



Microsoft

UBNetDef, Spring 2024

Week 4

Austin and Lauren!

Learning Goals

- Windows Basics
- Powershell Basics
- Identify the elements of an Active Directory system
- Create and configure group policy objects
- Distinguish between security groups and organizational units

Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Understanding Windows for Cybersecurity

■ Windows NT

- New Technology File System (NTFS)
 - File permissions, encryption
- Designed for business, professional users
- Set the stage for Active Directory (AD)

■ Widely used in corporate environments, enterprise IT

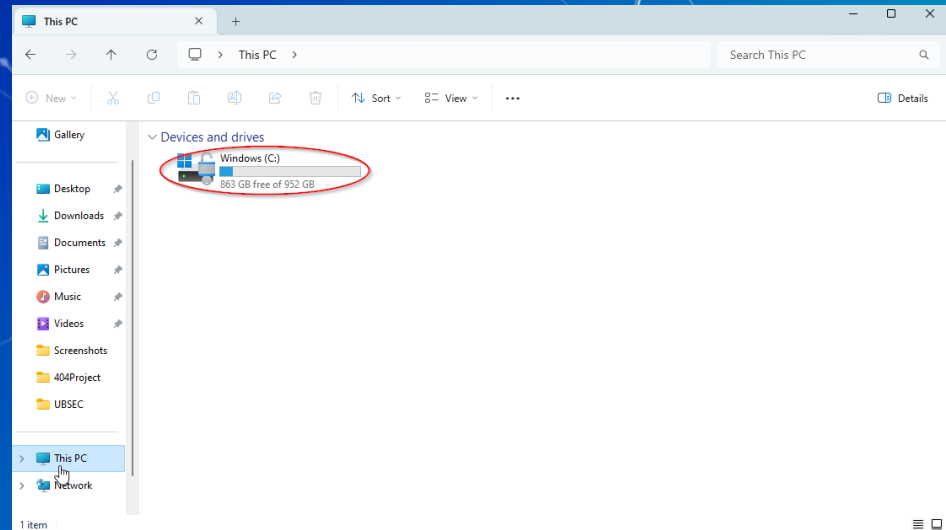
Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

File System Breakdown

■ C drive (C:) – main hard disk partition which contains:

- Operating system
- System files
- Applications



Major Directories to Know

■ System32 Folder

- Dynamic Link Library (DLL) files – shared library files
- EXE files – to launch applications/utilities
- Drivers – files associated with hardware devices

■ Program Files

- Designed to store files necessary to run applications

■ Users Folder

- Local file information (desktop config, application data)

Network File Paths Overview

- Universal Naming Convention (UNC)
- A standard path identify servers, devices, network resources for Microsoft Windows Operating Systems
- Example path:
 - `\\SERVERNAME\DIRECTORY\FILENAME`

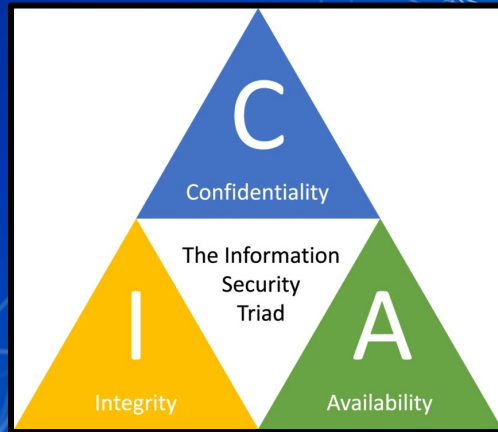
Identity and Access Management (IAM)

■ Authentication vs. Authorization

- Verifying users' identity (authentication)
- Granting them access to data based on their identity (authorization)

■ IAM and the Confidentiality, Integrity, and Availability (CIA) triad

- Which of the 3 pillars of the CIA triad does IAM support?



IAM

- Part of the Zero Trust security strategy
 - Never trust that a user is who they say they are
 - Always verify the user's identity and level of access
- Multi-Factor Authentication (MFA) components:
 - Something the user knows
 - Password
 - Something the user has
 - Duo, Secondary device
 - Something the user is
 - Biometrics (Fingerprint)
 - Less commonly used
- Case in point: UBLearns



Local Permissions

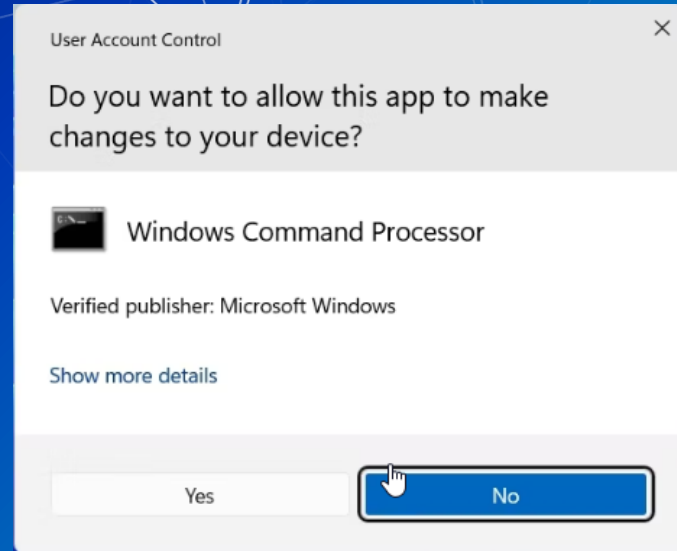
Different local permission levels

- System
 - Highest level of permissions – controlled by OS for system functionality
 - Service account
- Administrator
 - High level of control over computer, should only be used when necessary
- Standard User
 - Used for everyday computing

These accounts only exist on each individual computer

Can be shown through different sign-in method:

- .\AccountName → local sign-in
- Domain\AccountName → domain sign-in



Graphical User Interfaces: GUI

■ You don't have to look far for examples...

