Additional Training Topics

© Air Force Association

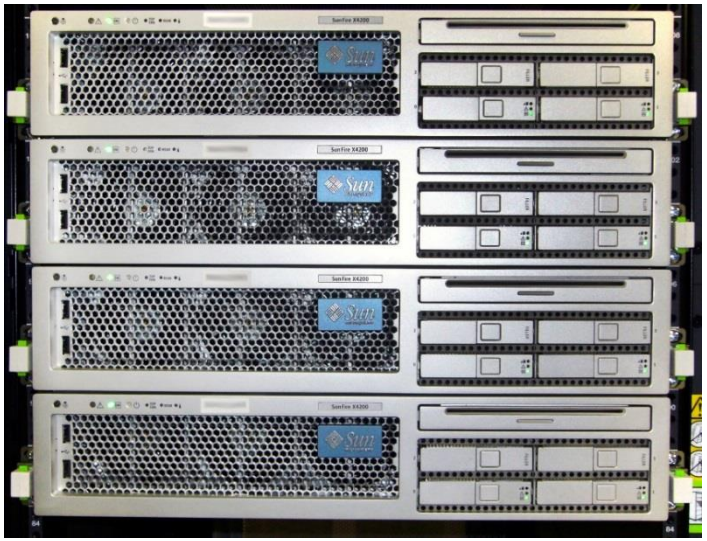
RON WOERNER, CP-VI MENTOR OF THE YEAR, TIPS

- Familiarize yourself with Microsoft Windows tools and resources
  - Microsoft SysInternals Suite Applications that help troubleshoot Windows issues and administer the operating system.
  - Windows God Mode. Windows 7 and 8 feature that allows all Control Panel and Policy functions from one folder on the desktop.
  - Microsoft Baseline Security Analyzer (MBSA) and Security Essentials
  - How to Geek School contains a number of tutorial videos on securing Windows and using SysInternals tools.
  - BleepingComputer Security Tutorials & Tools is another site with information and tools that will help.
- Familiarize yourself with the Ubuntu Linux Operating System
  - The official Ubuntu Desktop Guide is available at https://help.ubuntu.com/12.04/ubuntu-help/index.html. This will help introduce you to the operating system.
  - Fosswire has a couple of cheat sheets. These show commands to run on a terminal / command line.
    - http://www.cheat-sheets.org/saved-copy/fwunixref.pdf
    - http://www.cheat-sheets.org/saved-copy/ubunturef.pdf
- Make sure your team documents everything they do on the images
- Get hands-on practice with virtual images using your MSDN account
- Have students who are not “hands on” the images during competition are taking notes, doing research, and observing the students who are “hands on”
- Have fun!

© Air Force Association

WEB SERVERS

- A web server stores, processes, and delivers web pages to clients using HTTP
  - Definition and diagrams of a web server: http://www.pcmag.com/encyclopedia/term/54342/web-server
- The leading web server software is the Apache HTTP Server
  - Information on Apache: http://httpd.apache.org/ABOUT_APACHE.html



