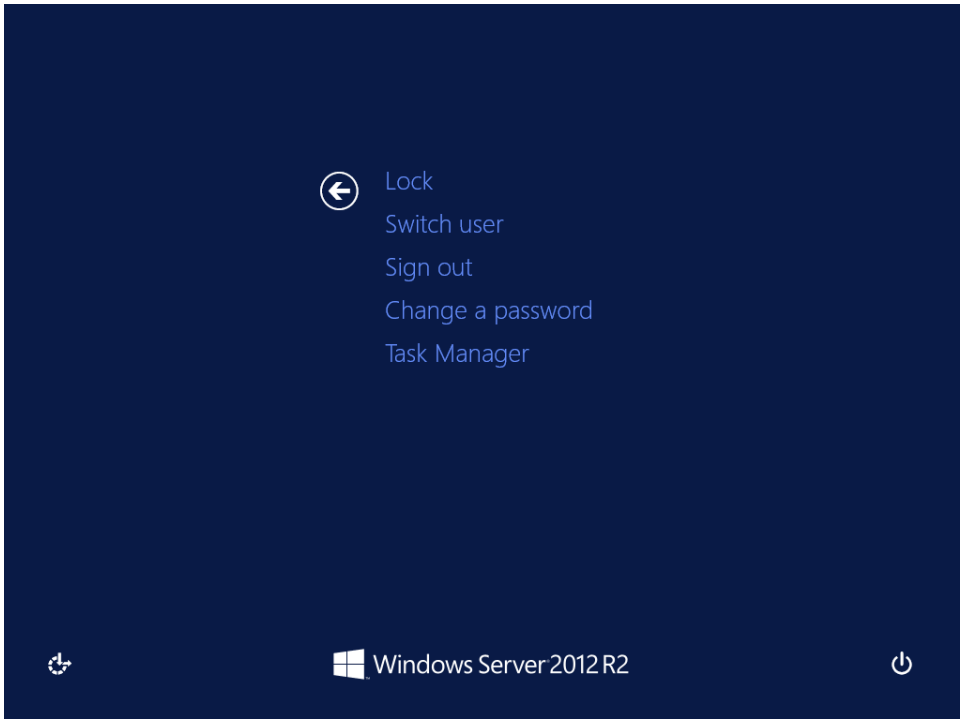
Created By: Will Novotny

Windows 2012 OS Hardening Playbook

1. **Change the default admin password**

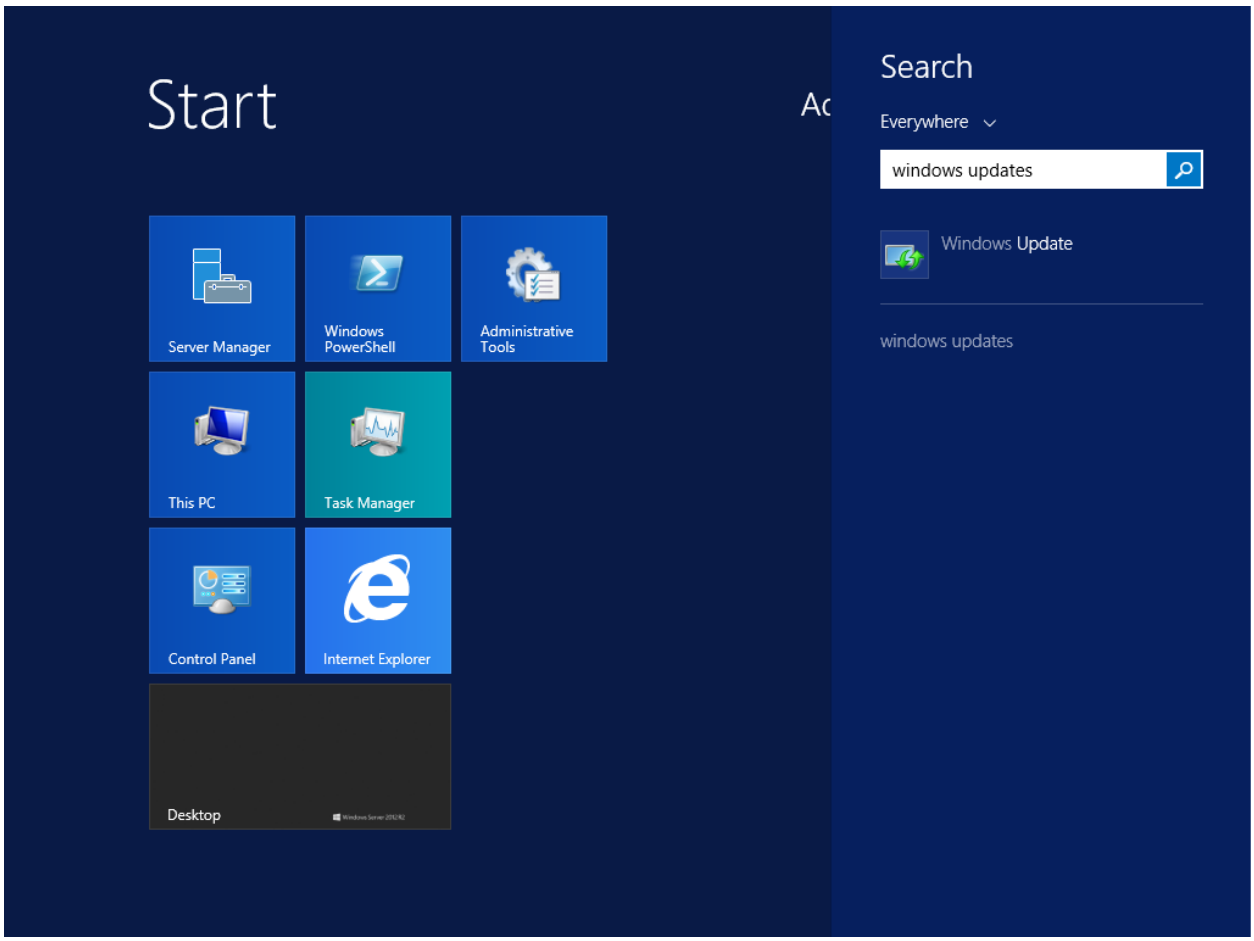


Press Crl+Alt+Del.

