Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

Lab 7.2.11 Scanning an Active Directory Domain Controller for Vulnerabilities and Remediating Them

From TestOut CompTIA Security+ Course

In this lab I will be scanning an Active Directory Domain Controller for Vulnerabilities and then taking the necessary actions to remediate them. I will be using a generic version of Greenbone's OpenVAS.

The scenario for this lab is as follows:

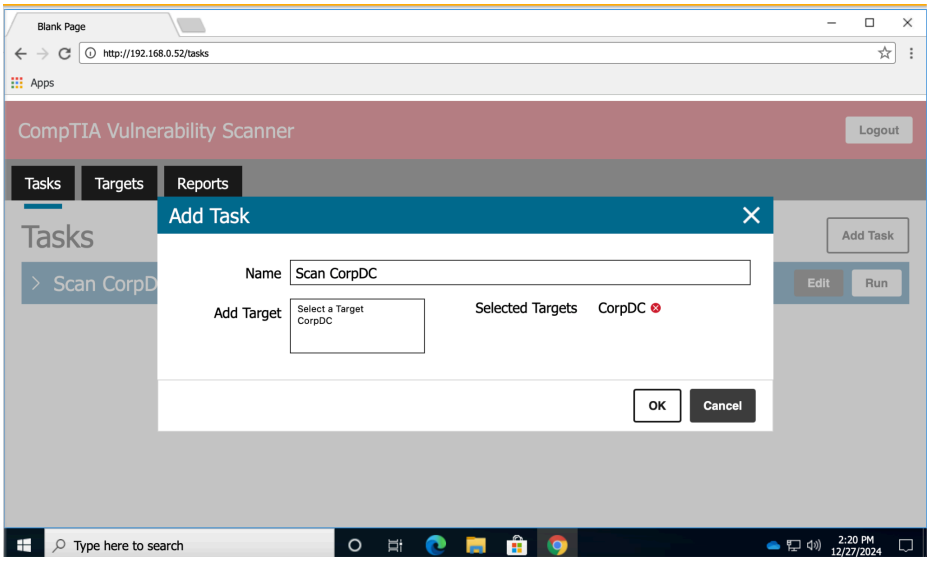
"You are the IT security administrator for a small corporate network. You are performing vulnerability scans on your network. Use the CompTIA Vulnerability Scanner tool to run a vulnerability scan on the CorpDC domain controller.

In this lab, your task is to:

- **Login to the CompTIA Vulnerability Scanner in Chrome.**
  - **URL: http://192.168.0.52**
  - **Username: securityadmin**
  - **Password: P@ssw0rd**
- **Create a target for the CorpDC server (192.168.0.11).**
- **Create a task and run a vulnerability scan for the CorpDC server.**
- **View the report for the scan task you created.**
- **Remediate the vulnerabilities in the Default Domain Policy using Group Policy Management on CorpDC.**
- **Re-run a vulnerability scan to make sure all of the issues are resolved."**

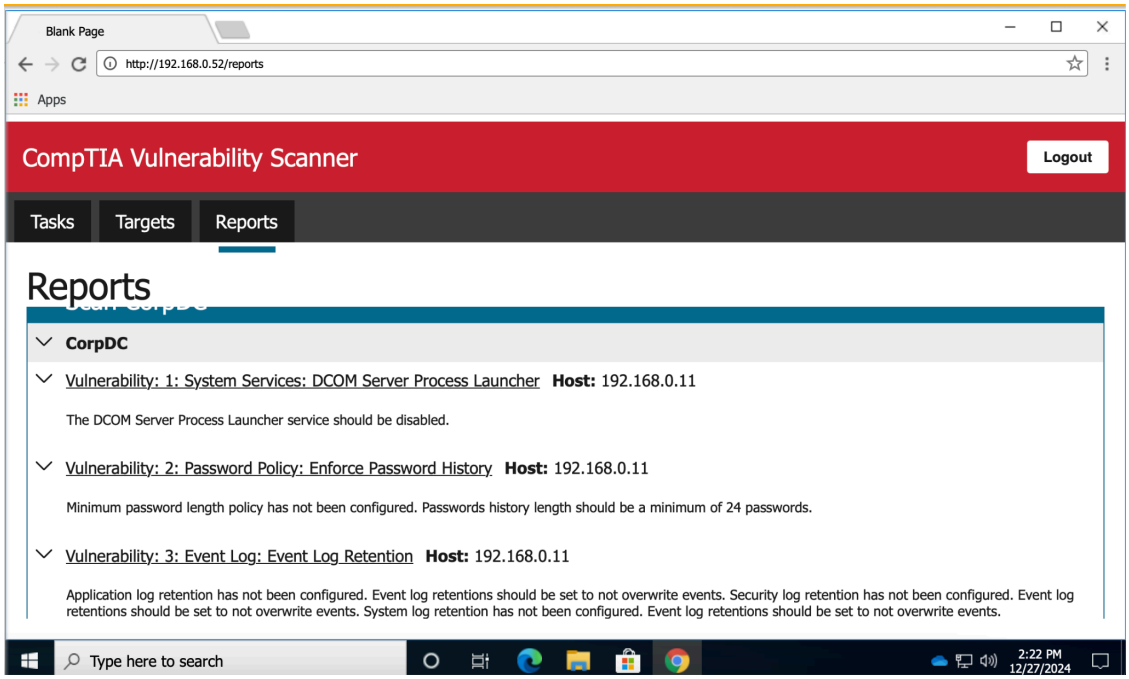
First I will start by logging into the scanner with the credentials provided. Then I will navigate to the **Targets** menu and enter the information for the Domain Controller.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



Once completed I will navigate to **Tasks** and add a new task for the scanner pointed at the Domain Controller. After adding the task, I will click the **Run** button to start the vulnerability scan.

Once it's finished I will head over to the **Reports** tab to see what the scanner found.



Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

The scanner has found a plethora of vulnerabilities as evidenced below:

Vulnerability: 1: System Services: DCOM Server Process Launcher

Host: 192.168.0.11

The DCOM Server Process Launcher service should be disabled.

Vulnerability: 2: Password Policy: Enforce Password History

Host: 192.168.0.11

Minimum password length policy has not been configured. Passwords history length should be a minimum of 24 passwords.

