AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT SEVEN

Microsoft Windows Security Tools

www.uscyberpatriot.org

Learning Objectives

- Participants will understand where basic Windows operating system security tools are located
  - Control Panel
  - Administrative Tools
  - Action Center
  - Windows Firewall
  - Windows Update
- Participants will learn how to manage Windows accounts and how accounts can affect security

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

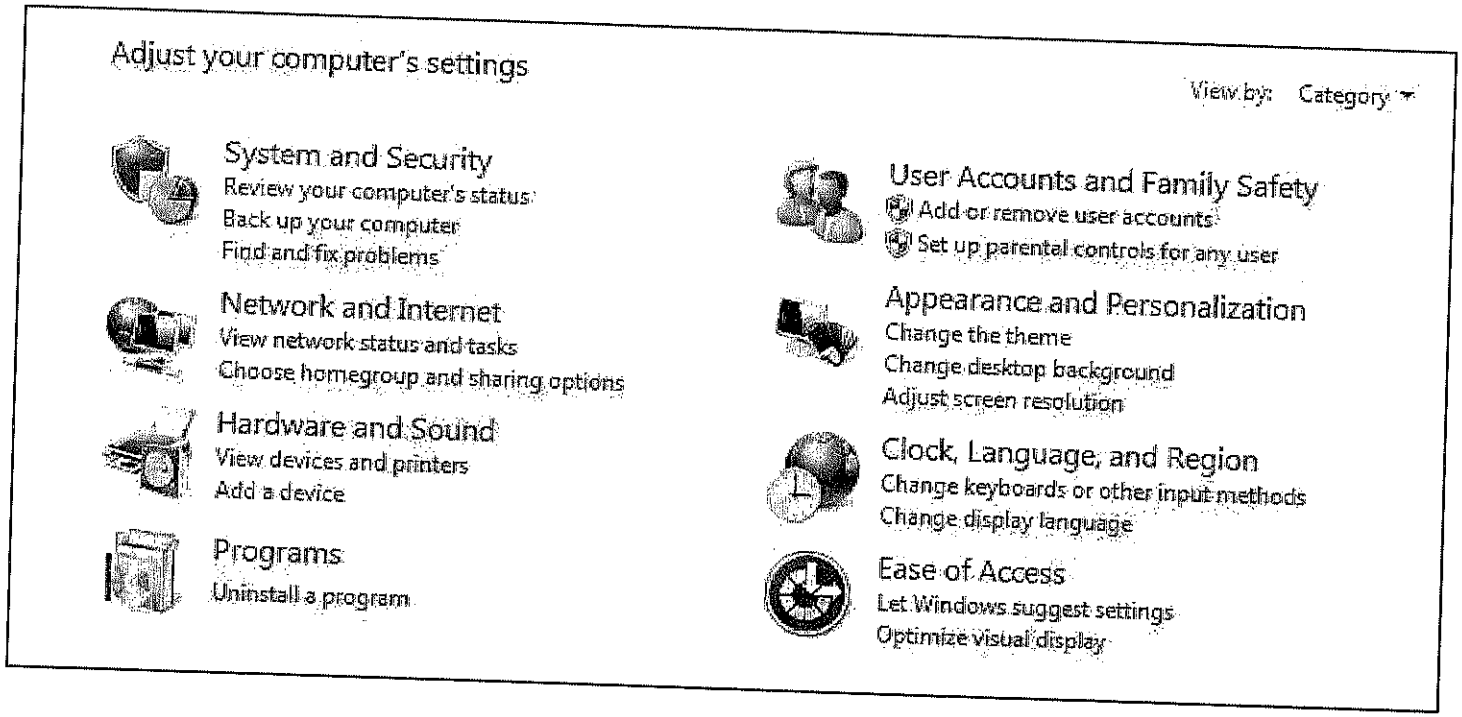
SECTION ONE

Basic Security Policies and Tools

www.uscyberpatriot.org

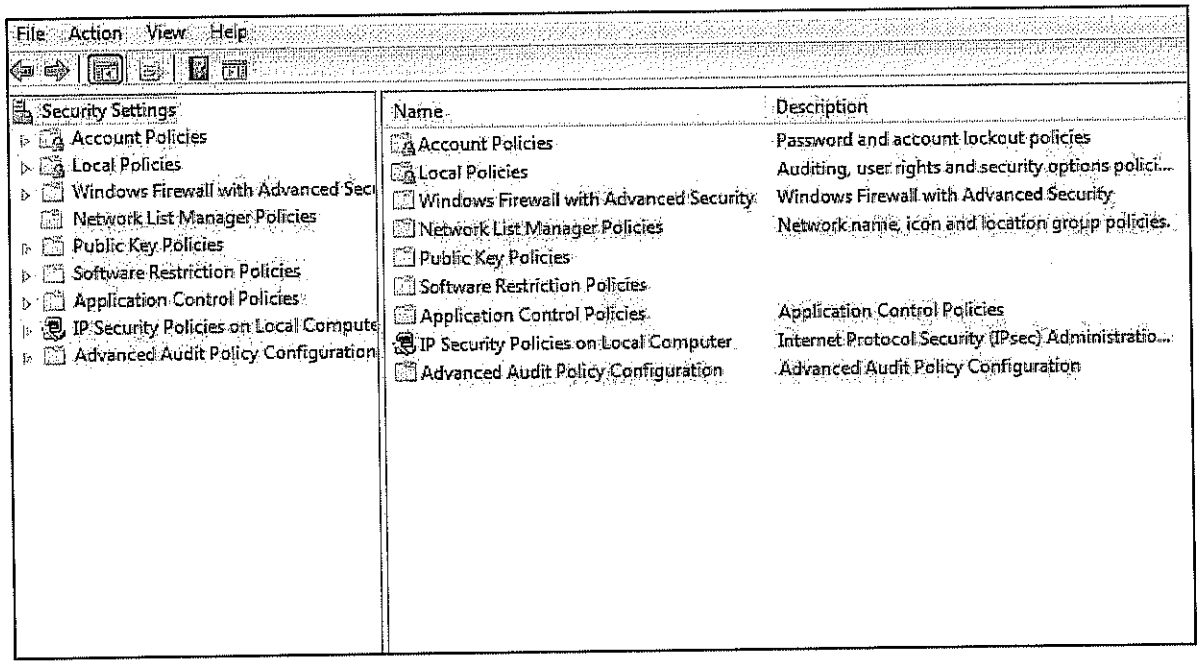
Control Panel

- Where many of the basic system changes and configurations can be set within a Windows operating system
- Click Start → Control Panel



Basic Local Security Policies

- Controls security settings on user computers within a network
- Click System and Security → Administrative Tools → Local Security Policy



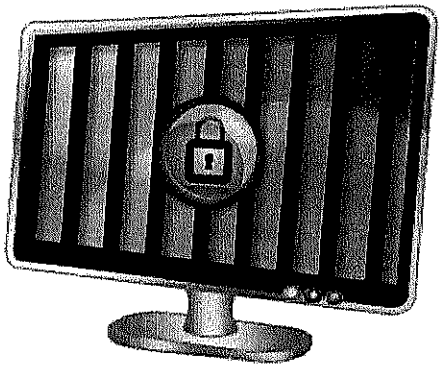
Password Policies

- Modify policies to require users create strong passwords
  - Remember CLOUDS Not SUN (Unit Four)
- Click Account Policies → Password Policies

Policies:	Recommended settings:
Password history: the number of old passwords the computer remembers and does not allow a user to reuse	5 passwords remembered
Maximum password age: how long a user can keep the same password	90 days for users, 30 for admins
Minimum password age: how long a user must keep a password before changing it	10-30 days
Minimum password length: how many characters passwords must be	8 characters
Complexity requirements: whether users must use at least three of the following in their passwords: upper case letters, lower case letters, numbers, symbols	Enable
Reversible encryption: whether the password file on the computer can be decrypted	Disable

Account Lockout Policies

- Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will
- Account policies govern unsuccessful attempts to log into an account
- Click Account Policies → Account Lockout Policies

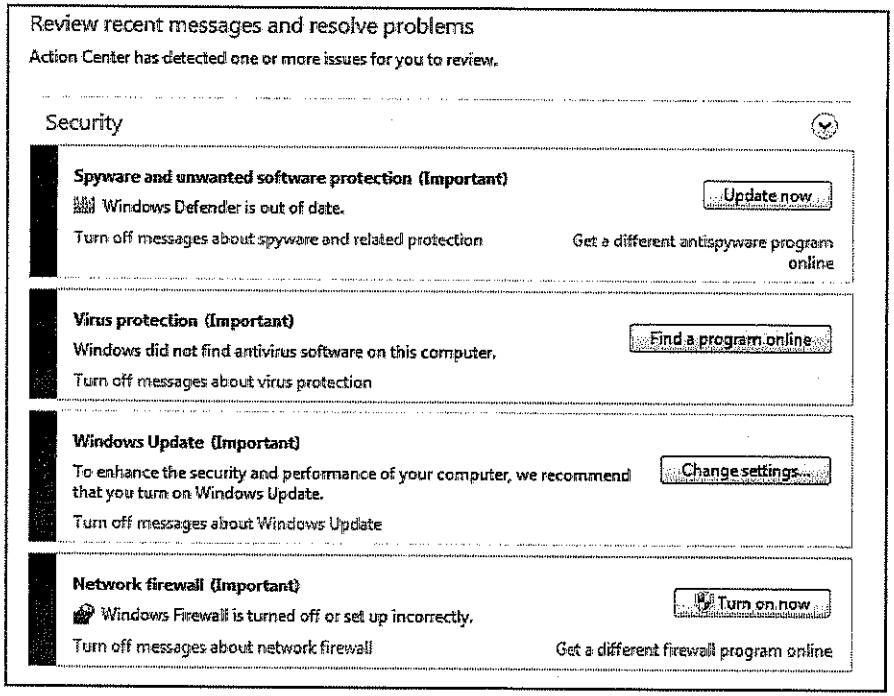


Policies:	Recommended settings:
Account lockout duration: the number of minutes a locked-out account remains locked before automatically becoming unlocked	30 minutes
Account lockout threshold: the number of failed logon attempts that causes a user account to be locked out	3-10 invalid login attempts
Reset account lockout counter after: the number of minutes that must elapse before the failed logon attempt threshold counter is reset to 0	30 minutes

Action Center

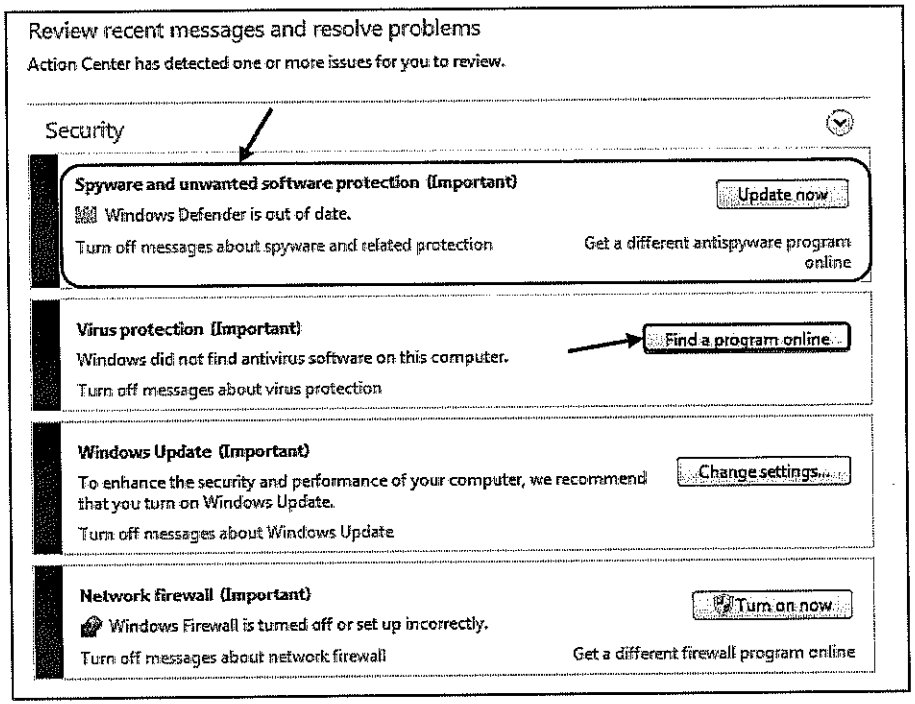
- Click Start → Control Panel → System and Security → Action Center
- Notifies you if Windows identifies problems with or updates for:

  - Windows Updates
  - Internet security settings
  - Network firewall
  - Spyware and related protection
  - User Account Control
  - Virus protections
  - Windows Backups
  - Windows Troubleshooting



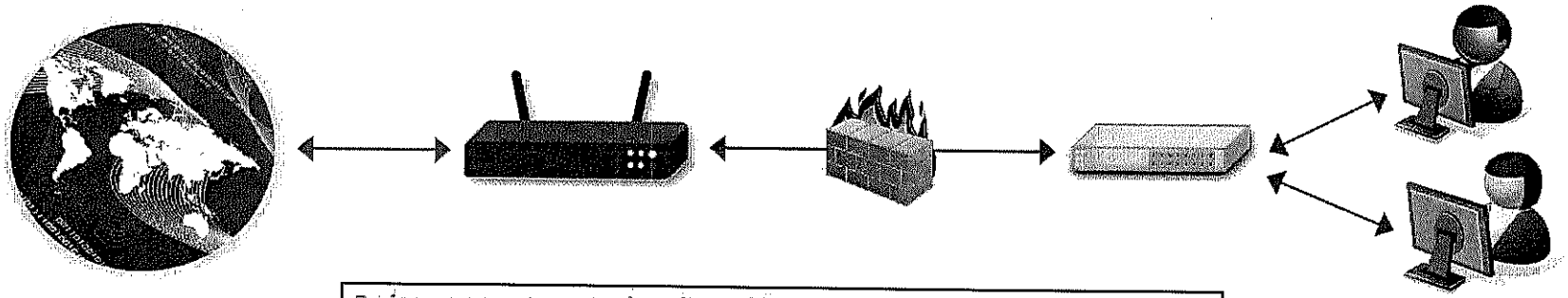
Windows Defender and Anti-Malware

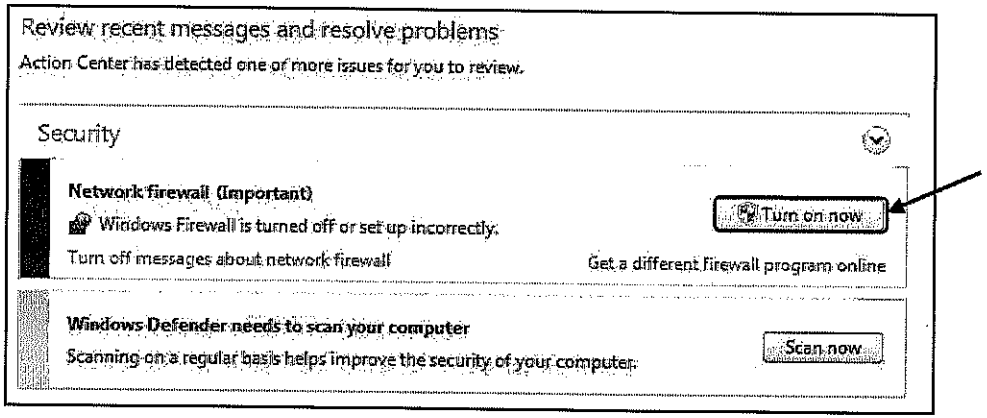
- Control Panel → System and Security → Action Center
- Anti-malware programs should be updated regularly
- Windows Defender is a very basic built-in spyware protection program in Windows
  - It only protects against known spyware, not viruses, worms or other malware
- Download a supplementary anti-virus program
  - Windows offers a free program called Windows Security Essentials
  - If you choose a different anti-malware program, disable Windows Defender first to avoid compatibility issues



Firewalls

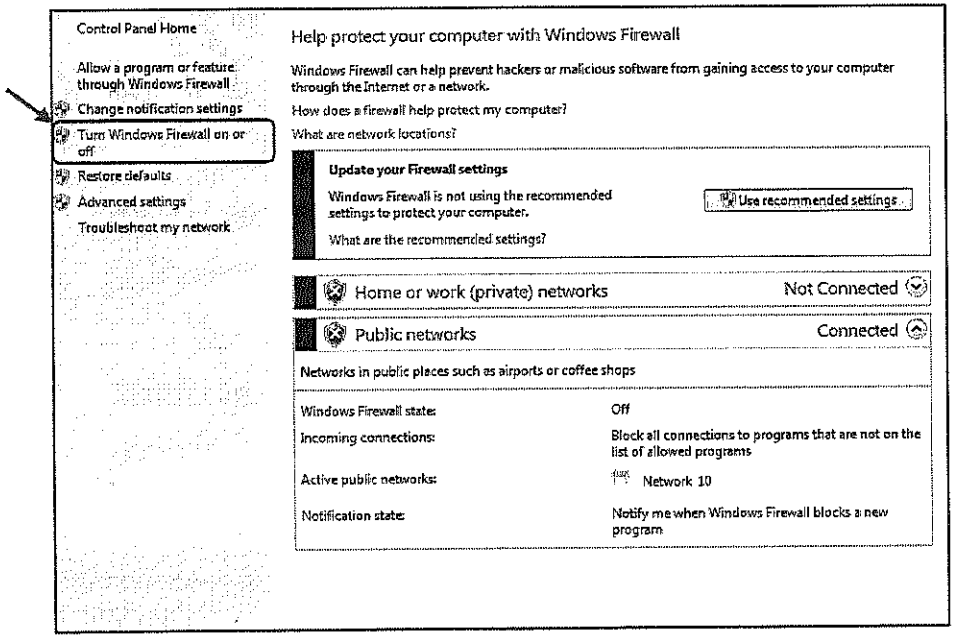
- Reject or allow data packets through to users based on custom settings
- Essential to security and should always be turned 'on'
- Control Panel → System and Security → Action Center → Turn on now

