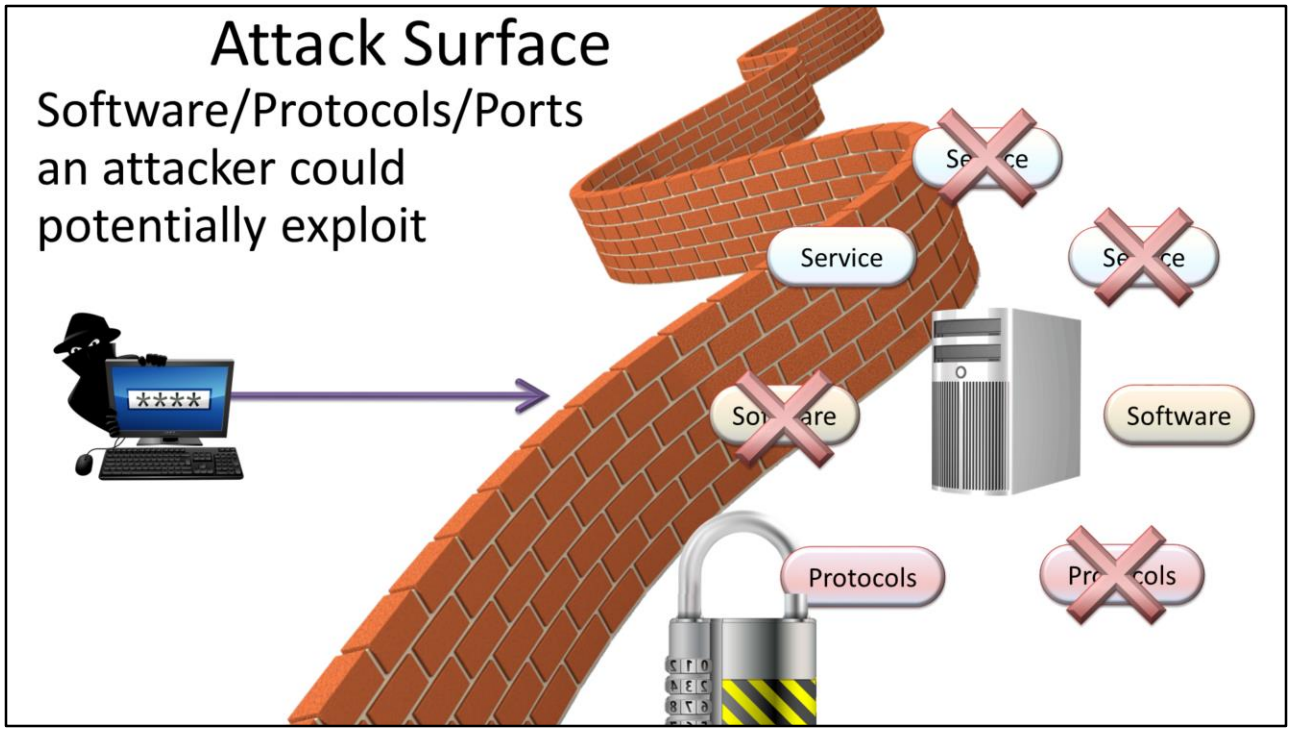
Security Configuration Wizard

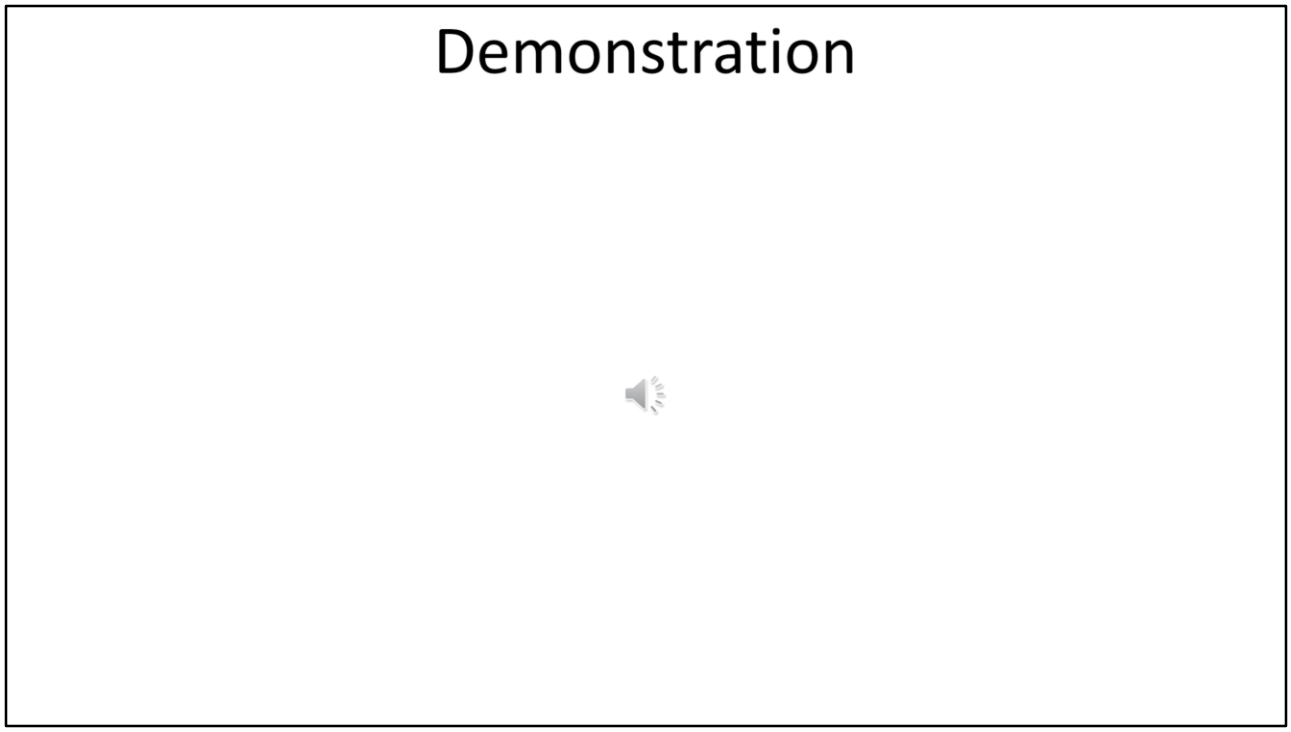
For the free video please see http://itfreetraining.com/70-640/security-configuration-wizard

The Security Configuration Wizard is a simple wizard that allows the administrator to tighten up security in Windows. This video looks how to run the wizard and configure the settings on multi computers.



Attack Surface

The attack surface on a computer system or device is the amount of software, protocols and ports that are open for use. If an exploit was found in any of these, an attacker could potentially use these to compromise the system. To reduce the attack surface, any software, protocols or ports that are not in use should be removed or disabled. Even if an exploit is not known today, tomorrow an exploit could be found that could be used to compromise your system. A firewall should also be used to increase the security of the system. Products like Security Configuration Wizard analyze Windows and gives the administrator configuration options that they can use to improve the security of their system. The process of increasing the security of a system is also known as hardening.



Demonstration
Security Configuration Wizard is available from the start menu under Administrative Tools. If you have additional software on the system that opens ports, you should run this software before you start the wizard so the wizard can detect these open ports.

The wizard will then go through different areas of the system list below.
Role-Based Service Configuration: Analyzes security settings depending on what roles are installed on the server. If you plan to add the role later, tick the option so the wizard can suggest settings for you.
Network Security: Settings regarding network security like firewall settings.
Registry Settings: Basic registry settings relating to authentication and security options for file sharing.
Audit Policy: Configures auditing settings to best audit changes to the system. There is also an option to apply an additional security template. This will greatly increase the security of your system. If you want to remove the settings applied from a security template later on you will need to use the roll back feature found at the start of the wizard.

Once you finish the wizard, these settings can be saved and applied to any computer.

The complete security template can be converted to a Group Policy Object using the following command.
scwcmd transform /p:(XMLFile) /g:(GPOName)

In The Real World

- Identify high risk servers
  - Internet accessible
- Security VS Cost
  - Lost productivity
  - Helpdesk calls

In the real world
Often a balance needs to be found between security and cost. If you apply to many security settings this can increase the number of helpdesk calls and reduce productivity. It is best to maximize your time on high risk computers like computers that are directly connected to the internet.

See http://YouTube.com/ITFreeTraining or http://itfreetraining.com for our always free training videos. This is only one video from the many free courses available on YouTube.

References
"MCTS 70-640 Configuring Windows Server 2008 Active Directory Second edition" pg 339-345
"Security Configuration Wizard" http://technet.microsoft.com/en-us/library/cc754997.aspx