Vulnerability: 3: Event Log: Event Log Retention

Host: 192.168.0.11

Application log retention has not been configured. Event log retentions should be set to not overwrite events. Security log retention has not been configured. Event log retentions should be set to not overwrite events. System log retention has not been configured. Event log retentions should be set to not overwrite events.

Vulnerability: 4: Password Policy: Minimum Password Age

Host: 192.168.0.11

Minimum password age policy has not been configured. Minimum password age should be 1 day or more.

Vulnerability: 5: Password Policy: Minimum Password Length

Host: 192.168.0.11

Minimum password length policy has not been configured. Passwords should be a minimum of 14 characters.

Vulnerability: 6: Account Lockout Policy: Reset Account Lockout Counter after

Host: 192.168.0.11

Reset account lockout counter should be set to a minimum of 60 minutes.

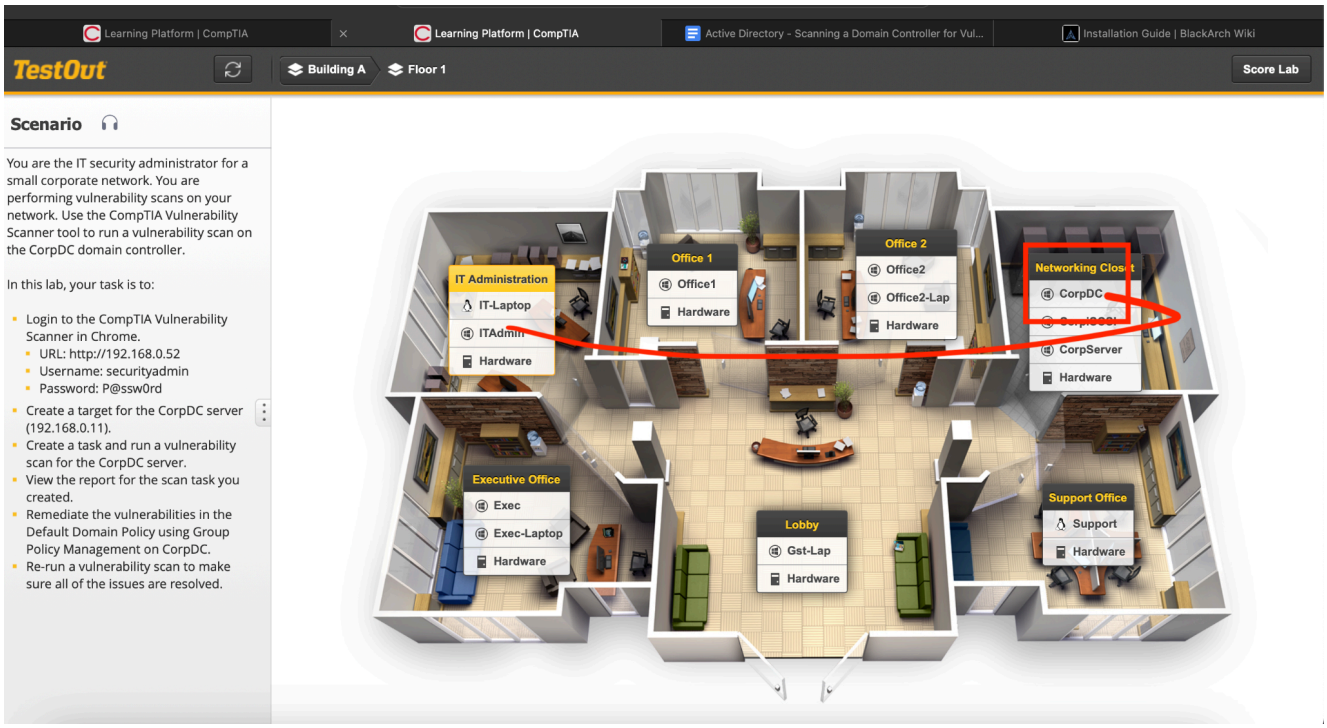
Vulnerability: 7: System Services: Task Scheduler

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024
Host: 192.168.0.11

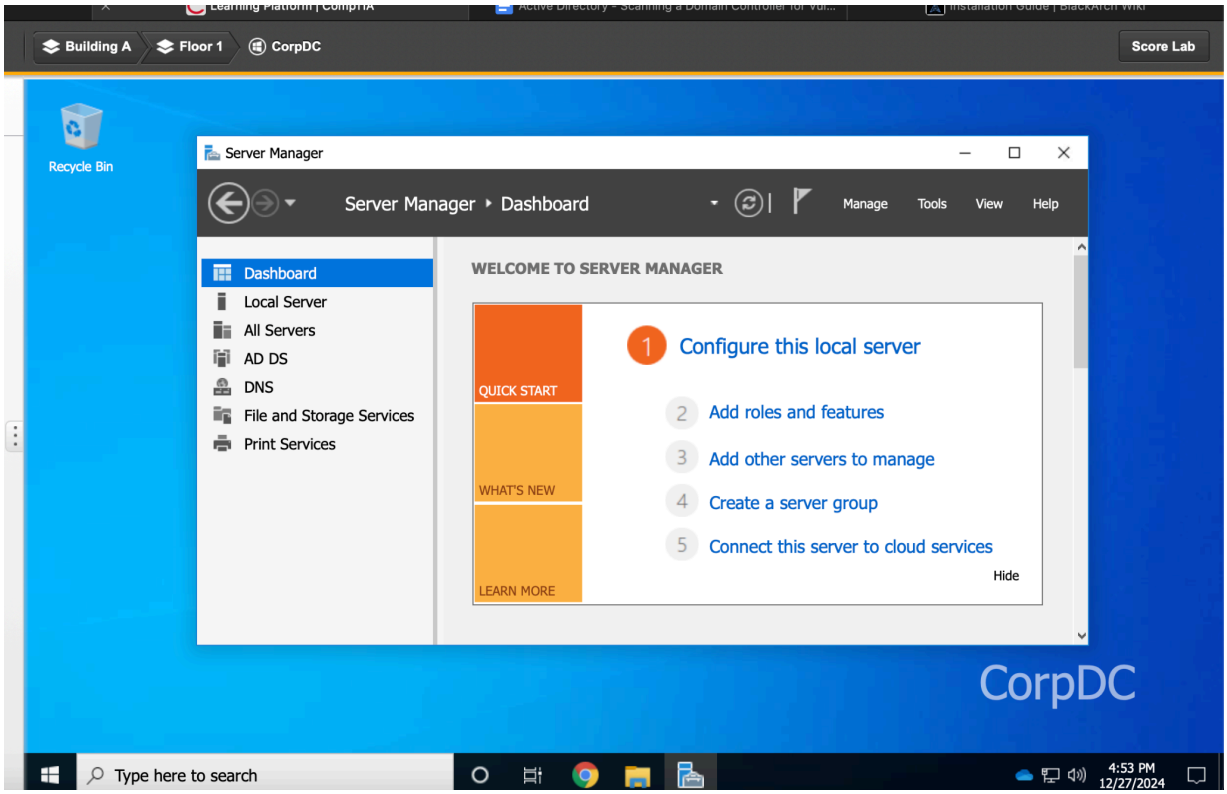
The Task Scheduler service should be disabled if not in use.