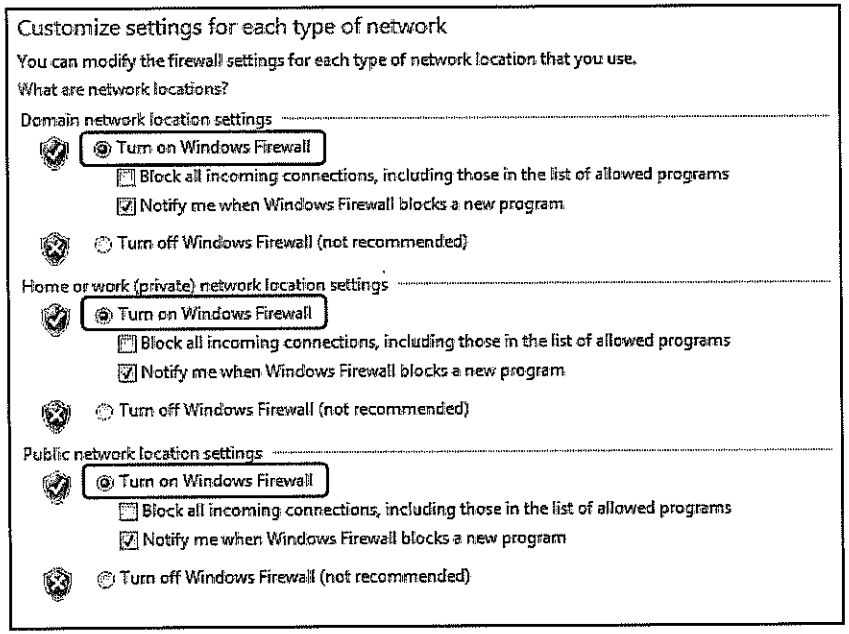




Windows Firewall Custom Settings

- For more advanced settings: Control Panel → System and Security → Windows Firewall
- Customize firewall settings for each type of network (e.g. Home, Public, Work)

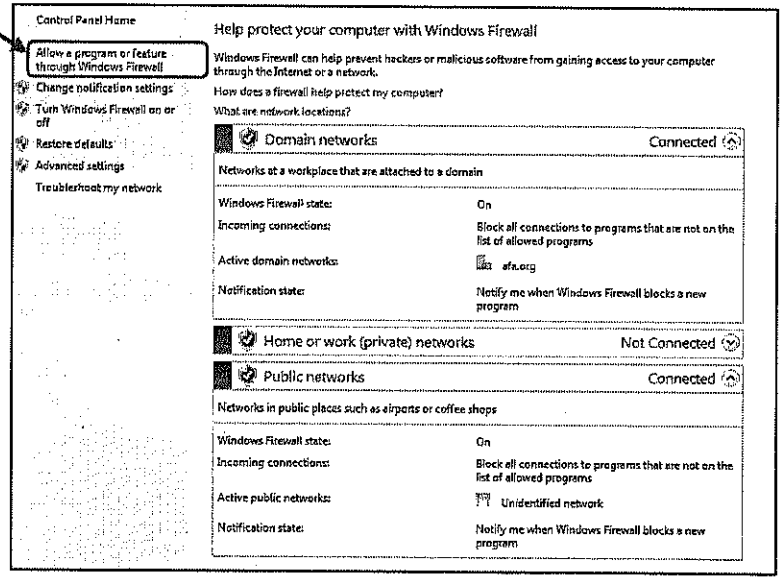




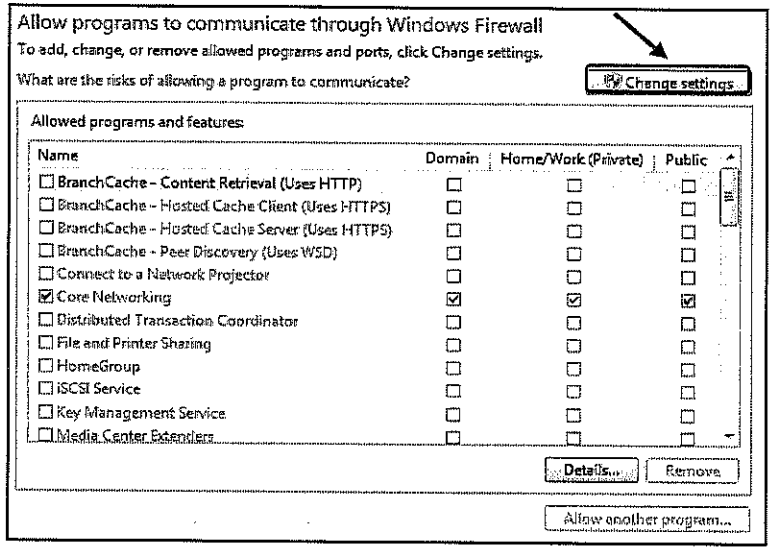
Enabling Windows Firewall Exceptions

- Allow trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list
  - For each network type, you can customize whether you want the programs allowed through
- It's much safer to allow only certain programs through your firewall than to open an entire port to traffic
  - Ports are numbers that identifies one side of a connection between two computers
- Control Panel → System and Security → Windows Firewall

1.



2.

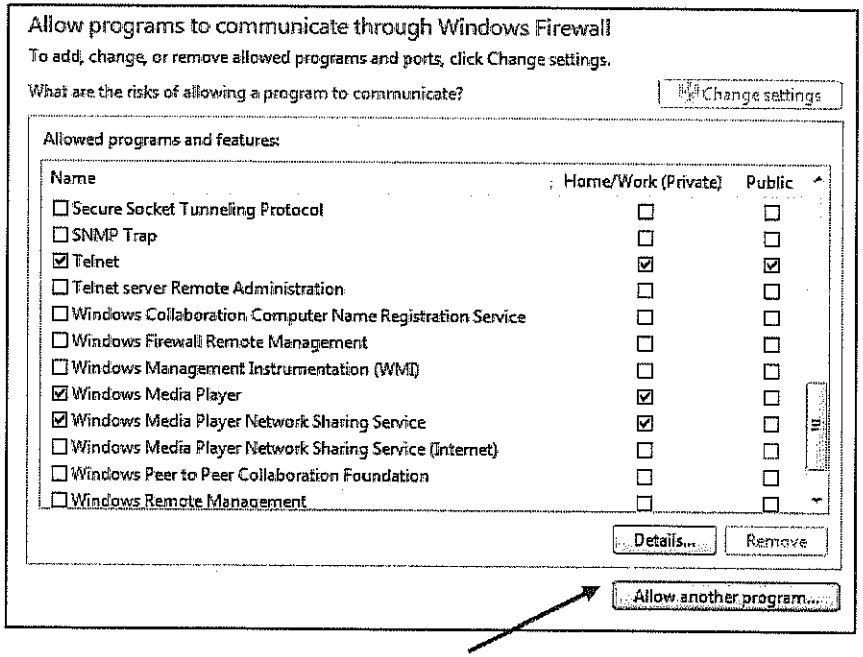


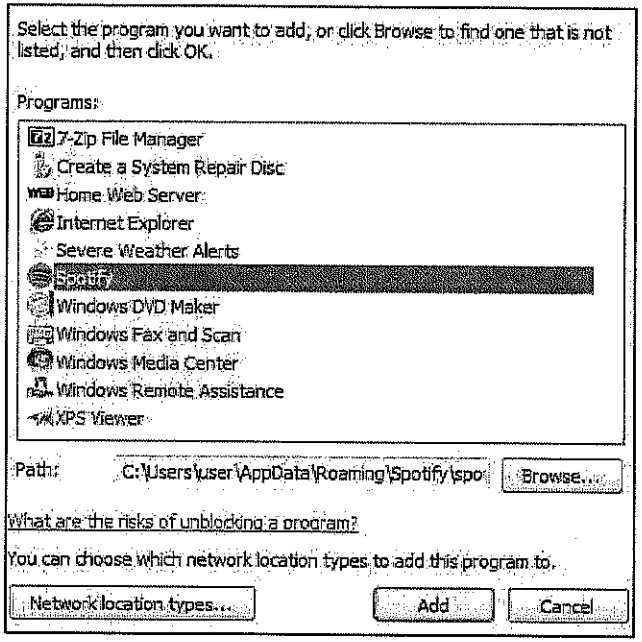
Common Exceptions

- Core Networking
  - Regular Microsoft Windows services that retrieve data from the Internet
  - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
- File and Printer Sharing
  - Allows you to share the contents of selected folders and locally attached printers with other computers
- Remote Assistance
  - Allows a user to temporarily remotely control another Windows computer over a network or the Internet to resolve issues
- Remote Desktop
  - Allows users to access their user accounts and files remotely
- UPnP Framework (Universal Plug-and-Play)
  - Allows devices to connect to and automatically establish working configurations with other devices on the same network

Adding Windows Firewall Exceptions

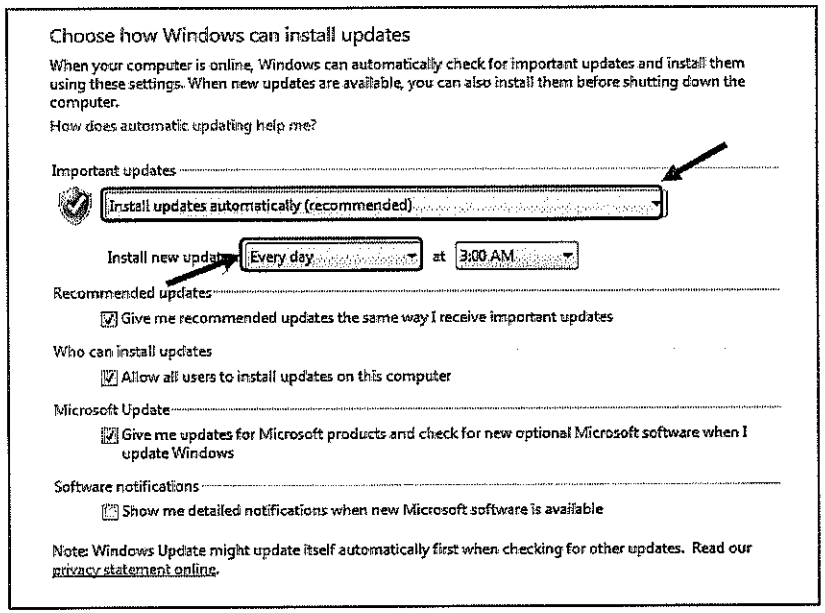
- If the program you want to allow through your firewall does not already appear on your exceptions list, click the "Allow another program" and select the program from the menu





Windows Updates

- Prevent or fix known problems in Windows software or improve user experience
- Should be installed regularly
  - To avoid missing updates, allow Windows Update to check for them daily and install them automatically
- Control Panel → System and Security → Windows Update



AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION TWO

Account Management

www.uscyberpatriot.org

Account Groups

System Accounts

Admin Accounts
- The most advanced accounts
- Typically held by IT Staff only
- Admins can change security settings for other users, install resources, and access and modify all files on a network

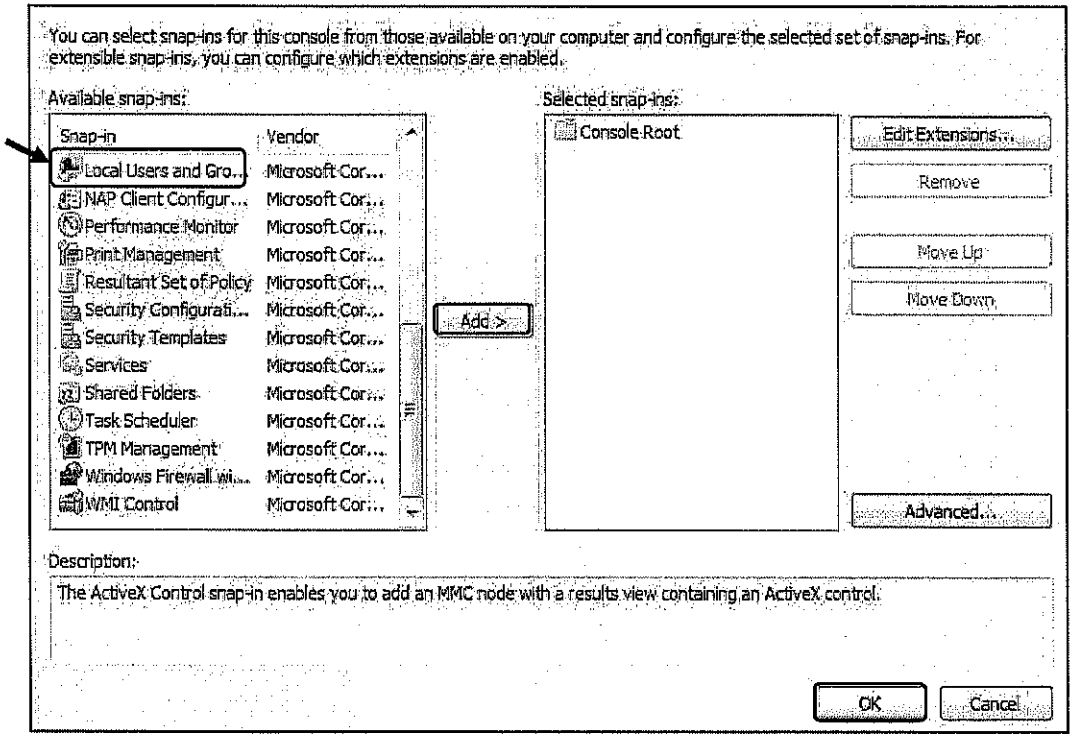
User Accounts
- Allow people to share a computer and network resources, but still have their own files and settings
- Have fewer rights and permissions than Admin accounts

Domain Accounts
- Allow users to access their accounts from any computer in the network
- Username and password reside on a domain controller (a type of server that manages all of the accounts on a network)

Local Accounts
- Allow access to a specific computer only
- Username and password are stored on the computer itself

Local Users and Groups Console

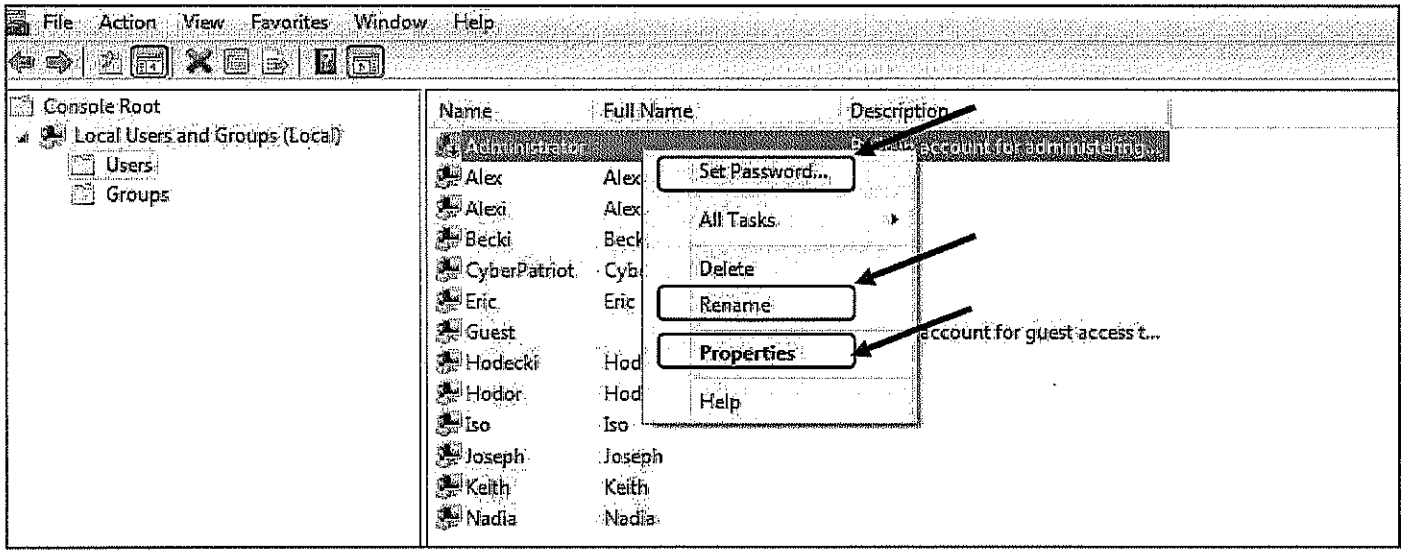
- Windows categorizes accounts as user or administrator accounts so that it can automatically apply the relevant permissions and rights
- Define a user's level of access by categorizing his or her account as a user or administrator
- To set up the Local Users and Groups Console: Start Menu → Search "mmc"→ Click "yes" to allow changes to computer → Click File → Add or Remove Snap-ins → Select "Local Users and Groups → When prompted, select "Add to Local Computer"



*The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.

Best Practice: Secure the Built-in Administrator Account

- Add a password
- Obfuscate the account by changing the name
  - Attackers will target known Admin accounts because successfully infiltrating those accounts will give them advanced permissions and access to the network
- Restrict use of the account
  - Use the Properties menu to remove unnecessary accounts from the Administrators group

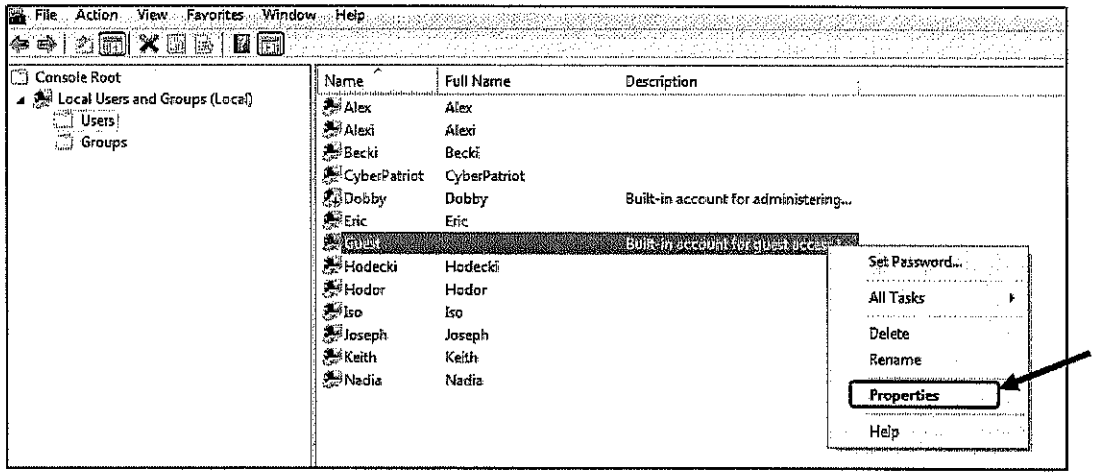


Best Practice: Disable the Built-in Guest Account

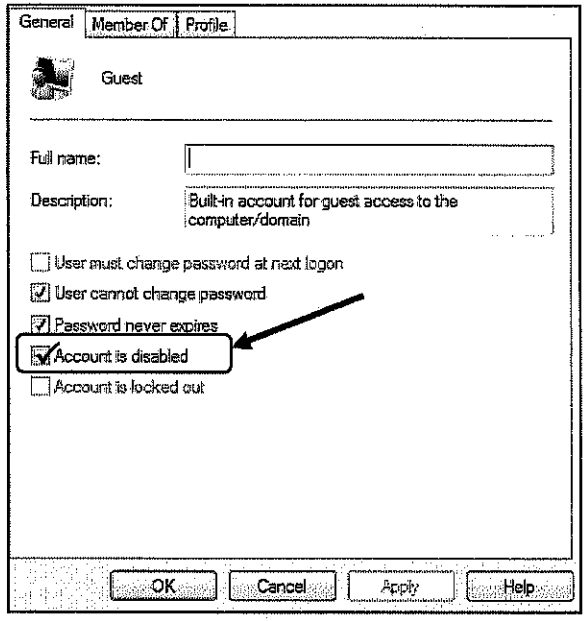
Console option:

- Disable this account so people cannot anonymously access a computer
- While someone on a Guest account will not have direct access to other users' information, he or she can still significantly disrupt the resources of the local computer

1.



