Rodrigo Brasil 11/2023

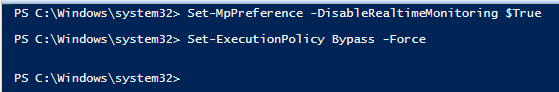
### **Part 1: Staging**



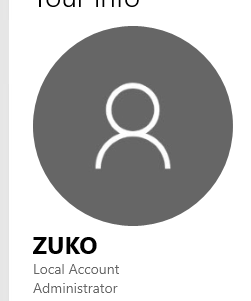
Windows Server 2019 EC2 connect remotely via RDP



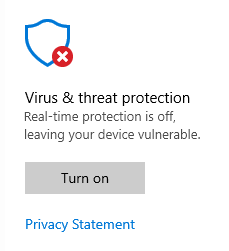
system-hardening.ps1 powershell script



Disable windows defender and bypass powershell script policy commands



After running the script, a new admin user was created called zuko

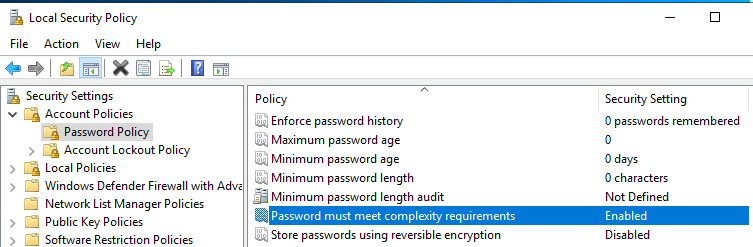


And Windows Defender is turned off

### 

### 

### **Part 2: Manual EC2 instance hardening with CIS**

* 1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)
* 1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)



* 1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)



(Will have to come back to this option it’s grayed out because the machine is not on a domain)

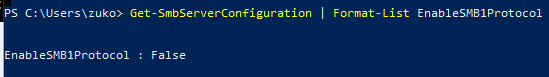
after performing the step below now this option is available



* 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)

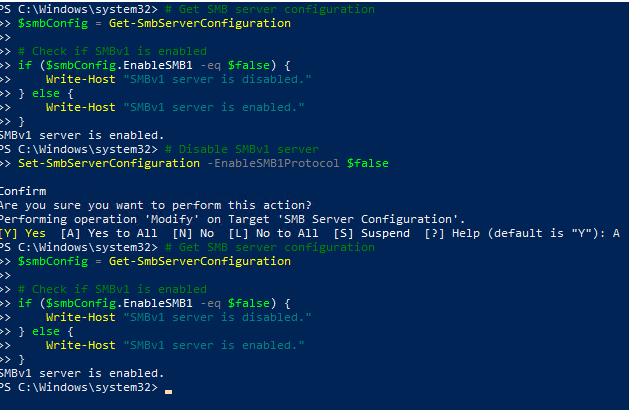


* 18.4.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)

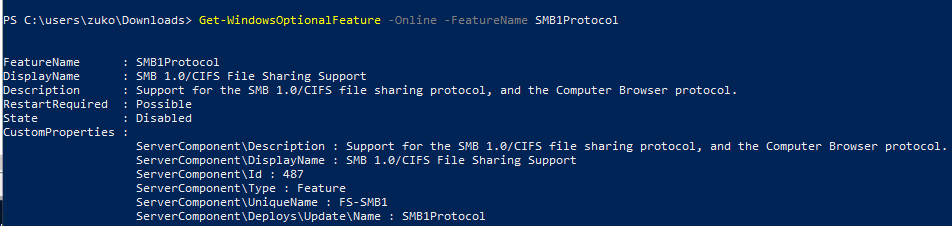


for some reason the policy doesn't show up on the local group policy editor so i had to check it using powershell console

* 18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)



SMBv1 is enabled, tried to run this commands to disable it but to no avail



after running the script below now the SMB v1 Server is disabled

### 

### 

### 

### 

### 

### 

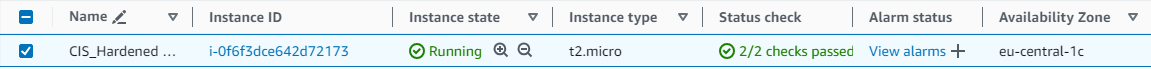
### **Part 3: Automating the Configuration**



