Lab #2: Configure Microsoft SQL Server

Purpose:

• We'll install the Microsoft SQL server inside the Windows "tester" VM. This server will eventually be used to test logging and monitoring.

Tasks:

- 1. Disable the Windows Firewall in Windows "Tester" VM
- 2. Install SQL Server and create vulnerabilities
- 3. Test the Linux "Tester" VM (ping and SSH)

Task 1: Disable the Windows Firewall in Windows "Tester" VM

- 1. Open windows-vm > open Windows Defender Firewall (wf.msc).
 - a. Windows Defender Firewall Properties > update Firewall State to OFF (in 3 tabs: Domain Profile, Private Profile, Public Profile) > select Apply > OK.



2. From your local PC, you should be able to ping the public IP of windows-vm.

Task 2: Install SQL Server and create vulnerabilities

1. In windows-vm, install SQL Server Evaluation:

<u>Note</u>: This will be another thing for attackers to attempt to attack.

- a. In windows-vm, open Edge > go to <u>Google.com</u> > search for **Download SQL Server** Evaluation.
- Select the first option (should be SQL Server 2019) > select Download the EXE > Enter information, and select Download Now > select EXE download (64-bit edition).
- c. Open the downloaded file to finish the install > select **Download Media** > Update **Download Location** to **Desktop** > select **Download**.
- d. Once the download completes, select Open Folder (you'll see the Desktop folder and the new ISO file) > right-click the ISO file, and select Mount > double-click setup [to start the installation of SQL Server] > select Installation, and select New SQL Server stand-alone... > select Next (3x) > in Feature Selection, select the Database Engine Services checkbox and select Next > select Next (2x) > select Mixed Mode (for authentication mode) > enter password > select Add Current User (wait 10s), then select Next > (select Finish on the last page).
- e. The install process will take 10-20min to complete.

a SQL Server 2019 Setup		- 0	×				
Complete Your SQL Server 2019 installat	ion completed successfully with product update	5.					
Install Rules Feature Selection	Information about the Setup operation or possible next steps:						
	Feature	Status					
Instance Conferentian	Database Engine Services	Successive					
indence consignation	SQL Browser	Succeeded					
Server Configuration	SOL Writer	Succouded					
Database Engine Configuration	SQL Client Connectivity SDK	Succeeded					
Feature Configuration Rules	SQL Client Connectivity	Succeeded					
Ready to Install							
Installation Program							
Complete	Details						
	Instill successful Summary log file has been saved to the follo CoBrogram Elect/Acrosoft SQL Server) 1501 vm. 2023/366-210550.tet	v ing location: Setup Biochtraph Log(2020936, 210350/Summary in Yorkow)	2				

2. In windows-vm, also install SQL Server Management Studio:

<u>Note</u>: This app lets us log into SQL Server and visualize data. We'll soon see logon attempts from attackers in Windows Event Viewer.

- a. Go back to Edge > go to <u>Google.com</u>, and search for **Download SSMS** > Under the **Download SSMS** section, select **Free Download...SSMS...19.1**.
- b. Open the downloaded file > select **Install** (it'll take 10-20min).
- c. Now, you'll need to restart your VM.
- 3. Enable logging for the SQL server (to receive logs for sign-in attempts):
 - a. Follow the steps in this Microsoft article: Write SQL Server Audit events to the Security log
 - b. Open the **Registry** (regedit.msc) > go to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Security

c. > right-click it and select **Permissions** > (System > **Add**) > type **Network Service** (select **Check Name**), and select **OK** > select **Full Control** checkbox, **Apply**, and **OK**.

File Edit View	Favorites Help	SYSTEM ConnectControlSe	f Service of Frankland	Samoito
2001000010100000 22 22 22 22 22 22 22 22 22 22 22 2	Duemfax Duemfax edgoupdate edgoupdate edgoupdate edgoupdatern BFS BrSter/Cass	 Name Name DepayMamelia Missistion Missistion Missistion Missistion Missistion Missistion Missistion Missistion Copy Key Name 	Type REG_SZ REG_DRAND_SZ REG_DRAND_SZ REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD REG_DWORD	Data (volue not set) SSpttamilizatSV/system32/voluevt5kopt/Security.s 6x00000002 (2) Ex01400000 (2) Ex01400000 (2) Security Ex00000000 (2) D1 c0 14 do w1 c0 c0 p0 60 00 c0 r0 14 00 c0 c0 44 0

- d. Copy the Windows Command Prompt prompt (from the above article).
 - i. In Command Prompt (run as admin) run the prompt > done (close any open windows).
- 4. Open the **SSMS** app and enable auditing:
 - a. **Properties > Security >** Select the **Both failed and successful logins** radio button > **OK**.
 - b. Disconnect and reconnect the SSMS server > intentionally attempt to log in using invalid credentials.

<u>Note</u>: This generated a few "Login Failed" alerts.

- 5. View the failed SQL login attempt:
 - a. Open **Event Viewer > Application** section (to view SQL login attempts) > we see the failed login attempts.

Event Viewer (Local)	Application Number of events: 822						
> Custom Views	Level	Date and Time	Source	Event ID			
Application	(1) Information	9/6/2023 9:25:11 PM	MSSQLSERVER	18456			
Security	(i) Information	9/6/2023 9:25:03 PM	MSSQLSERVER	18454			
E Setup	(1) Information	9/6/2023 9:25:03 PM	MSSQLSERVER	18454			
System	(1) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	3408			
Forwarded Events	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	9688			
> Applications and Services Logs	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	9666			
Subscriptions	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	9666			
	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	17117			
	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	17137			
	(1) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	17136			
	(1) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	17137			
	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	958			
	(i) Information	9/6/2023 9:24:56 PM	MSSQLSERVER	26067			
	Event 18456, MSSQLSERVER						
	General Details						
	Login failed for user ' Reasony Password did not match that for the login provided. [CLIENT: <local machine="">]</local>						

<u>Note</u>: Now, anybody can attempt to connect to this VM and SQL database. We're exposing all of this to the internet with the intent to analyze the logs and practice incident response later. We're setting up our environment, making it look enticing to hackers.

Task 3: Test the Linux "Tester" VM (ping and SSH)

- 1. Azure portal > Virtual Machines > start linux-vm.
- 2. Open terminal/PowerShell on our local PC.
 - a. Test that we can ping linux-vm: ping <the public IP>
 - b. Test that we can SSH (login) into linux-vm: ssh <username>@<VM public IP>
 i. "Are you sure...": yes
 - ii. "Password": <VM password>
 - iii. Disconnect from the SSH session: exit

<u>Note</u>: Successfully confirmed that we can ping and SSH to linux-vm.

3. <u>Stop</u> all of the running VMs.

End:

- In windows-vm, we disabled the internal firewall and installed SQL Server.
- Also we logged into linux-vm via SSH.