2.

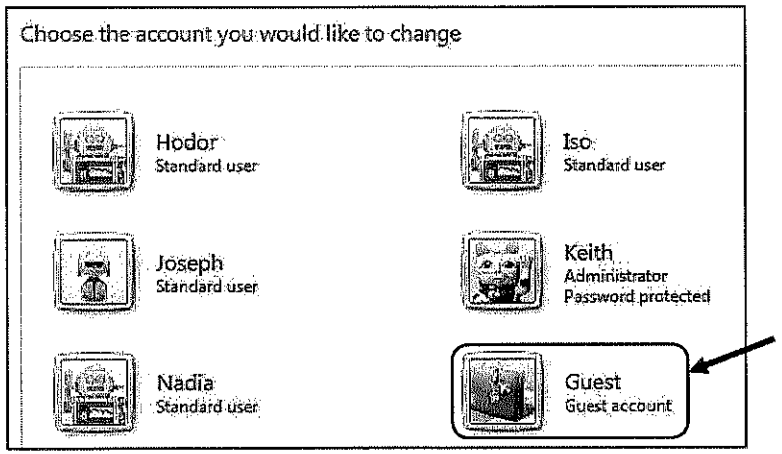


Best Practice: Disable the Built-in Guest Account

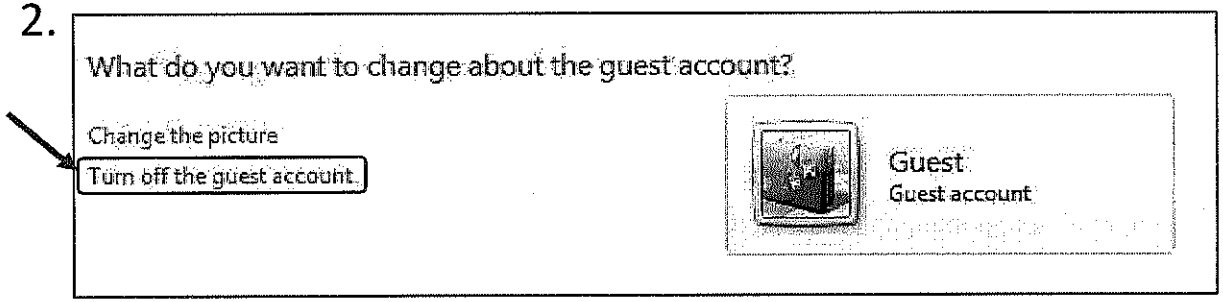
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

1.



2.

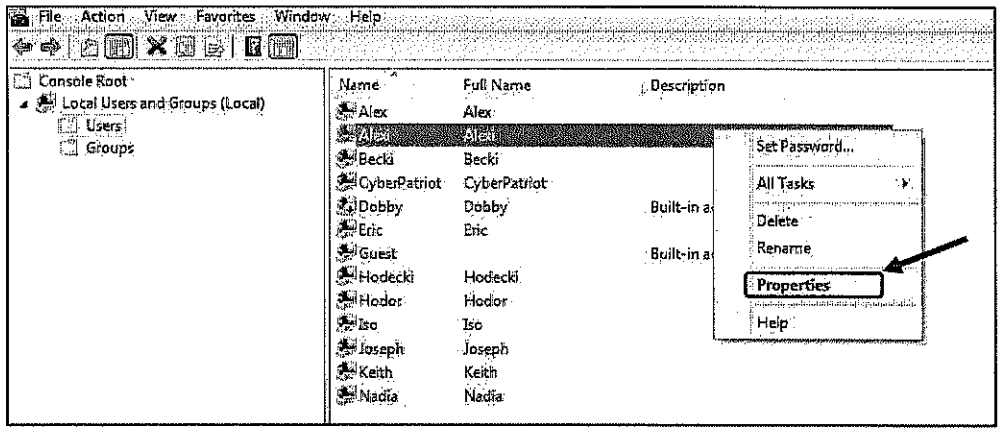


Best Practice: Restrict Administrator Group Membership

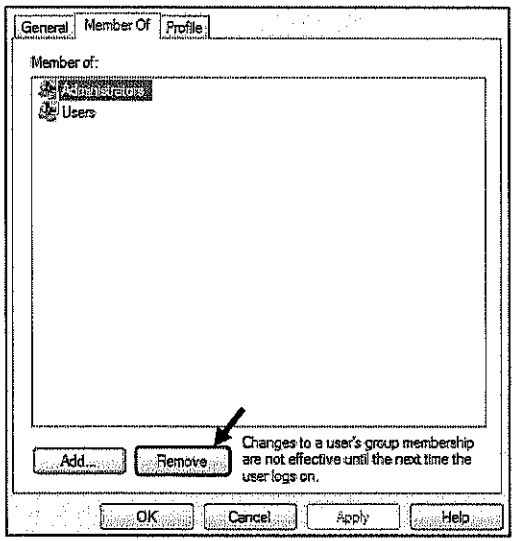
Console option:

- Administrator accounts allow people to efficiently make changes across a network or computer and to monitor and control the use of shared resources
  - Because of those advanced permissions, administrator accounts need to be especially well-protected and limited to only a few individuals
- Remove unnecessary users from the Administrators Group

1.



2.

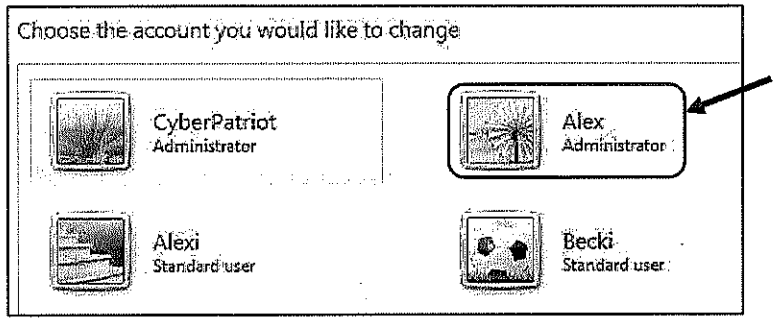


Best Practice: Restrict Administrator Group Membership

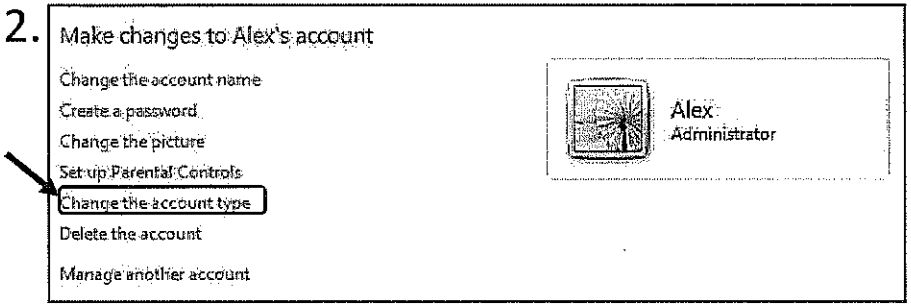
Control Panel option:

- Control Panel → User Accounts → Manage another account

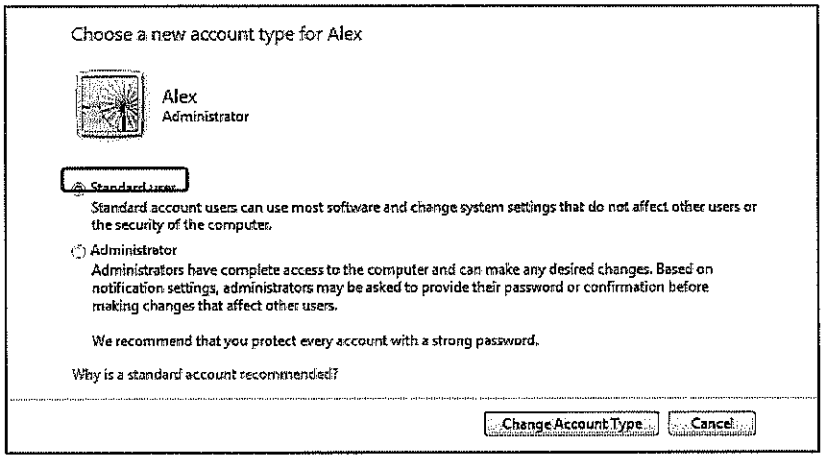
1.



2.



3.

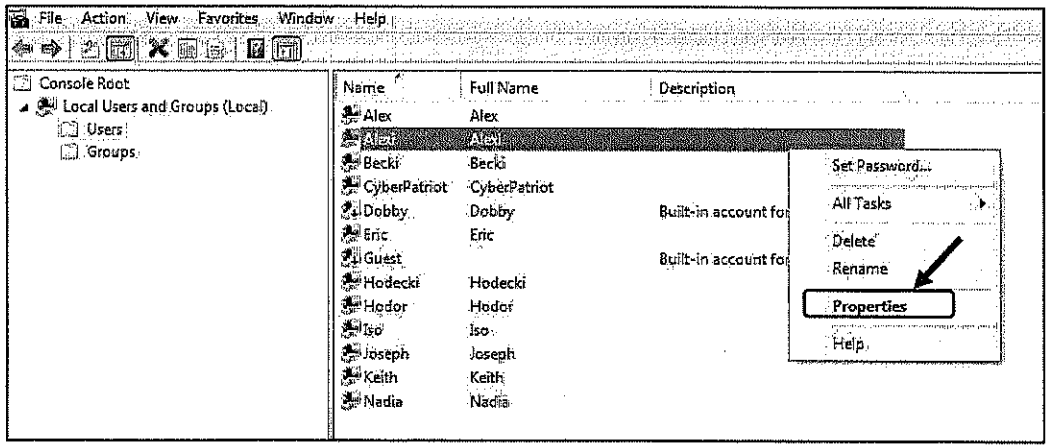


Best Practice: Set Passwords for all Accounts

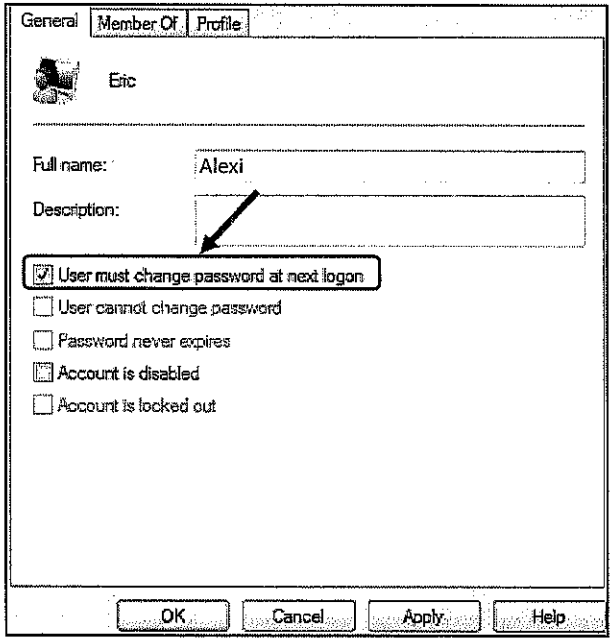
Console option:

- Make sure all accounts are password protected

1.



2.

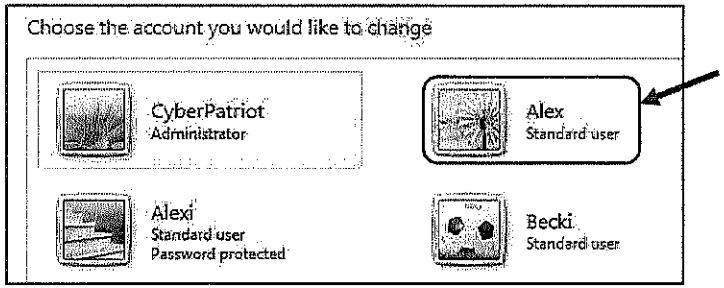


Best Practice: Set Passwords for all Accounts

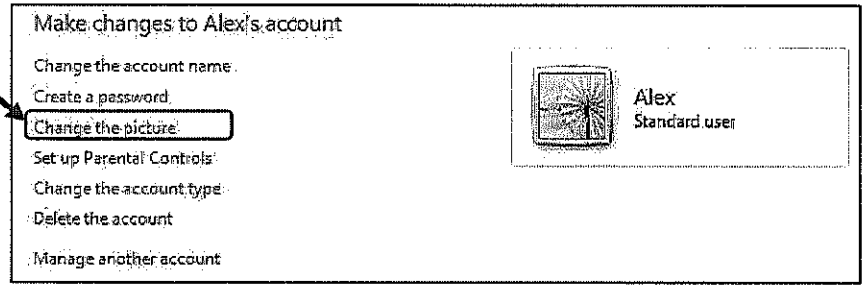
Control Panel option:

- Control Panel → User Accounts → Manage another account

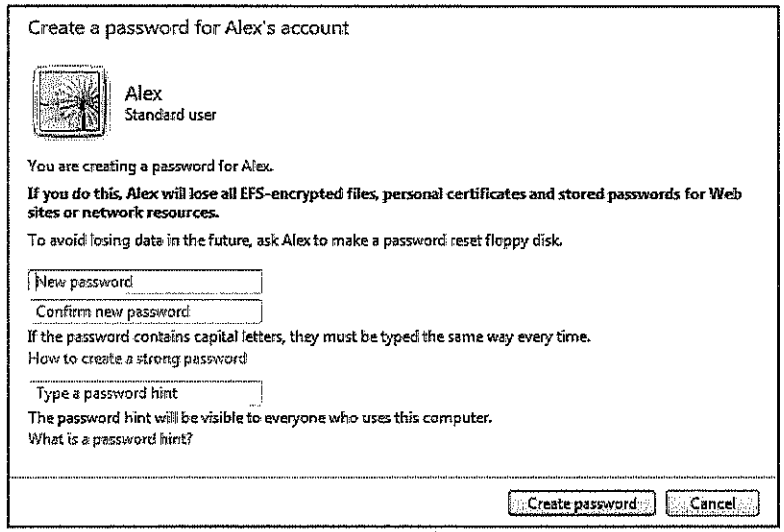
1.



2.



3.

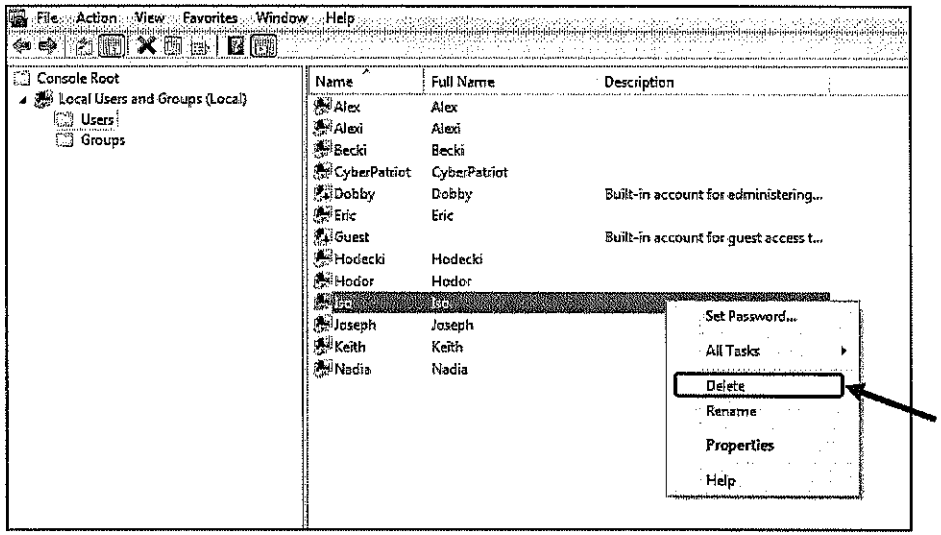


Removing Users

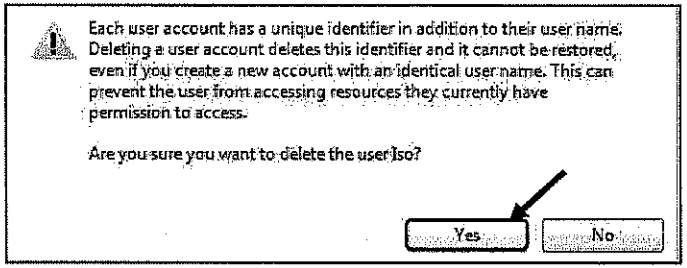
Console option:

- Only current, authorized employees should have access to a organization's network
- Make sure your user directory is up-to-date and remove unnecessary accounts

1.



2.

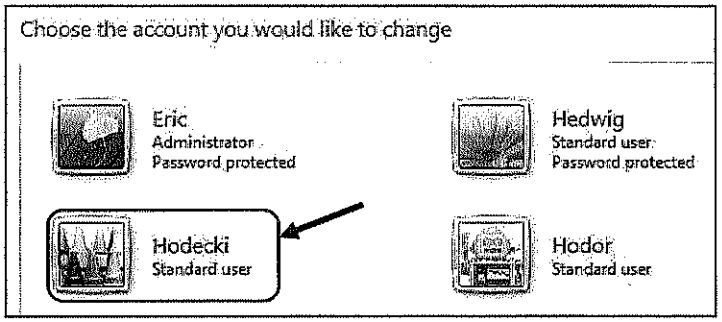


Removing Users

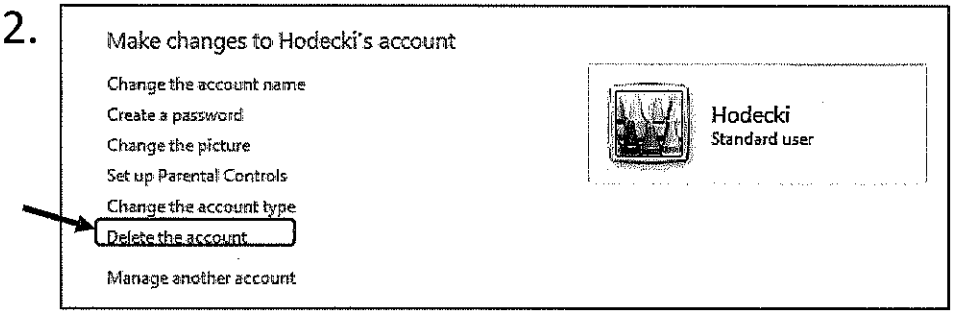
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

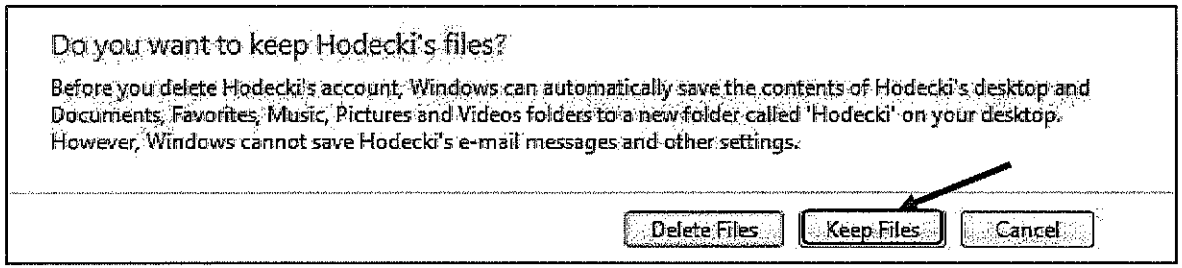
1.



