Step-by-Step Project Lab: Configuring Examples of Security Control Types - CompTIA Security+

This guide will walk you through the process of understanding and configuring the various types of security controls: **preventive, detective, directive, and corrective.** This project will guide you through configuring and demonstrating examples of the four types of security controls on a **Windows Virtual Machine (VM)**. You'll use built-in tools like PowerShell and the Windows GUI to implement and test these controls.

Step 1: Lab Setup

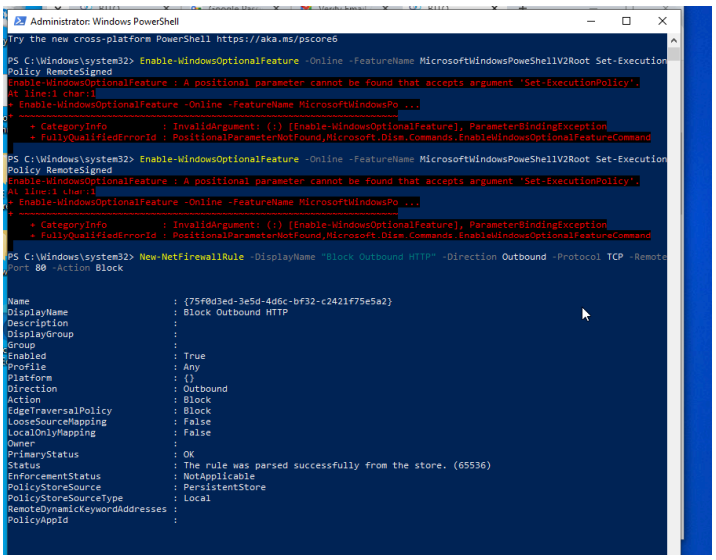
1. **Install a Windows Virtual Machine:**
    - Download and install a Windows VM (e.g., Windows 10/11 or Windows Server) using software like VirtualBox, VMware Workstation, or Hyper-V.
    - Allocate at least 4 GB of RAM and 40 GB of disk space.
2. **Enable PowerShell and Required Features:**
    - Launch PowerShell as an Administrator.
    - Run the following commands to ensure PowerShell and necessary features are enabled:

      -Enable-WindowsOptionalFeature -Online -FeatureName MicrosoftWindowsPowerShellV2Root Set-ExecutionPolicy RemoteSigne

Step 2: Configure Preventive Controls

Objective: Prevent security incidents by limiting or controlling access to systems or data.

1. **Step 2.1: Configure a Firewall Rule (Using Windows Defender Firewall)**
    - Open PowerShell as Administrator and run:

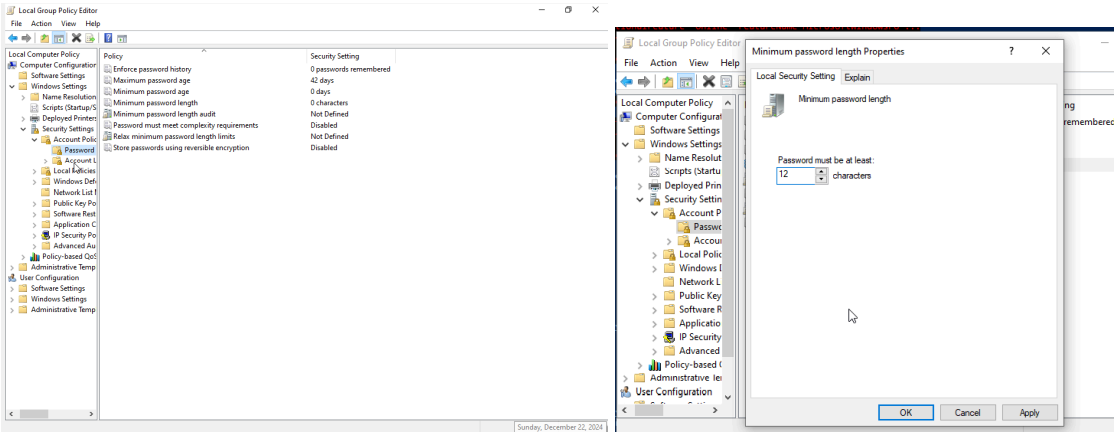


-New-NetFirewallRule -DisplayName "Block Outbound HTTP" -Direction Outbound -Protocol TCP -RemotePort 80 -Action Block