- Spotify web app GUI (In green)
- Google Chrome browser GUI (In blue)
- Windows 11 OS GUI (In yellow)



Windows Client

■ The main way that personal users interact and use Windows

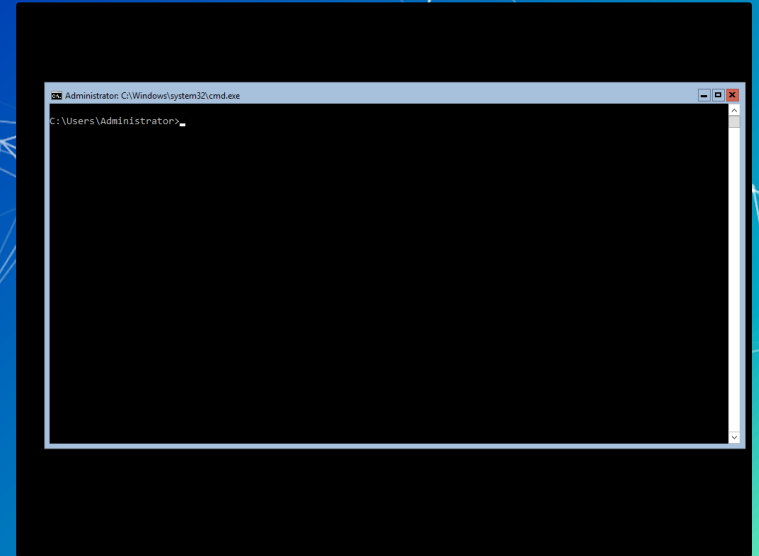
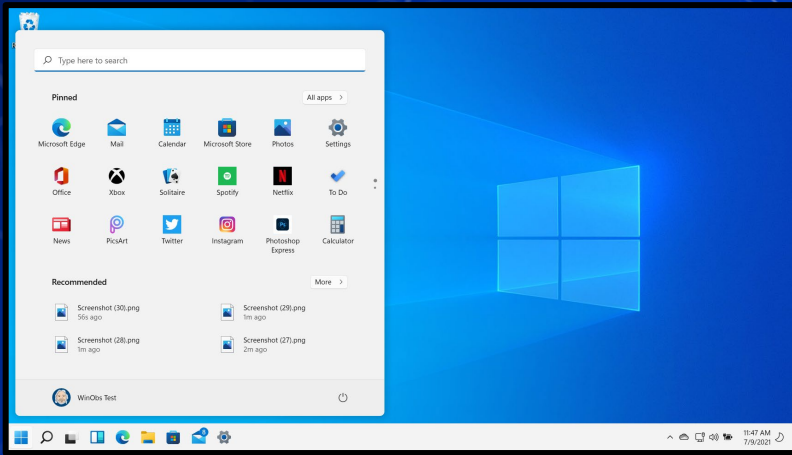
■ Notable features:

- Graphical user interface (GUI) – buttons, icons, menus
- File explorer - managing files, folders, organizing data
- Windows Defender – built-in antivirus
- Task Manager – monitor and manage running processes



Windows Server vs. Client

- Windows Client is the tried and true Windows OS that all of you are familiar with
- Windows Server is a OS designed to offer network based services on the Windows Platform

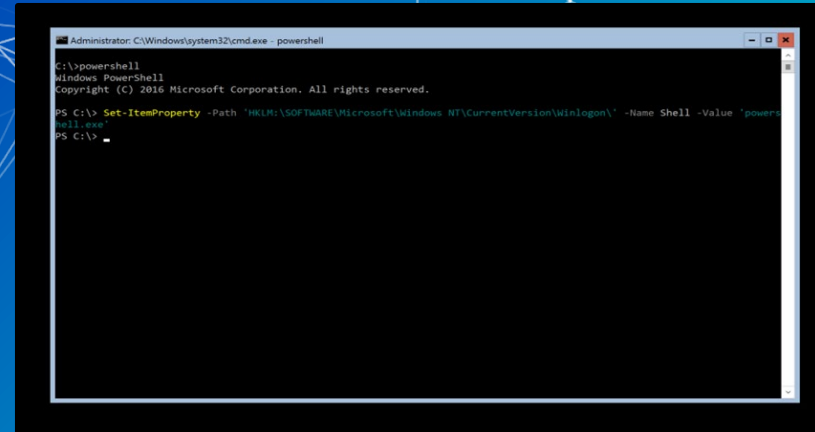
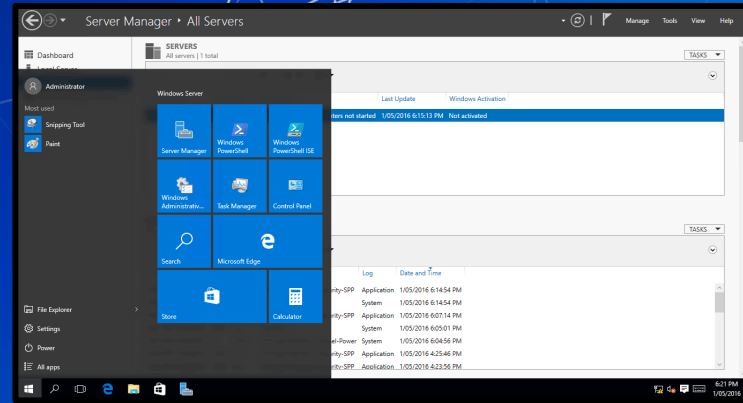


Windows Server Services

- Windows Server can provide a lot of services
 - Web Server
 - Internet Information Service (IIS)
 - File Share Services
 - Server Message Block (SMB)
 - Network file share / shared drive
 - Network Management Services
 - Domain Name System (DNS)
 - Dynamic Host Configuration Protocol (DHCP)
 - Active Directory
 - Identity and Access Management

Windows Server(s)

- Windows Server comes in 2 flavors
 - Server Desktop - Looks a lot like a Windows client
 - Server Core - Just a command line prompt
- Core and Desktop have the same functionality, but core is command based only.
 - Designed to be managed on a "headless system" or remotely