As you can see the scanner found a lot of vulnerabilities. I will need to head over to the Windows Server that's housing the Domain Controller so that I can remediate these vulnerabilities and push out the updates to sync with the other DCs.

I'll head over from my **ITAdmin** machine to the **Networking Closet** on **Floor1** and access the **CorpDC** machine.

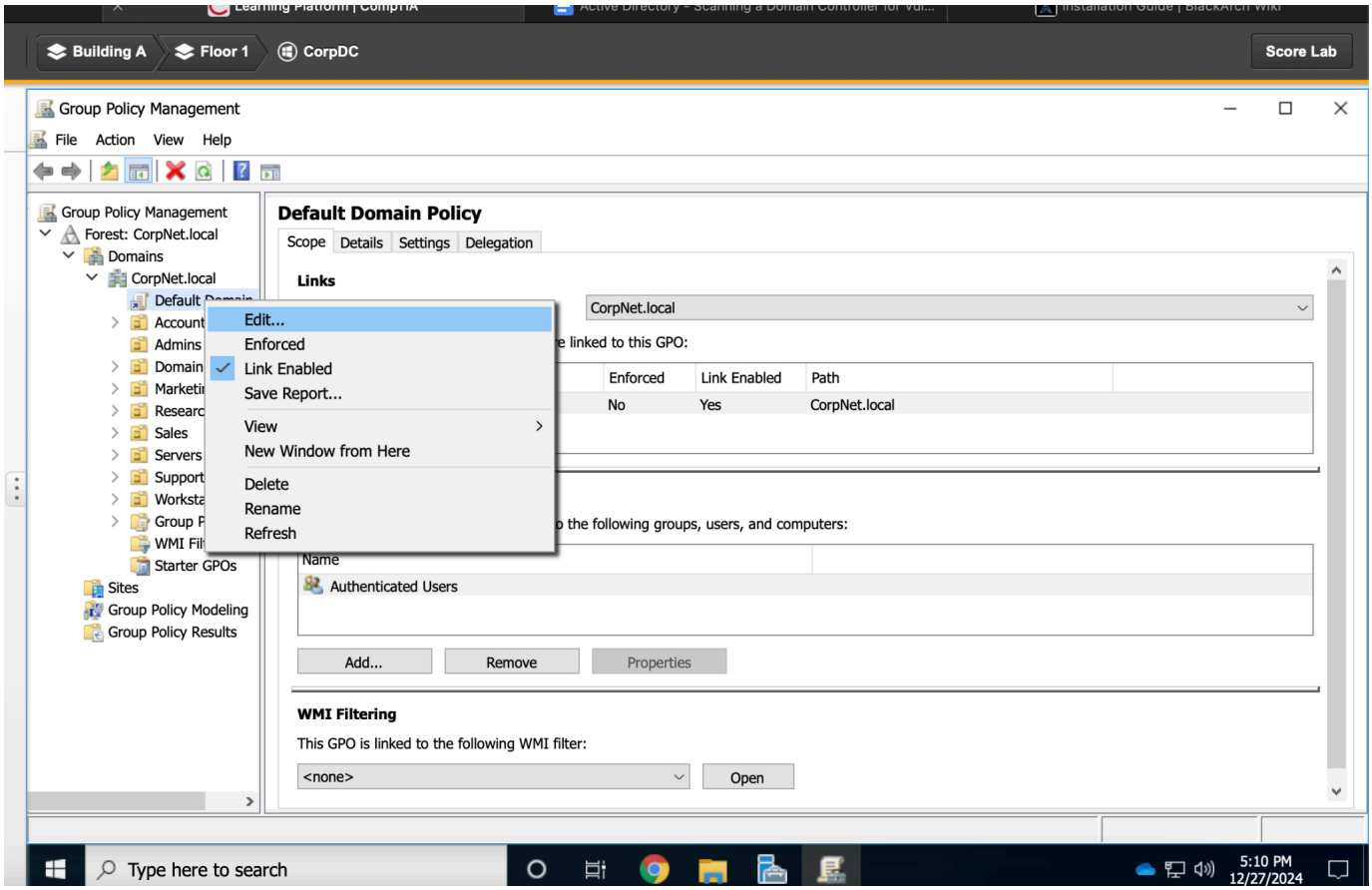


Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



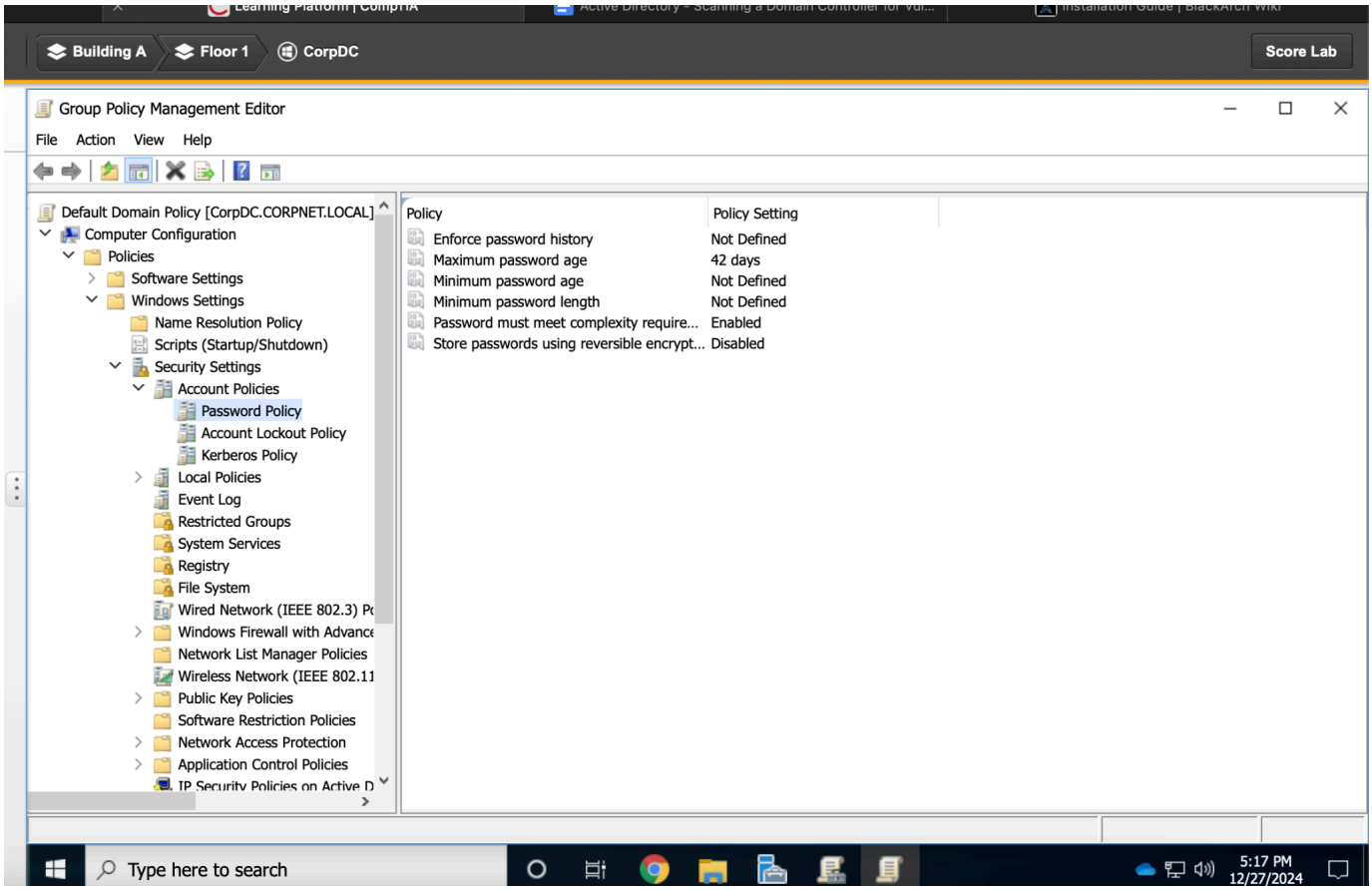
Now that I'm on the Domain Controller I can start to address these vulnerabilities. I notice that in the list provided above Vulnerabilities #2,4,5,6 all have to do with Passwords or accounts. To access this I can open my Server Manager (pictured above) and head to **Tools > Group Policy Management.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



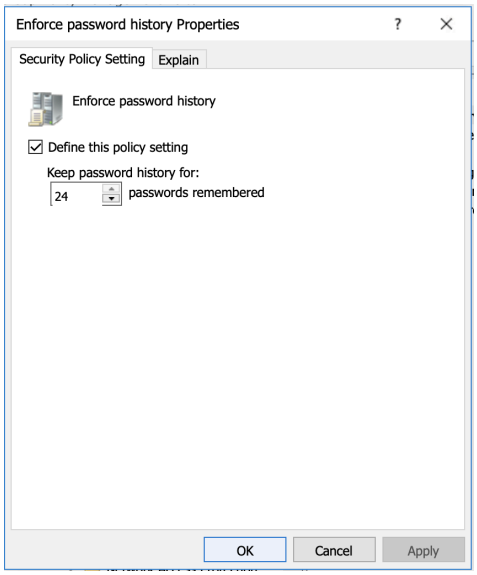