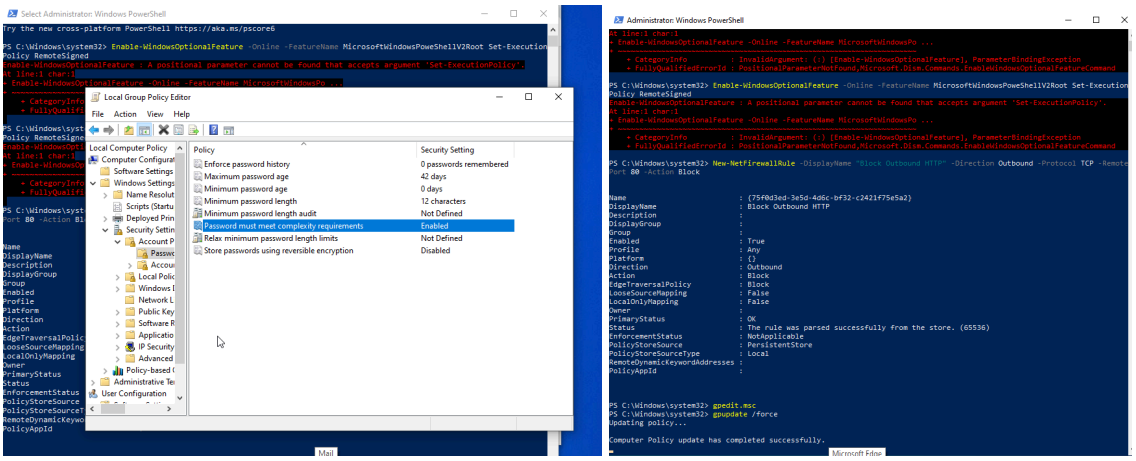
- This blocks outbound HTTP traffic on port 80

2 **Step 2.2: Enforce Password Policies**

- Open the Local Group Policy Editor:
  - Run `gpedit.msc`.
  - Navigate to **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**.

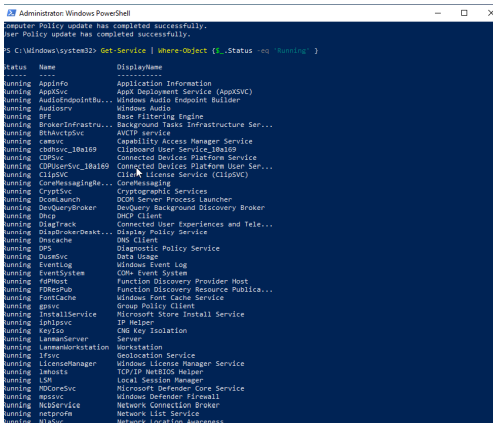


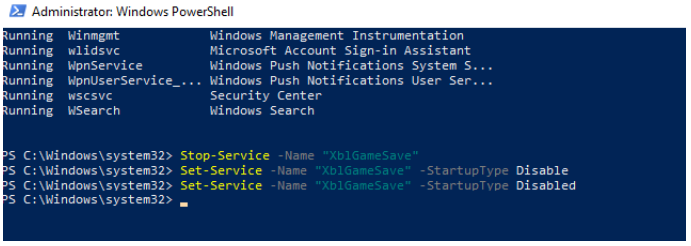
- Configure the following:
  - **Minimum password length**: Set to 12 characters.
  - **Password must meet complexity requirements**: Enable.
- Apply the policy by running: **gpupdate /force**



Step 2.3: Disable Unused Services

- List all services: **Get-Service | Where-Object { $_.Status -eq 'Running' }**
- Disable unnecessary services (e.g., Xbox Live Game Save service): **Stop-Service -Name "XblGameSave" Set-Service -Name "XblGameSave" -StartupType Disabled**



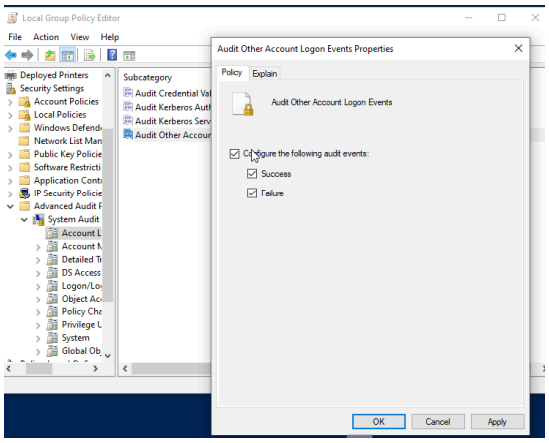


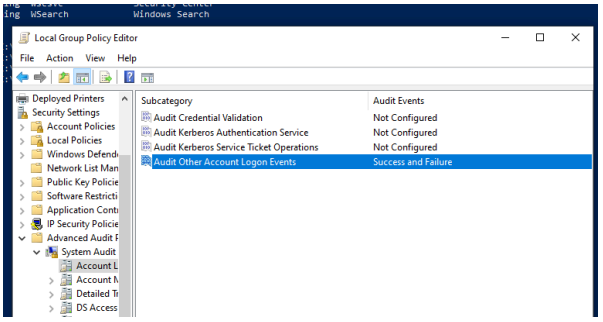
Make sure the spelling is Good, don't rush like me…