Source: http://upload.wikimedia.org/wikipedia/commons/f/f6/SunFire-X4200.jpg

© Air Force Association

FILE SYSTEMS

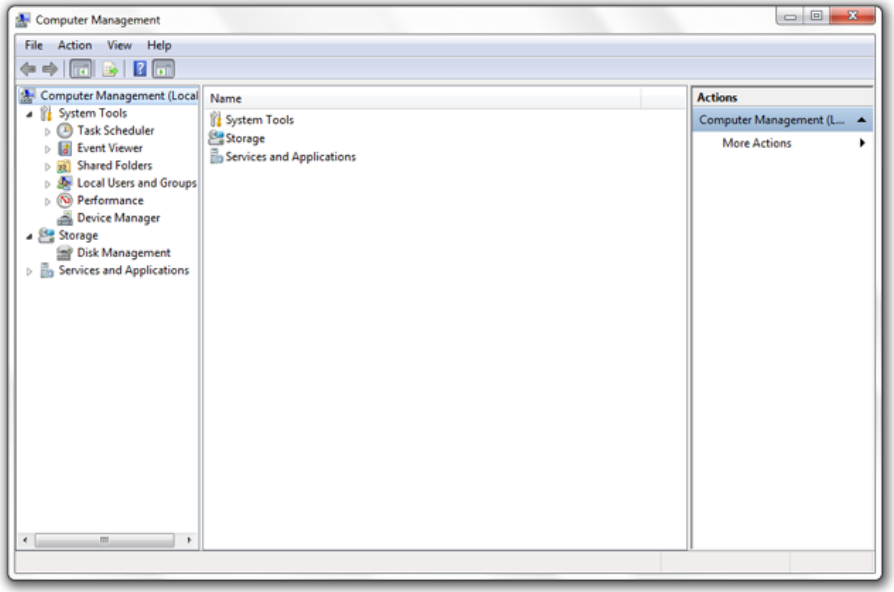
- Windows operating systems typically use one of two file systems to organize data on hard discs
  - FAT32
    - Used in older operating systems such as Windows 95 and 98
  - NTFS
    - Modern file system currently used in Windows XP onward
- Comparison of FAT32 and NTFS: http://windows.microsoft.com/en-us/windows-vista/comparing-ntfs-and-fat-file-systems

Ubuntu Tip: Linux systems use the Ext2, Ext3, or Ext4 file systems: https://help.ubuntu.com/community/LinuxFilesystemsExplained

© Air Force Association

MICROSOFT MANAGEMENT CONSOLE

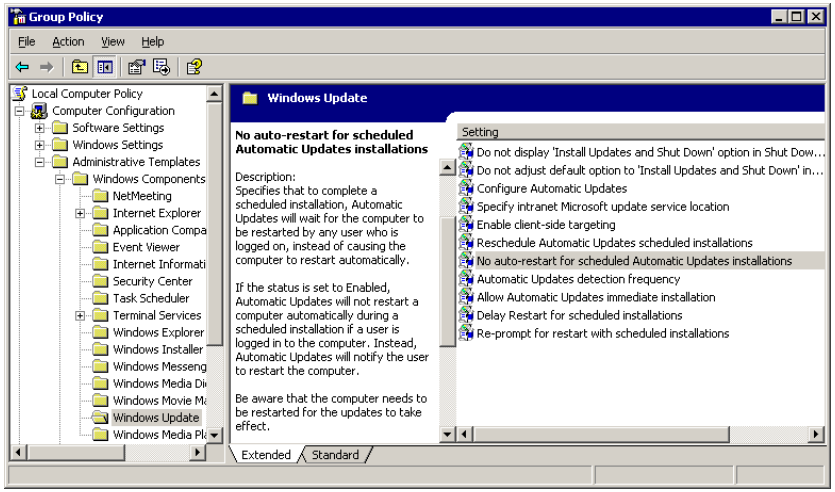
- MMC is a Windows component that allows customization and configuration of a system via GUI objects called snap-ins.
- Common snap-ins include:
  - Computer Management
  - Group Policy Management
  - Services
  - Performance
  - Event Viewer
- Microsoft's MMC guide:
http://technet.microsoft.com/en-us/library/bb742442.aspx



© Air Force Association

GROUP POLICY

- Group Policy: Settings for groups of users and computers, including those regarding registry-based policy, security, computer startup and shutdown, and logon and logoff
  - Details on Microsoft group policy: http://technet.microsoft.com/en-us/library/bb742376.aspx
- Some useful settings may be:
  - Not displaying last user name on login screen
    - How to: http://support2.microsoft.com/kb/310125
  - Requiring Ctrl Alt Del before signing on
    - How to: http://support.microsoft.com/kb/308226



Source: http://blog.codinghorror.com/content/images/uploads/2005/05/6a0120a85dcdae970b0128776fbe89970c-pi.png

© Air Force Association

NT LAN MANAGER (NTLM)