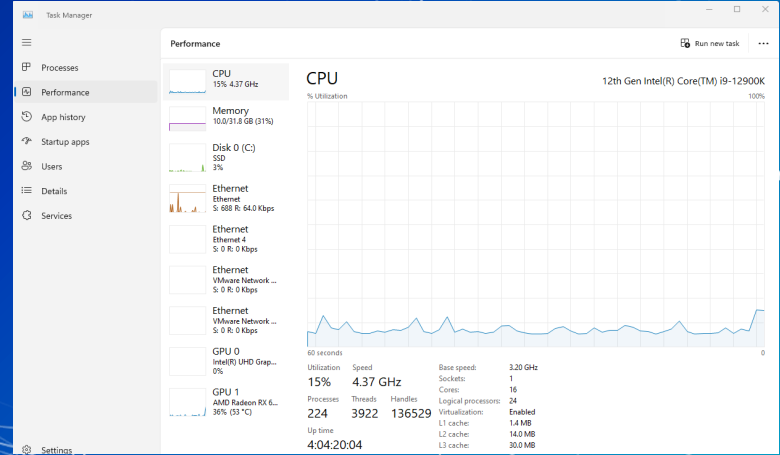
Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Process Management Overview

Task Manager

- Built-in Windows service that can provide information on running processes, CPU/memory usage, and allows users to start or stop processes



Event Viewer

- Freeware that logs events and errors on a Windows system
- Provides valuable + detailed information on how issues occur
- Can be leveraged for security auditing by system administrators
 - Custom views
 - Log aggregation through SIEMs

The screenshot shows the Windows Event Viewer application. The left sidebar displays a tree view of event logs, with 'Administrative Events' selected. The main pane shows a list of events with columns for Level, Date and Time, Source, Event ID, and Task Category. The events listed include three errors from Security-SPP and two warnings from DNS Client and csc_vpnagent.

Level	Date and Time	Source	Event ID	Task Category
Error	2/4/2024 8:58:24 PM	Security-SPP	8198	None
Error	2/4/2024 8:58:24 PM	Security-SPP	8198	None
Error	2/4/2024 8:58:01 PM	Security-SPP	8198	None
Warning	2/4/2024 8:57:23 PM	DNS Client Ev...	1014	(1014)
Warning	2/4/2024 8:57:16 PM	csc_vpnagent	2	Engineering D...
Warning	2/4/2024 8:57:16 PM	csc_vpnagent	2	Engineering D...

Services and Processes

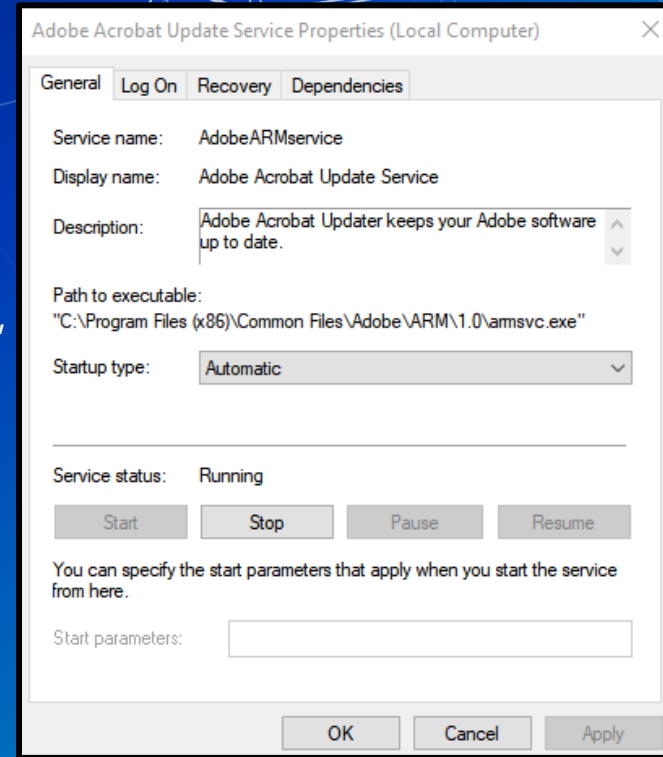
■ Services and Processes

- Common processes are instances of a program
 - notepad.exe, mspaint.exe, Rocket League
 - Often initiated and terminated by user action
- Active services are persistent processes
 - Xbox Live Game Service, Windows Update Manager
 - Often run in the background
- Services are known to the OS whether they are running or not
 - Typically manage things that make the system work

```
PS C:\WINDOWS\system32> get-service
Status Name DisplayName
-----
Stopped AarSvc_517345d Agent Activation Runtime_517345d
Running AdobeARMService Adobe Acrobat Update Service
Stopped AJRouter AllJoyn Router Service
Stopped ALG Application Layer Gateway Service
Stopped AppIDSvc Application Identity
Running Appinfo Application Information
Stopped AppMgmt Application Management
Stopped AppReadiness App Readiness
Stopped AppVClient Microsoft App-V Client
Stopped AppXSvc AppX Deployment Service (AppXSVC)
Stopped aspnet_state ASP.NET State Service
Stopped AssignedAccessM... AssignedAccessManager Service
Running AtherosSvc AtherosSvc
Running AudioEndpointBu... Windows Audio Endpoint Builder
Running Audiosrv Windows Audio
Stopped autotimesvc Cellular Time
Stopped AxInstSV ActiveX Installer (AxInstSV)
Stopped BcastDVRUserSer... GameDVR and Broadcast User Service
Stopped BcastDVRUserSer... Bitstream Driver Encryption Service
```

Services

- Services in Windows have a trait called a “start-up type”
 - Automatic
 - Starts automatically (on system boot)
 - Automatic Delayed Start
 - Starts after a set amount of time
 - Manual
 - Needs to be manually started
 - Disabled
 - Service won't start unless re-enabled



```
PS C:\WINDOWS\system32> Restart-Service Spooler -v
VERBOSE: Performing the operation "Restart-Service" on target "Print Spooler (Spooler)".
```