Step 3: Configure Detective Controls

Objective: Identify potential security incidents or unauthorized activities.

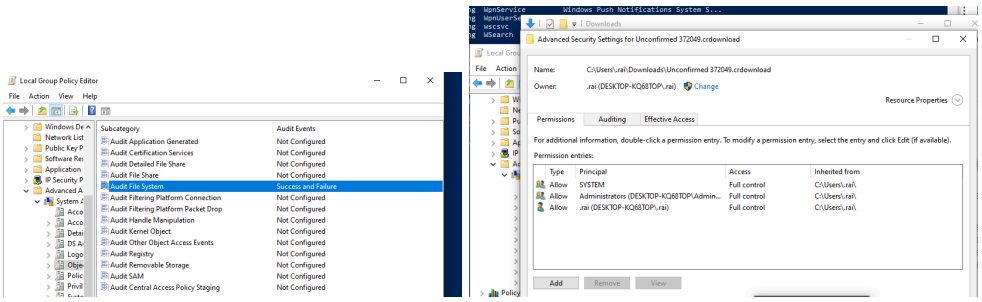
1. **Step 3.1: Enable Audit Logging**
   - Open the Local Group Policy Editor:
     - **Navigate to Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies.**

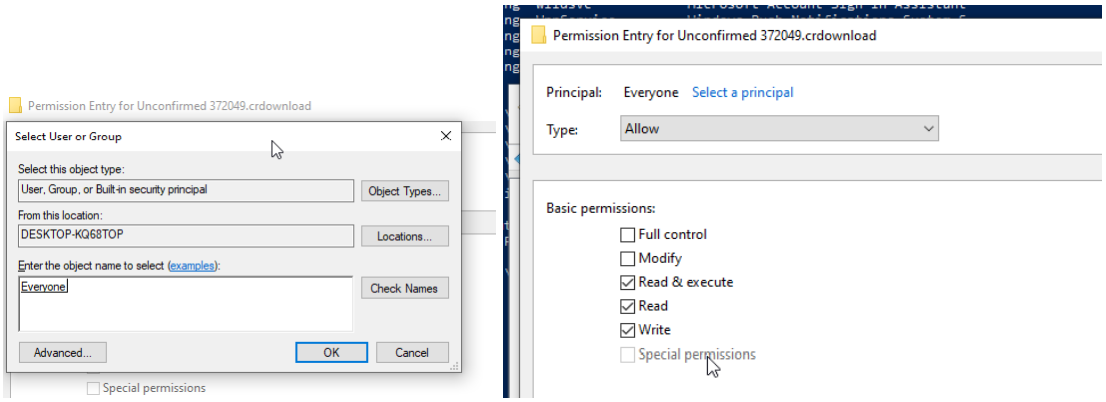




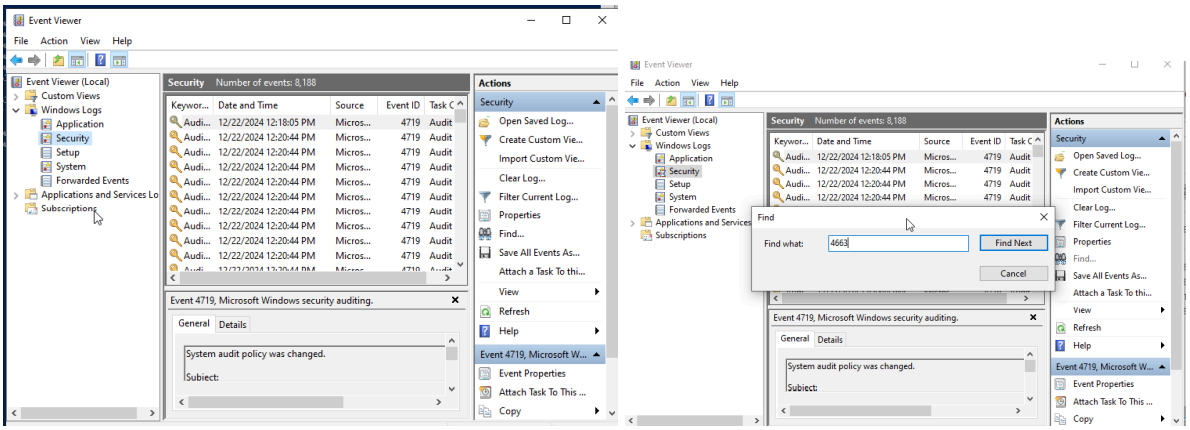
   - Enable the following:
     - **Audit logon events (Success and Failure).**
     - **Audit object access (Failure).**
   - Apply the policy by running: **gpupdate /force**
2. **Step 3.2: Monitor File Access Using File System Auditing**

