automatic	Local System
Auto Time Zone Updater	Automatica...		Disabled	Local Service
Avast Antivirus	Manages an...	Running	Automatic	Local System
Background Intelligent Transfer Service	Transfers fil...		Automatic (Delayed Start)	Local System
Background Tasks Infrastructure Service	Windows in...	Running	Automatic	Local System
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption Service	BDESVC hos...		Manual (Trigger Start)	Local System
Block Level Backup Engine Service	The WBENG...		Manual	Local System
Bluetooth Handsfree Service	Enables wir...		Manual (Trigger Start)	Local Service
Bluetooth Support Service	The Bluetoo...		Manual (Trigger Start)	Local Service
BranchCache	This service ...		Manual	Network Service
Certificate Propagation	Copies user ...	Running	Manual	Local System
Client License Service (ClipSVC)	Provides inf...		Manual (Trigger Start)	Local System
CNG Key Isolation	The CNG ke...	Running	Manual (Trigger Start)	Local System
COM+ Event System	Supports Sy...	Running	Automatic	Local Service

Extended Standard

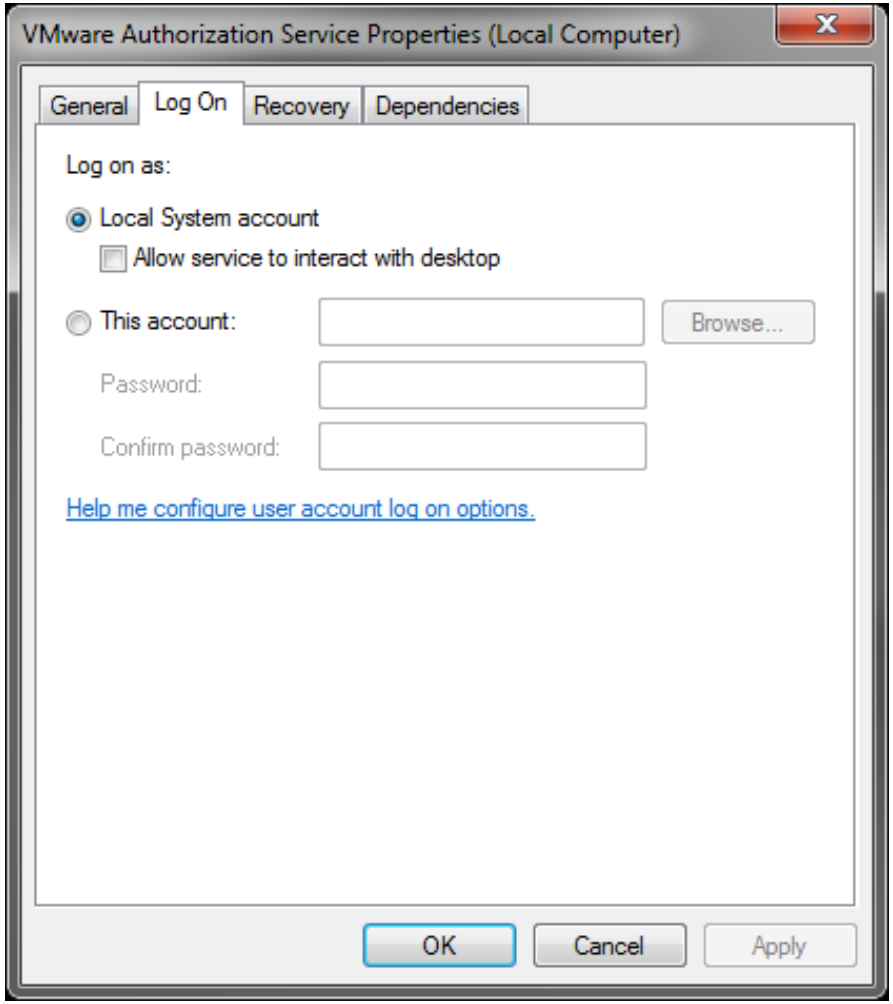
Services.msc Properties

- The services.msc properties windows has tabs that show details
  - General
    - Details about service
  - Log On account associated with service
  - Recovery action to take if services fails
    - Reboot, restart, run a program, no action
  - List of dependencies
    - Other services that must run to support this services