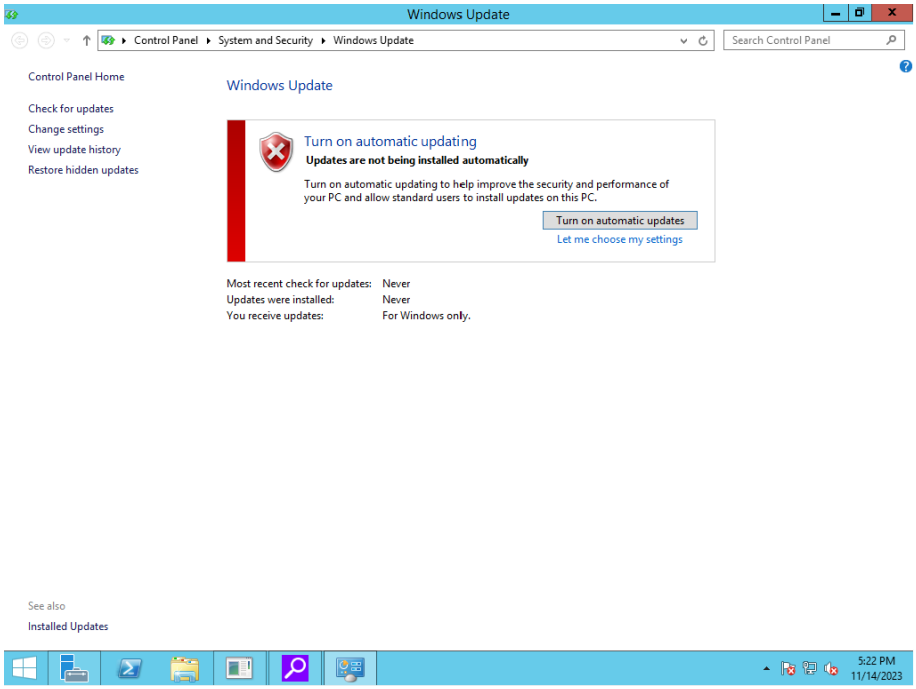
Click "Change a password".

Change the Password.

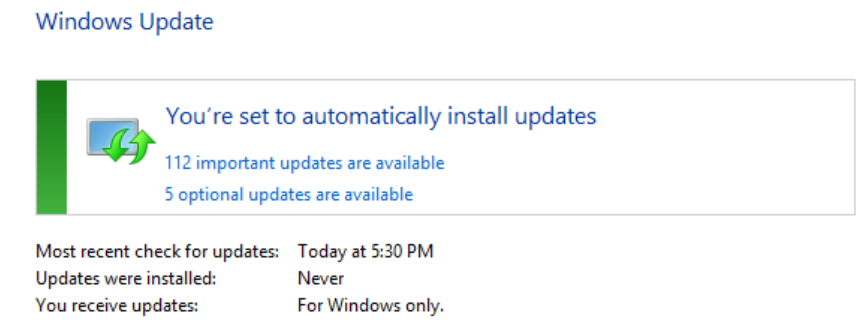
2. **Start Windows updates for security patches (approx. 25 updates, no idea of time for completion, but will probably take more than 15 minutes)**



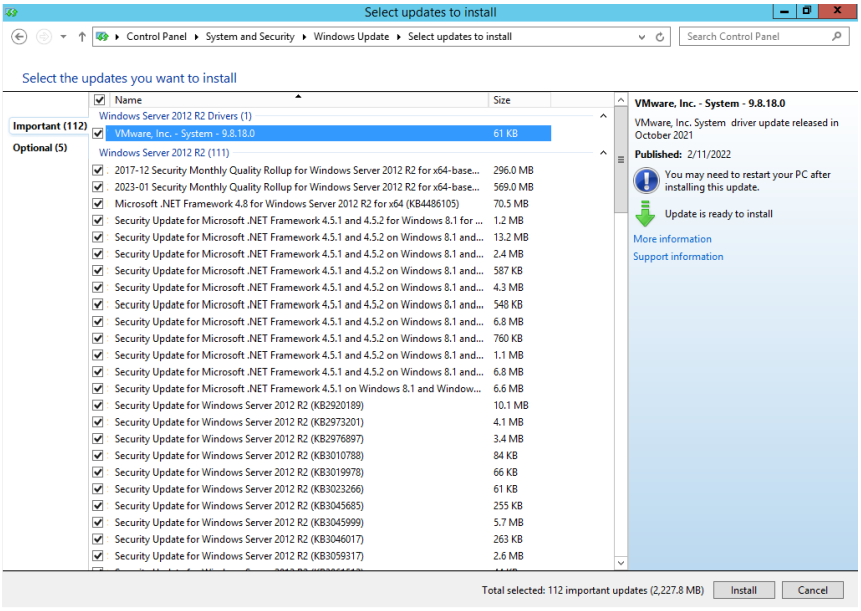
Search “Windows Update” and click on the application.



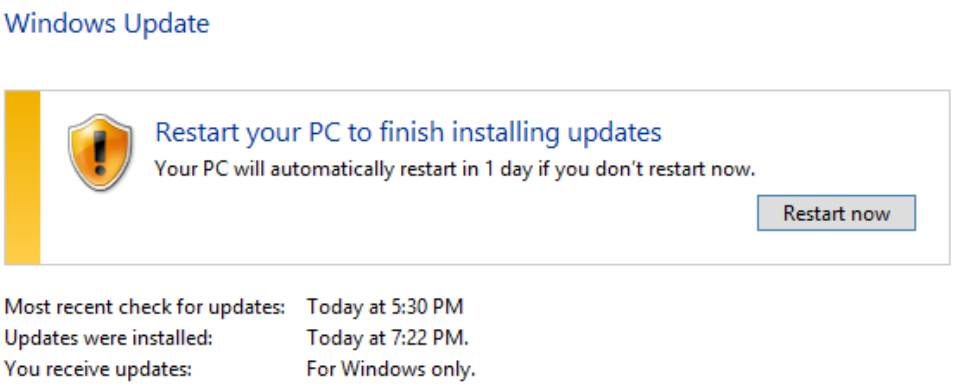
Click on “Turn on automatic updates.”



Click on “# important updates are available.”

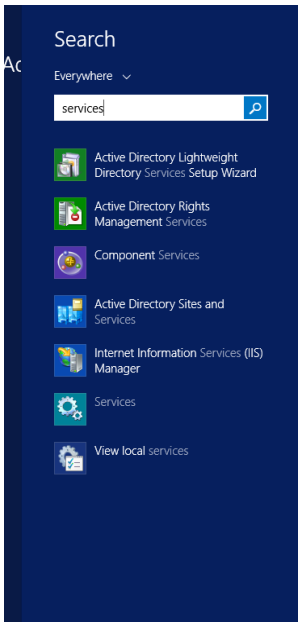


Click on “Install” in the lower right-hand corner. The updates will begin downloading. Wait for the updates to install.