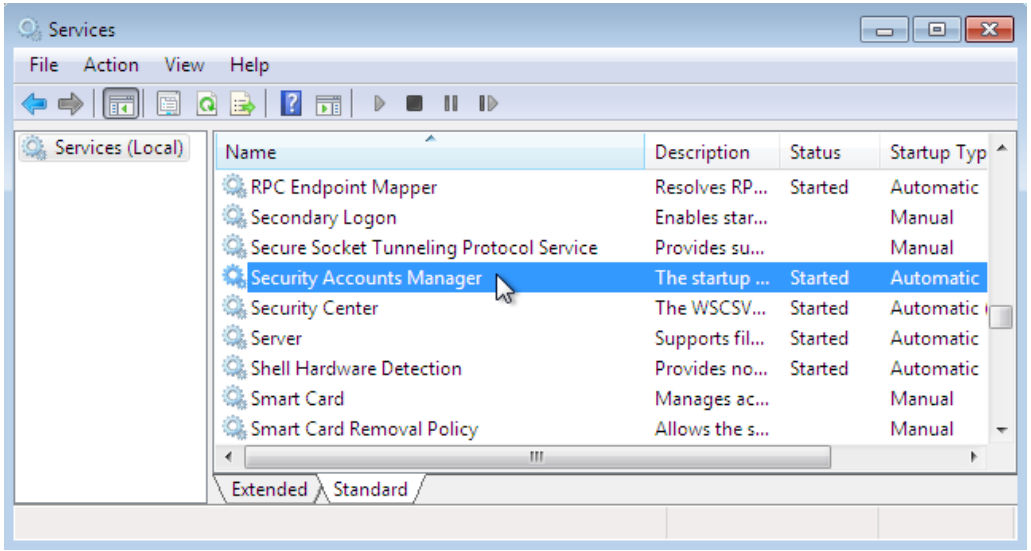
- Authentication protocol
  - Authentication protocol confirms the identity of any user logging on to a domain or access network resources
  - NTLM is a Microsoft authentication protocol: http://msdn.microsoft.com/en-us/library/windows/desktop/aa378749(v=vs.85).aspx
- Password hashing
  - Method of taking a variable-length password and creating a cryptic, fixed-length password from it
  - Details on password hashing: http://security.blogoverflow.com/2013/09/about-secure-password-hashing/
  - LanMan Hash is a password hashing function of NTLM
    - Details on the security risk of LanMan Hash: http://www.microsoft.com/security/sir/strategy/default.aspx#!password_hashes

Ubuntu Tip: Ubuntu 8.10 and later use salted SHA-512 based password hashes: https://wiki.ubuntu.com/Security/Features

© Air Force Association

SECURITY ACCOUNT MANAGER (SAM)

- The Security Account Manager (SAM) is a Windows database that stores user accounts and security descriptors for users on the local computer
  - Information on the SAM: http://searchenterprisedesktop.techtarget.com/definition/Security-Accounts-Manager
  - Possible security issues: https://technet.microsoft.com/en-us/library/security/ms14-016.aspx