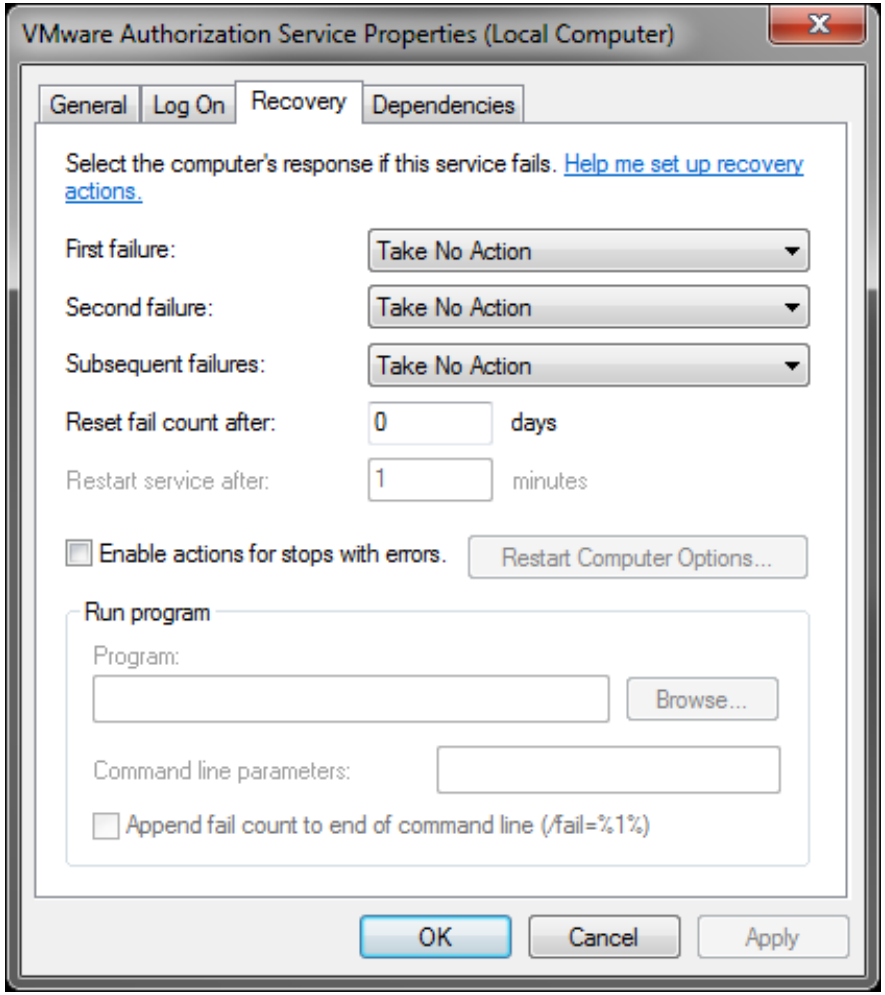
General Tab


VMware Authorization Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Service name:
VMAuthdService
Display name:
VMware Authorization Service
Description:
Authorization and authentication service for starting and accessing virtual machines.
Path to executable:
"C:\Program Files (x86)\VMware\VMware Workstation\vmware-authd.exe"
Startup type:
Automatic
Help me configure service startup options.
Service status:
Started
Start
Stop
Pause
Resume
You can specify the start parameters that apply when you start the service from here.
Start parameters:
OK
Cancel
Apply

