SYSTEM HARDENING

- *defense in depth*

JASPREET SINGH

Jr. Consultant

CERT-In

AGENDA

- INTRODUCTION
- Techniques Briefing – System Hardening

What is hardening

- Step by step procedure of securely configuring a system to protect it against unauthorized access, while also taking actions to make the system more reliable.
- Generally anything that is done in the name of System Hardening ensures the system is both secure and reliable.
- Saving system from exploitation and attacks.

PURPOSE & REASON

- The idea is to make your Systems & Network a little harder to into than your neighbors.
- All the computers are INSECURED to some degree.
- Easy to be Cracked.
- Reverse of Hacking
- Part of Security Lifecycle.
  - Prevention >Detection >Response >Hardening

HARDENING IS IMPORTANT

- Most Crackers are lazy. They won't keep bothering you unless they have an easy way in. If no Hardening, Hackers move in quickly.
- Your system might be hijacked without your knowledge, and then used to attack another system, or spread viruses, or distribute illegal content such as pornography or software.
- Your company's proprietary information could be stolen.
- Reducing financial & trust loss

BENEFITS

- Establish the trust relationship and enhance the business with other company and hence do more business.
- You can have more confidence in the integrity of your data.
- Performance improvements can be experienced since unnecessary services are removed, and inefficiencies in system configuration are detected.
- The company’s reputation is protected.
- Clients are happier as a result of fewer system failures or delays.

Approaches to Hardening

- Develop and ship in Hardened State.
- Hardened after Setup.

How To

- Updating Kernel/Software and apply Patches
  - Apply security patches in Linux Kernel
  - Apply bug patches in software
- Security Tools like extra system logs and auditing.
- System rules and policies
  - Restrict user privileges
  - Disabling unnecessary processes
  - Disabling unnecessary ports
  - Disabling unnecessary services