Services Continued

- Services and processes run at the permissions of the user that is signed in
- Can significantly change what the service is capable
- When compromised, can greatly reduce attack surface

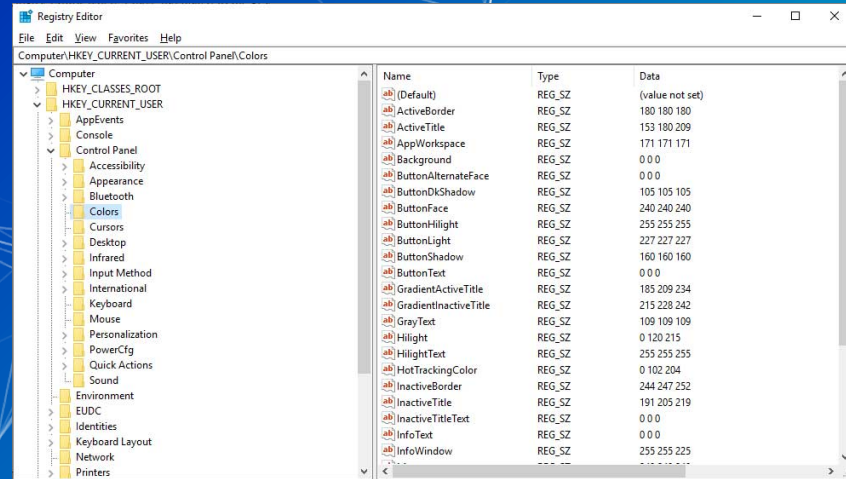
Windows Registry Overview

Database that contains the state of the device you are currently on

- Configuration settings:
 - Operating System settings
 - Application settings
 - User preferences

Windows Registry contains vital configurations for the OS and applications

- Making incorrect or careless changes can cause applications to break or render the system unbootable!



How is Windows Registry Organized?

■ Registry contains keys and values

- **Registry Key** – each folder-like structure in Windows Registry to help organize the registry values
- **Registry Values** – the information that applications can access and use

■ There are five main branches of the registry:

- HKEY_CLASSES_ROOT – default file associations, wide range of file types are associated with the software that knows how to process them
- HKEY_CURRENT_USER – specific configurations for individual user
- HKEY_LOCAL_MACHINE – passwords, boot files, security settings
- HKEY_USERS – for when there are multiple users logged onto same device
- HKEY_CURRENT_CONFIG – configuration data for current hardware profile

Security Account Manager (SAM)

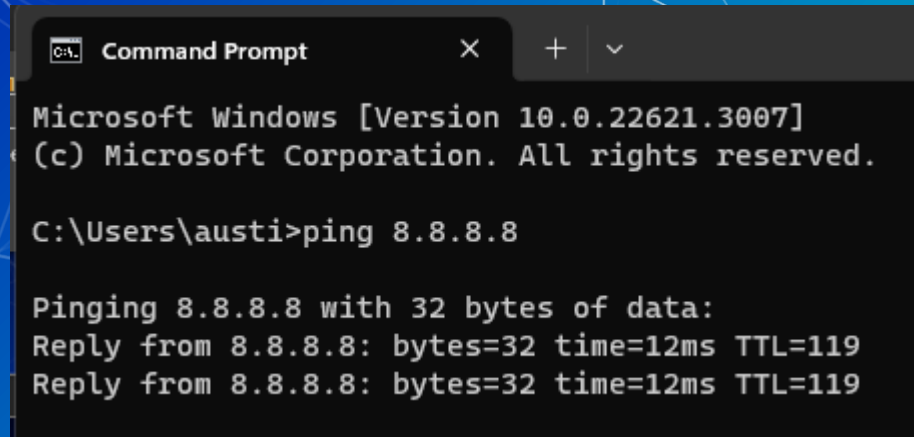
- The Security Account Manager (SAM) is a Windows OS database that stores user accounts and security information for the local groups
 - The SAM file contents can look like this:

```
Administrator:500:NO PASSWORD*****:31D6CFE0D16AE931B73C59D7E0C089C0:::  
Guest:501:NO PASSWORD*****:NO PASSWORD*****:::  
raj:1000:NO PASSWORD*****:7CE21F17C0AEE7FB9CEBA532D0546AD6:::  
pentest:1001:NO PASSWORD*****:7CE21F17C0AEE7FB9CEBA532D0546AD6:::  
:
```

- HKEY_LOCAL_MACHINE\SAM
 - User accounts, administrator accounts, hashed passwords
- Since this is a common directory for bad actors to target...
 - Audit access
 - Access controls
 - Validate accounts on system

Command Lines

- Command Prompt (CMD)
 - Based on MS-DOS
 - No scripting capabilities
 - Legacy scripts/tools
 - Limited scope



```
Command Prompt
Microsoft Windows [Version 10.0.22621.3007]
(c) Microsoft Corporation. All rights reserved.

C:\Users\ austi>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=12ms TTL=119
Reply from 8.8.8.8: bytes=32 time=12ms TTL=119
```

Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

PowerShell Overview

■ PowerShell

- Newer CLI designed for server administration
- Access to many more utilities compared to command prompt
- Many commands are in the Verb-Noun format
 - Get-WebContent, ForEach-Object etc.