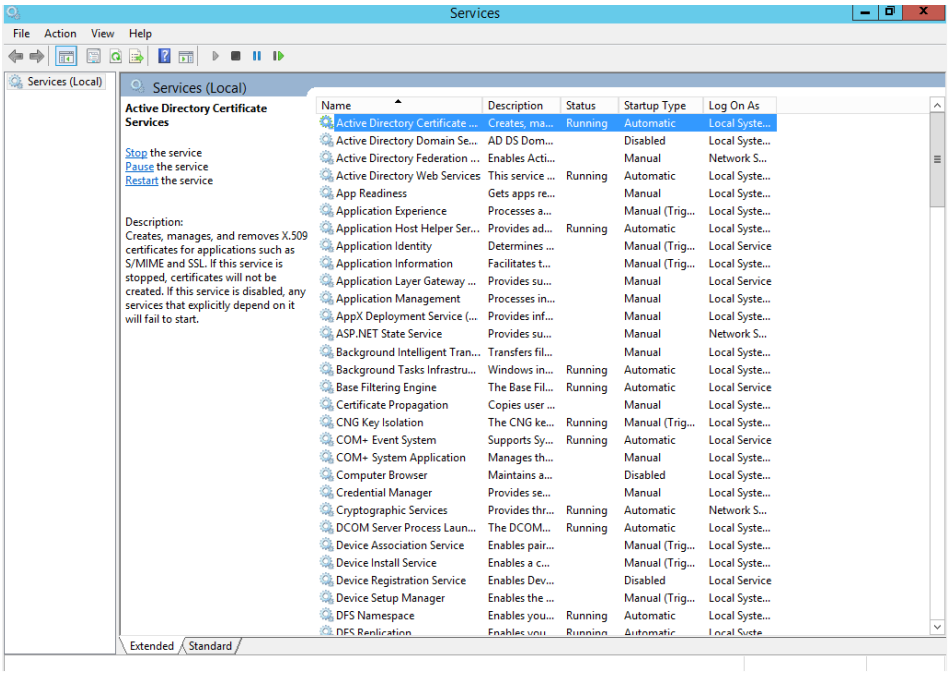


After the updates are installed, click on “Restart now”.

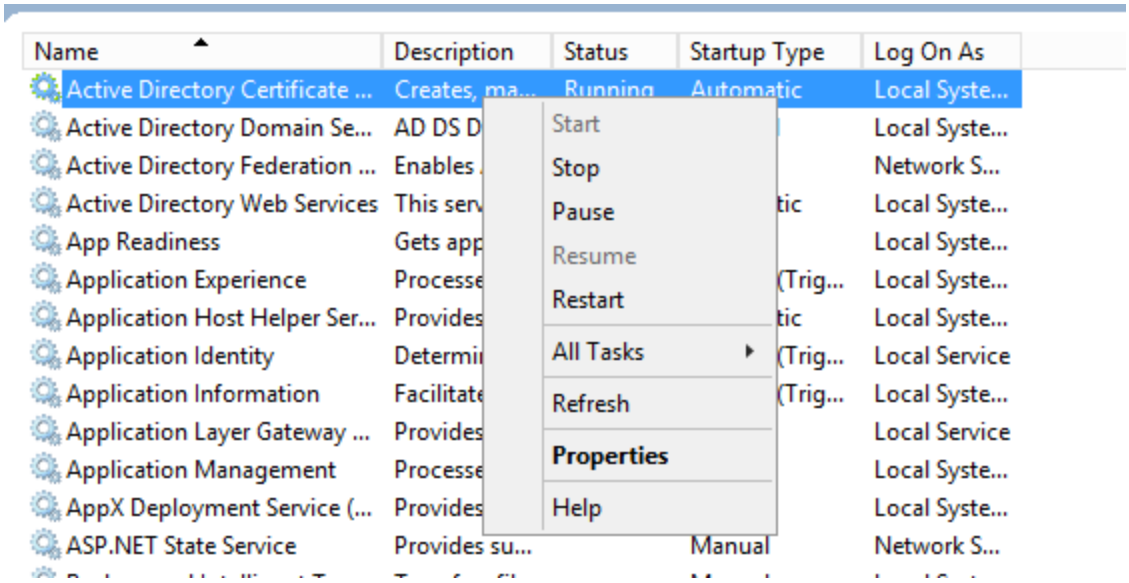
3. **Check services, and stop all services that are not necessary (Be mindful if there are any services that are needed for scoring)**



Search “Services” in Windows and click on the Services application.

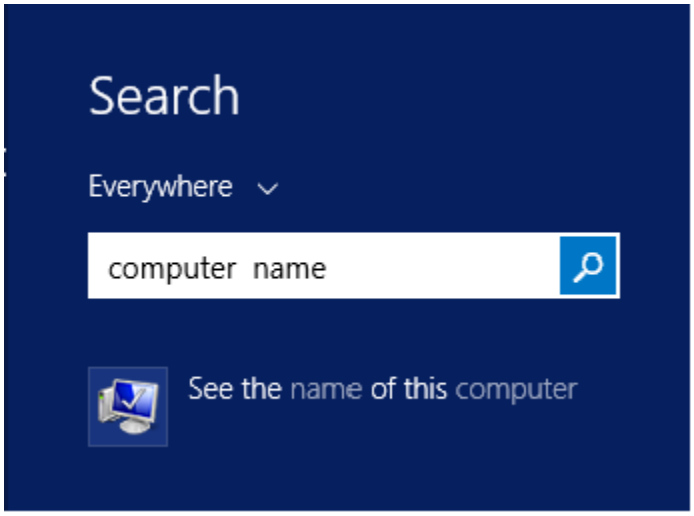


Find Services that are not needed.