Now that Group Policy Management is open I will expand the Forest on the left side and head to **Forest: CorpNet.local > Domains > CorpNet.local > Default Domain Policy** and right click it. On the menu click **Edit** to bring up the **Group Policy Management Editor**. Once that opens I can head to **Computer Configuration** and navigate to **Computer Configuration > Policies > Windows Settings > Security Settings > Account Policies.** (see below screenshot)

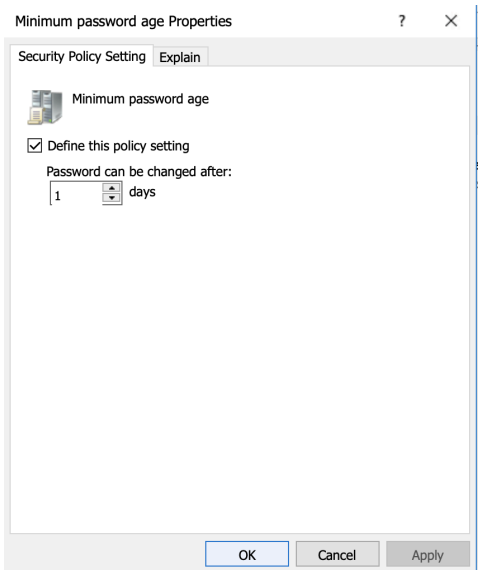
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

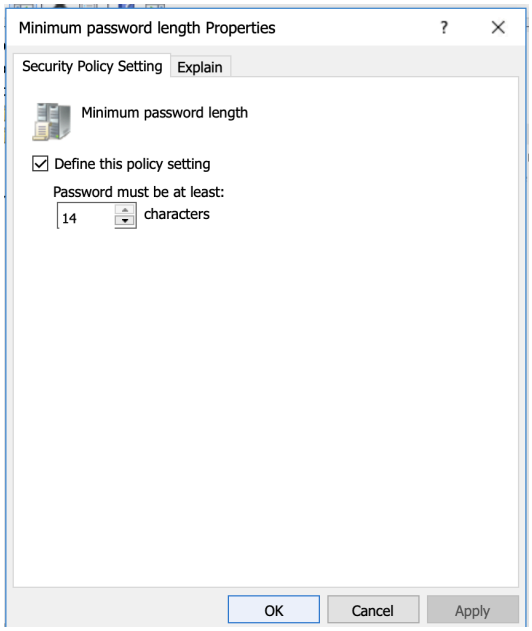


I will now double click **Password Policy** to bring up the configurator. Vulnerabilities 2, 4 , and 6 all have to do with incorrectly configured password settings. As you can see alot of these policies are undefined. I will fix that now.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024