Essential PowerShell Commands

- **get-help** → provides information about commands, functions... with helpful documentation!
- **get-process** → give us information about running processes and statistics about them
- **get-member** → shows us all the properties and methods associated with an object
 - Properties – characteristics of an object that describe it (or the state that it is in)
 - Method – an action that you can make on an object

```
Administrator: Windows PowerShell
PS C:\WINDOWS\system32> get-help get-process

NAME
    Get-Process

SYNOPSIS
    Gets the processes that are running on the local computer or a remote computer.

SYNTAX
    Get-Process [[-Name] <System.String[]>] [-ComputerName <System.String[]>] [-FileVersionInfo] [-Module]
    [<<CommonParameters>>]

    Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -Id <System.Int32[]> [-Module]
    [<<CommonParameters>>]

    Get-Process [-ComputerName <System.String[]>] [-FileVersionInfo] -InputObject <System.Diagnostics.Process[]>
    [-Module] [<<CommonParameters>>]

    Get-Process -Id <System.Int32[]> -IncludeUserName [<<CommonParameters>>]

    Get-Process [[-Name] <System.String[]>] -IncludeUserName [<<CommonParameters>>]

    Get-Process -IncludeUserName -InputObject <System.Diagnostics.Process[]> [<<CommonParameters>>]
```

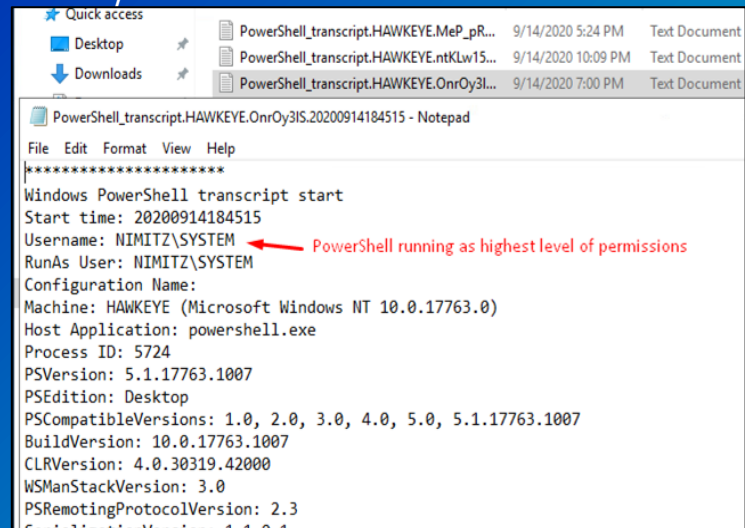
PowerShell Execution Policies

- Controls the conditions under which PowerShell loads configuration files and runs scripts.
 - Helps prevent execution of malicious scripts
 - Can help to mitigate your risk

```
PS /home/sysadmin> Set-ExecutionPolicy RemoteSigned
```

PowerShell Transcription

- Transcription is a method of logging PowerShell activity
- Why would we do this?
- Not enabled by default
 - Needs to be enabled by group policy