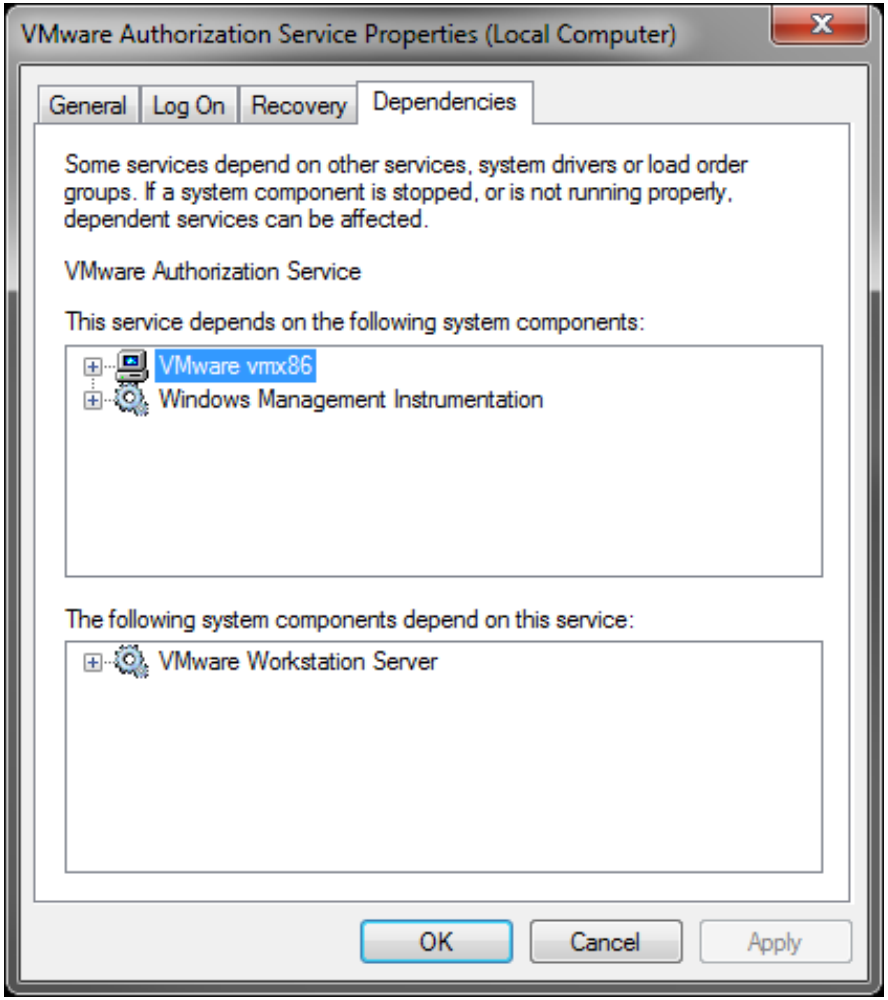
Log On Tab


VMware Authorization Service Properties (Local Computer)
General
Log On
Recovery
Dependencies
Log on as:
Local System account
Allow service to interact with desktop
This account:
Browse...
Password:
Confirm password:
Help me configure user account log on options.
OK
Cancel
Apply

Recovery Tab



Dependencies



Tasklist Command

- The programs and services running on a computer can be displayed with the tasklist.exe command
- Tasklist will display all running programs and services by process id (pid)
- Tasklist also shows if the process started as a service or through the interactive console
  - With the /v option
- Tasklist /svc will…
  - Tasklist /? For help

Tasklist Command

Command Prompt

```
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Spengler>tasklist /svc

Image Name                     PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       440 N/A
csrss.exe                      632 N/A
wininit.exe                    732 N/A
csrss.exe                      740 N/A
services.exe                   780 N/A
lsass.exe                      788 KeyIso, SamSs, VaultSvc
svchost.exe                    864 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
svchost.exe                    908 RpcEptMapper, RpcSs
winlogon.exe                   996 N/A
svchost.exe                    524 Appinfo, Browser, CertPropSvc, gpsvc,
                                   iphlpsvc, LanmanServer, lfsvc, ProfSvc,
                                   Schedule, SENS, SessionEnv,
                                   ShellHWDetection, Themes, UserManager,
                                   Winmgmt, wuauserv
svchost.exe                    552 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc, TermService
svchost.exe                    512 AudioEndpointBuilder, CscService,
                                   DeviceAssociationService, DsSvc, hidserv,
                                   NcbService, Netman, PcaSvc, StorSvc,
                                   SysMain, TrkWks, UmRdpService, wudfsvc
WUDFHost.exe                  1092 N/A
svchost.exe                   1172 FDResPub, SSDPSRV, TimeBroker
svchost.exe                   1180 Audiosrv, Dhcp, EventLog,
                                   HomeGroupProvider, lmhosts, Wcmsvc, wscsvc
```

Svchost

- Svchost – Service Host Process
  - Not all services have there own executable .EXE
  - Svchost acts as a shell for services implemented as DLLs instead of an executable
    - You can’t directly run a DLL
  - Any Windows Machine will have many instances of svchost running
  - Each instance can host one or more services

Svchost

- Svchost.exe can be tricky as attackers may hide Malicious software behind this process
- Tasklist can be used to determine which services are running under a svchost.exe process

tasklist /svc /fi "imagename eq svchost.exe"