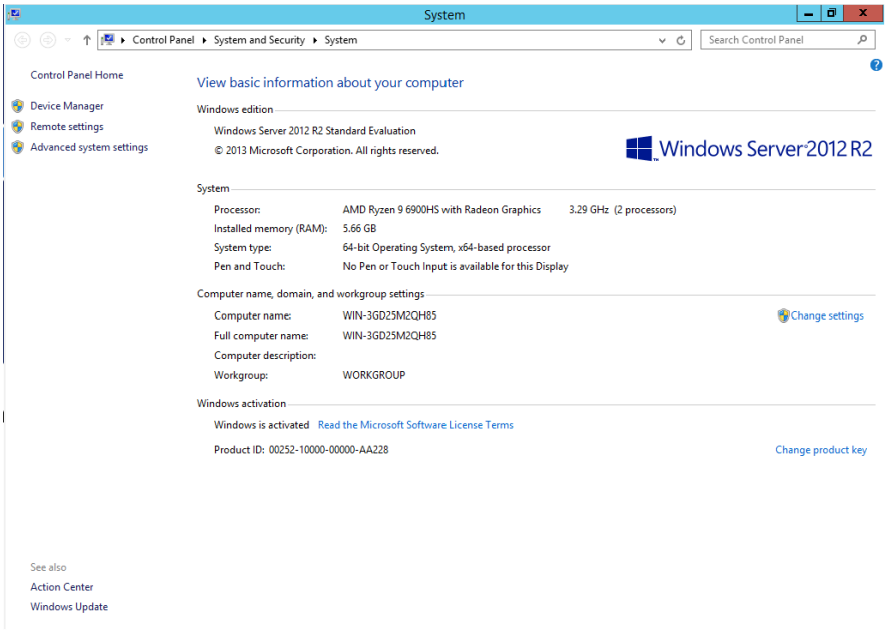


To stop a service right click and click on the “Stop” button.

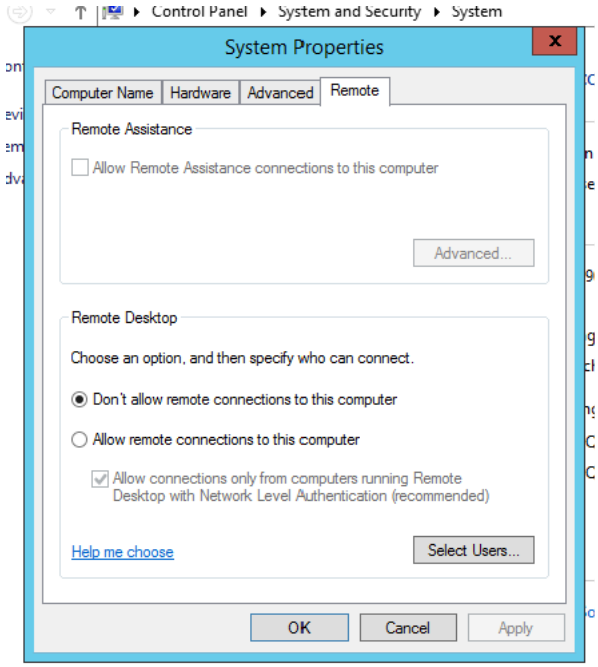
4. **Disable Remote Desktop**



Search for “computer name” in the Windows search bar. Click on “See the name of this computer”.

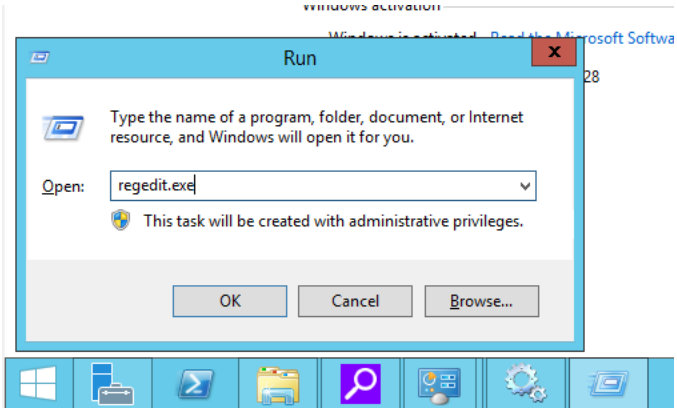


Click on “Change settings” in the middle right of the screen.

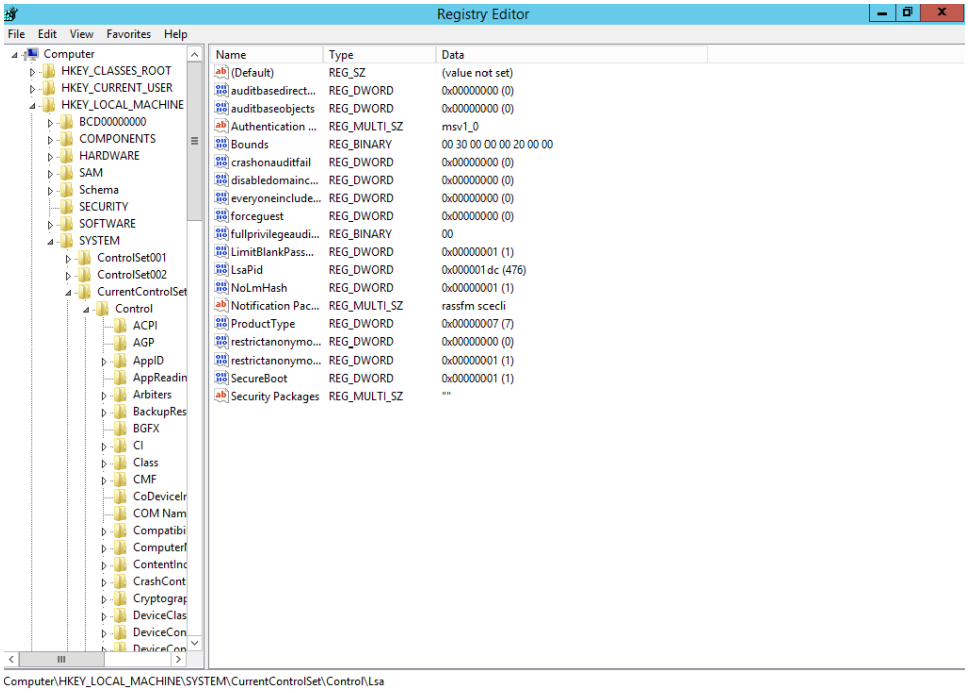


Navigate to the “Remote” tab in the System Properties window. Make sure that Remote Desktop is set to “Don’t allow remote connections to this computer”.