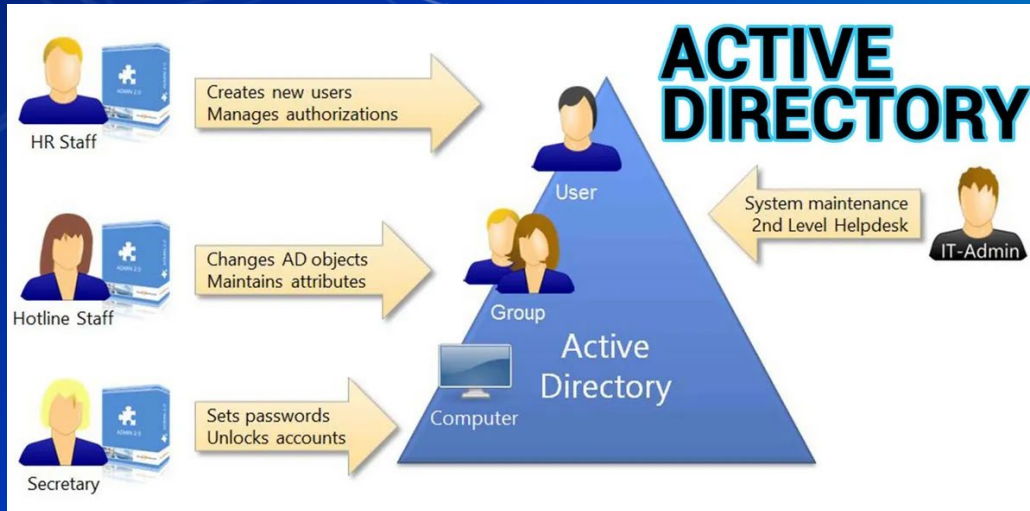
```
PS>CommandInvocation(Out-String): "Out-String"
>> ParameterBinding(Out-String): name="InputObject"; value="Attempted to perform an unauthorized operation."
New-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1
+ New-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows Defender\Exc ... Windows protects Defender's registry keys
+ ~~~~~
+ CategoryInfo          : PermissionDenied: (HKEY_LOCAL_MACH...ions\Extensions:String) [New-ItemProperty],
UnauthorizedAccessExcep
+ FullyQualifiedErrorId : System.UnauthorizedAccessException,Microsoft.PowerShell.Commands.NewItemPropertyCommand
New-ItemProperty : Attempted to perform an unauthorized operation.
At line:1 char:1
```

Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Active Directory (AD)

- AD is a directory service for Windows domain networks
 - Controls access to each object based on user authorization
- Objects are users, computers, files, anything networked

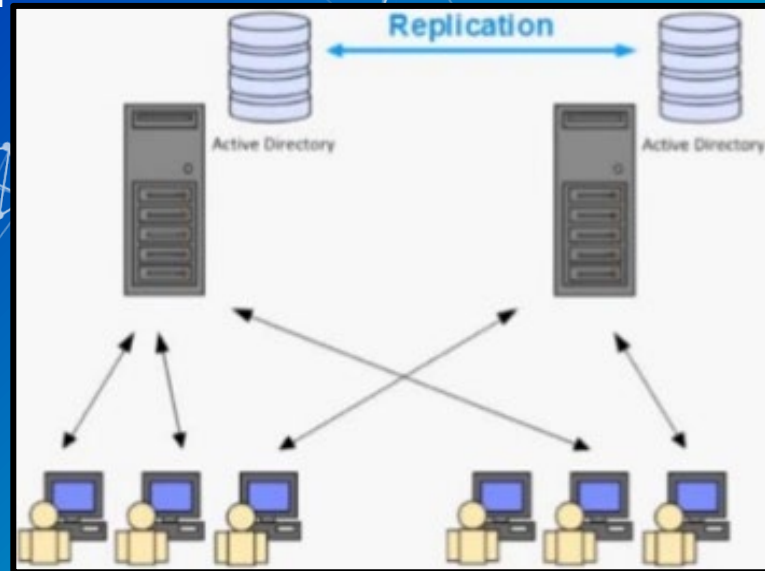


Components of Active Directory

- Database of objects in a network (Domain)
 - Users
 - Computers
 - Printers
 - Security Groups
 - More
- The database is hosted on a Windows Server (called the Domain Controller)
 - Domain controllers handle IAM
 - The Domain Controller serves Active Directory to Windows domain network.

Domain Controllers (DCs)

- Can have multiple Domain Controllers to have redundancy or server load balancing
- Handles authentication requests for the domain
 - May require running DNS
 - Will require Network Time Protocol (NTP)
 - And more!



Components of Active Directory Continued

- Large component of Active Directory is the ability to manage authentication and granting permissions based off policies defined in directory
- Lightweight Directory Access Protocol (LDAP)
 - Primary protocol used to query AD
 - Supports common functions including search, add, delete, modify...
 - Can extract and edit data with other compatible directory providers

Components of Active Directory Continued

■ Kerberos Protocol

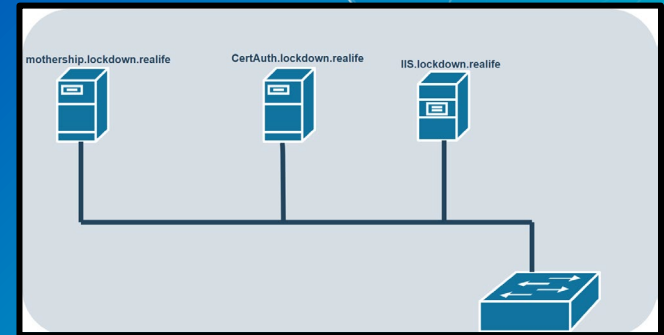
- Establishes mutual authentication
- Shared key cryptography through key distribution center (KDC)
- Used for single sign-on (SSO)

■ When a user logs into an Active Directory domain, both LDAP and Kerberos will be leveraged to...

- Authenticate the user
- Search for the user account and retrieve information for group membership