2.



3.

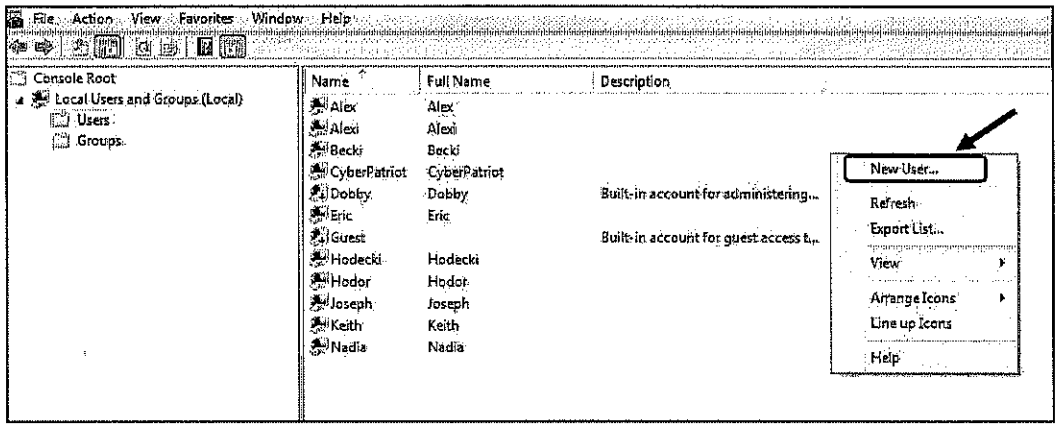


Adding Users

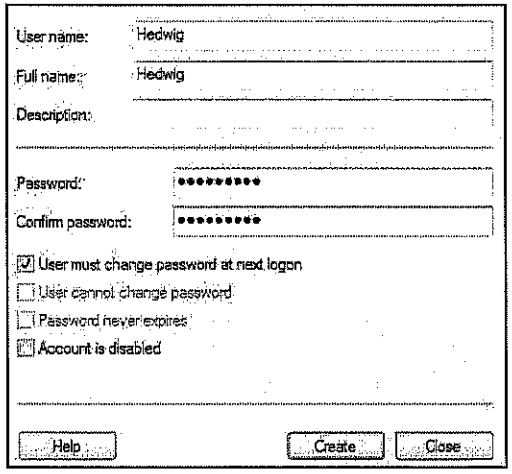
Console option:

- When adding new accounts, make sure to put the account in the right User Group and password protect the new user's account

1.



2.

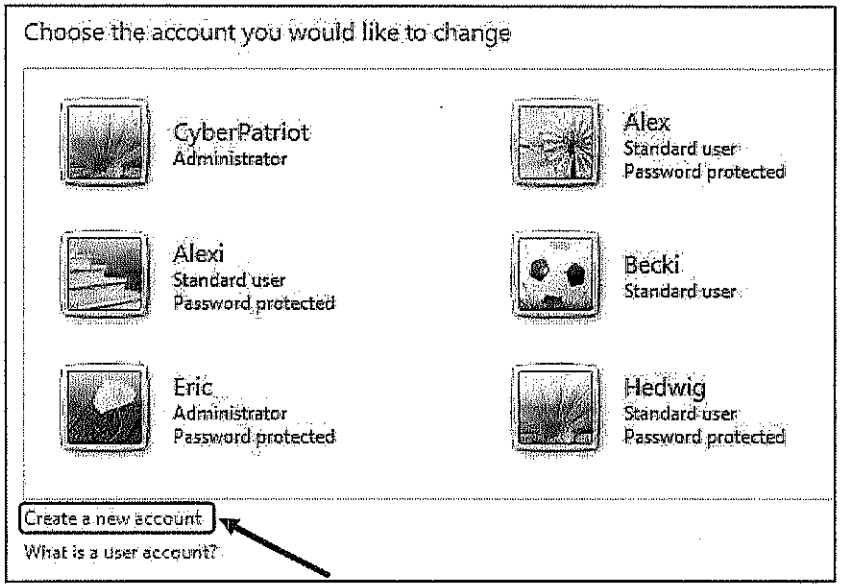


Adding Users

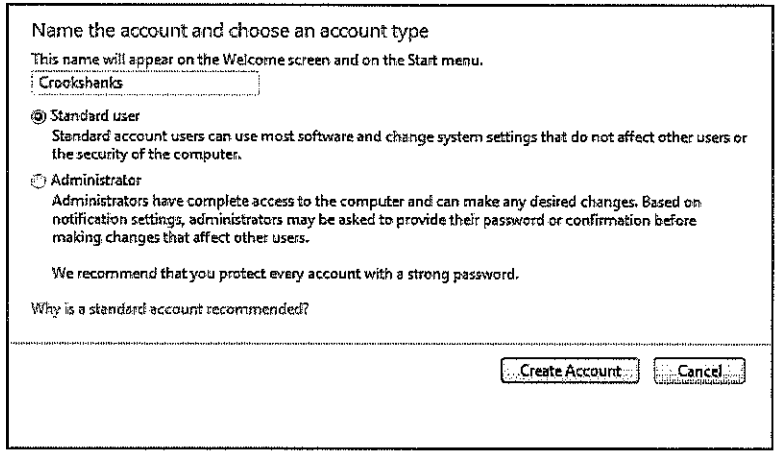
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

1.

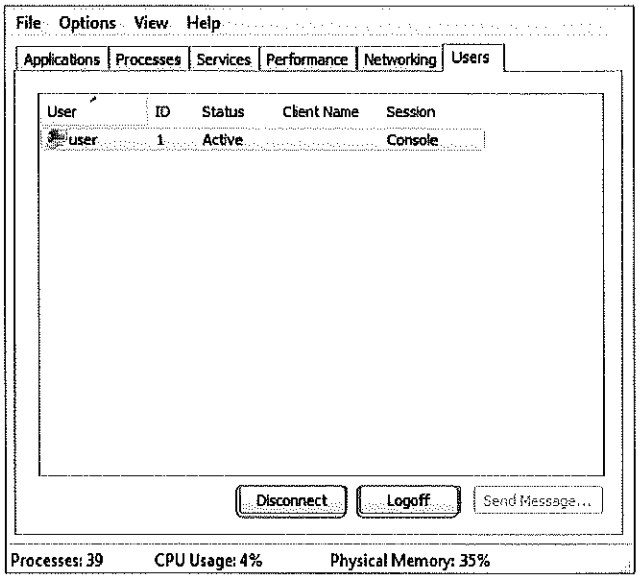


2.



Task Manager: Users Tab

- Shows you all of the users currently logged on to the system
- Allows you to "disconnect" users
  - Terminate the user's connection without shutting down the programs they were running
- Allows you to "logoff" users
  - Log the user off the computer completely and terminate any running programs



Source: http://www.bleepingcomputer.com/tutorials/how-to-use-the-windows-task-manager/#networking

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

UNIT FIVE

Microsoft Windows Security

www.uscyberpatriot.org

AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

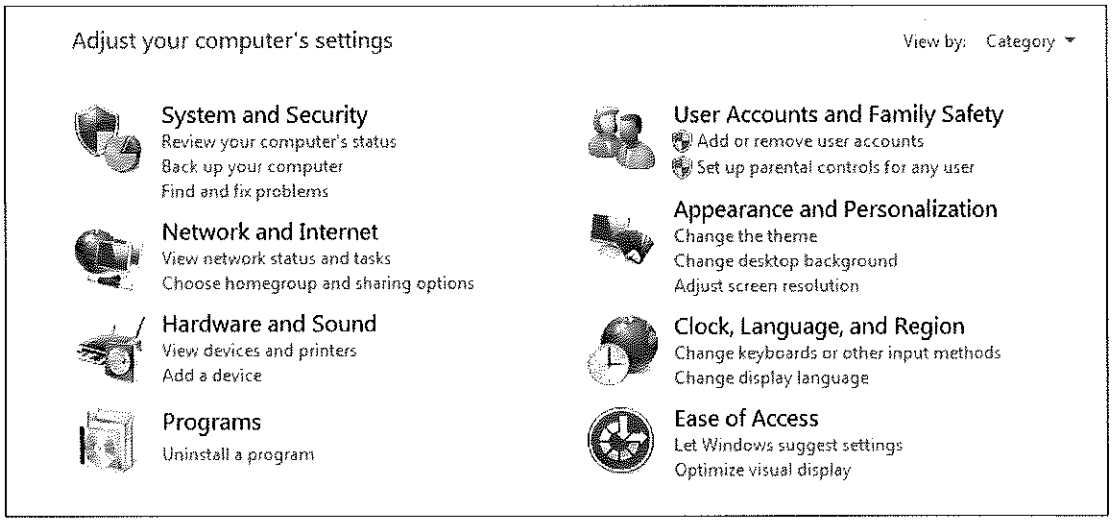
SECTION ONE

Basic Security Policies and Tools

www.uscyberpatriot.org

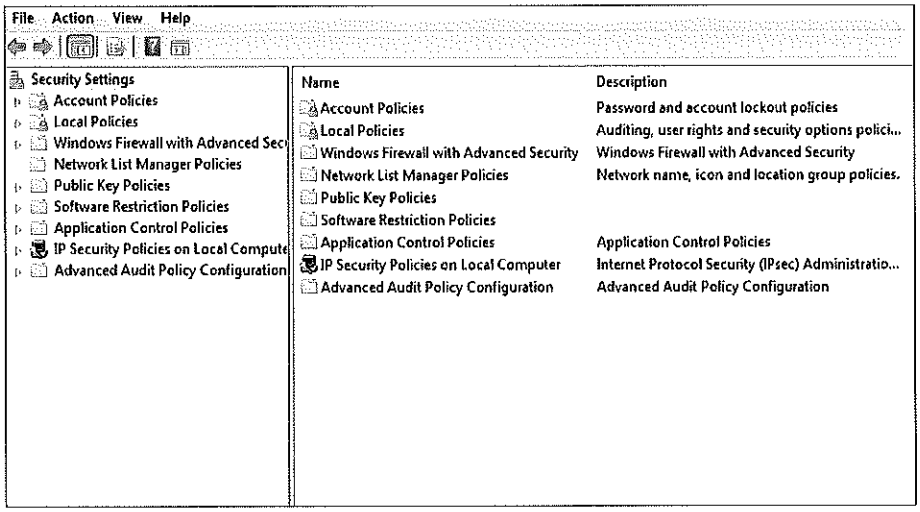
Control Panel

- Where many of the basic system changes and configurations can be made with a Windows operating system
- Click Start → Control Panel



Basic Local Security Policies

- Controls security settings on user computers within a network
- Click System and Security → Administrative Tools → Local Security Policy



Password Policies

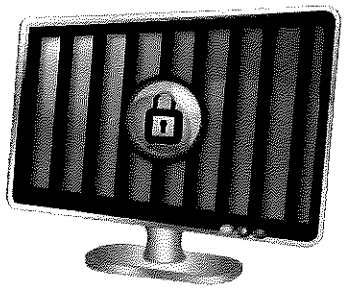
- Modify policies to require users create strong passwords
  - Remember CLOUDS Not SUN (Unit Four)
- Click Account Policies → Password Policies

Policies:	Recommended settings:
Password history: **the number of old passwords the computer remembers and does not allow a user to reuse**	5 passwords remembered
Maximum password age: **how long a user can keep the same password**	90 days for users, 30 for admins
Minimum password age: **how long a user must keep a password before changing it**	10-30 days
Minimum password length: **how many characters passwords must be**	8 characters
Complexity requirements: **whether users must use at least three of the following in their passwords: upper case letters, lower case letters, numbers, symbols**	Enable
Reversible encryption: **whether the password file on the computer can be decrypted**	Disable

secpol.msc

Account Lockout Policies

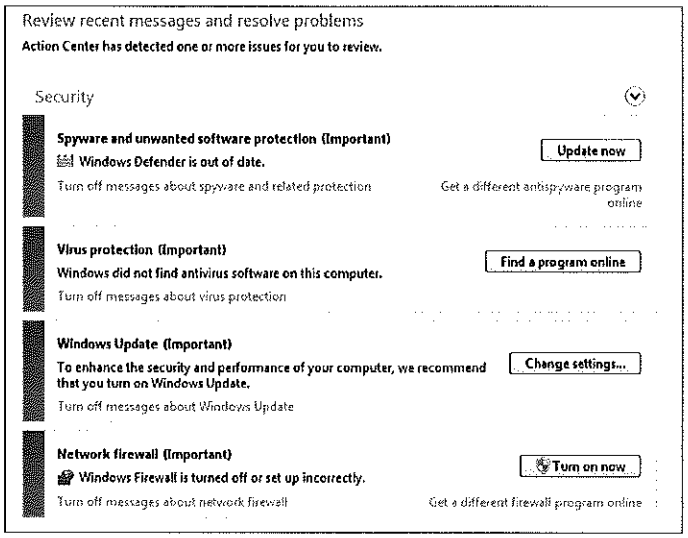
- Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will
- Account policies govern unsuccessful attempts to log into an account
- Click Account Policies → Account Lockout Policies



Policies:	Recommended settings:
Account lockout duration: **the number of minutes a locked-out account remains locked before automatically becoming unlocked**	30 minutes
Account lockout threshold: **the number of failed logon attempts that causes a user account to be locked out**	3-10 invalid login attempts
Reset account lockout counter after: **the number of minutes that must elapse before the failed logon attempt threshold counter is reset to 0**	30 minutes

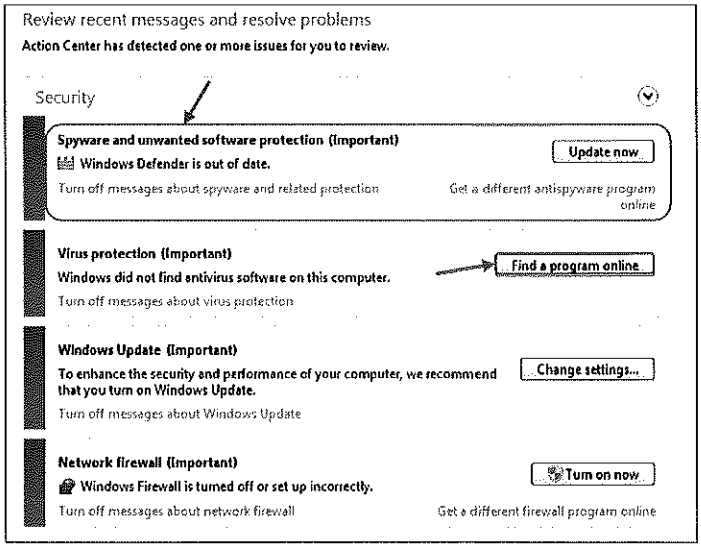
Action Center

- Click Start → Control Panel → System and Security → Action Center
- Notifies you if Windows identifies problems with or updates for:
  - Windows Updates
  - Internet security settings
  - Network firewall
  - Spyware and related protection
  - User Account Control
  - Virus protections
  - Windows Backups
  - Windows Troubleshooting



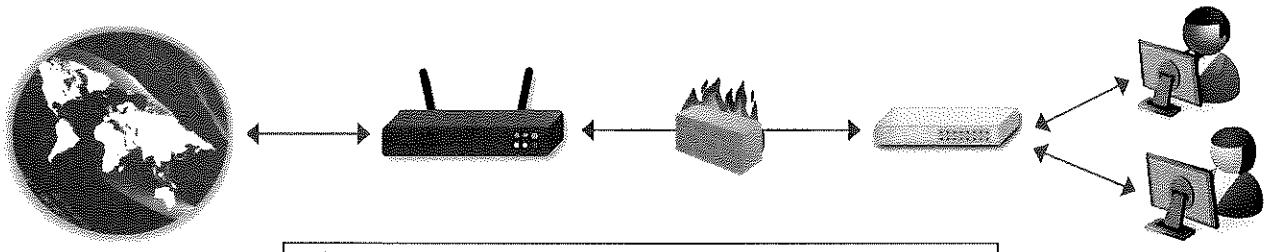
Windows Defender and Anti-Malware

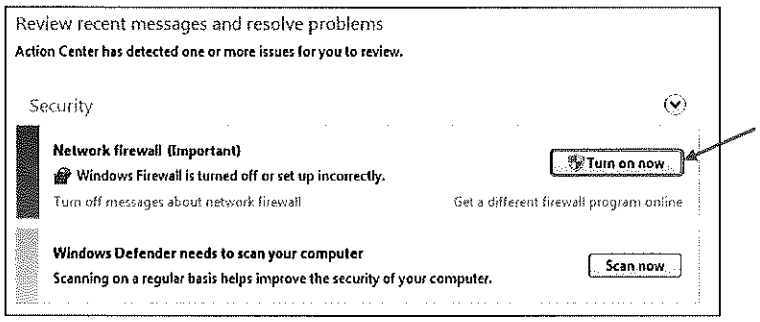
- Control Panel → System and Security → Action Center
- Anti-malware programs should be updated regularly
- Windows Defender is a very basic built-in spyware protection program on Windows
  - It only protects against known spyware, not viruses, worms or other malware
- Download a supplementary anti-virus program
  - Windows offers a free program called Windows Security Essentials
  - If you choose a different anti-malware program, disable Windows Defender first to avoid compatibility issues.