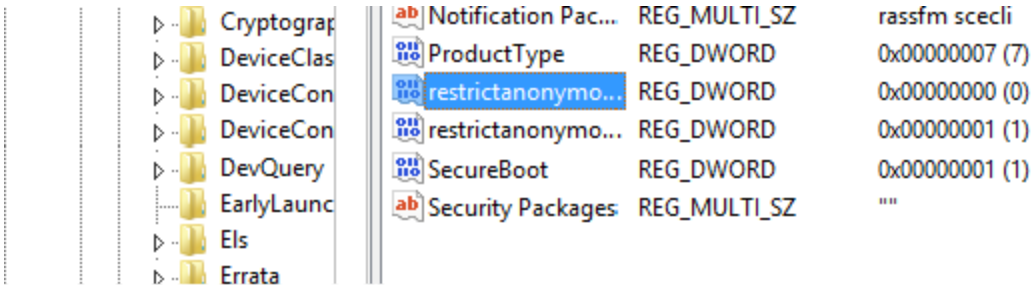
5. Restrict Anonymous Access



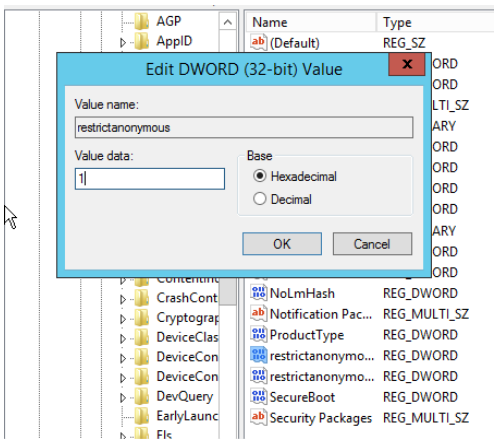
Press windows key+R on your keyboard. In the “Run” window type in regedit.exe and click OK.



Follow the path: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.

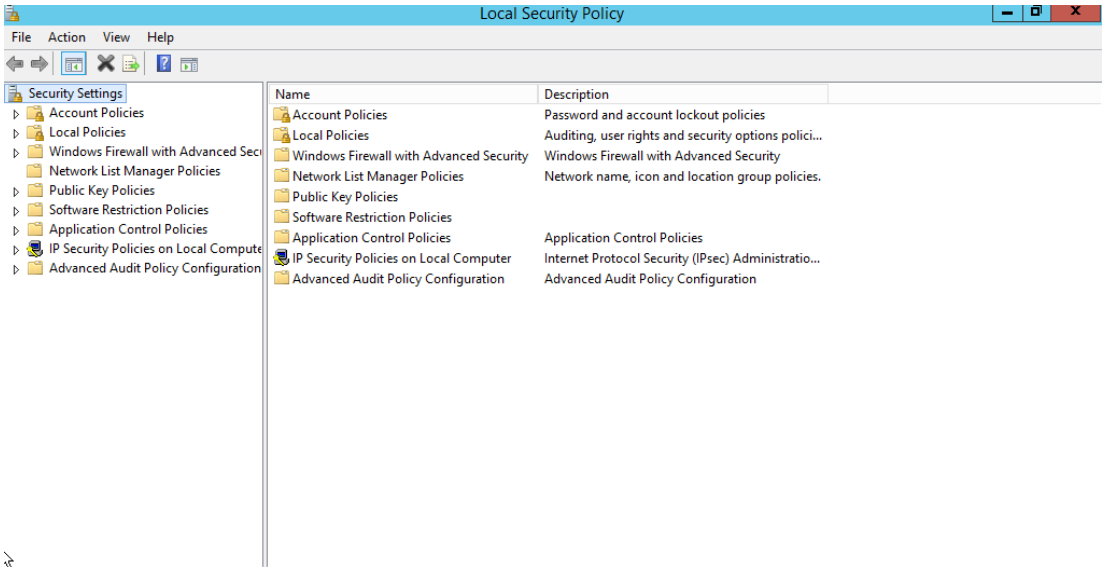


You should find a registry value named “restrictanonymous”.

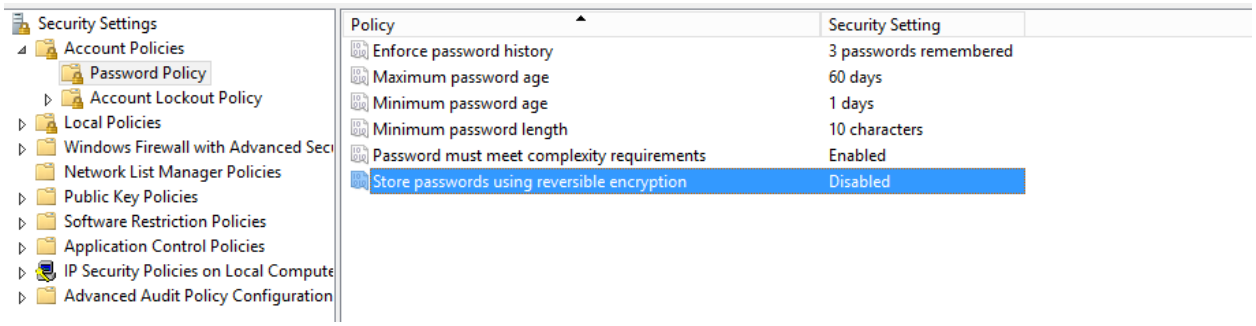


Double click RestrictAnonymous and set the value to 1 and click OK. Reboot if necessary.

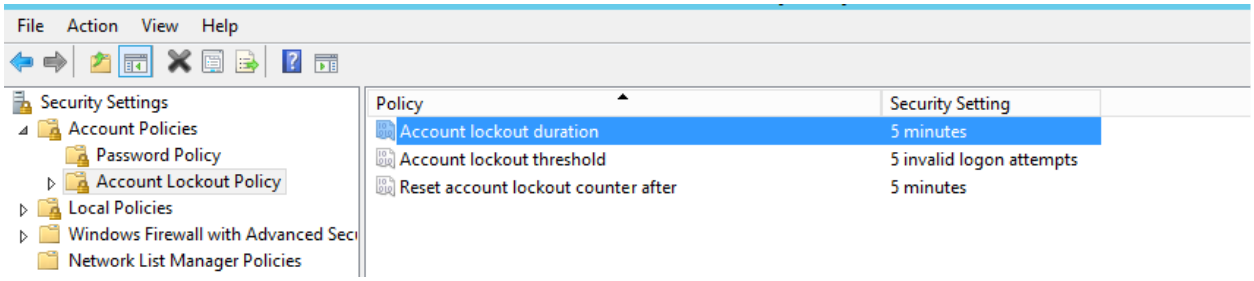
6. Set Account Policies for Password Policy & Account Lockout Policy



In Windows navigate to “Local Security Policy” and open the application.