Using Tasklist for svchost.exe Services

Command Prompt

```
C:\Users\Spengler>tasklist /svc /fi "imagename eq svchost.exe"

Image Name                     PID Services
========================= ======== ============================================
svchost.exe                    864 BrokerInfrastructure, DcomLaunch, LSM,
                                   PlugPlay, Power, SystemEventsBroker
svchost.exe                    908 RpcEptMapper, RpcSs
svchost.exe                    524 Appinfo, Browser, CertPropSvc, iphlpsvc,
                                   LanmanServer, lfsvc, ProfSvc, Schedule,
                                   SENS, SessionEnv, ShellHWDetection, Themes,
                                   UserManager, Winmgmt, wuauserv
svchost.exe                    552 CryptSvc, Dnscache, LanmanWorkstation,
                                   NlaSvc, TermService
svchost.exe                    512 AudioEndpointBuilder, CscService,
                                   DeviceAssociationService, DsSvc, hidserv,
                                   NcbService, Netman, PcaSvc, StorSvc,
                                   SysMain, TrkWks, UmRdpService, wudfsvc
svchost.exe                   1172 FDResPub, SSDPSRV, TimeBroker
svchost.exe                   1180 Audiosrv, Dhcp, EventLog,
                                   HomeGroupProvider, lmhosts, Wcmsvc, wscsvc
svchost.exe                   1268 EventSystem, fdPHost, FontCache,
                                   LicenseManager, netprofm, nsi,
                                   WdiServiceHost, WinHttpAutoProxySvc
svchost.exe                   1772 BFE, CoreMessagingRegistrar, DPS, MpsSvc,
                                   NcdAutoSetup
svchost.exe                   2696 W3SVC, WAS
svchost.exe                   2716 stisvc
svchost.exe                   2768 DiagTrack
svchost.exe                   2872 StateRepository, tiledatamodelsvc
svchost.exe                   2896 AppHostSvc
svchost.exe                   3416 PolicyAgent
svchost.exe                   9908 N/A

C:\Users\Spengler>
```

Sysinternals Power Tools

Sysinternals

- Sysinternals was created in 1996 by Mark Russinovich and Bryce Cogswell
- Was later bought by Microsoft because the tools were so valuable to system administrators and security people
- www.sysinternals.com now redirects to Technet

Process Explorer

- Windows Sysinternals Process Explorer will display many details for running programs and services
- The tool can be downloaded from:

http://technet.microsoft.com/en-us/sysinternals/bb896653

Process Explorer

- The next screen shows the processes running on a Windows 10 computer
- There are several instances of svchost running
  - Each has a separate PID (process id)
- But note the services running with the one instance of svchost (PID 552)
  - Cryptographic Services
  - DNS Client
  - Network Location Awareness
  - Workstation

Process Explorer

Process Explorer - Sysinternals: www.sysinternals.com [Spengler-PC\Spengler]

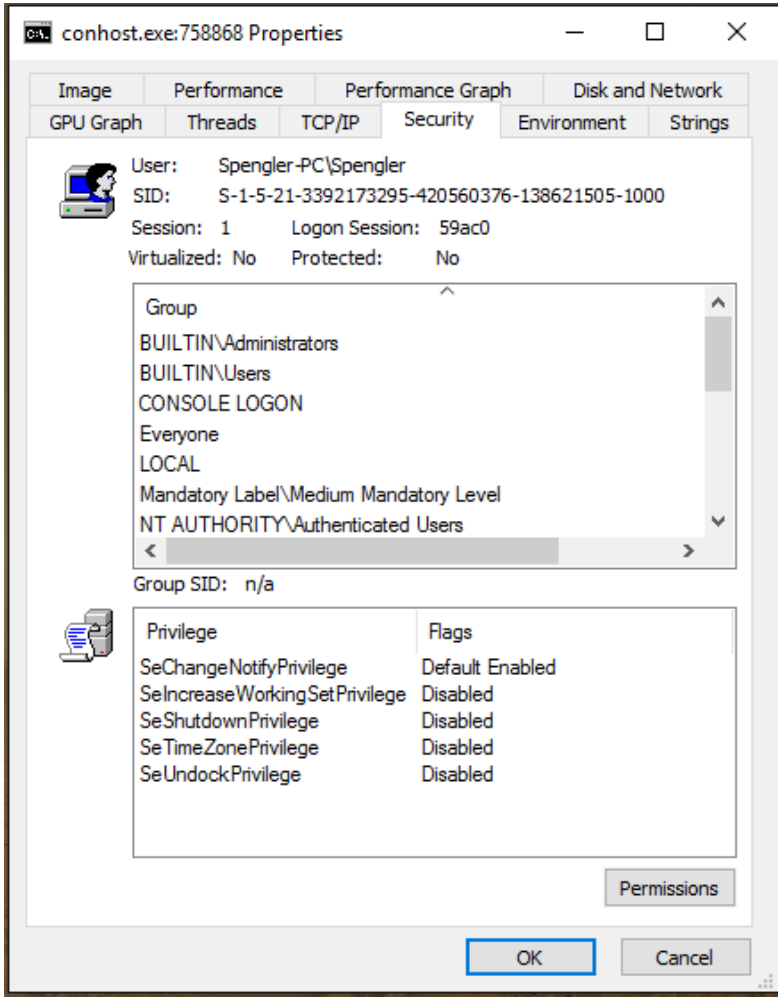
File Options View Process Find Users Help