Firewalls

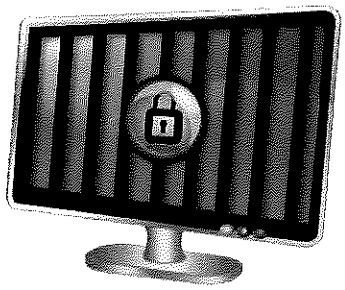
- Reject or allow data packets through to users based on custom settings
- Essential to security and should always be turned 'on'
- Control Panel → System and Security → Action Center → Turn on now





Account Lockout Policies

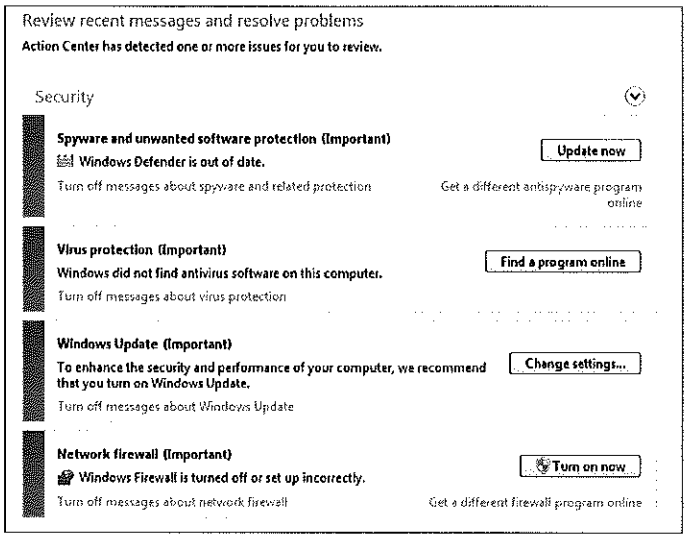
- Even if you have the strongest password possible, if you give hackers unlimited attempts to break it, they eventually will
- Account policies govern unsuccessful attempts to log into an account
- Click Account Policies → Account Lockout Policies



Policies:	Recommended settings:
Account lockout duration: **the number of minutes a locked-out account remains locked before automatically becoming unlocked**	30 minutes
Account lockout threshold: **the number of failed logon attempts that causes a user account to be locked out**	3-10 invalid login attempts
Reset account lockout counter after: **the number of minutes that must elapse before the failed logon attempt threshold counter is reset to 0**	30 minutes

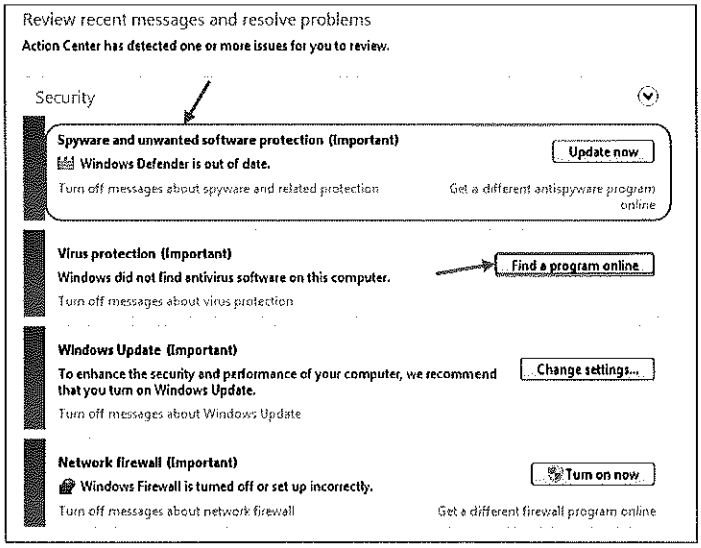
Action Center

- Click Start → Control Panel → System and Security → Action Center
- Notifies you if Windows identifies problems with or updates for:
  - Windows Updates
  - Internet security settings
  - Network firewall
  - Spyware and related protection
  - User Account Control
  - Virus protections
  - Windows Backups
  - Windows Troubleshooting



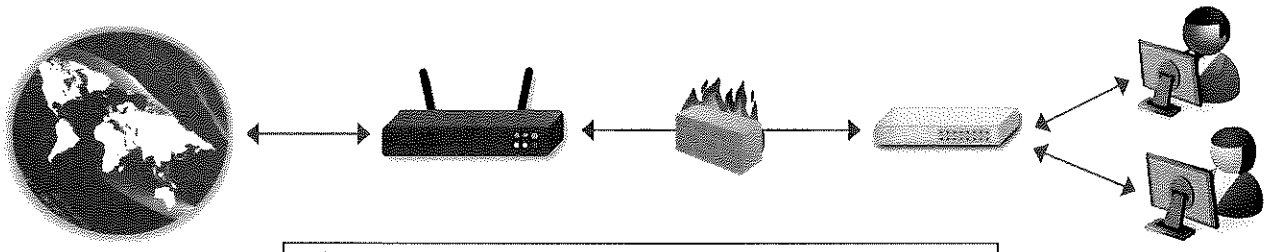
Windows Defender and Anti-Malware

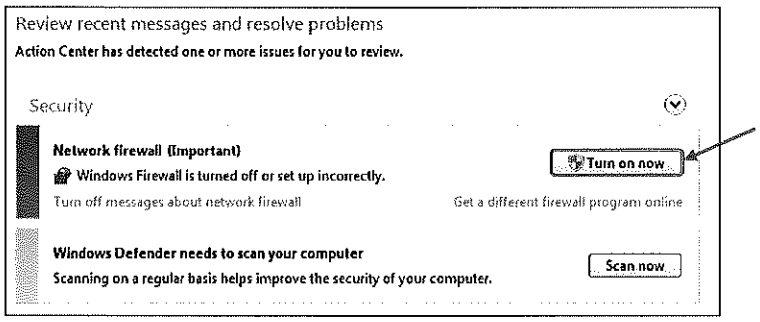
- Control Panel → System and Security → Action Center
- Anti-malware programs should be updated regularly
- Windows Defender is a very basic built-in spyware protection program on Windows
  - It only protects against known spyware, not viruses, worms or other malware
- Download a supplementary anti-virus program
  - Windows offers a free program called Windows Security Essentials
  - If you choose a different anti-malware program, disable Windows Defender first to avoid compatibility issues.



Firewalls

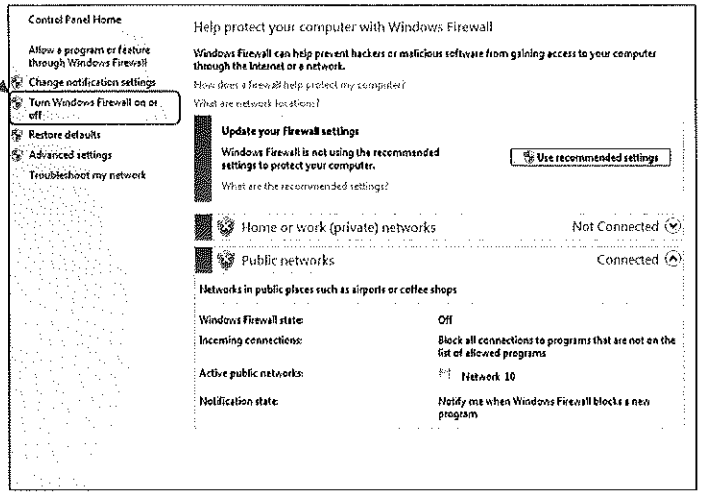
- Reject or allow data packets through to users based on custom settings
- Essential to security and should always be turned 'on'
- Control Panel → System and Security → Action Center → Turn on now

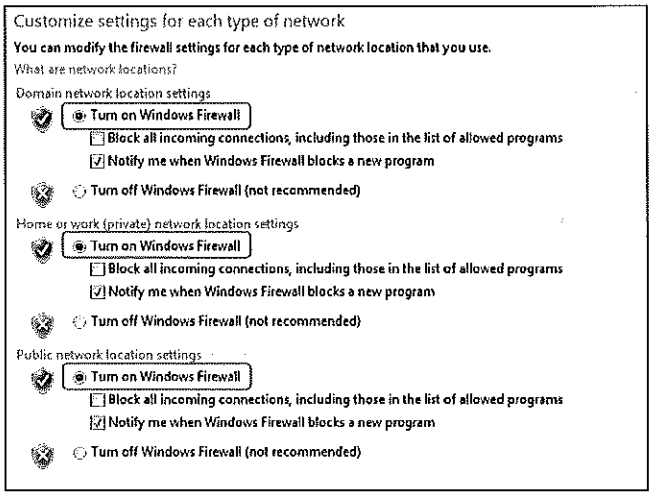




Windows Firewall Custom Settings

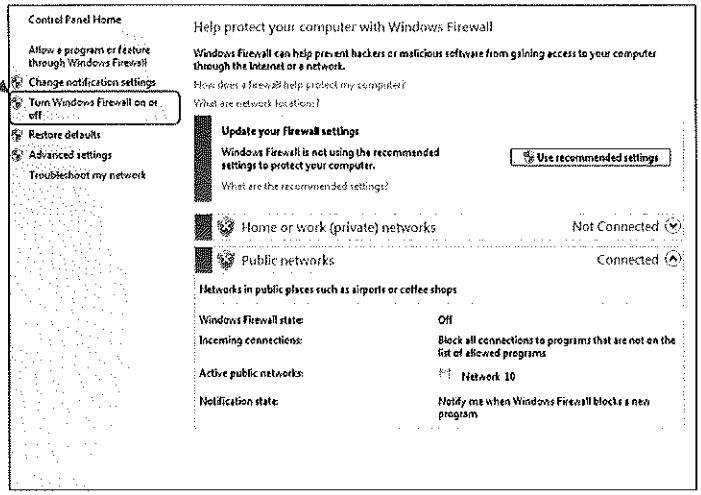
- **For more advanced settings:** Control Panel → System and Security → Windows Firewall
- **Customize firewall settings for each type of network (e.g. Home, Public, Work)**

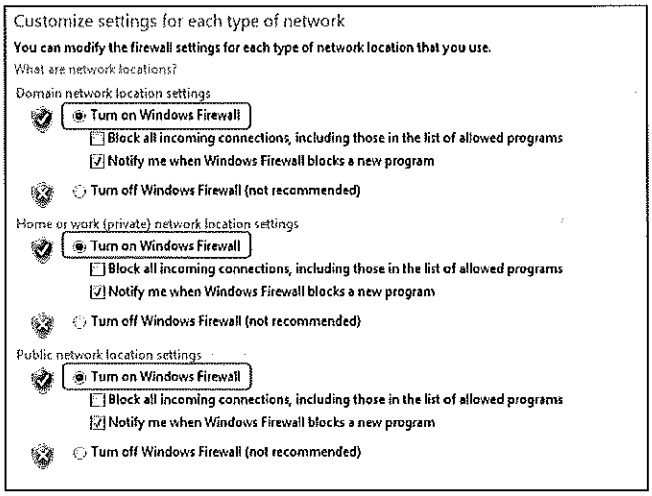




Windows Firewall Custom Settings

- **For more advanced settings:** Control Panel → System and Security → Windows Firewall
- **Customize firewall settings for each type of network (e.g. Home, Public, Work)**

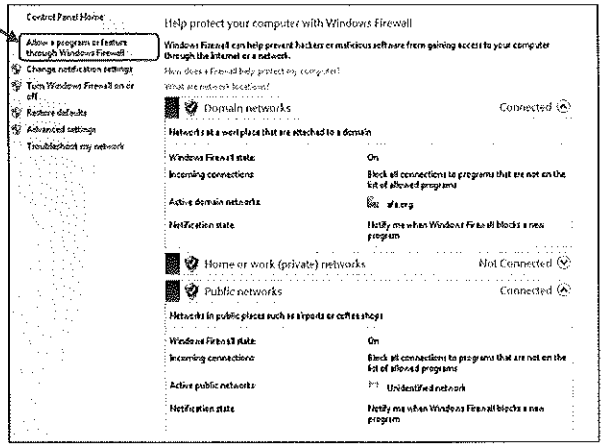




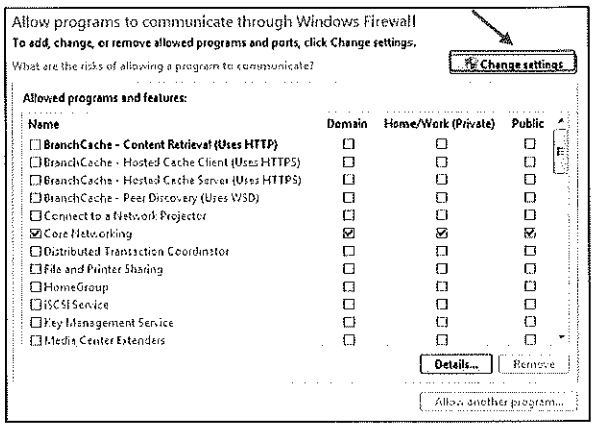
Enabling Windows Firewall Exceptions

- Allow trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list
  - For each network type, you can customize whether you want the programs allowed through
- It's much safer to allow only certain programs through your firewall than to open an entire port to traffic
  - Ports are numbers that identifies one side of a connection between two computers
- Control Panel → System and Security → Windows Firewall

1.



2.

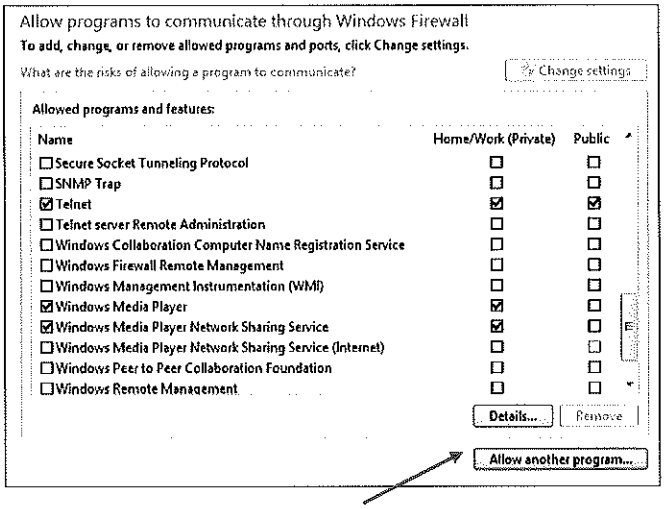


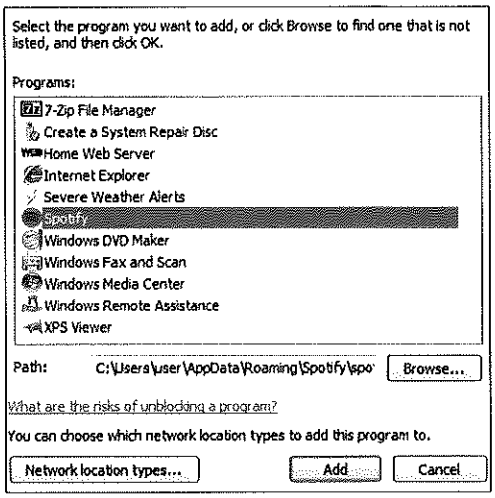
Common Exceptions

- Core Networking
  - Regular Microsoft Windows services that retrieve data from the Internet
  - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
- File and Printer Sharing
  - Allows you to share the contents of selected folders and locally attached printers with other computers
- Remote Assistance
  - Allows a user to temporarily remotely control another Windows computer over a network or the Internet to resolve issues
- Remote Desktop
  - Allows users to access their user accounts and files remotely
- UPnP Framework (Universal Plug-and-Play)
  - Allows devices to connect to and automatically establish working configurations with other devices on the same network

Adding Windows Firewall Exceptions

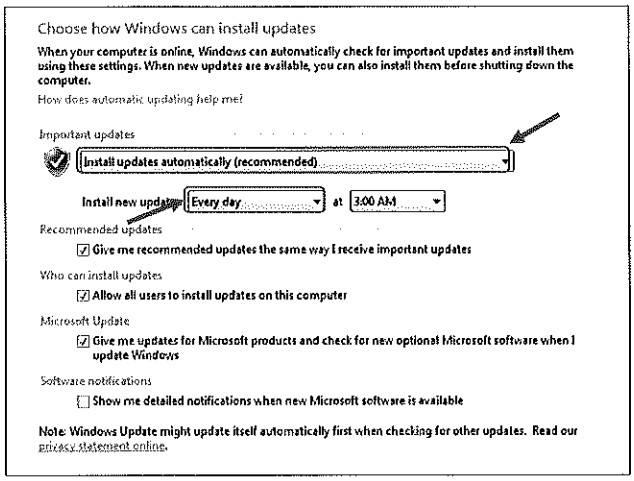
- If the program you want to allow through your firewall does not already appear on your exceptions list, click the "Allow another program" and select the program from the menu





Windows Updates

- Prevent or fix known problems in Windows software or improve user experience
- Should be installed regularly
  - To avoid missing updates, allow Windows Update to check for them daily and install them automatically
- Control Panel → System and Security → Windows Update



AIR FORCE ASSOCIATION'S

CYBERPATRIOT

NATIONAL YOUTH CYBER EDUCATION PROGRAM

SECTION TWO

Account Management

www.uscyberpatriot.org

Account Groups

System Accounts

Admin Accounts
- The most advanced accounts
- Typically held by IT Staff only
- Admins can change security settings for other users, install resources, and access and modify all files on a network

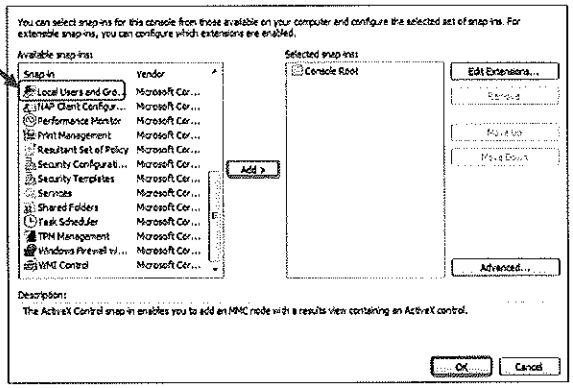
User Accounts
- Allow people to share a computer and network resources, but still have their own files and settings
- Have fewer rights and permissions than Admin accounts

Domain Accounts
- Allow users to access their accounts from any computer in the network
- Username and password reside on a domain controller (a type of server that manages all of the accounts on a network)

Local Accounts
- Allow access to a specific computer only
- Username and password are stored on the computer itself

Local Users and Groups Console

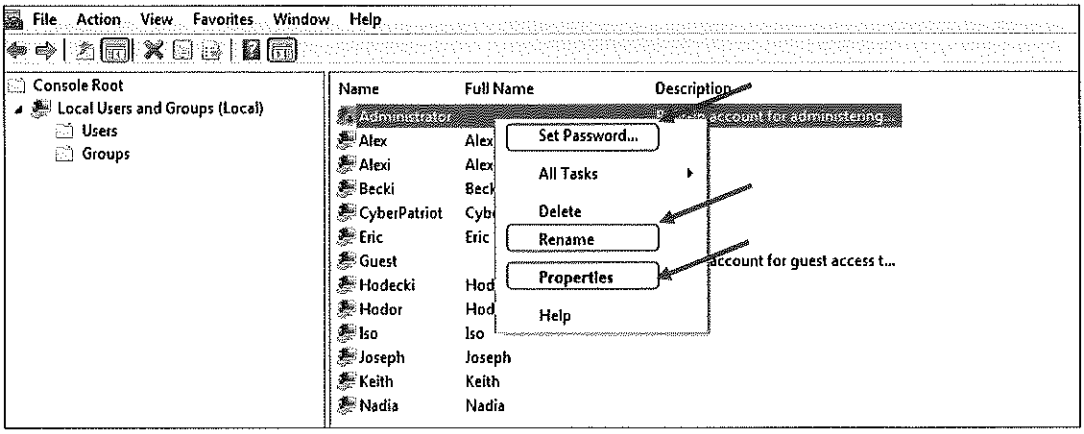
- Windows categorizes accounts as user or administrator accounts so that it can automatically apply the relevant permissions and rights
- Define a user's level of access by categorizing his or her account as a user or administrator
- **To set up the Local Users and Groups Console:** Start Menu → Search "mmc"→ Click "yes" to allow changes to computer → Click File → Add or Remove Snap-ins → Select "Local Users and Groups → When prompted, select "Add to Local Computer"



*The following slides will show you how to control user access through Control Panel and through the Local Users and Groups Console. Other methods exist and you can choose which to use based on personal preference.