Navigate to Account Policies-> Password Policy. The most important policy is to make sure “Store passwords using reversible encryption” is set to “Disabled” and that “Password must meet complexity requirements” is set to “Enabled”. Follow the above screenshot for the rest of the configurations (may be subject to change).



Configure Account Lockout Policy, the account lockout policy should be configured as followed:

Account lockout duration — 5 minutes

Account lockout threshold — 5 failed attempts

Reset account lockout counter — 5 minutes

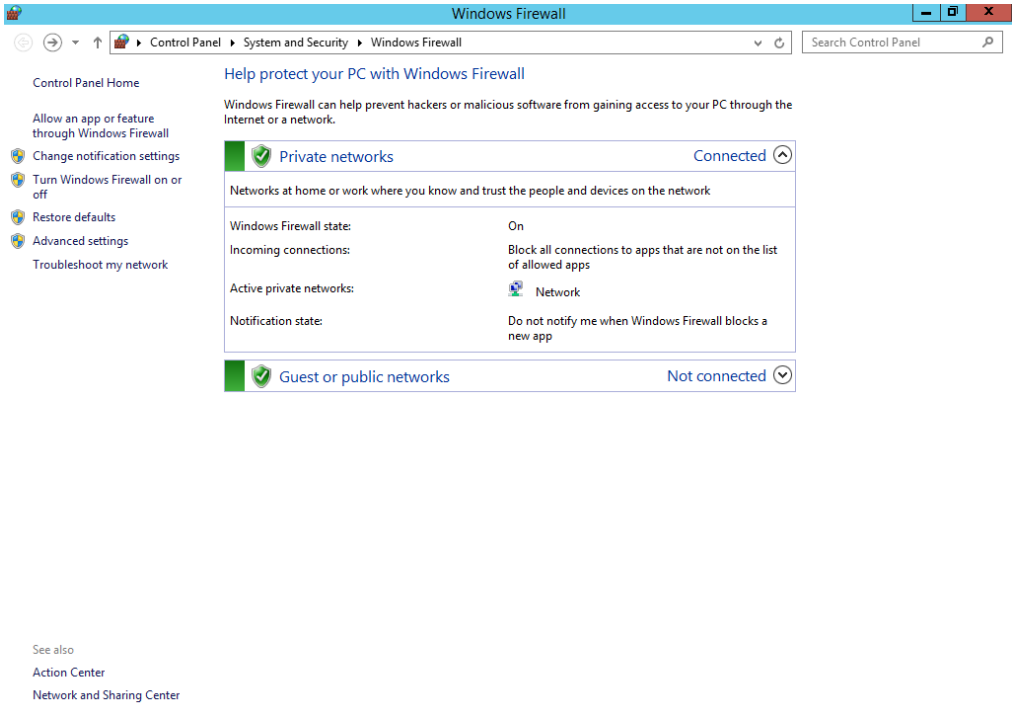
*May be subject to change.

7. Disable IE password cache

To disable password caching, follow these steps:

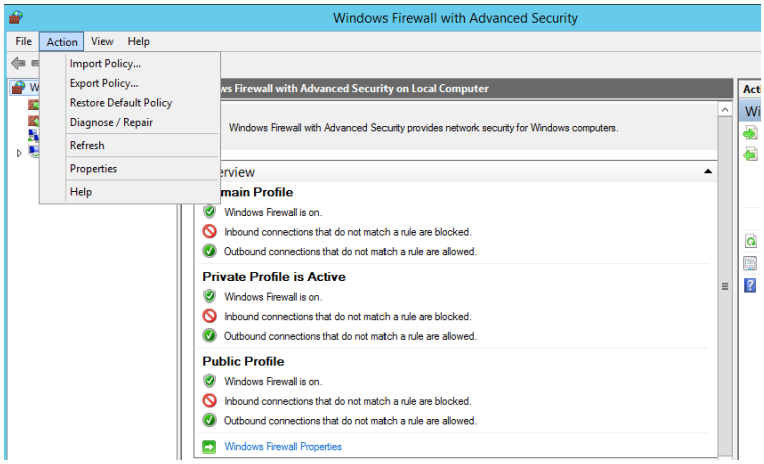
1. Click **Start**, click **Run**, type *regedit*, and then click **OK**.
2. Locate and then click the following registry subkey:
   `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings`
3. On the **Edit** menu, click **New**, and then click **DWORD Value**.
4. Type *DisablePasswordCaching* to name the new registry entry, and then press ENTER.
5. Right-click **DisablePasswordCaching**, and then click **Modify**.
6. Make sure that the **Hexadecimal** option button is selected, type *1* in the **Value data** box, and then click **OK**.
7. Quit Registry Editor.

8. Enable Firewall Logging

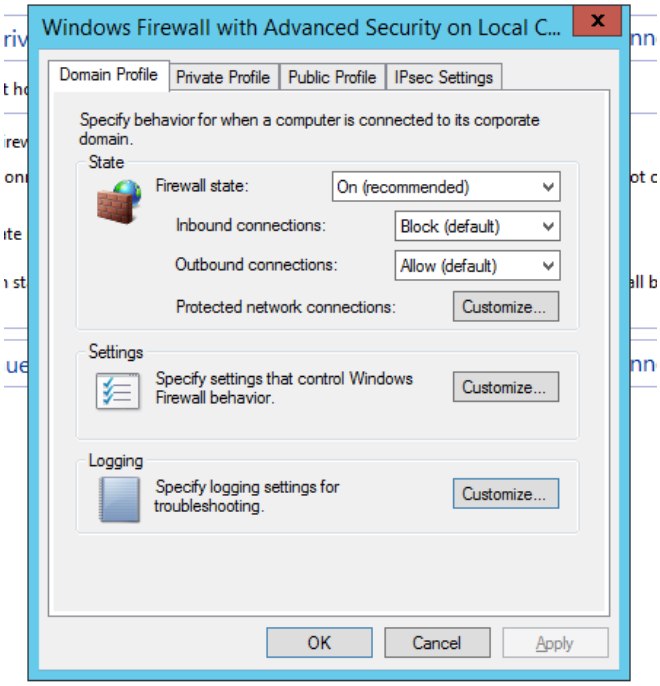


In Windows search type in “Windows Firewall”, in the left hand side click on “Advanced settings”.