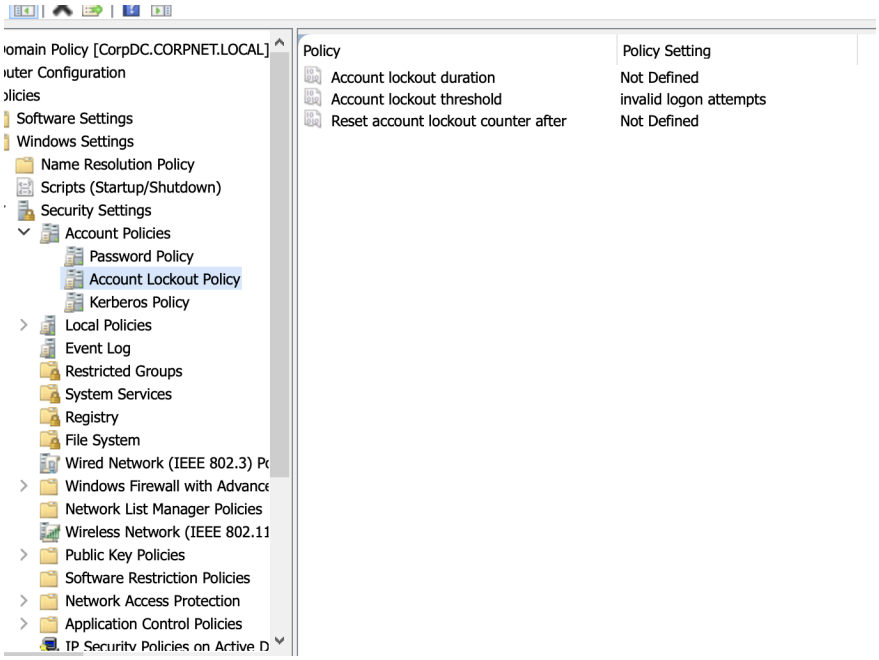


Once these above Password policies are configured I will hit **Apply** then **OK.**

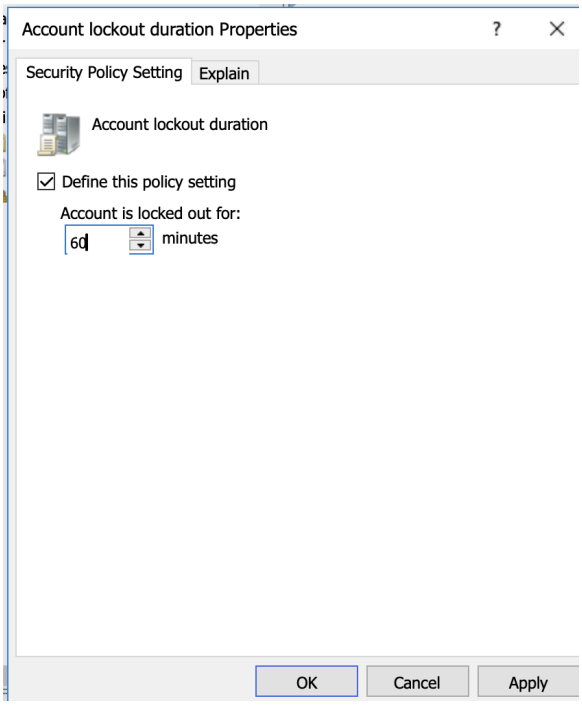
Now that I've configured the Password Policies I can now move on to remediating the vulnerability regarding the Account Lockout policy.

In the same Account Policies pane where I selected **Password Policies** I can select **Lockout Policy.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



I will double click **Account lockout Duration** and set the time to 60 minutes as suggested by the vulnerability scanner.



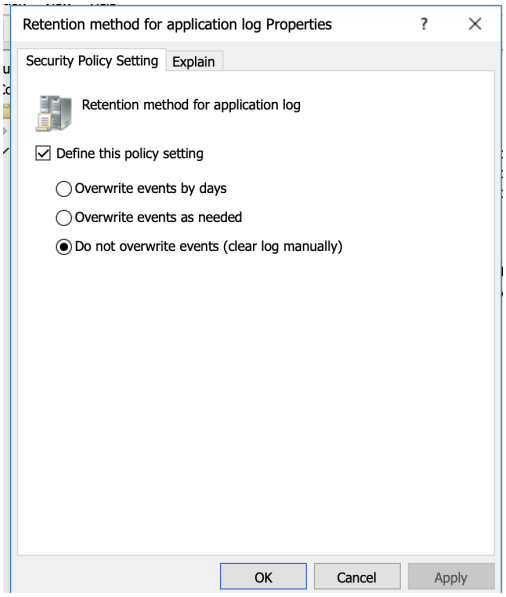
Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

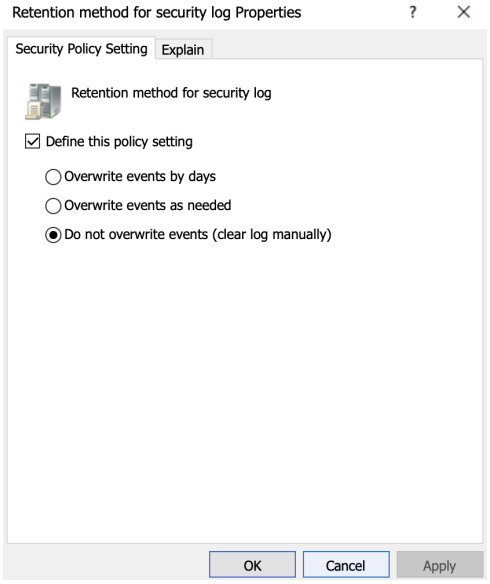
Once that's applied I will hit **Apply** then **OK.** I will now head to the same left window pane and select **Event Log,** in order to remediate **Vulnerability #3: Event Log Retention which states:**