Script to enable the policies

After multiple tries finally was able to create a script that works

### **Part 4: Pre-hardened EC2 instance deployment**



EC2 Used

* 1.1.5 (L1) Ensure 'Password must meet complexity requirements' is set to 'Enabled' (Automated)



* 1.1.6 (L1) Ensure 'Store passwords using reversible encryption' is set to 'Disabled' (Automated)



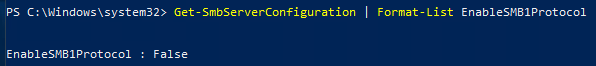
* 1.2.1 (L1) Ensure 'Account lockout duration' is set to '15 or more minute(s)' (Automated)



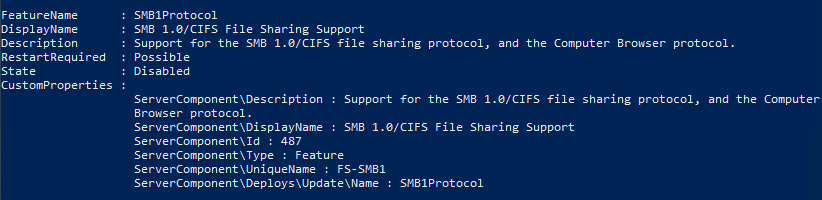
* 1.2.2 (L1) Ensure 'Account lockout threshold' is set to '5 or fewer invalid logon attempt(s), but not 0' (Automated)



* 18.4.3 (L1) Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver (recommended)' (Automated)



* 18.4.4 (L1) Ensure 'Configure SMB v1 server' is set to 'Disabled' (Automated)