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
services.exe		3,464 K	5,428 K	780		
svchost.exe	< 0.01	7,792 K	13,608 K	864	Host Process for Windows S...	Microsoft Corporation
WmiPrvSE.exe		12,444 K	18,076 K	3344		
WmiPrvSE.exe	< 0.01	14,304 K	17,896 K	4696		
RuntimeBroker.exe	< 0.01	32,036 K	54,876 K	5380	Runtime Broker	Microsoft Corporation
ShellExperienceHost....	Susp...	51,032 K	83,908 K	5868	Windows Shell Experience H...	Microsoft Corporation
unsecapp.exe		1,272 K	2,112 K	7776		
unsecapp.exe		1,628 K	3,228 K	8248		
SkypeHost.exe	Susp...	4,532 K	2,248 K	2424	Microsoft Skype	Microsoft Corporation
ApplicationFrameHost...	< 0.01	17,384 K	28,936 K	12104	Application Frame Host	Microsoft Corporation
SystemSettings.exe	Susp...	19,188 K	1,308 K	523932	Settings	Microsoft Corporation
Calculator.exe	Susp...	20,504 K	33,628 K	624440		
LockAppHost.exe		5,716 K	24,556 K	682676	LockAppHost	Microsoft Corporation
Microsoft.Photos.exe	Susp...	47,796 K	48,756 K	747280	Microsoft Photos	
SearchUI.exe	Susp...	87,984 K	137,344 K	761432	Search and Cortana applicati...	Microsoft Corporation
svchost.exe	0.08	7,708 K	10,224 K	908	Host Process for Windows S...	Microsoft Corporation
svchost.exe		34,764 K	47,124 K	524	Host Process for Windows S...	Microsoft Corporation
sihost.exe		8,512 K	24,020 K	5032	Shell Infrastructure Host	Microsoft Corporation
taskhostw.exe	0.01	36,616 K	43,824 K	5044	Host Process for Windows T...	Microsoft Corporation
svchost.exe		21,280 K	26,676 K	552	Host Process for Windows S...	Microsoft Corporation
svchost.exe		16,352 K	23,796 K	512	Host Process for Windows S...	Microsoft Corporation
WUDFHo				92		
WUDFHo				68		
dasHost.e				36		
svchost.exe				72	Host Process for Windows S...	Microsoft Corporation
svchost.exe				80	Host Process for Windows S...	Microsoft Corporation
audiodg.e				64		
nvvsvc.exe				88	NVIDIA Driver Helper Servic...	NVIDIA Corporation
nvxdsync				08		

Command Line:
C:\WINDOWS\system32\svchost.exe -k NetworkService
Path:
C:\Windows\System32\svchost.exe (NetworkService)
Services:
Cryptographic Services [CryptSvc]
DNS Client [Dnscache]
Network Location Awareness [NlaSvc]
Remote Desktop Services [TermService]
Workstation [LanmanWorkstation]

CPU Usage: 11.60% | Commit Charge: 20.93% | Processes: 168 | Physical Usage: 34.50%