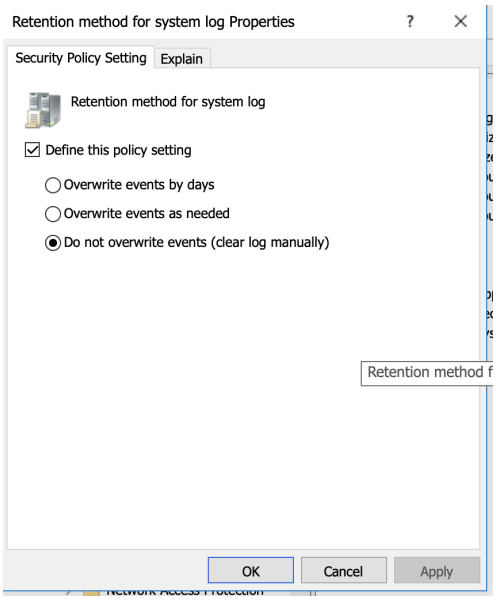
"Application log retention has not been configured. Event log retentions should be set to not overwrite events. Security log retention has not been configured. Event log retentions should be set to not overwrite events. System log retention has not been configured. Event log retentions should be set to not overwrite events."

This isn't good because an attacker can easily overwrite events.I will configure each of these settings and hit **Apply** then **Ok** on each one.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



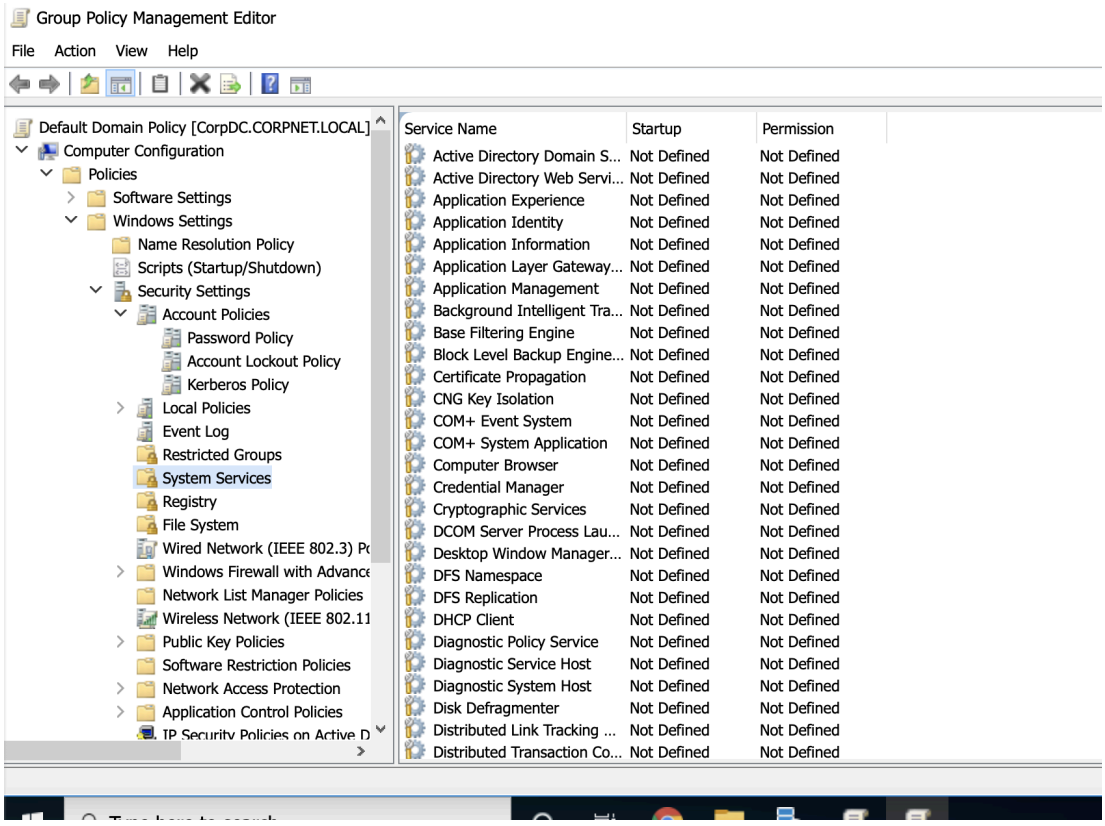




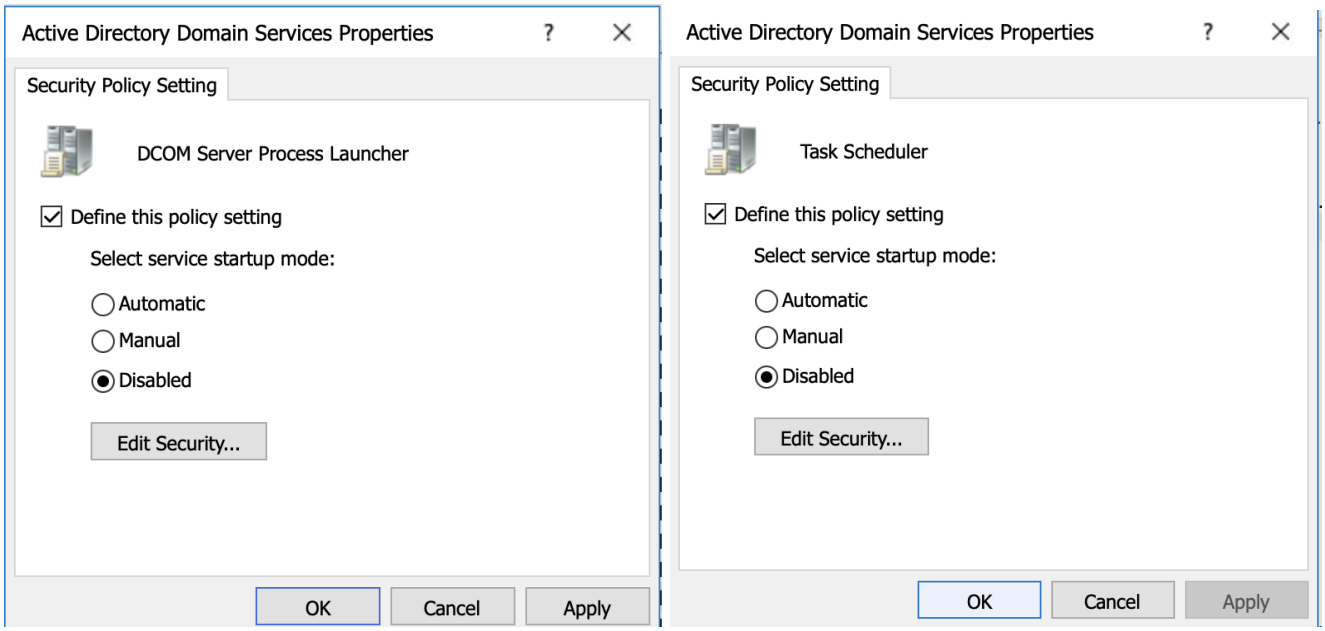
I can now move on to tackling **Vulnerability #1 and #7** which have to do with Windows background Services like DCOM and Task Scheduler.