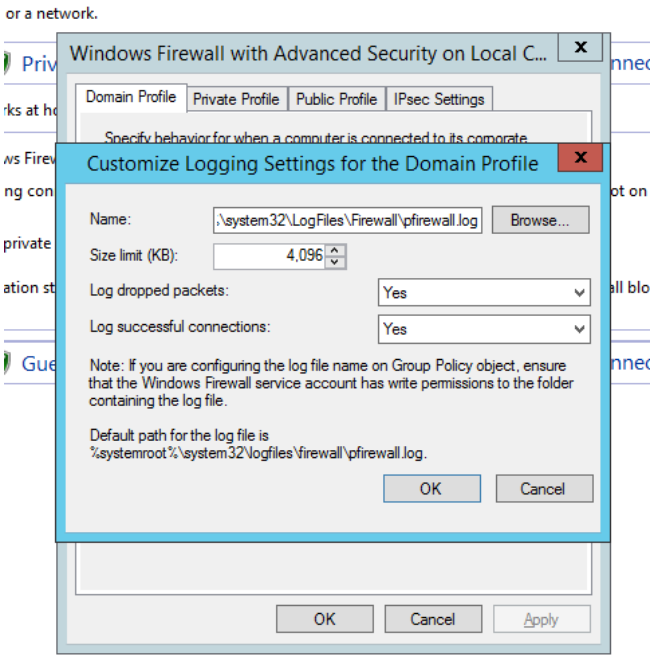
Created By: Will Novotny



In Windows Firewall with Advanced Security in the top left click Actions->Properties.

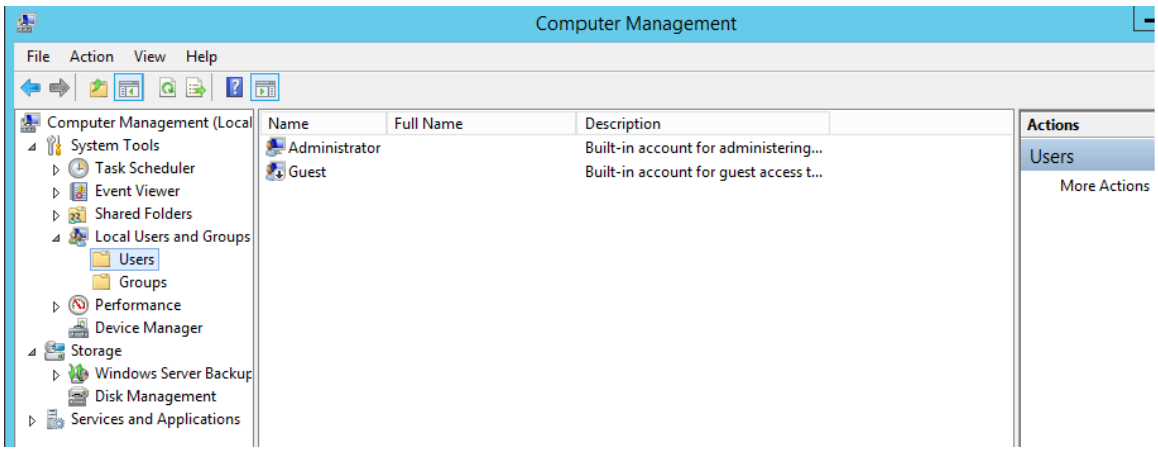


On the "Domain Profile" tab, click "Customize" under Logging.



On the "Log dropped packets" drop down, select "Yes" and on the “Log successful connections, select “Yes. Then click OK and OK.

9. **Install Wireshark. This is to watch the Palo Alto for shenanigans (Xtra layer of protection and eyes)**
10. **Check for users with privilege escalation**

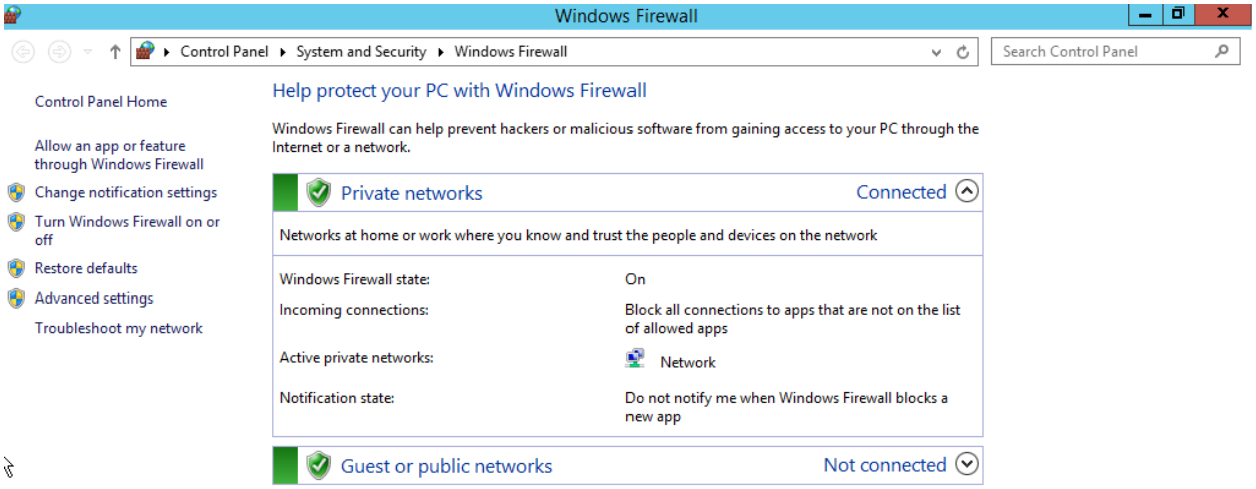


Navigate to Computer Management->Local Users and Groups->Users. Look through each user to see if they are in the administrators group, and any other suspicious privilege assigned to them.