Process Explorer



The security tab displays the SID for the user that started the process

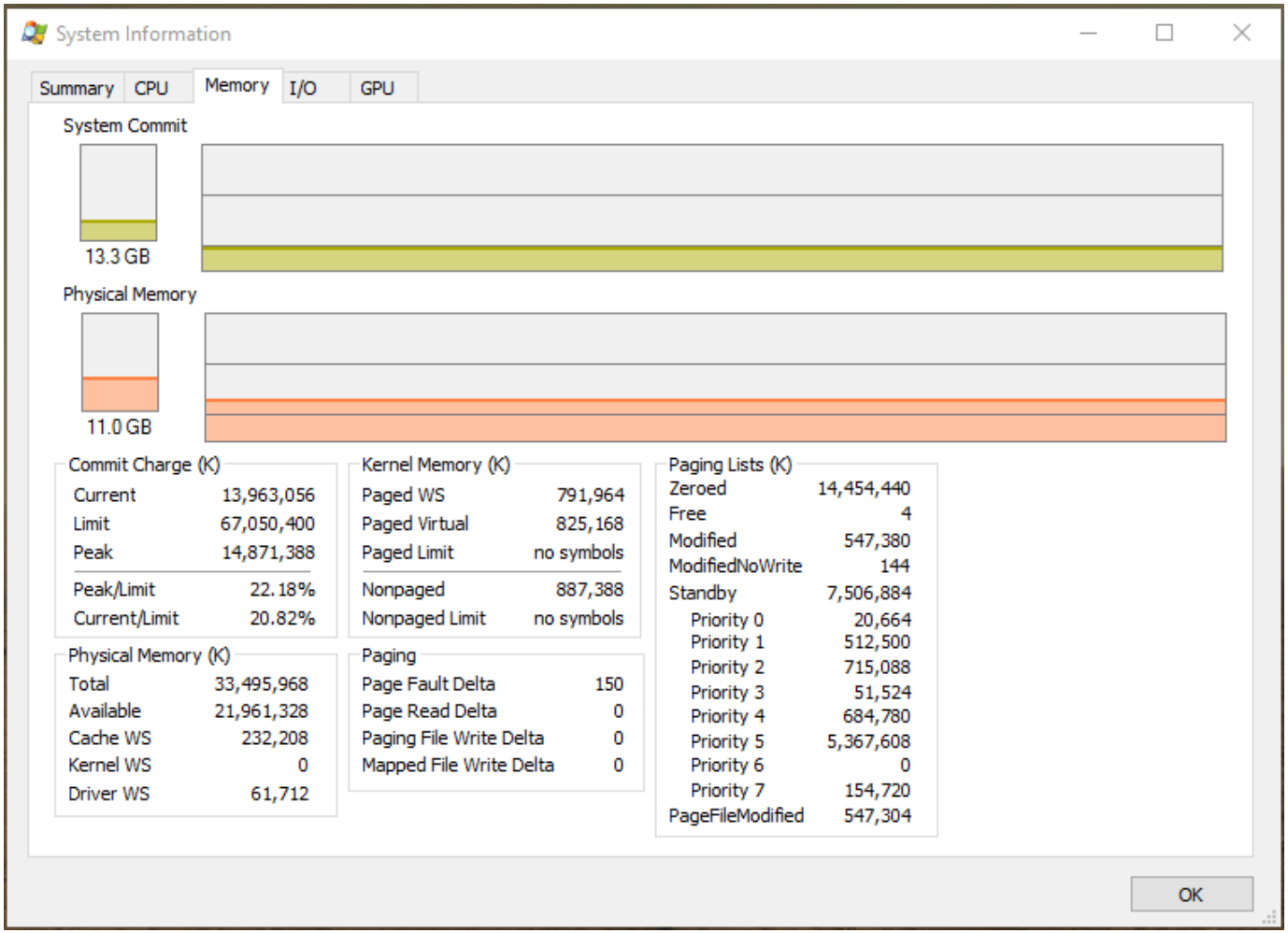
This is the security token for the user Spengler that started cmd.exe

PID 758868

Process Explorer

- In addition to processes, etc. Process Explorer can also be a good tool to provide you with information about the system
- The next slide displays information about Memory Usage on a Windows 10 Machine

Process Explorer Memory Usage Info



Service Security Concepts

Windows Services

- Since Windows Vista / Server 2008 services have been assigned a SID
  - They are now security principals
  - The SID is used to restrict the access a service has to securable objects
- When services are started by a process they all run under the security context of that process

Service Vulnerabilities

- Services can be vulnerable to buffer overflow attacks
- Services can be vulnerable to password guessing attacks in some versions of Windows
- Terminal services, remote desktop, FTP services:
  - All provide a logon point that can be attacked
  - Should check logs for invalid attempts
  - Administrator accounts can not be locked out

Service Vulnerabilities

- A number of services send data across network in plain text
  - Telnet, FTP, POP, SNMP
- Sniffers can read the information which could contain logon names & passwords