From the same left pane in **Group Policy Management Editor** I will select **System Services.**

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



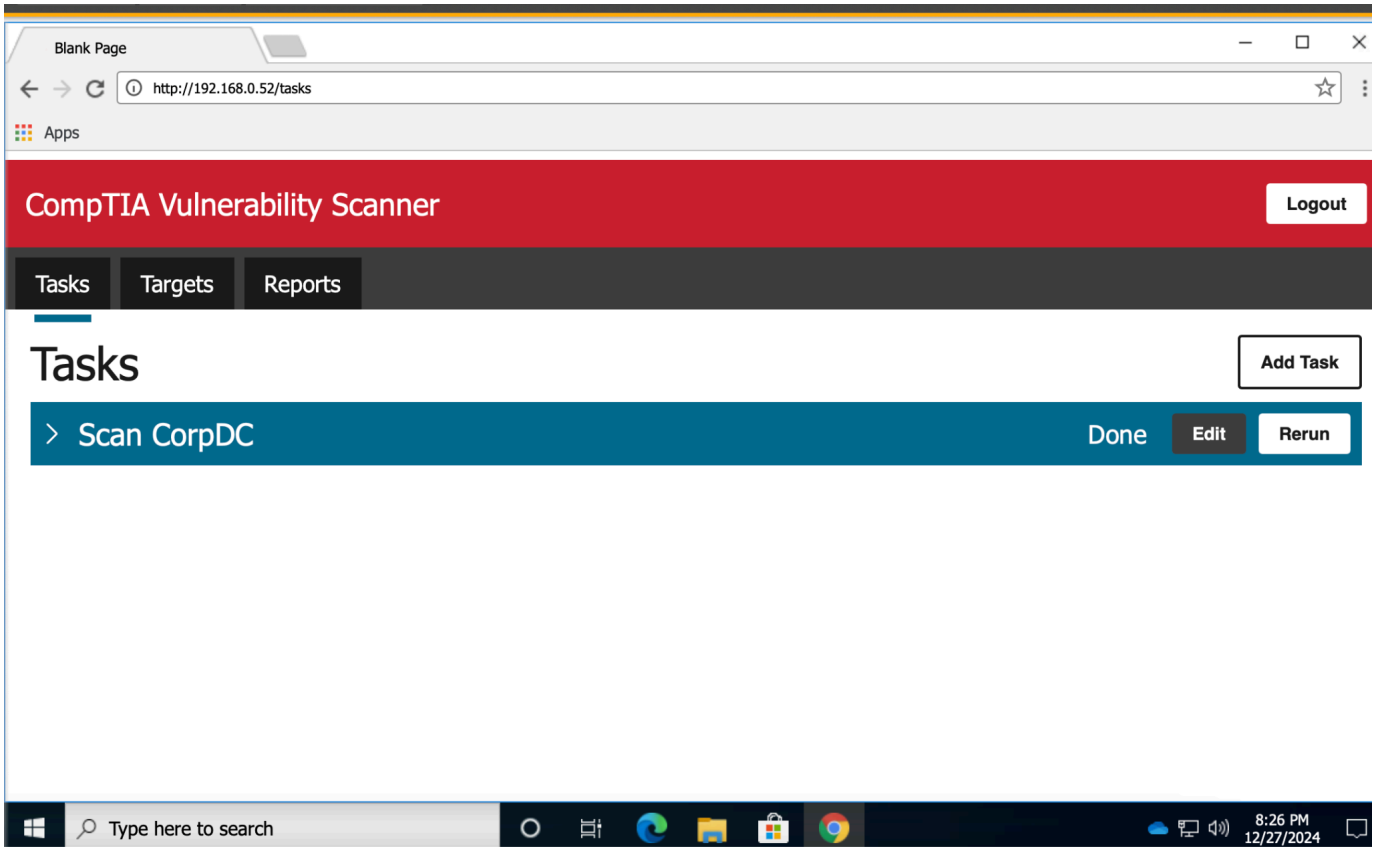
I will scroll down and Disable **DCOM Server Process Launcher** and **Task Scheduler.**



Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024

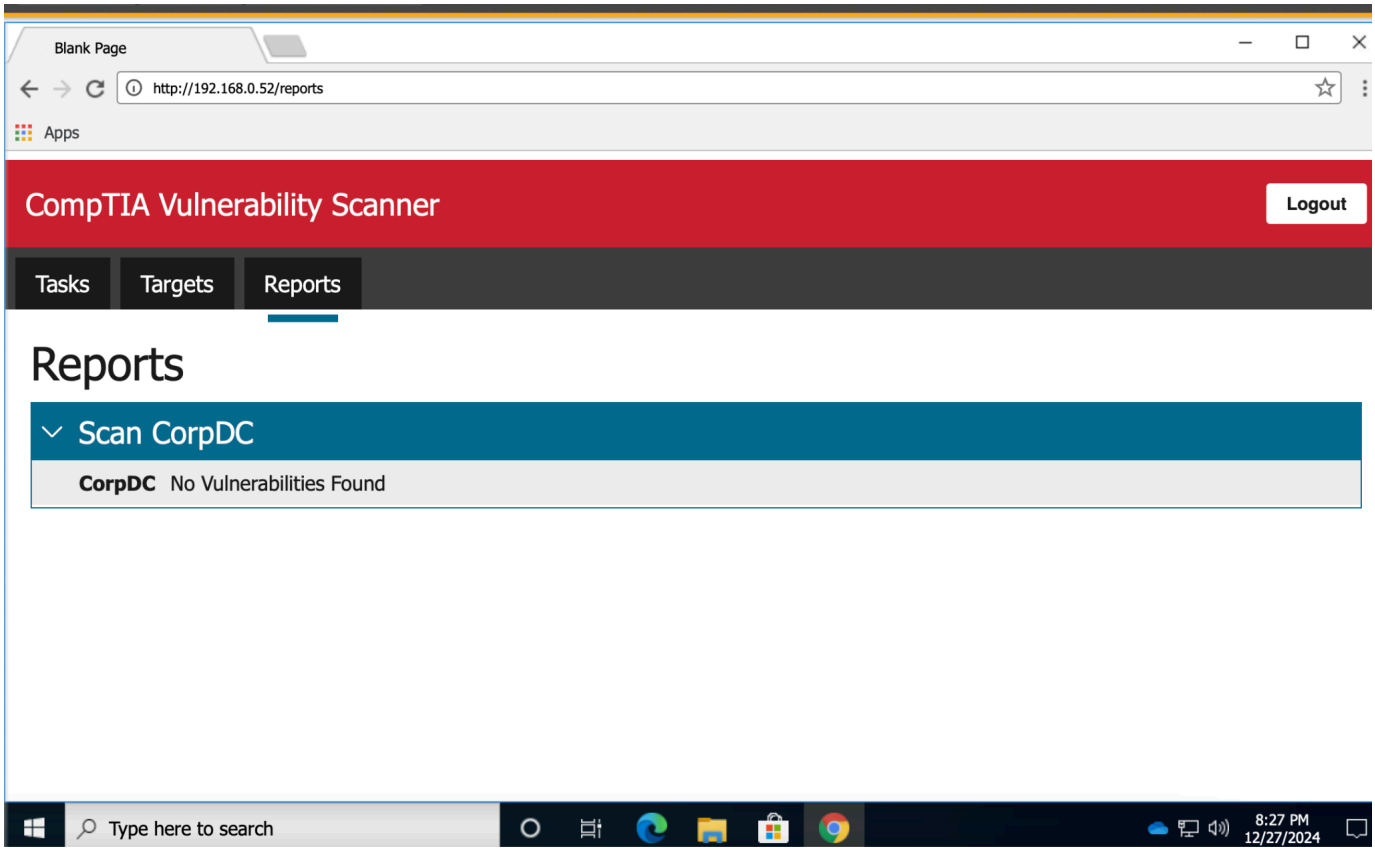
After disabling these services, I will head back to the **ITAdmin** Machine so I can re-run the scanner to verify all of the vulnerabilities have been remediated.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



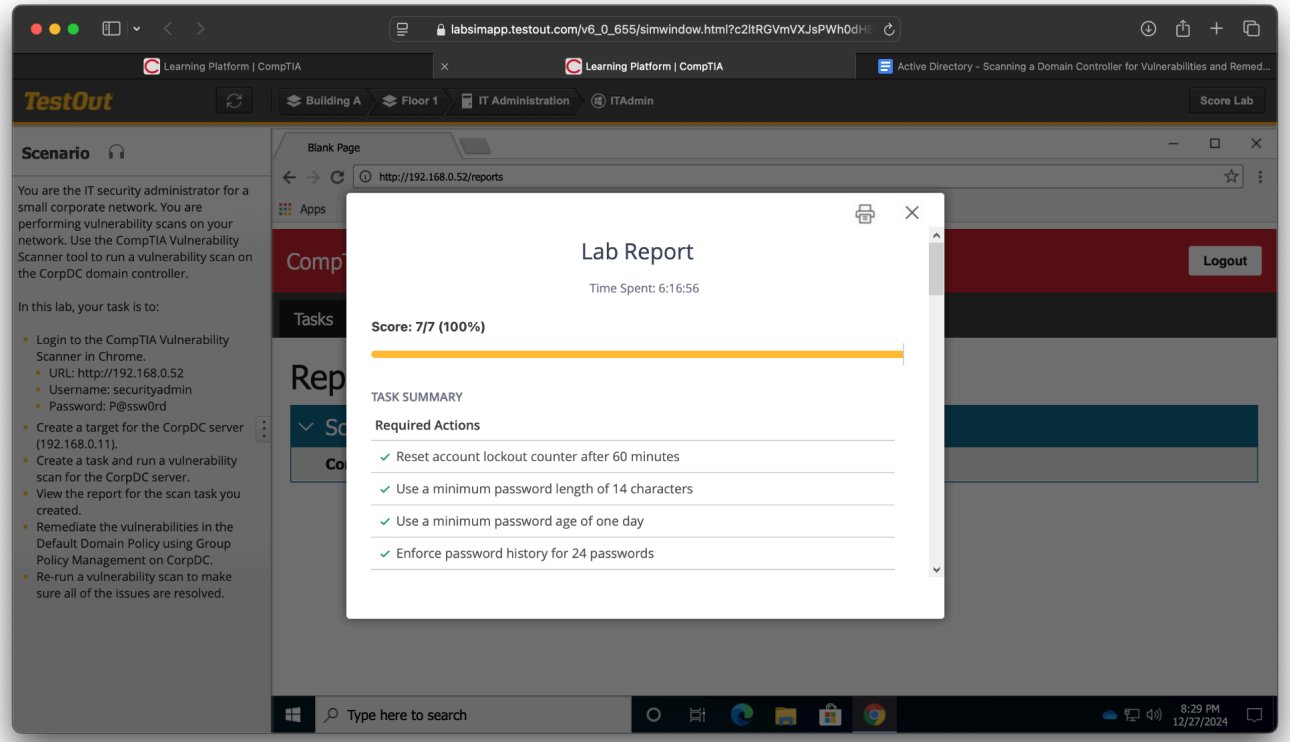
I will click the re-run button on the **Tasks** menu. Once completed I will head over to the **Reports** tab to check for any remaining vulnerabilities that need to be remediated.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



SUCCESS! I have successfully discovered and remediated the vulnerabilities found. This now concludes this lab.

Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024



Robert Carpenter
github.com/robertmcarpenter
Thurs December 26th 2024