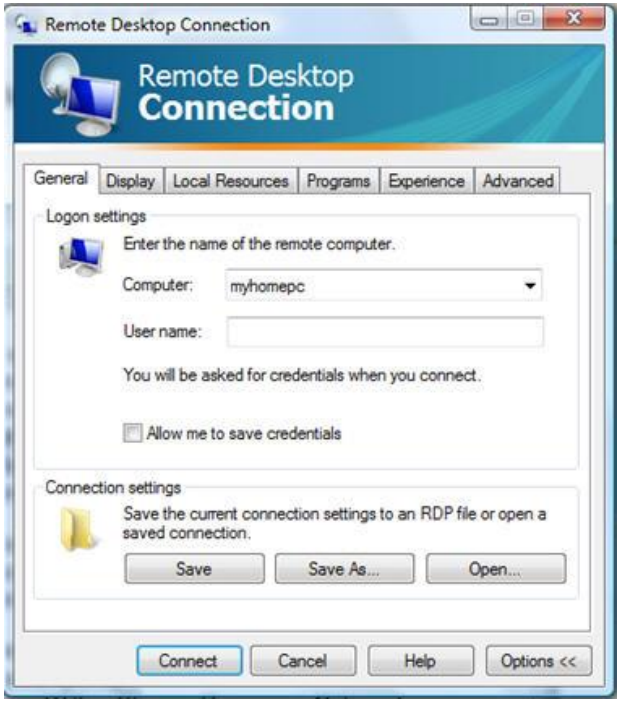


Source: http://computerstepbystep.com/wpimages/wp8863e5cd_01.png

© Air Force Association

SHARING SYSTEMS AND REMOTE CONNECTIONS

- Remote connections are ways of sharing systems.
- Examples:
  - Virtual Network Computing (VNC)
    - VNC allows you to share and give control of your desktop to another user
    - VNC variants and applications: http://ipinfo.info/html/vnc_remote_control.php
  - Remote Desktop
    - Similar to VNC, Remote Desktop Protocol (RDP), allows a user to control a remote system
    - Using RDP: http://windows.microsoft.com/en-us/windows/connect-using-remote-desktop-connection#connect-using-remote-desktop-connection=windows-7



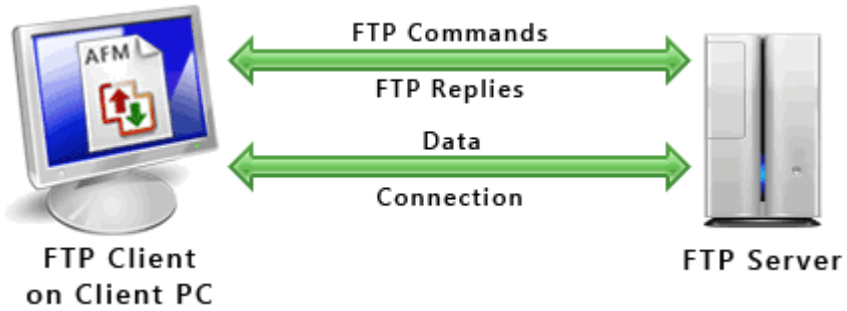
Source: http://blog.tmcnet.com/blog/tom-keating/images/remote-desktop-general-tab.jpg

Ubuntu Tip: If using a Gnome desktop, Remote desktop is easy in Ubuntu: http://www.makeuseof.com/tag/ubuntu-remote-desktop-builtin-vnc-compatible-dead-easy/

© Air Force Association

FTP, TFTP, AND SFTP

- The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another over the Internet
  - FTP FAQ: http://windows.microsoft.com/en-us/windows-vista/file-transfer-protocol-ftp-frequently-asked-questions
- Secure File Transfer Protocol works similarly to FTP but is more secure
  - How to use SFTP: https://www.digitalocean.com/community/tutorials/how-to-use-sftp-to-securely-transfer-files-with-a-remote-server
- Trivial File Transfer Protocol (TFTP) is a simplified version of FTP
  - Details on TFTP: http://compnetworking.about.com/od/ftpfiletransfer/g/tftp-trivial-file-transfer-protocol.htm

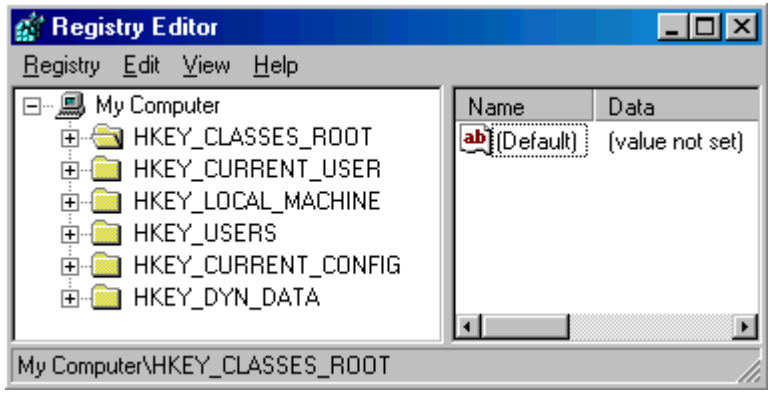


Source: http://www.deskshare.com/resources/articles/images/ftp-protocol.gif

© Air Force Association

WINDOWS REGISTRY

- The registry is a hierarchical database that stores configuration settings and options
  - WARNING: If you do not know what you are doing, editing the registry can cause serious problems that may require you to reinstall Windows
  - Explanation of the registry and how to make edits: http://pcsupport.about.com/od/termsr/p/registrywindows.htm
  - Managing remote access to the registry: http://support2.microsoft.com/kb/314837