- **Enable auditing for a specific folder:**
  - **Right-click a folder (e.g., `C:\SensitiveData`) > Properties > Security > Advanced.**
  - **Go to the Auditing tab and add a new entry for "Everyone" with access type "Read".**





- **View logs in the Event Viewer under Security Logs.**



3. **Step 3.3: Configure Real-Time Monitoring**

- Use PowerShell to monitor failed logon attempts: **Get-EventLog -LogName Security -InstanceId 4625 | Select-Object TimeGenerated, Message**

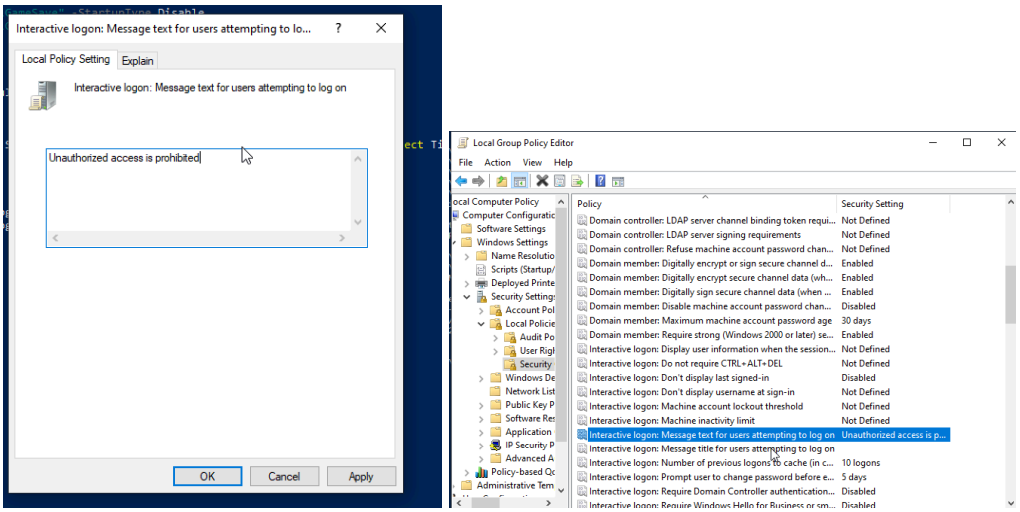
```
PS C:\Windows\system32> eventvwr.msc
PS C:\Windows\system32> Get-EventLog -LogName Security | Where-Object { $_.EventID -eq 4625 } | Select-Object TimeGenera
ted, Message

TimeGenerated          Message
-------------          -------
12/22/2024 11:38:08 AM An account failed to log on....
11/3/2024 12:57:43 PM  An account failed to log on....


PS C:\Windows\system32>
```

Soo cool right

Step 4: Configure Directive Controls

Objective: Guide users or systems on appropriate actions and enforce organizational policies.

1. **Step 4.1: Deploy a Security Warning via Group Policy**
    - Open Local Group Policy Editor:
        - **Navigate to Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options.**
        - Configure Interactive logon: **Message text for users attempting to log on with a security warning (e.g., "Unauthorized access is prohibited.").**



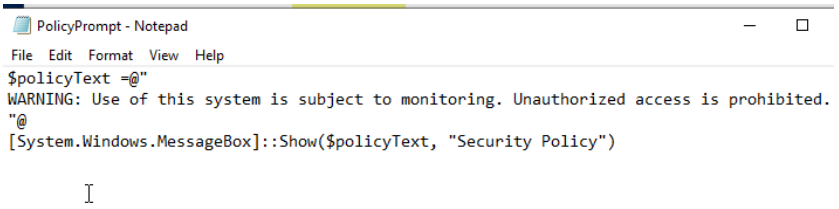
    - Test by logging off and back on.
2. **Step 4.2: Enforce Acceptable Use Policy with a Script**
    - Create a PowerShell script (`PolicyPrompt.ps1`):

    $policyText = @"

    WARNING: Use of this system is subject to monitoring. Unauthorized access is prohibited.