AD and DNS

- AD uses DNS so that clients can locate domain controllers and communicate with each other.
 - IP's can change.
 - AD computer names are unique per domain.
- Domain controllers (that run AD) also can serve as the local AD DNS & DHCP server.
 - DHCP automatically assigns IPs.



Break

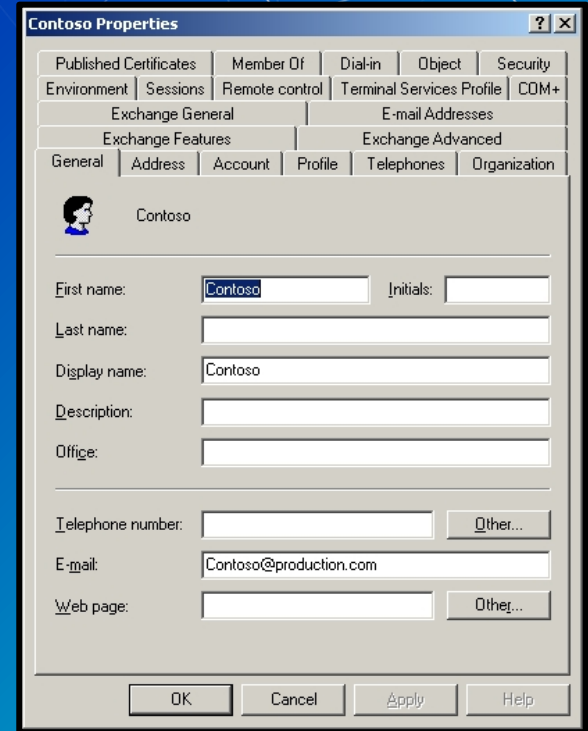
10 mins

Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Active Directory - User Objects

- What people authenticate against when they sign on
- Stores information on user
 - **Username**
 - Display name
 - Email
 - Phone number
 - Address
 - Location in organization
 - **Password (hashed)**

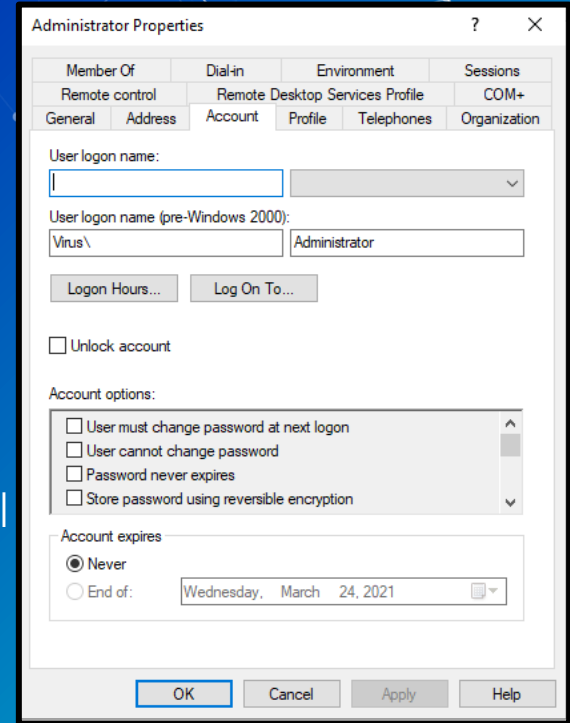


The screenshot shows the 'Contoso Properties' dialog box with the following fields and values:

Field	Value
First name	Contoso
Last name	
Display name	Contoso
Description	
Office	
Telephone number	
E-mail	Contoso@production.com
Web page	

Active Directory - User Objects

- AD cybersecurity features
 - File and folder access
 - VPN access
 - Password management
 - Active account
 - Access control
 - Ability to control total network access
- Map drives to computer (Network drives)
 - UB uses this as well. Log into a ub computer. You'll see an S: drive.
- Folder redirection



Active Directory - Security Concerns

■ We need a new object for each user.

- Too many to safely manage
 - UB has about 50,000 users on its main domain

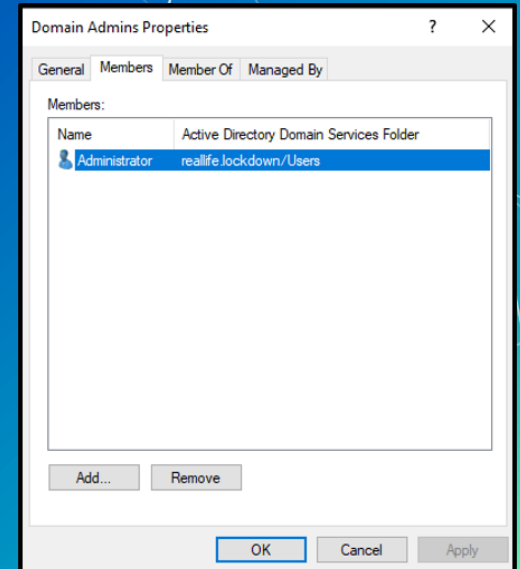
■ Security issues:

- What happens when we add a new filestore in which we need to grant permissions to only the School of Management?
- What happens when someone leaves?
- What if you discover the need for a host-based firewall?

Active Directory - Groups

- Groups are a special “folder”
 - Objects can be put in groups
 - Helps keep organized
 - Can assign settings to groups
 - Acts similarly to users configuration
 - Manage every user at once that in the group

Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Domain Ad...	Security Group...	Designated administrato...
Domain Co...	Security Group...	All workstations and ser...
Domain Con...	Security Group...	All domain controllers i...
Domain Gue...	Security Group...	All domain guests
Domain Users	Security Group...	All domain users
Enterprise A...	Security Group...	Designated administrato...
Enterprise K...	Security Group...	Members of this group ...



North America Division