Source: http://www.computerhope.com/reg1.gif

Ubuntu Tip: There is no registry in Ubuntu *per se*, but if using a GNOME desktop, dconf is similar: https://wiki.gnome.org/action/show/Projects/dconf?action=show&redirect=dconf

© Air Force Association

WINDOWS COMMAND PROMPT

- Like Linux, the command line in Windows allows you to enter commands without a GUI.
- Sample commands are:
  - Ipconfig is used to view or modify a computer's IP addresses
  - Bcedit is used to view or make changes to Boot Configuration Data
  - Cmd starts a new instance of the command line interpreter
  - Convert is used to change FAT32 formatted volumes to NTFS
  - Nslookup is used to display the hostname of an entered IP address
- Opening the command prompt: http://windows.microsoft.com/en-us/windows-vista/open-a-command-prompt-window
- Detailed list of commands: http://pcsupport.about.com/od/commandlinereference/tp/windows-7-commands-p1.htm

© Air Force Association

PORTS AND PROTOCOLS

- TCP/IP is a set of communication protocols
  - Transmission Control Protocol (TCP) provides reliable, ordered, and error-checked delivery of data
  - User Datagram Protocol (UDP) uses a simple connectionless transmission model
- TCP/IP applications send data to specific ports to help computer systems understand what to do with the data that flows into them.
- Examples of c

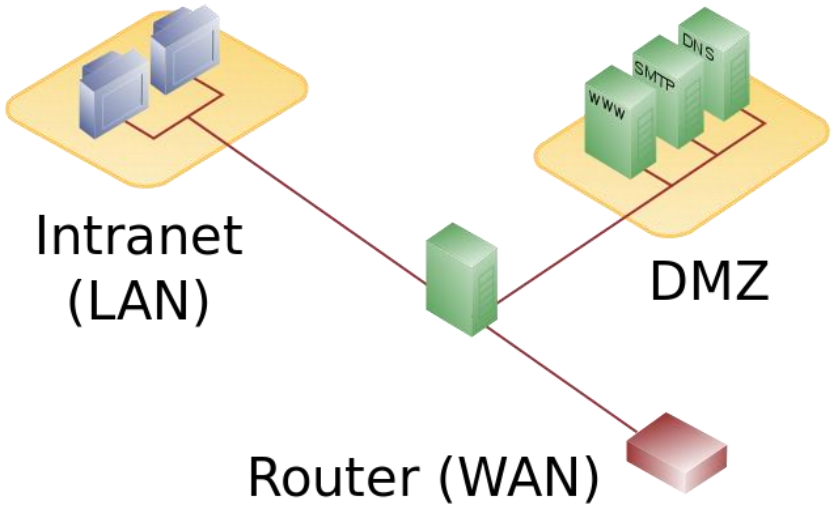
Service	Protocol	Port
FTP	TCP	20, 21
TFTP	UDP	69
HTTP	TCP	80
HTTPS	TCP	443
RDP	TCP	3389

- Open ports can be a security risk by allowing attackers into your system
  - Firewalls typically block unnecessary ports, but it is unwise to blindly rely on one
  - Information on determining which ports are open and which should be closed: http://www.techrepublic.com/article/lock-it-down-develop-a-strategy-for-securing-ports-on-your-servers/

© Air Force Association

DEMILITARIZED ZONE (DMZ)

- A DMZ acts as a gateway to the public internet that acts as an additional layer of security to an organizations local area network
  - An external attacker only has direct access to equipment in the DMZ
- A typical DMZ may look like the following (the unlabeled green icon in the center is a firewall):



Source:
http://en.wikipedia.org/wiki/DMZ_(computing)#/media/File:DMZ_network_diagram_1_firewall.svg

© Air Force Association

DISTRIBUTED COMPONENT OBJECT MODEL (DCOM)

- DCOM is a technology for communication among software components distributed across networked computers
  - In depth information on DCOM: https://www.princeton.edu/~achaney/tmve/wiki100k/docs/Distributed_Component_Object_Model.html
  - Mitigating DCOM Vulnerabilities: http://technet.microsoft.com/en-us/library/dd632946.aspx

© Air Force Association