Best Practice: Secure the Built-in Administrator Account

- Add a password
- Obfuscate the account by changing the name
  - Attackers will target known Admin accounts because successfully infiltrating those accounts will give them advanced permissions and access to the network
- Restrict use of the account
  - Use the Properties menu to remove unnecessary accounts from the Administrators group

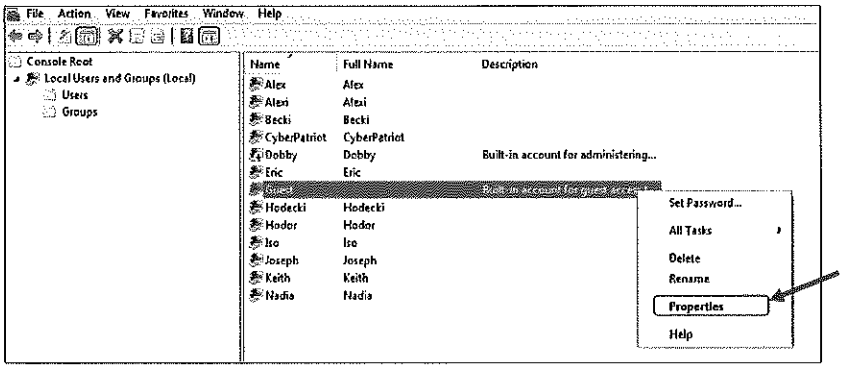


Best Practice: Disable the Built-in Guest Account

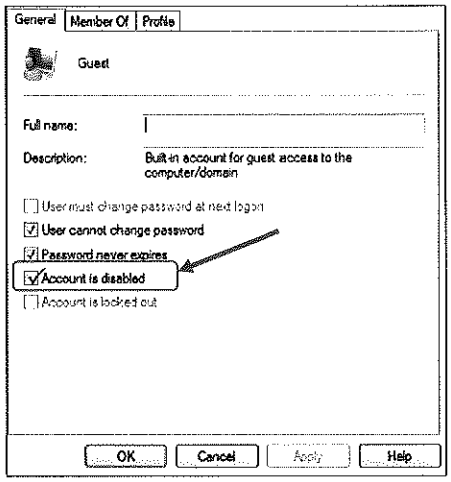
Console option:

- Disable this account so people cannot anonymously access a computer
- While someone on a Guest account will not have direct access to other users' information, he or she can still significantly disrupt the resources of the local computer

1.



2.

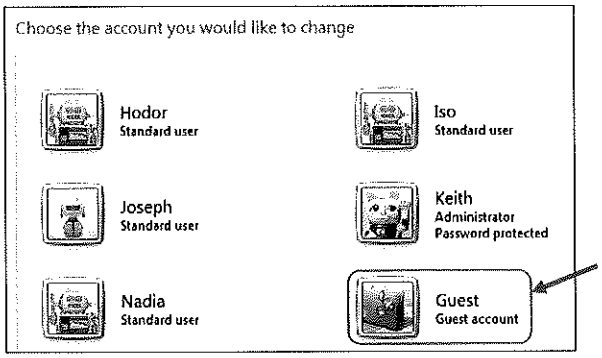


Best Practice: Disable the Guest Account

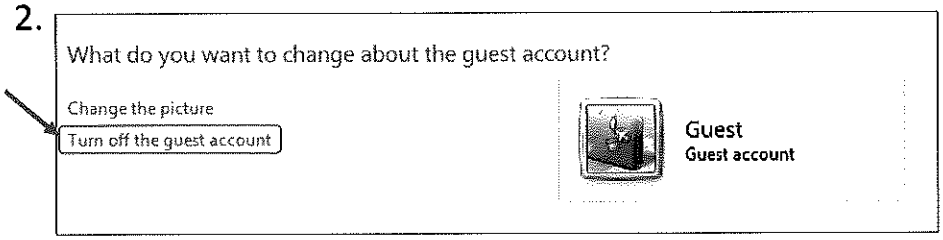
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

1.



2.

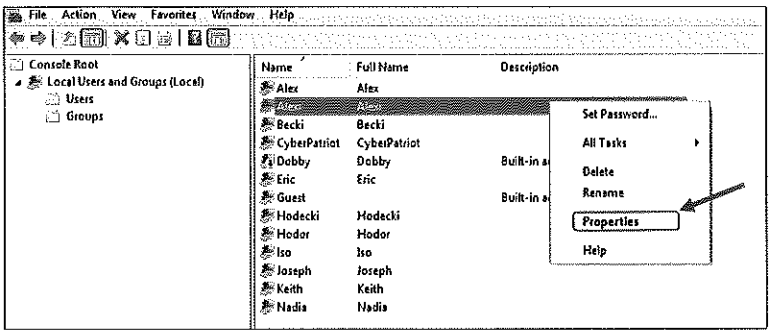


Best Practice: Restrict Administrator Group Membership

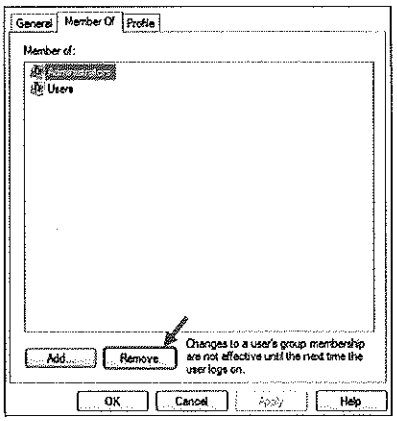
Console option:

- Administrator accounts allow people to efficiently make changes across a network or computer and to monitor and control the use of shared resources
  - Because of those advanced permissions, administrator accounts need to be especially well-protected and limited to only a few individuals.
- Remove unnecessary users from the Administrators Group

1.



2.

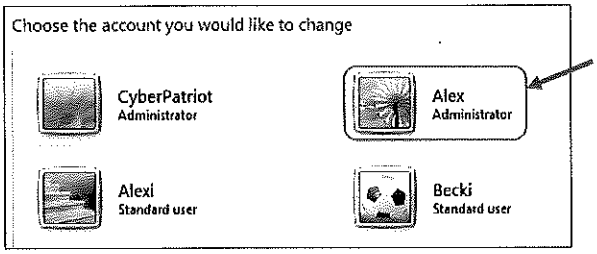


Best Practice: Restrict Administrator Group Membership

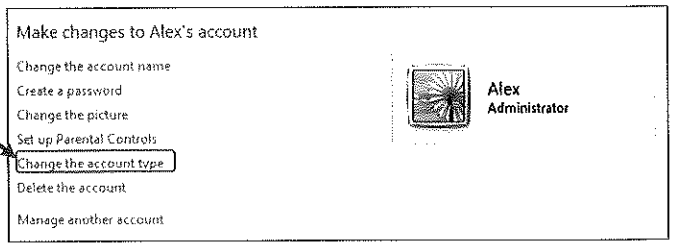
Control Panel option:

- Control Panel → User Accounts → Manage another account

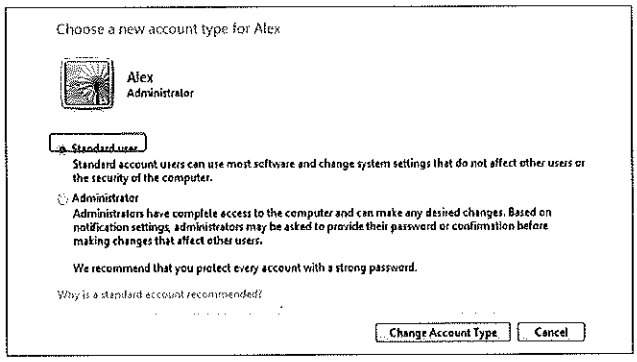
1.



2.



3.

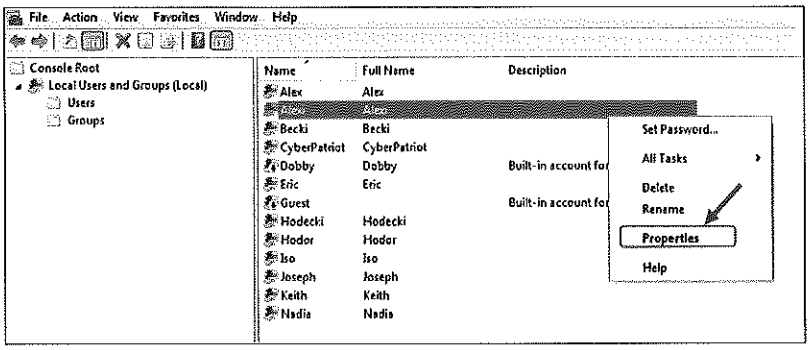


Best Practice: Set Passwords for all Accounts

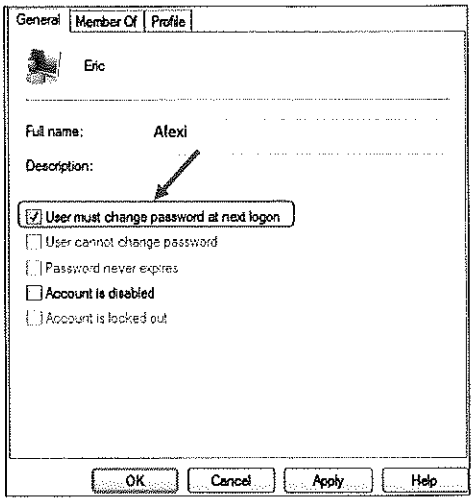
Console option:

- Make sure all accounts are password protected

1.



2.

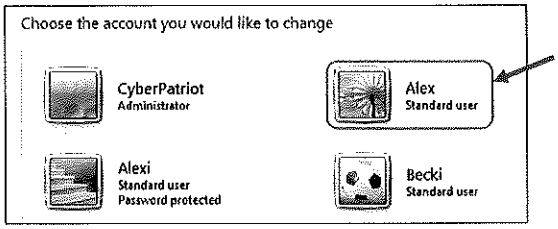


Best Practice: Set Passwords for all Accounts

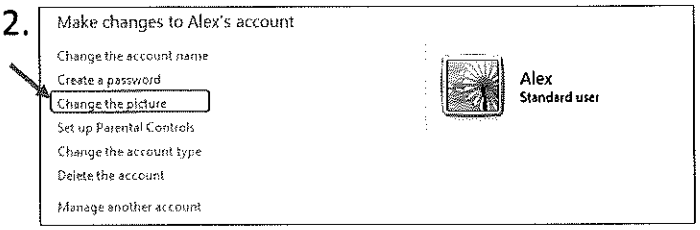
Control Panel option:

- Control Panel → User Accounts → Manage another account

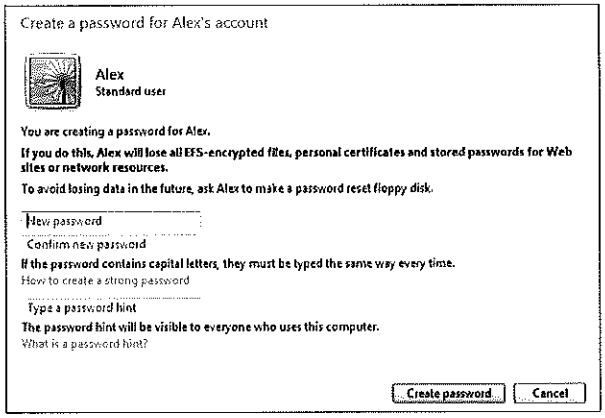
1.



2.



3.

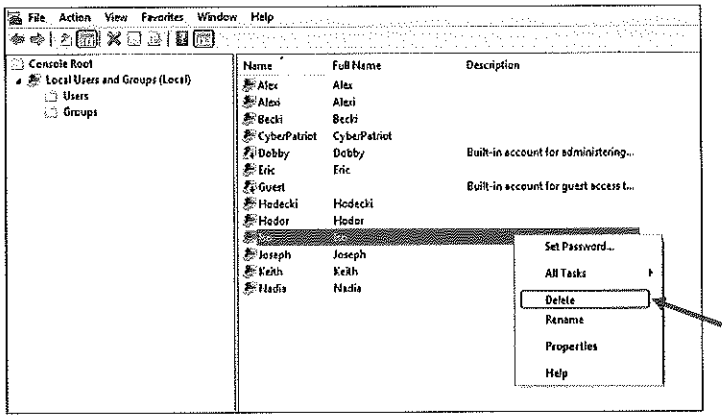


Removing Users

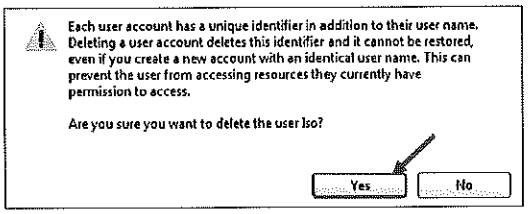
Console option:

- Only current, authorized employees should have access to a organization's network
- Make sure your user directory is up-to-date and remove unnecessary accounts

1.



2.

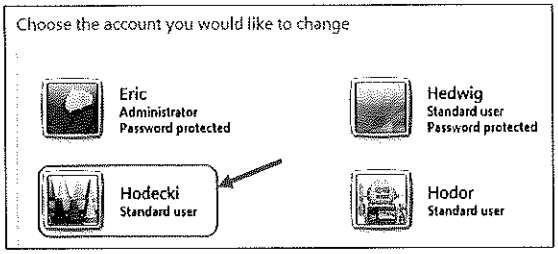


Removing Users

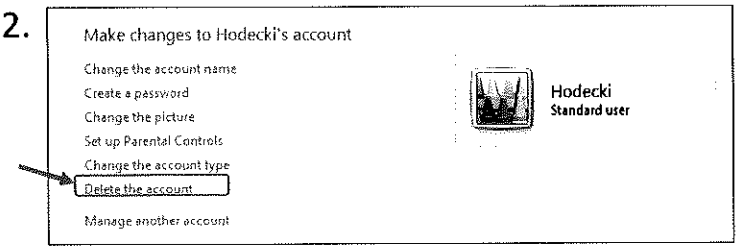
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

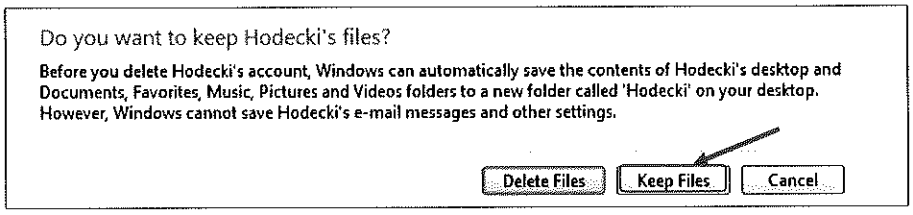
1.



2.



3.

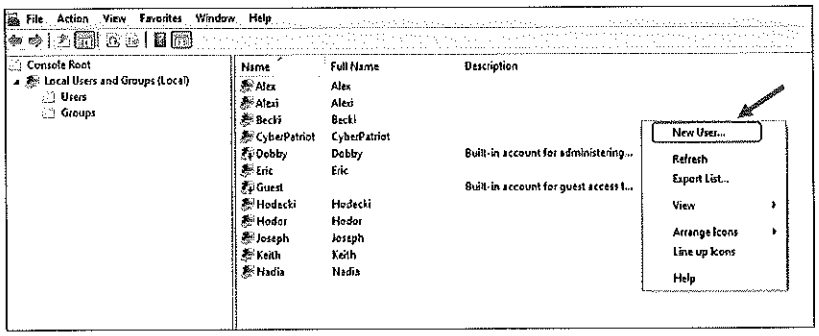


Adding Users

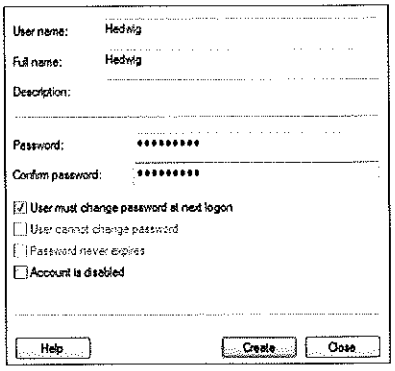
Console option:

- When adding new accounts, make sure to put the account in the right User Group and password protect the new user's account

1.



2.

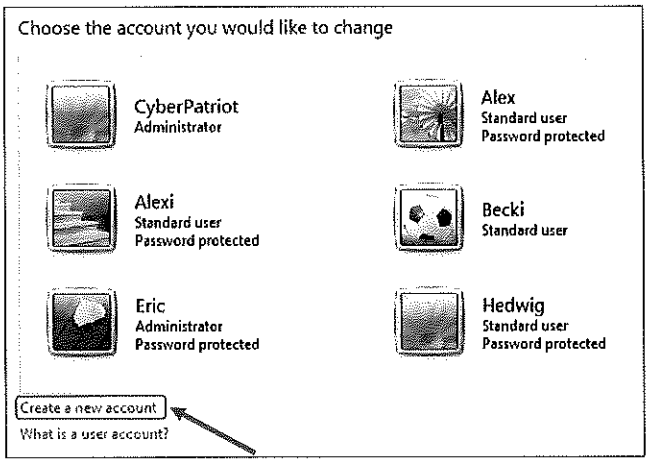


Adding Users

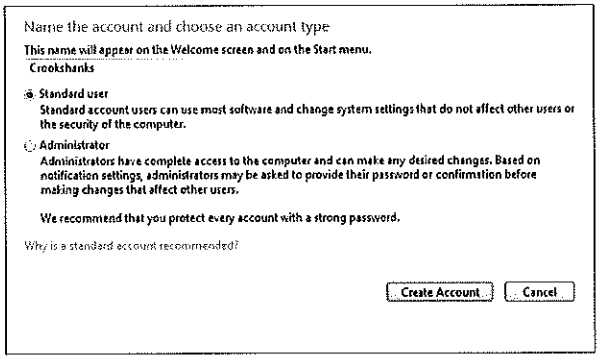
Control Panel option:

- Control Panel → User Accounts → Add or remove user accounts

1.