Service Vulnerabilities

- Services can have configuration errors
- Weak passwords on service
- Shared folders used by a service
- Some services send information to client during connection request
  - Can send more detail than intended
  - Error response to incorrect input can provide info with service and computer information

Service Vulnerabilities

- MS SQL uses Extended Stored Procedures which can have flaws
- A lack of proper input validation can allow an attacker to execute code in the security context in which SQL Server is running

Windows Services

- Many services listen on a TCP/UDP port for remote network access
- The port used can be monitored with netstat
  - The RPC port mapper listens on TCP port 135
  - SMB listens on TCP port 139
  - CIFS listens on TCP port 445
  - Ports 137 & 138 are used by the Computer Browser service to find NetBIOS computer names and NetBIOS service
    - No longer needed in Vista / S2008 Networks, but often still enabled for compatibility
    - Unless required, these services should be disabled

Windows Services

- The port a service is listening on can be shown with: netstat -nao

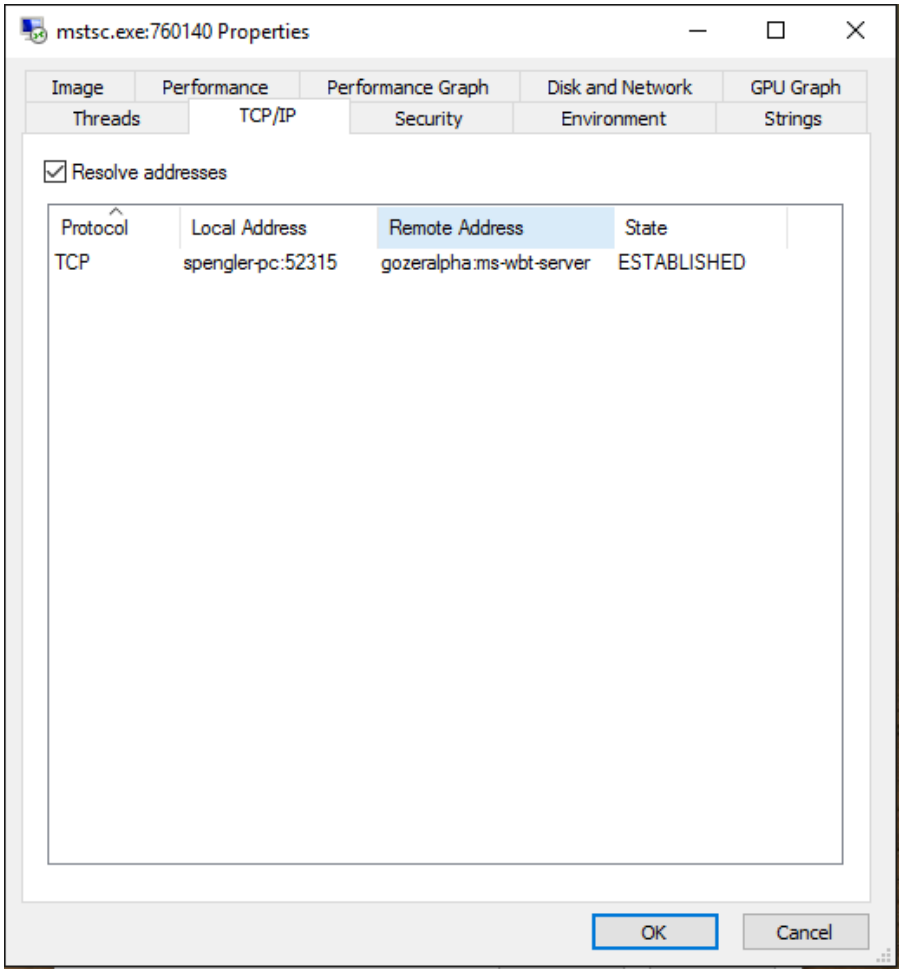
Command Prompt

```
C:\Users\Spengler>netstat -nao

Active Connections

  Proto  Local Address          Foreign Address        State           PID
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       908
  TCP    0.0.0.0:443            0.0.0.0:0              LISTENING       4176
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:902            0.0.0.0:0              LISTENING       2880
  TCP    0.0.0.0:912            0.0.0.0:0              LISTENING       2880
  TCP    0.0.0.0:1801           0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:2103           0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:2105           0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:2107           0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:3389           0.0.0.0:0              LISTENING       552
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:47984          0.0.0.0:0              LISTENING       3364
  TCP    0.0.0.0:47989          0.0.0.0:0              LISTENING       3364
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       732
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1180
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2440
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       2776
  TCP    0.0.0.0:49676          0.0.0.0:0              LISTENING       780
  TCP    0.0.0.0:49678          0.0.0.0:0              LISTENING       788
  TCP    127.0.0.1:5939         0.0.0.0:0              LISTENING       2948
  TCP    127.0.0.1:8307         0.0.0.0:0              LISTENING       4176
  TCP    127.0.0.1:9990         0.0.0.0:0              LISTENING       2804
  TCP    127.0.0.1:12025        0.0.0.0:0              LISTENING       1960
  TCP    127.0.0.1:12110        0.0.0.0:0              LISTENING       1960
  TCP    127.0.0.1:12119        0.0.0.0:0              LISTENING       1960
  TCP    127.0.0.1:12143        0.0.0.0:0              LISTENING       1960
  TCP    127.0.0.1:12465        0.0.0.0:0              LISTENING       1960
```