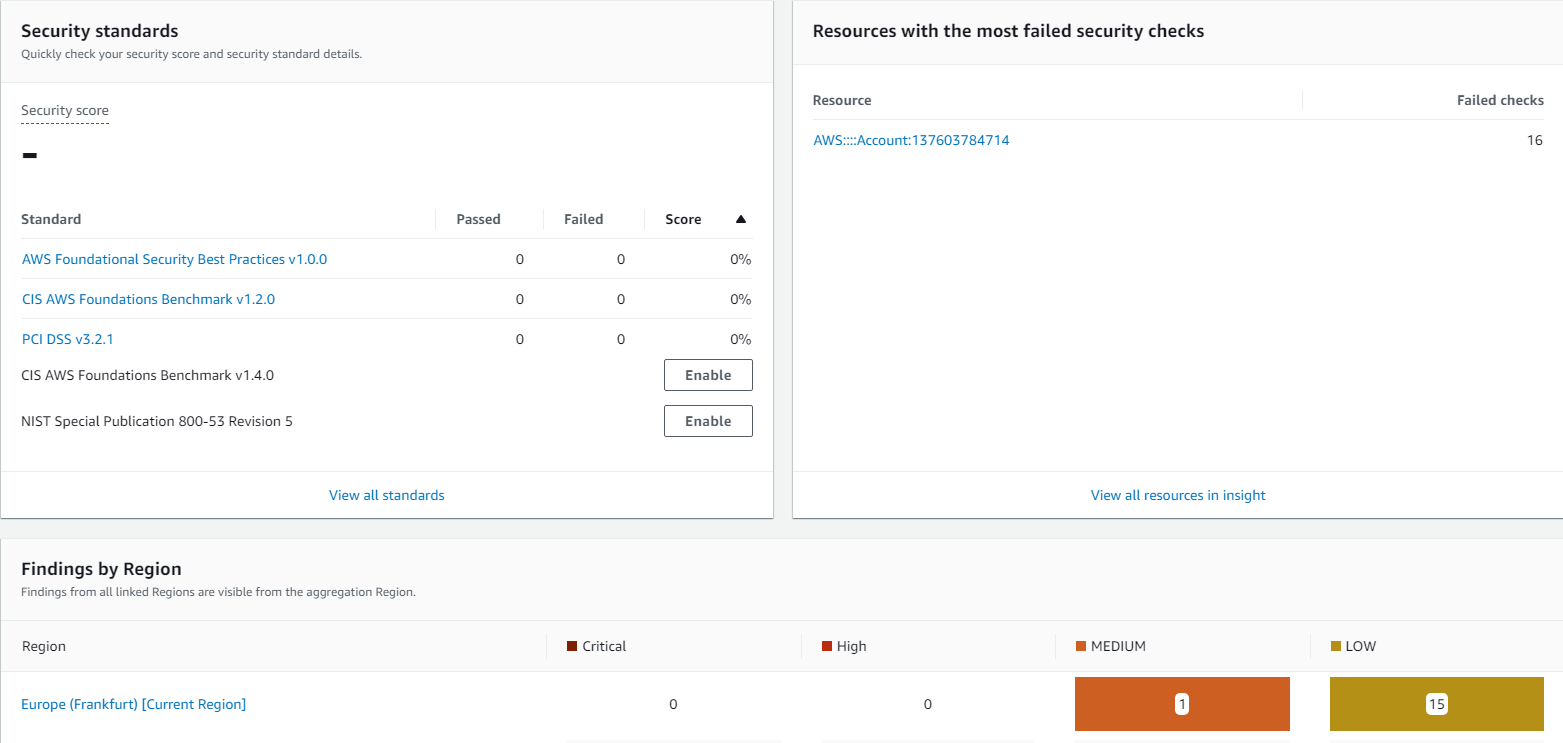


* Does the hardened instance achieve the security standard on deployment?

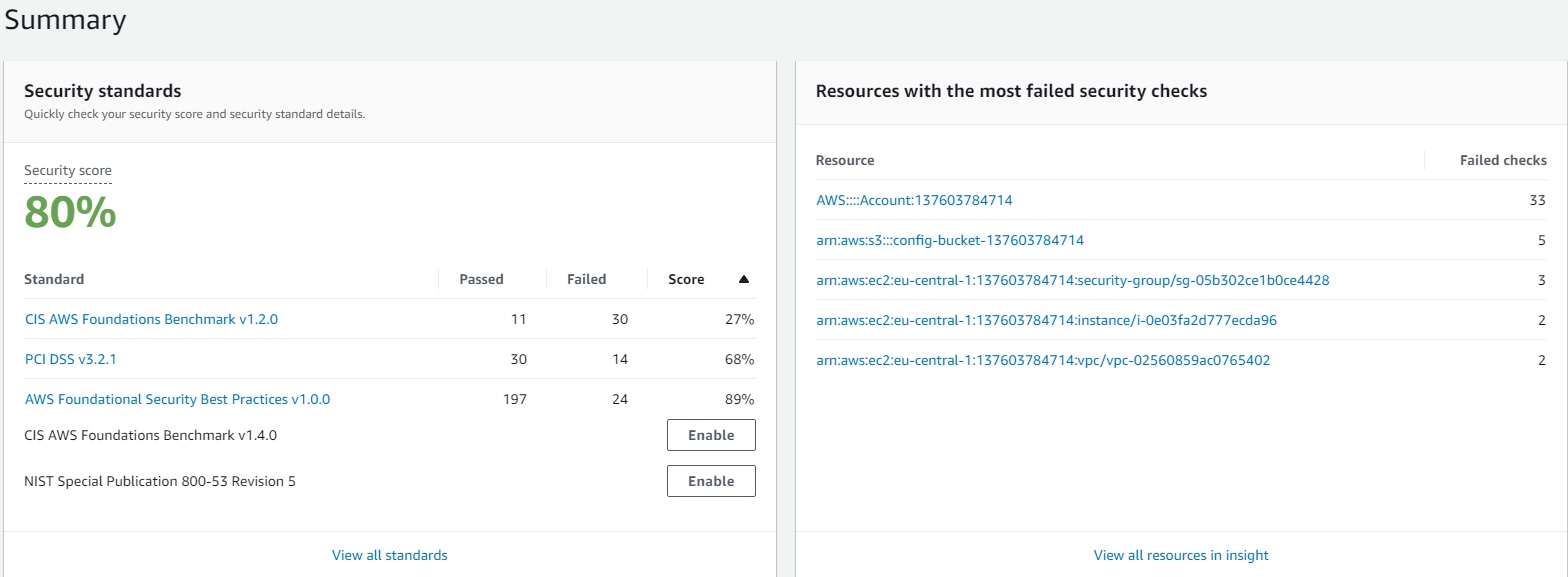
Yes it does. Everything is already pre-configured.

### **Part 5: Scanning for CIS Benchmarks**

I already terminated the first EC2 before i made the scan so i can only show from the hardened



I left the scan open for 1 hour and this was the result



A day later this was the result