2.



SECURITY INCIDENT SURVEY CHEAT SHEET FOR SERVER ADMINISTRATORS

Tips for examining a suspect system to decide whether to escalate for formal incident response.

Assessing the Suspicious Situation

Retain attacker's footprints, avoid taking actions that access many files or installing tools.

Look at system, security, and application logs for unusual events.

Look at network configuration details and connections; note anomalous settings, sessions or ports.

Look at the list of users for accounts that do not belong or should have been disabled.

Look at a listing of running processes or scheduled jobs for those that do not belong there.

Look for unusual programs configured to run automatically at system's start time.

Check ARP and DNS settings; look at contents of the hosts file for entries that do not belong there.

Look for unusual files and verify integrity of OS and application files.

Use a network sniffer, if present on the system or available externally, to observe for unusual activity.

A rootkit might conceal the compromise from tools; trust your instincts if the system just doesn't feel right.

Examine recently-reported problems, intrusion detection and related alerts for the system.

If You Believe a Compromise is Likely...

Involve an incident response specialist for next steps, and notify your manager.

Do not panic or let others rush you; concentrate to avoid making careless mistakes.

If stopping an on-going attack, unplug the system from the network; do not reboot or power down.

Take thorough notes to track what you observed, when, and under what circumstances.

Windows Initial System Examination

Look at event logs	`eventvwr`
Examine network configuration	`arp -a`, `netstat -nr`
List network connections and related details	`netstat -nao`, `netstat -vb`, `net session`, `net use`
List users and groups	`lusrmgr`, `net users`, `net localgroup administrators`, `net group administrators`
Look at scheduled jobs	`schtasks`
Look at auto-start programs	`msconfig`
List processes	`taskmgr`, `wmic process list full`
List services	`net start`, `tasklist /svc`
Check DNS settings and the hosts file	`ipconfig /all`, `ipconfig /displaydns`, `more %SystemRoot%\System32\Drivers\etc\hosts`
Verify integrity of OS files (affects lots of files!)	`sigverif`
Research recently-modified files (affects lots of files!)	`dir /a/o-d/p %SystemRoot%\System32`

Avoid using Windows Explorer, as it modifies useful file system details; use command-line.

Unix Initial System Examination

Look at event log files in directories (locations vary)	`/var/log`, `/var/adm`, `/var/spool`
List recent security events	`wtmp`, `who`, `last`, `lastlog`
Examine network configuration	`arp -an`, `route print`
List network connections and related details	`netstat -nap` (Linux), `netstat -na` (Solaris), `lsof -i`
List users	`more /etc/passwd`
Look at scheduled jobs	`more /etc/crontab`, `ls /etc/cron.*`, `ls /var/at/jobs`
Check DNS settings and the hosts file	`more /etc/resolv.conf`, `more /etc/hosts`
Verify integrity of installed packages (affects lots of files!)	`rpm -Va` (Linux), `pkgchk` (Solaris)
Look at auto-start services	`chkconfig --list` (Linux), `ls /etc/rc*.d` (Solaris), `smf` (Solaris 10+)
List processes	`ps aux` (Linux, BSD), `ps -ef` (Solaris), `lsof +L1`
Find recently-modified files (affects lots of files!)	`ls -lat /`, `find / -mtime -2d -ls`

Incident Response Communications

Do not share incident details with people outside the team responding to the incident.

Avoid sending sensitive data over email or instant messenger without encryption.

If you suspect the network was compromised, communicate out-of-band, e.g. non-VoIP phones.

Key Incident Response Steps

1. Preparation: Gather and learn the necessary tools, become familiar with your environment.
2. Identification: Detect the incident, determine its scope, and involve the appropriate parties.
3. Containment: Contain the incident to minimize its effect on neighboring IT resources.
4. Eradication: Eliminate compromise artifacts, if necessary, on the path to recovery.
5. Recovery: Restore the system to normal operations, possibly via reinstall or backup.
6. Wrap-up: Document the incident's details, retail collected data, and discuss lessons learned.

Other Incident Response Resources

Windows Intrusion Discovery Cheat Sheet
http://sans.org/resources/winsacheatsheet.pdf

Checking Windows for Signs of Compromise
http://www.ucl.ac.uk/cert/win_intrusion.pdf

Linux Intrusion Discovery Cheat Sheet
http://sans.org/resources/linsacheatsheet.pdf

Checking Unix/Linux for Signs of Compromise
http://www.ucl.ac.uk/cert/nix_intrusion.pdf

Authored by Lenny Zeltser, who leads a security consulting team at SAVVIS, and teaches malware analysis at SANS Institute. Special thanks for feedback to Lorna Hutcheson, Patrick Nolan, Raul Siles, Ed Skoudis, Donald Smith, Koon Yaw Tan, Gerard White, and Bojan Zdrnja.

netstat
see open ports and connections

schtasks
- shows jobs

net users
- shows users

net group administrators
- shows admins

CyberPatriot Competition Checklist

Manual	Automated
☐ Read the Read Me file – highlight, take notes	☐ User Rights – update registry
☐ Answer Forensics Question(s)	☐ MalwareBytes for malware
☐ Turn on Firewall	☐ Automatic Updates – download and install
☐ Action Center	☐ AV scan
☐ User Account Control	
☐ Secure Users and Groups (Guest/Admin, etc.)	
☐ Passwords for accounts	
☐ Password Policies	
☐ Remove/Disable Insecure Services	
☐ Local Security Policy (if not by .inf file)	
☐ Update appropriate software	
☐ Uninstall unnecessary software	
☐ Search for inappropriate files – media, hack tools, etc.	
☐ Secure File and Directory shares	
☐ Check Open Ports	
☐ Check for Anti-Virus Program	
☐ Check for abnormal behavior	

Ensure you are not rebooting the machine for updates with less than an hour to go!

Document each and every action you perform – whether the setting works or not.

Windows 8

- Right click on windows symbol to get to actions.
- Right click on windows system and then System then Control Panel then Administrative tools then Local Security Policy.

Firewall

- Windows → Control Panel → System and Security → Windows Firewall
- Turn Windows Firewall On or Off
- Then turn it on

Action Center

Click on the flag on the bottom right and then click on Action Center. You can manage a lot of things from right here.

You can also get into it from Control Panel (Windows) → Systems and Security → Action Center

Users

- To remove a user that should not be there.
- Control Panel (Windows) → Computer Right mouse click and Manage → Then go to Local Users and Groups and then click on the Folder Users.
- Click on the User you don't want and right click and go to properties and click on Account is disabled. Then Apply and OK.

- Ubuntu - Administration → Users and Groups → Click to Unlock it and then Advanced Settings. Type in your password and then you can make your changes.

Passwords

- Stay with the users and click on the user and then right click and then set the account.

- Ubuntu - settings and go to Users and Groups, unlock and the unlock and hit set password.

- To remove someone from admin - Right click on Computer and then Manage.
- Then click on Local Users and Group then on Groups and click on Administrators.
- Then click on the user you want to remove and then click on remove.
- You can then Add someone in the same pane.

Password Policies and User Rights

- Search type in local security policy
- click on Local Policies or Account Policies
- Under Account Policies click on Password Policy
- Under Local Policies there are Audit Policy (we have never gotten points for it) They should all be turned on.
- User Rights Assignment is VERY important
- This is where you could find things like not allowing access through remote desktop
- If you double click on any of them, then you can make changes.

Services

There are things that could be running on your computer and things that you might want to get rid of. Use the 3 page Vulnerabilities List that was provided. You should check these to make sure that none of these services are running.

How to turn them off.

- Windows → Right click on Computer and then Manage. click on Services and Application and Services. then click on the service and right click and then click on Properties and then change the Startup type to Disabled. To make it quicker, click on Status and then you can see what is "Started". Make sure it has Stopped and then click on Apply.

Ubuntu - Go to the Software Center and then download Synaptic Software Manager and search for _____
Using the command line: sudo service -- status - all
To disable sudo _____

Local Security Policy (if not by .inf file)

- Use the .inf tool that we have provided. Run this according the directions. Follow the directions step-by-step and this should set everything needed.

Update Software (Automatic Updates)

- Make sure we have automatic updates on. This will assure you of points.
- Click on Windows → Control Panel → System and Security → Windows Update
- Click on Check for Updates and Turn Automatic Updating on or off

- Ubuntu - Linux - Update Manager hit settings button and turn on recommended updates
- System → Administration → Update Manager

Unwanted Software

Go to Program Files and then remove software that does not belong. This will be identified in the readme file.

Or go to Start and Control Panel and Programs and features. You will see all the programs listed.

Ubuntu - go to command line and type "find nc". This pops open the file manager and you can look through this.

Search for files

- Bring up Windows and use the Search in the right corner to look for *.mp4 files or *.jpeg files. Then you can remove files if needed.

Shares

- Windows and right click on computer and Manage and then Shared Folders and check your shares. There should only be 3 ADMIN$, C$, IPC$. Right mouse click and the Stop Shares.

Check Open Ports

We need to add something for this one. Check another page.

Automated Programs

Go to the folder on regular computer (minimize vm). Click on CyberPatriot → Tools. There are the different tools there that automate updates, check processes, etc. Auto runs

Shortcuts

- Click on the Windows button CTRL - R - Opens to run a program.
- Secpol.msc - type this in the MS button in the search bar. From here you can set the security policy.

Process Explorer

Use Process Explorer to find processes. When they come up red, right click and it will tell you the path so we can see where a bad process is running.

Bash Scripting can be used to write scripts to be used with LINUX.
Power Shell Scripting for Windows
Command line scripting Warriors

Cyber Patriot
Securing Windows 7

Secure Windows Password (Press start and search for local security policy or go to the control panel\System and Security\Administrative tools)
•Password History 5 Days
•Maximum Password age 30-90 days
•Minimum Password age 5 days
•Minimum Password Length 8 char.
•Password Complexity Enabled
•Reverse Encryptions Disabled

Account Lockout Policies (Right under Password policies)
•Account Lockout Duration 30 minutes
•Account Lockout Threshold 3
•Reset account lockout counter 30 minutes

Set up Windows Audit Policies (Right under Account Polices in Local Policies)
•Audit Logon Events Failure
•Audit Account Management Success
•Audit Directory Service ND
•Audit logon Events Failure
•Audit Objects Access ND
•Audit Policy Change Success
•Audit Privilege use success failure
•Audit Process tracking Success Failure
•Audit System Events failure
Security Options (Beneath User Rights Assignment in Local Policies)
•Disable Administrator account
•Disable Guest account
•Rename administrator and guest accounts
•Shutdown Without Log on.

TURN ON WINDOWS FIREWALL

Change Passwords for Each User (User policy)

Install automatic updates (Control Panel Action Tools under System in security.)

Update Windows Programs (i.e. PowerShell, IE all the way to 10)

Set local user Admin password to not expire and account enable Admin tools\Computer management\users and group\use R

Disable and Stop Services in the services menu
- RDP
- ICS
- RDP UserMode
- Remote Registry
- RD Configuration
- SSDP Discovery
- UPnP Device Host
- Remote Desktop
- WWW Publishing Service

Clean the Host File (C:\Windows\System32\drivers\etc\host.txt

Deny Following Ports
- FTP
- SSH
- TelNet
- SNMP
- LDAP
- RDP

Windows 7 Service packs Installed

Check List: Windows Machines

High Level

- Start Downloading Important Service Packs and Windows Updates.
  - DO NOT RESTART UNTIL LATER!!
- Look for alternatives to default applications
  - Install Firefox
- Install and maintain malware protection software
  - Install MalWare (Defender)
  - Install AntiVirus (Microsoft Security Essentials)
- Uninstall Dangerous Software
- Account Management
  - Remove guest user
  - Remove old accounts
  - Ensure all accounts use strong passwords
- Security Settings
  - Account Policies
  - Local Policies
- Action Center
- Windows Firewall
- Secure Internet Connections
- Services
  - Disable unnecessary services
    - IIS
    - Telnet
    - Web Services
    - FTP
- Delete Suspicious Files (Write down file names and locations that were deleted)
- Delete Unauthorized Files Write down file names and locations that were deleted)
- Disable dangerous features
- Configure System Startup
- Attach Detection
  - Task Scheduler & Task Manager
  - Monitor Performance and Resource Usage
  - Port Checks
  - Event Viewer
- Windows Update – Restart

Low Level

- Download Important Service Packs and Windows Updates.
  - **Control Panel -> Windows Update -> Install Updates**
  - Iconize Windows Update Window
  - **DO NOT RESTART UNTIL LATER!!! (Takes a while to update system)**
- Install/Update Firefox Browser as alternate to Internet Explorer
  - Firefox - https://www.mozilla.org/en-US/firefox/new/
- Install Malware and Anti-Virus Software
  - Install MalWare (Defender)
  - Install AntiVirus (Microsoft Security Essentials) - http://windows.microsoft.com/en-US/windows/security-essentials-download
- Unistall Dangerous Software
  - **Control Panel -> Programs and Features**
- Account Management
  - **Control Panel -> User Accounts -> Manage another account**
  - Delete or Turn off Guest Account
  - Delete Unauthorized Accounts
    - Write down deleted Account Names
  - Make sure all accounts are User accounts except those that authorized as Administrators
  - Ensure that all accounts are password protected.
- Security Settings
  - **Control Panel -> Administrative Tools -> Local Security Policy**
  - Account Policies
    - Password Policy
      - Enforce password history – 5
      - Maximum password age – 90 user 30 admin
      - Minimum password age – 10–30 days
      - Minimum password length – 8
      - Password must meet complexity requirement – Enable
      - Store password using reversible encryption – Disable
      - Passwords
        - Always use at least 3 of the following
          - Numbers
          - Lower case letters
          - Upper case letters
          - Symbols (%#*&!;{">|)
        - Always use at least 8 characters
        - Use different password for each login
      - Do not use any personal info –can be easily found by other means
        - -Name
        - -Birthday
        - -Pet's Name
        - -Mother's Maiden Name
        - -Hometown
    - Account Lockout Policy
      - Account lockout duration - 30
      - Account lockout threshold – 3-10
      - Reset account lockout counter after - 30
  - Local Policy
    - Audit Policy Settings
      - Control Panel →System and Security → Administrative Tools → Local Security Policy → Local Policies → Audit Policy
        - Success: generates an event when the requested action succeeds
        - Failure: generates an event when the requested action fails

        - No Auditing: does not generate an event for the action
    - Right click the Security Setting column → Properties → Success, Failure
    - Must be set and enabled for logs to be available in the Event Viewer
        - Account logon events: Attempts to log into system accounts
        - Account management: Account creation or deletion, password changes, user group changes
        - Directory service access: Changes to shared resources on a network
        - Logon events: Attempts to log into a specific shared computer
        - Object access: Access to sensitive, restricted files
        - Policy change: Attempts to change local security policies, user rights, and auditing policies
        - Privilege use: Attempts to execute restricted system changes
        - Process tracking: Attempts to modify program files, which have rewritten or disrupted program processes (*key to detecting virus outbreaks)
        - System events:Computer shutdowns or restarts
        - *Recommended for Windows 7 users and Windows Server 2008 users
        - *Recommended only for Windows Server 2008 users
    - User Rights Assignment
        - Access this computer from the network – Remove "Everyone"
- Action Center
    - **Control Panel -> System and Security -> Action Center**
    - Windows Updates
        - Install Updates Automatically
- Windows Firewall
    - **Control Panel -> System and Security -> Windows Firewall->Change notification settings**
    - Turn Firewall on for Home, Work, and Public
    - Select "Block all incoming connections, including those in the list of allowed programs" for both
    - Select "Notify me when Windows Firewall blocks a new program" for both
    - **Control Panel -> System and Security -> Windows Firewall->Advanced settings**
    - Allow trusted programs to connect without being blocked by adding them to your Windows Firewall Exceptions list
        - For each network type, you can customize whether you want the programs allowed through
    - It's much safer to allow only certain programs through your firewall than to open an entire port to traffic
        - Ports are numbers that identifies one side of a connection between two computers
    - Common Exceptions
        - Core Networking
            - Regular Microsoft Windows services that retrieve data from the Internet
            - If you don't enable this exception across all three types of networks, some Microsoft services and programs will not run properly
        - File and Printer Sharing - off
        - Remote Assistance - off
        - Remote Desktop - off
        - UPnP Framework (Universal Plug-and-Play) -off
    - Advanced Settings
        - Inbound Rules
        - Outbound Rules
        - Connection Security Rules
        - Monitoring
- Secure Internet Connections
    - **Control Panel -> Internet Options**
    - Security Tab
        - Security Level – High
    - Privacy Tab
        - Block All Cookies
        - Never allow websites to request your physical location
        - Turn on Pop-up Blocker

        - Disable toolbars and extensions when InPrivate Browsing starts
    - Advanced
- Services
    - **Control Panel -> Administrative Tools -> Services**
    - Disable unnecessary services (Stop and Disable)
        - IIS
        - NetMeeting Remote Desktop Sharing – VoIP
        - Remote Desktop Help Session Manager
        - Remote Registry
        - Routing and Remote Access
        - Simple File Sharing
        - SSD Discovery Service
        - Telnet
        - FTP
        - Universal Plug and Play Device Host
        - Windows Messenger Service
- Delete Suspicious Files
    - Look in C:\Windows\System & C:\Windows\System32 for programs with recent timestamps
    - Look in C:\Program Files\ for any suspicious programs
    - Write down file names and locations that were deleted
- Delete Unauthorized Files
    - Remove any unauthorized media files
    - Write down file names and locations that were deleted
- Disable Dangerous Features
    - **Control Panel -> System -> Remote settings**
    - Select "Don't allow connections to this computer"
- Configure System Startup
    - **Control Panel -> Control Panel -> System and Security -> Administrative Tools -> System Configuration**
    - **Control Panel -> Control Panel -> Administrative Tools -> System Configuration**
    - Remove any unnecessary startup processes
- Attach Detection
    - Task Scheduler & Task Manager
        - Check for unusual processes
        - Check for any netcat processes running
    - Performance Monitoring
        - Allows you to track the use and performance of hardware and software resources on a system
        - Allows you to view real-time and historical data
            - Stop problems as they're happening
            - Predict future problems
            - Conduct forensics to close vulnerabilities and stop intrusions of the same type from happening again
        - Allows you to decide if hardware or software needs updating
        - Allows you to determine if unknown programs and/or malware are running
        - Allows you to monitor and restrict user access
        - Task Manager
            - **Menu Bar -> Start Task Manager**
            - Applications
                - Programs you interact with on the desktop
                - Three tasks:
                    1. Close programs that are not responding
                    2. Check if an unnecessary piece of software is running
                    3. Find the process that is associated with certain software, so you do not shut it down when looking for illegitimate services
            - Processes
                - Some processes are essential for Windows and should not be shut down

- Some malware are not visible as applications and can only be ended by shutting down associated services
- Lookup processes to determine whether they are legitimate: www.processlibrary.com
- Terminate
- Set Priorites
- View CPU Usage
- View Memory Usage
-

- Services
  - Services are programs that run invisibly and automatically in the background
  - List of processes running in the background
    - Status:
      - Started: Currently running
      - Blank: Not running
    - Startup Type (how services start when the computer is booted up):
      - Automatic: Starts when computer is booted up
      - Manual: Starts when prompted to by user
      - Disabled: Cannot be re-enabled automatically or manually by regular users (only Admins)
  - Disable Services
    - Two reasons to disable services:
      i. Unnecessary
         - E.g. Spotify or other programs that decrease student/worker efficiency
      ii. Insecure
         - E.g. Remote Desktop Services or others than allow people to access your file systems from outside the organization's networks
    - To disable a service or otherwise change its startup type, right-click it and select "Properties"
  - Click the "Services" button to manage services in advanced window
- Performance
  - Monitor performance and resources
  - Overall statistics for system usage
    - CPU Usage by core
    - Memory Usage
      - Displays the amount of RAM being used over time. Extremely high values could indicate hidden malware is operating on your system.
      - Provides details on how RAM is being used. Cached RAM is used by system resources, available RAM is the amount immediately available for use by processes, drivers, or the OS, and free RAM is unused or does not contain useful information
      - Lists how much memory is being used by the OS as a whole. If these numbers are very high, Windows might be corrupt or there is a piece of malware that is hampering its ability to run effectively.
    - Number of processes
- Network Activity
  - Shows wired and wireless activity
  - Network connectivity problems can arise from a broken router, switch, or cable, or from the computer itself
    - The Networking tab will allow you to check whether the computer is the origin of the problem

- Lists the names of your connections and tells you the percentage of your overall network that each connection is utilizing, the speed of the link, and whether or not that link is fully connected.
- Shows network performance over time. If utilization is very high one or more programs on your may be eating up all of your available bandwidth. Or, if you are not currently using any programs connected to the Internet, a high number could indicate you have malware on your computer or that an intruder is accessing your computer remotely.