Windows Services



Process Explorer TCP/IP tab shows listening ports and established connections associated with a service

Netstat States

- When you are using netstat you will see the services in a variety of states
  - ESTABLISHED: Indicates that the server received the SYN signal from the client and the session is established
  - LISTENING: Indicates that the server is ready to accept a connection
  - TIME_WAIT: Indicates that the client recognizes the connection as still active but not currently being used

Windows Services Summary

- The registry contains information used by the Services Control Manager (SCM) when starting services
- The registry contains information on startup type and other dependent services
  - Registry Start values
    - Auto Start
    - Auto Start (Delayed)
    - Manual
    - Disabled

Windows Services Summary

- Services run in the security context of the logon account that starts the service
  - Local System
  - Local Service
  - Network Services
- Not all services are independent programs and require svchost to launch the service

Windows Services Summary

- Services can be viewed with tasklist.exe
- Services can be viewed, managed and configured with services.msc
- Sysinternals Process Explorer displays the most detailed information on a running service

Applications

- An Application is a program that users interact with on their desktops
  - Applications may have numerous processes running at the same time
  - Applications are executable files (.exe)
  - Applications may depend on specific services such as a print spooler service in order to print documents

Processes

- A process is an instance of a particular executable
  - Processes may interact with the user directly
  - Modern browsers will run numerous processes for every tab a user has open in their web browser application

Services

- A Service is a process which runs in the background and does not interact with the user directly
  - Services work across the system, but don't interact with users directly
  - A lot of Services will run under the Windows Service Host Process (svchost.exe) if they do not have their own executable

Session Isolation

Session Isolation

- Past Windows operating systems developed bad habits in users that have led to many security problems
- 95+ per cent of users log on as administrators
  - This meant that malware that is introduced to the computer during an attack would install with admin privileges
    - The owner of the process
- In UNIX/Linux system most users log on as the a limited user and only change to root or super user account when needed

Session Isolation

- All Windows operating systems prior to Vista started all built in services in session 0, the Local System context which has access to the kernel
- All applications started by the first logged on user also ran in session 0
- Many drivers and 3rd party programs installed and interacted with session 0 even if they did not require those privileges

Session Isolation

- The first logged on user ran in session 0
- Other users and applications would be started in the next session 1
- 86% of all Windows vulnerabilities reported were from users running malware on the desktop due to social engineering
  - If started by first logged on user, they were running in session 0
- Since Vista installed malware will now run in session 1 and be isolated from kernel

Session Isolation

- Session 0 now reserved for Windows kernel
  - Users and programs can not directly communicate with session 0
    - Prevents shatter attacks
    - Shatter attacks allowed an application in session 1 to access session 0 and gain all the privileges and rights of the Local System
      - Privilege escalation attack
- Applications that install services such as graphic drivers are no longer allowed to directly interact with system services

Session Isolation

- Users never interact directly with session 0
- Legacy drivers are no longer able to interact with system services
- Interactive Service Detection Service
  - User will be prompted to accept any new application trying to install on the system
  - Malware can not install automatically

Homework

- Reading

http://technet.microsoft.com/en-us/library/dd772681(v=WS.10).aspx

- Market Share of Mobile and Desktop Operating Systems

http://www.w3schools.com/browsers/browsers_mobile.asp

https://www.netmarketshare.com/operating-system-market-share.aspx

Lab 05 – Process Explorer & ABE

Lab 05 Details

- Exploring Process Explorer
- Access Control Lists
- Changing Permissions
- Registry Permissions