```
graph TD; NA[North America Division] --- M[Marketing]; NA --- S[Sales]; NA --- Serv[Service];
```



Marketing

Sales

Service

Name: Jon Pestinger
Email: Jon@company.com
Department: Marketing
Phone: 123
Title: Technical Writer

Active Directory - Nesting

- Can put groups in groups
- Layout organization before building AD
 - Build domain based on network layout and permissions
 - Doesn't always look like your organization's hierarchy chart
 - Should the CEO have admin access? Network Admin?
Why?
- Leads to group inheritance



Active Directory - Inheritance

- Subgroups (children objects) inherit permissions from group above (parent object)
- Users in a group, within another group, will get settings placed on top level group

Parent Group

North America Division

Child Groups

User Objects

Name: Jon Pestinger
Email: Jon@company.com
Department: Marketing
Phone: 123
Title: Technical Writer



Marketing

Sales

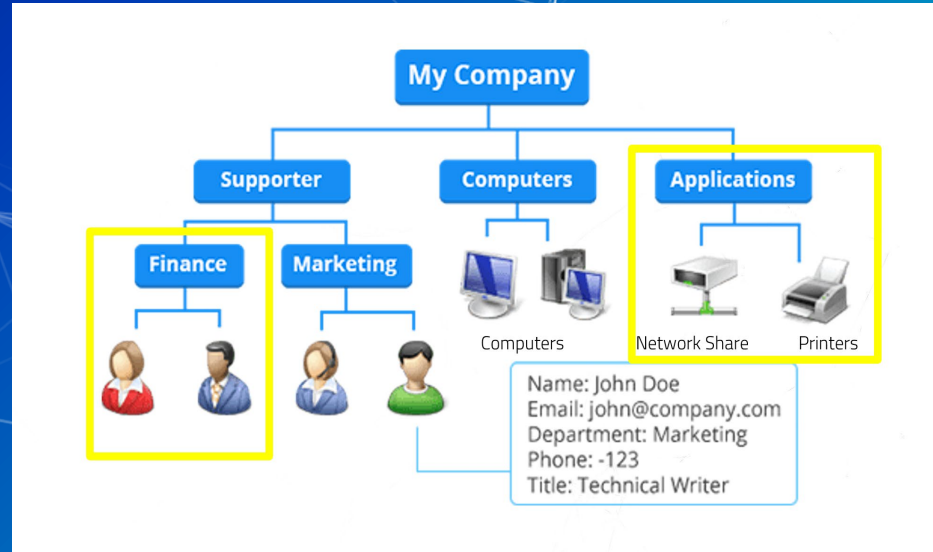
Service

Only marketing can use Canva!

Only Sales gets Excel!

Active Directory - Computers and Devices

- Like users, devices can also be managed by AD
 - E.g., computers, printers, other servers
- Control who gets to log-on
- AD allows for cross-device permissions
 - Have certain computers access certain printers



Active Directory - Organizational Units (OU)

- Organizational Units (OU) are used to organize Active Directory so it's easier to manage.
- **Differ from Security Groups**
 - Security Groups are going to be IAM based!
 - Access control, membership
 - OUs are for...
 - Administrative control
 - Hierarchy (for organizational control)
 - Group policy management
- **You can't be in more than one OU at the same level**
- OUs cannot be security-grouped together. They are not objects. They are not groups.

North America Division

Marketing



Sales



Service



Marketing and Sales OUs
have separate policies and
administrative controls

Confused? TL;DR so far:

- Domains control networks
- Organizational Units (OU's) are collections of things (Objects)
- Groups also contain objects
- Groups can go in groups
- Children objects inherit permissions from parent objects
- Everything is inherited top to bottom

QUESTIONS?

Break

Please return in 10 mins

Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Group Policy Objects in Active Directory

- Group policies are settings that can be enforced on an entire domain
- Example: We want all desktops to have a certain background.
- Enforced in a hierarchical top down format from the domain level to the object level
 - If a higher policy exists, the higher policy is enforced

Group Policy Examples

- Can be used to force any setting on objects/groups/OUs in AD
- Pretty much anything you can think of
- Security
 - Password policy
 - Powershell transcription
 - Set firewall policy
- Functional
 - Mapped network drives
 - Sleep settings
 - Remote desktop access
 - Windows Update timing
- Appearance
 - Change background
 - Change cursor

Group Policy Key Terms

■ Enforced

- Can not be overwritten by other policy

■ Linked

- Link policy to specific OU

■ Filtering

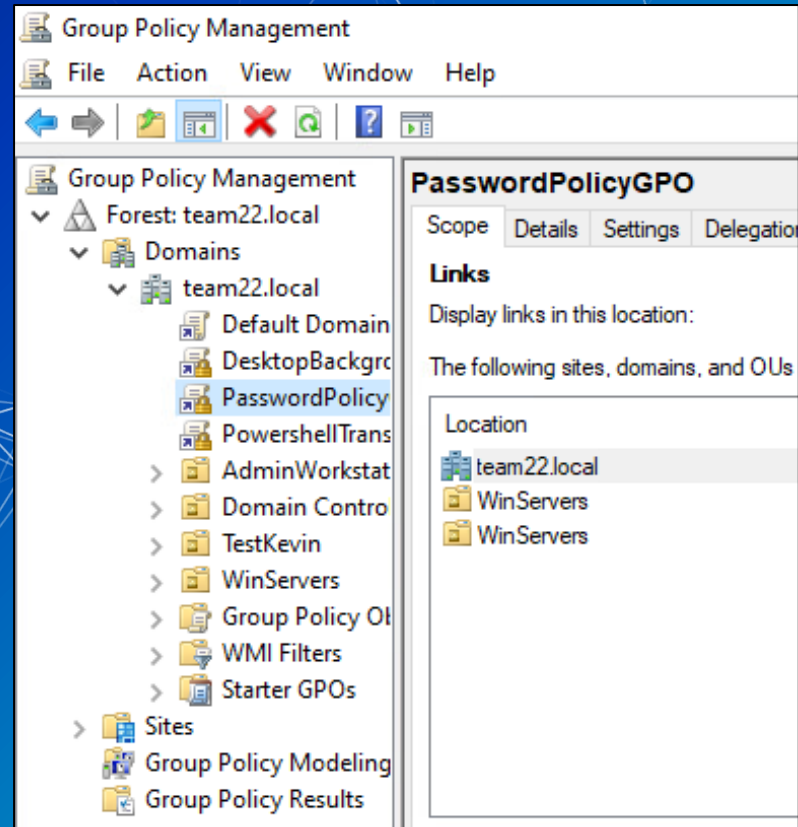
- Can choose to apply Group policy to objects that meet criteria
 - < 8GB RAM

■ Group Policy Object (GPO)

- A set of rules that can be applied to any object

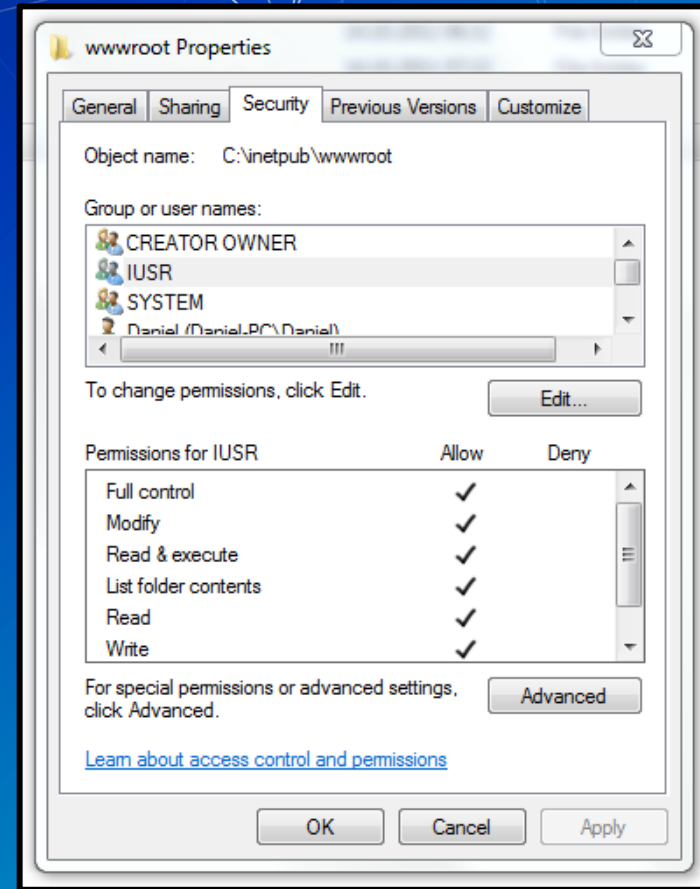
Multiple Group Policies

- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group
- **Group policies can be applied to any domain object**
 - Users, Computers, Groups, OUs



File Permissions

- Can be set on individual files, folders, network shares, hard drives
- Can specify who has read, write, or modify permissions
- File permissions can be inherited from containing folder
- Ex) Can share whole folder instead of every file
- Can be set using group policy and Active Directory



Agenda

1. Windows History
2. Windows Basics
3. Process Management
4. PowerShell
5. Active Directory
6. Components of Active Directory
7. Group Policy
8. HW

Homework

Summary and Wrap-up

Today's achievements:

- We identified the difference between Server Desktop and Server Core
- We learned about Windows basics
- We learned about AD and how it works
- We identified different group policies within AD