- Users
  - Look for unknown users
  - Users can be disconnected and/or logged off
  - Shows you all of the users currently logged on to the system
  - Allows you to "disconnect" users
    - Terminate the user's connection without shutting down the programs they were running
  - Allows you to "logoff" users
    - Log the user off the computer completely and terminate any running programs

- View performance data for system, both real time and logs
  - Event Log Performance
    - **Control Panel -> Performance Information and Tools -> Advanced Tools -> View performance details in Event Log**
  - Resource Monitor
    - **Control Panel -> Performance Information and Tools -> Advanced Tools -> Open Resource Monitor**
- Obtain information about hardware, software components, and monitor security events on a local or remote computer
- Look for processes that may be over utilizing resources or not functioning properly
- Look for unknown processes running
- Identify and diagnose current system problems
- Predict potential system problems

- Port Checks
  - Open command prompt and run command: netstat -aon
- Event Viewer
  - Control Panel → System and Security → Administrative Tools → Event Viewer
  - Security tool that allows you to view records of changes and other events that have happened on a computer
  - Used by cybersecurity professionals to monitor system changes and the inner workings and less visible processes run by a computer
  - Security logs can be a useful last defense against attacks and a tool for forensics investigations into the source of a past attack or unauthorized entry
  - Customize what security logs are kept by setting Audit Policies
  - Windows Log
    - Application – Events logged by programs
    - Security – Any successful or unsuccessful logon attempts
    - Setup – Events that occurred during installation
    - System – Events logged by system componenets
    - Forward Events – Events forwarded from other computers

- Updates/Patches
  - Windows Update
    - **Control Panel -> Windows Update -> Restart**

Ed's Windows 7 Checklist

Reminder that your checklist is on the internet for all to see, and all to edit. I could have deleted all of this. I recommend you take this down. I didn't even need a real email address to sign up.

- Michael

'*1.* **Document the Readme and all forensics questions:** Ensure that you have created a good record of what the readme is telling you, and what the forensics questions are asking for. **MAKE SURE YOU HOLD ON TO THIS.** Your documentation will not only help you during the competition, but can also help you prepare for future images.

2. Search for forensics questions answers: I like to do this first because sometimes the forensics questions deal with malware, incorrect settings, or other items you would change. If you remove malware that the forensics question is asking you about, you're not going to be able to find the answer. This is an easy way to earn points.

3. Go through the User Accounts section of the Control Panel: Look through all of the users. Make sure that they are at the level that they need to be at, are adhering to password policies, and are actually supposed to be there. Disable the guest account unless the readme specifically tells you not to.

4. Set the security policies in secpol.msc: Go through secpol.msc and set the Password and Audit log settings. They should look something like this:

- Enforce Password History: 5 passwords remembered
- Maximum Password Age: 30 to 90 days
- Minimum Password Age: 5 days
- Minimum Password Length: 8 characters
- Password must meet complexity requirements?: Yes
- Store passwords using reversible encryption?: No.

You should also go through and turn on auditing for failed and successful log-ons while in secpol.msc.

5. Enable UAC (User Account Control): Turning UAC up to the highest level is generally a good practice and will earn you points in most cases.

6. Enable Windows Firewall: Turning on the Windows Firewall is a requirement in most images. The level of protection for your system may vary, and some exceptions in the firewall may apply. Be sure to check that the firewall is still up periodically after you do it the first time.

8. Check the Windows Scheduled Tasks: If you've been experiencing any unexplained settings changing, pop-ups, or any other odd behavior, check the Scheduled Tasks. Look for anything that runs suspicious programs, opens error messages, etc. This is tedious, but is a good way to earn some extra points. Figuring out how often the nuisance

occurs is a good way to nail down exactly what scheduled task is causing your problem.

9. Look at Windows features in Programs and Features: Look for anything that you know that your computer shouldn't have. Telnet is usually a no-no, but sometimes the Readme tells you to leave it on, or even enable it. Make sure your computer isn't running a web server if it shouldn't be.

10. Look for junk programs, malware, and hacking tools: The Programs and Features section of the control panel will display a list of programs that are installed. This is a good place to find programs that you can install for some extra points. Tools like JRT and PC Decrapifier help expedite this process, but there's no alternative to looking for yourself.

11. Ensure that all required programs are running correct versions: Note that the latest version is not always the correct version. The readme will usually tell you what version of a program to have.

12. Enable Antivirus Software: Free antivirus software like AVG or Avast will do, but it has to be a free trial version for the competition. Scanning the system with MalwareBytes is a good idea, too.

13. Use Process Explorer to see what's running on your computer: I could write an article just about this. Look for anything suspicious. Remove. Repeat.

14. Use Autoruns to see what's running when you first start up your computer: This will help you locate pop-ups, and speed up start times.

15. Make sure any important Windows Updates and Patches are installed: This can be a long and tedious process, so see what you can bring in on removable media to help speed up the process.

16. Verify that your browser is in good, working, uncluttered order: Make sure that there are no unauthorized add ons, plug-ins, un-needed toolbars, etc. The process for removing these items varies by browser.

17. Make sure your image doesn't contain any unauthorized media files: Things like .mp3, .mov, have to go. Using the Windows search bar (*.mp3 searches the selected area for .mp3 files) is a good place to quickly find these media files.

18. Use netstat -a to look for unauthorized ports: Netstat -a in the command prompt will show you all of the entries and exits going through your computer. Check iana's list of common ports to help decide what you should keep.

19. Go through everything more than once, and document everything: Going back through and making sure everything is exactly how you left it and how you want it is a good way to find errors that you might have missed. Documenting everything helps identify errors that you may have caused.

☺

Reg Command

Adding Keys and Values:

```
C:\> reg add
[\\TargetIPaddr\] [RegDomain]\[Key]
```

Add a key to the registry on machine `[TargetIPaddr]` within the registry domain `[RegDomain]` to location `[Key]`. If no remote machine is specified, the current machine is assumed.

Export and Import:

```
C:\> reg export [RegDomain]\[Key]
[FileName]
```

Export all subkeys and values located in the domain `[RegDomain]` under the location `[Key]` to the file `[FileName]`

```
C:\> reg import [FileName]
```

Import all registry entries from the file `[FileName]`

Import and export can only be done from or to the local machine.

Query for a specific Value of a Key:

```
C:\> reg query
[\\TargetIPaddr\] [RegDomain]\[Key] /v
[ValueName]
```

Query a key on machine `[TargetIPaddr]` within the registry domain `[RegDomain]` in location `[Key]` and get the specific value `[ValueName]` under that key. Add /s to recurse all values.

WMIC

Fundamental grammar:

```
C:\> wmic [alias] [where clause] [verb
clause]
```

Useful `[aliases]`:

```
process          service
share            nicconfig
startup          useraccount
qfe  (Quick Fix Engineering – shows patches)
```

Example `[where clauses]`:

```
where name="nc.exe"
where (commandline like "%stuff")
where (name="cmd.exe" and
    parentprocessid!="[pid]")
```

Example `[verb clauses]`:

```
list [full|brief]
get [attrib1,attrib2…]
call [method]
delete
```

List all attributes of `[alias]`:

```
C:\> wmic [alias] get /?
```

List all callable methods of `[alias]`:

```
C:\> wmic [alias] call /?
```

Example:

List all attributes of all running processes:

```
C:\> wmic process list full
```

Make WMIC effect remote `[TargetIPaddr]`:

```
C:\> wmic /node:[TargetIPaddr]
/user:[User] /password:[Passwd] process
list full
```

Windows Command Line Cheat Sheet

By Ed Skoudis

POCKET REFERENCE GUIDE

SANS INSTITUTE
http://www.sans.org

Purpose

The purpose of this cheat sheet is to provide tips on how to use various Windows command that are frequently referenced in SANS 504, 517, 531, and 560.

Process and Service Information

List all processes currently running:

```
C:\> tasklist
```

List all processes currently running and the DLLs each has loaded:

```
C:\> tasklist /m
```

Lists all processes currently running which have the specified `[dll]` loaded:

```
C:\> tasklist /m [dll]
```

List all processes currently running and the services hosted in those processes:

```
C:\> tasklist /svc
```

Query brief status of all services:

```
C:\> sc query
```

Query the configuration of a specific service:

```
C:\> sc qc [ServiceName]
```

Shutdown and Restart

Shutdown Windows immediately:
```
C:\> shutdown /s /t 0
```

Note: Command may not power down the hardware.

Restart Windows immediately:
```
C:\> shutdown /r /t 0
```

Abort shutdown/restart countdown:
```
C:\> shutdown /a
```

Useful Netstat Syntax

Show all TCP and UDP port usage and process ID:
```
C:\> netstat -nao
```

Look for usage of port `[port]` every `[N]` seconds:
```
C:\> netstat -nao [N] | find [port]
```

Dump detailed protocol statistics:
```
C:\> netstat -s -p [tcp|udp|ip|icmp]
```

Installing Built-in Packages on Vista

Install telnet service on Vista:
```
C:\> pkgmgr /iu:"TelnetServer"
```

Install telnet client on Vista:
```
C:\> pkgmgr /iu:"TelnetClient"
```

Install IIS on Vista:
```
C:\> pkgmgr /iu:IIS-WebServerRole;WAS-
WindowsActivationService;WAS-
ProcessModel; WAS-NetFxEnvironment;WAS-
ConfigurationAPI
```
To remove any of these packages, replace install update (/iu) with uninstall update (/uu)

File Search and Counting Lines

Search directory structure for a file in a specific directory:
```
C:\> dir /b /s [Directory]\[FileName]
```

Count the number of lines on StandardOuy of `[Command]`:
```
C:\> [Command] | find /c /v ""
```

Finds the count (/c) of lines that do not contain (/v) nothing (""). Lines that do not have nothing are all lines, even blank lines, which contain CR/LF

Command Line FOR Loops

Counting Loop:
```
C:\> for /L %i in
([start],[step],[stop]) do [command]
```

Set `%i` to an initial value of `[start]` and increment it by `[step]` at every iteration until its value is equal to `[stop]`. For each iteration, run `[command]`. The iterator variable `%i` can be used anywhere in the command to represent its current value.

Iterate over file contents:
```
C:\> for /F %i in ([file-set]) do
[command]
```

Iterate through the contents of the file on a line-by-line basis. For each iteration, store the contents of the line into `%i` and run `[command]`.

Invoking Useful GUIs at the Command Line

Local User Manager (includes group management):
```
C:\> lusrmgr.msc
```

Services Control Panel:
```
C:\> services.msc
```

Task Manager:
```
C:\> taskmgr.exe
```

Security Policy Manager:
```
C:\> secpol.msc
```

Event Viewer:
```
C:\> eventvwr.msc
```

Control Panel:
```
C:\> control
```

Close GUI windows by hitting Alt-F4

Interacting with the Network Using Netsh

Turn off built-in Windows firewall:
```
C:\> netsh firewall set opmode disable
```

Configure interface "Local Area Connection" with `[IPaddr] [Netmask] [DefaultGW]`:
```
C:\> netsh interface ip set address
local static [IPaddr] [Netmask]
[DefaultGW] 1
```

Configure DNS server for "Local Area Connection":
```
C:\> netsh interface ip set dns local
static [IPaddr]
```

Configure interface to use DHCP:
```
C:\> netsh interface ip set address
local dhcp
```

Unusual Log Entries

Check your logs for suspicious events, such as:

- "Event log service was stopped."
- "Windows File Protection is not active on this system."
- "The protected System file [file name] was not restored to its original, valid version because the Windows File Protection..."
- "The MS Telnet Service has started successfully."
- Look for large number of failed logon attempts or locked out accounts.

To do this using the GUI, run the Windows event viewer:

```
C:\> eventvwr.msc
```

Using the command prompt:

```
C:\> eventquery.vbs | more
```

Or, to focus on a particular event log:

```
C:\> eventquery.vbs /L security
```

Other Unusual Items

Look for unusually sluggish performance and a single unusual process hogging the CPU: Task Manager → Process and Performance tabs

Look for unusual system crashes, beyond the normal level for the given system.

Additional Supporting Tools

The following tools are not built into Windows operating system but can be used to analyze security issues in more detail. Each is available for free download at the listed web site.

DISCLAIMER: The SANS Institute is not responsible for creating, distributing, warranting, or supporting any of the following tools.

Tools for mapping listening TCP/UDP ports to the program listening on those ports:

Fport – command-line tool at www.foundstone.com

TCPView – GUI tool at www.microsoft.com/technet/sysinternals

Additional Process Analysis Tools:

- Process Explorer – GUI tool at www.microsoft.com/technet/sysinternals
- TaskMan+ -- GUI tool at http://www.diamondcs.com.au

The Center for Internet Security has released various Windows security templates and security scoring tools for free at www.cisecurity.org.

SANS INSTITUTE

Intrusion Discovery

Cheat Sheet v2.0

Windows XP Pro / 2003 Server / Vista

POCKET REFERENCE GUIDE

SANS Institute
www.sans.org and isc.sans.org

Download the latest version of this sheet from http://www.sans.org/resources/winsacheatsheet.pdf

Purpose

System Administrators are often on the front lines of computer security. This guide aims to support System Administrators in finding indications of a system compromise.

How To Use This Sheet

On a periodic basis (daily, weekly, or each time you logon to a system you manage,) run through these quick steps to look for anomalous behavior that might be caused by a computer intrusion. Each of these commands runs locally on a system.

This sheet is split into these sections:

- Unusual Processes and Services
- Unusual Files and Reg Keys
- Unusual Network Usage
- Unusual Scheduled Tasks
- Unusual Accounts
- Unusual Log Entries
- Other Unusual Items
- Additional Supporting Tools

If you spot anomalous behavior: **DO NOT PANIC!** Your system may or may not have come under attack. Please contact the Incident Handling Team immediately to report the activities and get further assistance.

Unusual Processes and Services

Look for unusual/unexpected processes, and focus on processes with User Name "SYSTEM" or "Administrator" (or users in the Administrators' group). You need to be familiar with normal processes and services and search for deviations.

Using the GUI, run Task Manager:

```
C:\> taskmgr.exe
```

Using the command prompt:

```
C:\> tasklist
C:\> wmic process list full
```

Also look for unusual services.

Using the GUI:

```
C:\> services.msc
```

Using the command prompt:

```
C:\> net start
C:\> sc query
```

For a list of services associated with each process:

```
C:\> tasklist /svc
```

Unusual Files and Registry Keys

Check file space usage to look for sudden major decreases in free space, using the GUI (right-click on partition), or type:

```
C:\> dir c:\
```

Look for unusually big files: Start→Search→For Files of Folders... Search Options→Size→At Least 10000KB

Look for strange programs referred to in registry keys associated with system start up:

- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
- HKLM\Software\Microsoft\Windows\CurrentVersion\Runonce
- HKLM\Software\Microsoft\Windows\CurrentVersion\RunonceEx

Note that you should also check the HKCU counterparts (replace HKLM with HKCU above).

Using the GUI:

```
C:\> regedit
```

Using the command prompt:

```
C:\> reg query <reg key>
```

Unusual Network Usage

Look at file shares, and make sure each has a defined business purpose:

```
C:\> net view \\127.0.0.1
```

Look at who has an open session with the machine:

```
C:\> net session
```

Look at which sessions this machine has opened with other systems:

```
C:\> net use
```

Look at NetBIOS over TCP/IP activity:

```
C:\> nbtstat -S
```

Look for unusual listening TCP and UDP ports:

```
C:\> netstat -na
```

For continuously updated and scrolling output of this command every 5 seconds:

```
C:\> netstat -na 5
```

The –o flag shows the owning process id:

```
C:\> netstat -nao 5
```

The –b flag shows the executable name and the DLLs loaded for the network connection.

```
C:\> netstat -naob 5
```

Note that the –b flag uses excessive CPU resources.

Again, you need to understand normal port usage for the system and look for deviations.

Also check Windows Firewall configuration:

```
C:\> netsh firewall show config
```

Unusual Scheduled Tasks

Look for unusual scheduled tasks, especially those that run as a user in the Administrators group, as SYSTEM, or with a blank user name.

Using the GUI, run Task Scheduler:
Start→Programs→Accessories→System Tools→Scheduled Tasks

Using the command prompt:

```
C:\> schtasks
```

Check other autostart items as well for unexpected entries, remembering to check user autostart directories and registry keys.

Using the GUI, run msconfig and look at the Startup tab:

Start → Run, `msconfig.exe`

Using the command prompt:

```
C:\> wmic startup list full
```

Unusual Accounts

Look for new, unexpected accounts in the Administrators group:

```
C:\> lusrmgr.msc
```

Click on Groups, Double Click on Administrators, then check members of this group.

This can also be done at the command prompt:

```
C:\> net user

C:\> net localgroup administrators
```