    "@

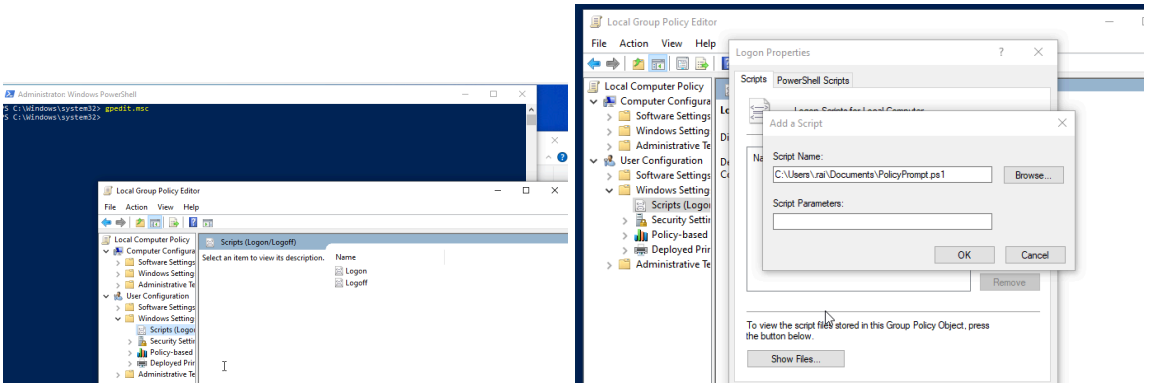
    [System.Windows.MessageBox]::Show($policyText, "Security Policy")



Configure it to run on startup:

- Run `gpedit.msc` and navigate to **User Configuration > Windows Settings > Scripts (Logon/Logoff).**

- Add the script to the Logon section.



Step 5: Configure Corrective Controls

Objective: Respond to and mitigate the effects of a security incident.

1. **Step 5.1: Create a Backup and Recovery Script**
   - Use PowerShell to back up critical data: ***$source = "C:\SensitiveData"$destination = "D:\Backups"Copy-Item -Path $source -Destination $destination -Recurse -Force***

```
PS C:\Windows\system32> $source = "C:\SensitiviData"
PS C:\Windows\system32> $destination = "D:\Backups"
PS C:\Windows\system32> Copy-Item -Path $source -Destination $destisnation -Recurse -Force
PS C:\Windows\system32>
```

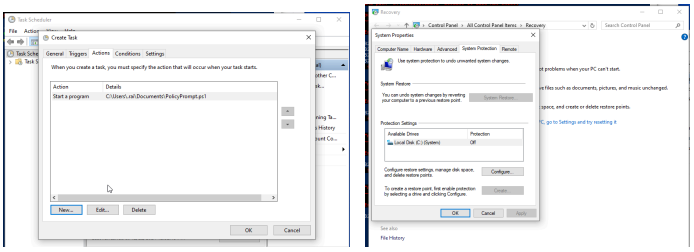
   - Automate the backup using Task Scheduler:
     i. Open Task Scheduler and create a new task.
     ii. In the **Action** tab, specify the PowerShell script.

2. Step 5.2: Quarantine a Malicious Process

- Use PowerShell to identify and terminate a suspicious process: *Get-Process -Name "malicious_process" | Stop-Process -Force*

3. Step 5.3: Restore System Settings

- Use System Restore:
  - Open **Control Panel > Recovery > Configure System Restore**.
  - Create a restore point: *Checkpoint-Computer -Description "Pre-Incident" -RestorePointType MODIFY_SETTINGS*



Step 6: Testing and Verification

1. Test each control individually:
    - Attempt to bypass firewall rules (Step 2.1).
    - Log a failed login attempt and verify logs (Step 3.1).
    - Test the startup message or policy prompt (Step 4.2).
2. Document findings:
    - Record actions and results in a lab report.
3. Reset the VM for repeated practice:
    - Take a snapshot of the VM before starting the lab.

Conclusion

This project covers practical implementations of preventive, detective, directive, and corrective controls using a Windows VM and PowerShell. By following this guide, you'll gain hands-on experience with configuring and testing security controls, which aligns with the objectives of the CompTIA Security+ certification.

I am exhausted as I finish this project, Will drop more labs…. Kisses n Hugs - Gamu