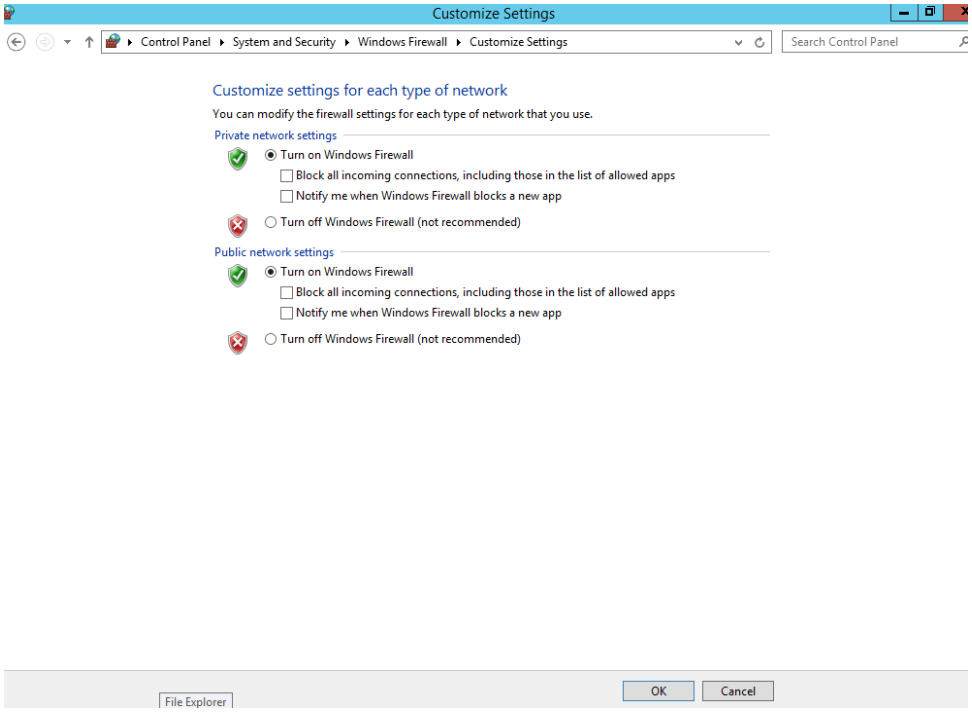
Accounts: Rename administrator account = pick something unique

Accounts: Guest account status - Disabled

11. Turn on Windows Firewalls



Navigate to Windows Firewall, on the left-hand corner click “Turn Windows Firewall on or off”.



Ensure that the Private and Public Firewall is turned on.

12. Disable SSH and Telnet

-Click on the Start button and select Control Panel.

-In the Control Panel window, click on the System and Security option.

-In the System and Security window, click on the Windows Firewall option.

-In the Windows Firewall window, click on the Advanced Settings option.

-In the Windows Firewall with Advanced Security window, click on the Inbound Rules option in the left pane.

-In the Inbound Rules section, locate the port you want to disable and right-click on it.

-From the context menu, select Disable Rule.

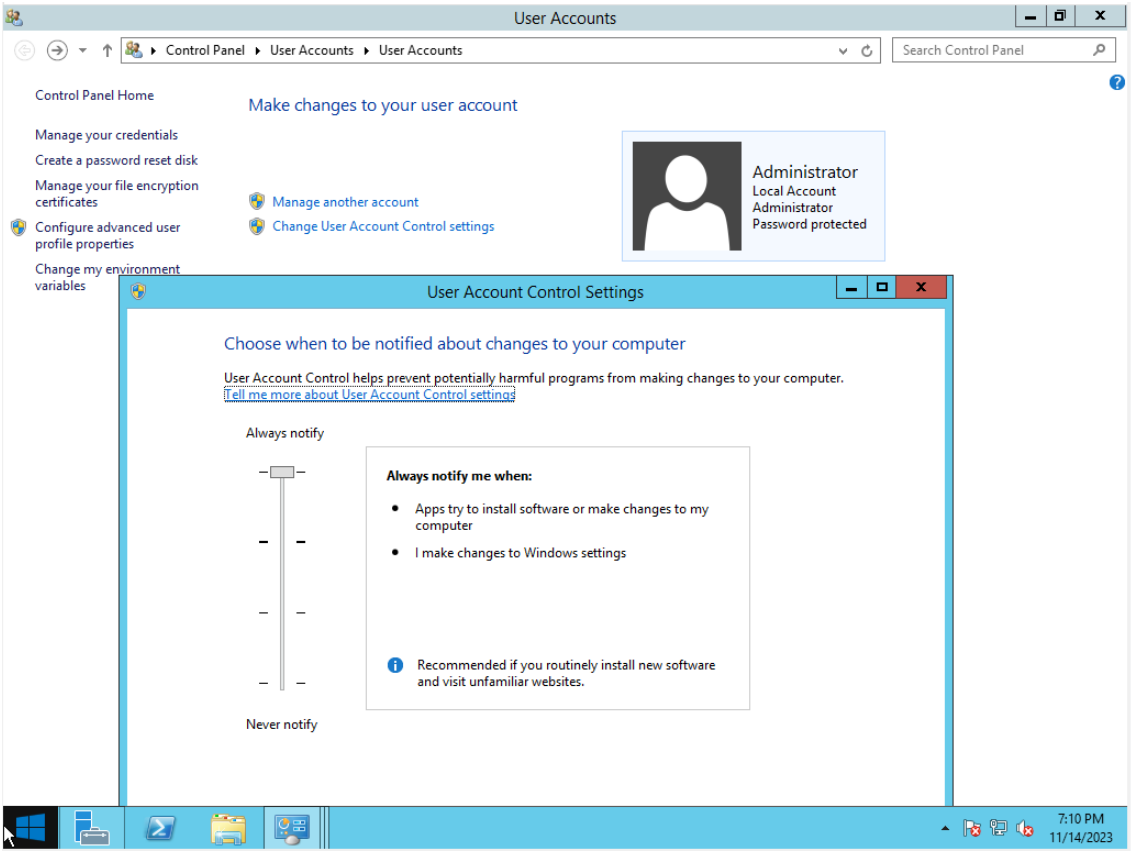
-Repeat the steps for the Outbound Rules section if you want to disable the same port for outbound traffic.

13. To disable root login in Windows Server 2012, you need to follow these steps:

1. Click the "Start" button and select "Server Manager."
2. In the "Server Manager," select "Local Server."
3. In the Properties section, scroll down and find the "Remote Management" row.
4. Click "Configure Remote Management" to open the settings.
5. Under the "Basic" settings, turn off "Enable Remote Management of this server."
6. Click "Save changes."

Note: Disabling root login in Windows Server 2012 does not actually disable the root user account. However, by disabling remote management, you are effectively preventing unauthorized users from logging in as the root user remotely. It is recommended to create a separate non-root user account for daily use and perform administrative tasks using the Run as administrator option.

14. Change User Account Control Settings



Navigate to User Accounts->Change User Account Control Settings, set the bar to the highest.

15. Install and enable anti-virus software

https://www.malwarebytes.com/mwb-download

*Any free open source anti-virus software will work.

Created By: Will Novotny

****Document all IP addresses and passwords, so everyone has access to machine****

IF done early, talk to the team to assist anyone who needs it.

Refer to the book BTFM starts at Ch 2 for hardening, for more hardening techniques.

Stay POSITIVE, Communicate, and Dominate.