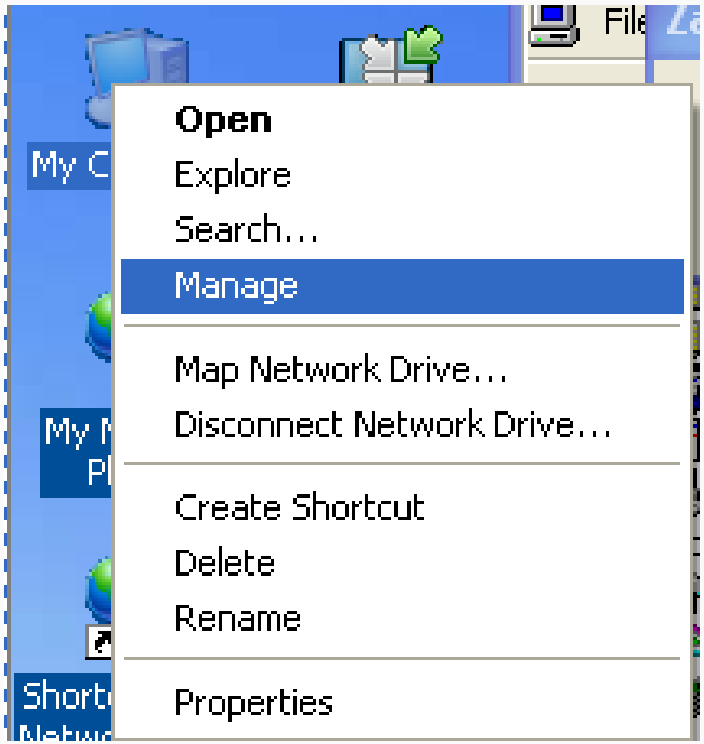
Personal Computer Security

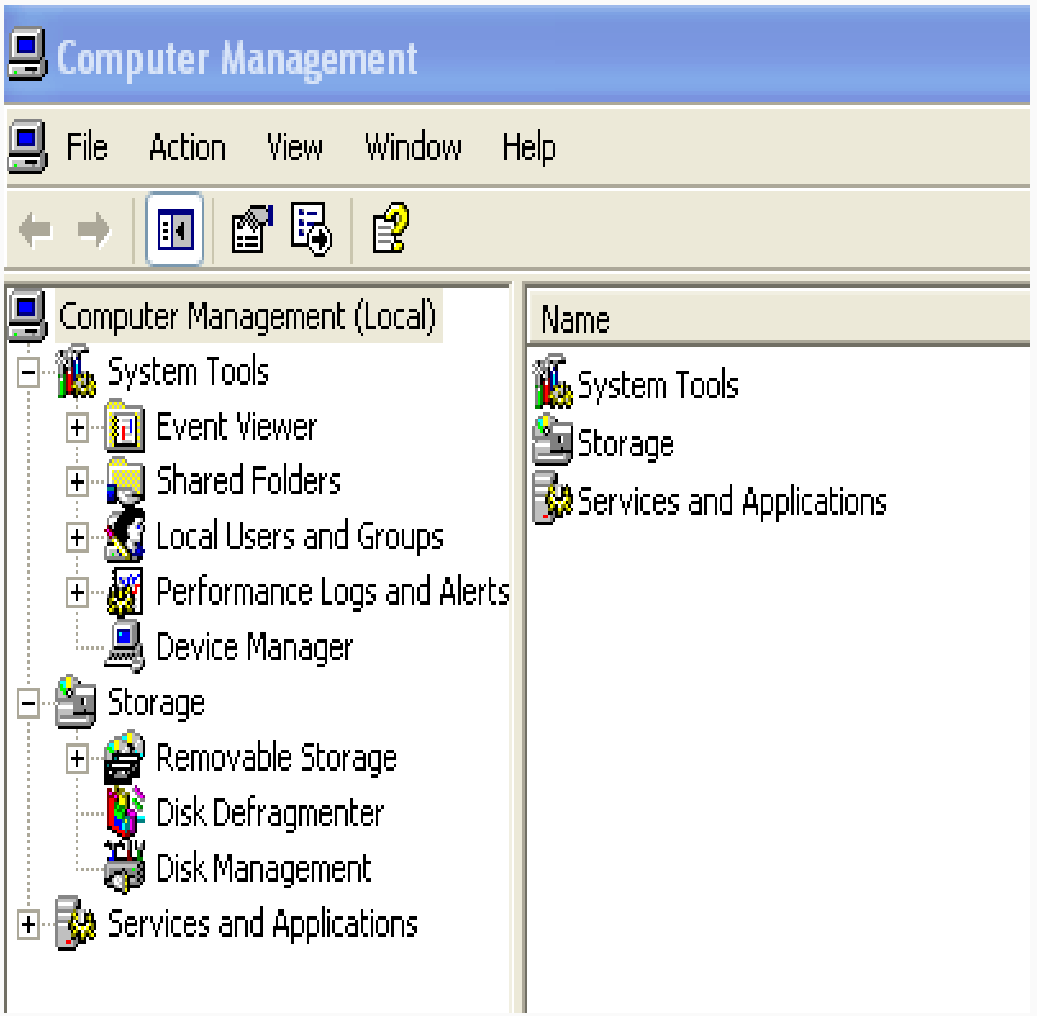
- No matter your platform, you should…
  - Have separate accounts for each user
  - Protect ALL accounts with a password
  - Run as a “non-privileged” user
  - Use an inactivity time-out that locks the screen
  - Use a firewall
  - Perform regular backups
  - Use antivirus software *(yes, Mac users, you too!)*
  - Disable Auto run as well. (Used by Conficker etc and other malwares)

Enable Appropriate Logging/Auditing

- By default logging is not enabled.
- Turning it on after an incident is as bad as locking the door after the horse is gone.
- Increase the log size from the default 512 KB to some GB's.
- It's zero maintenance, and it's a reasonable policy for when (not if) something happens.
- Occasionally archiving logs is also a good practice

COMPUTER MANAGEMENT

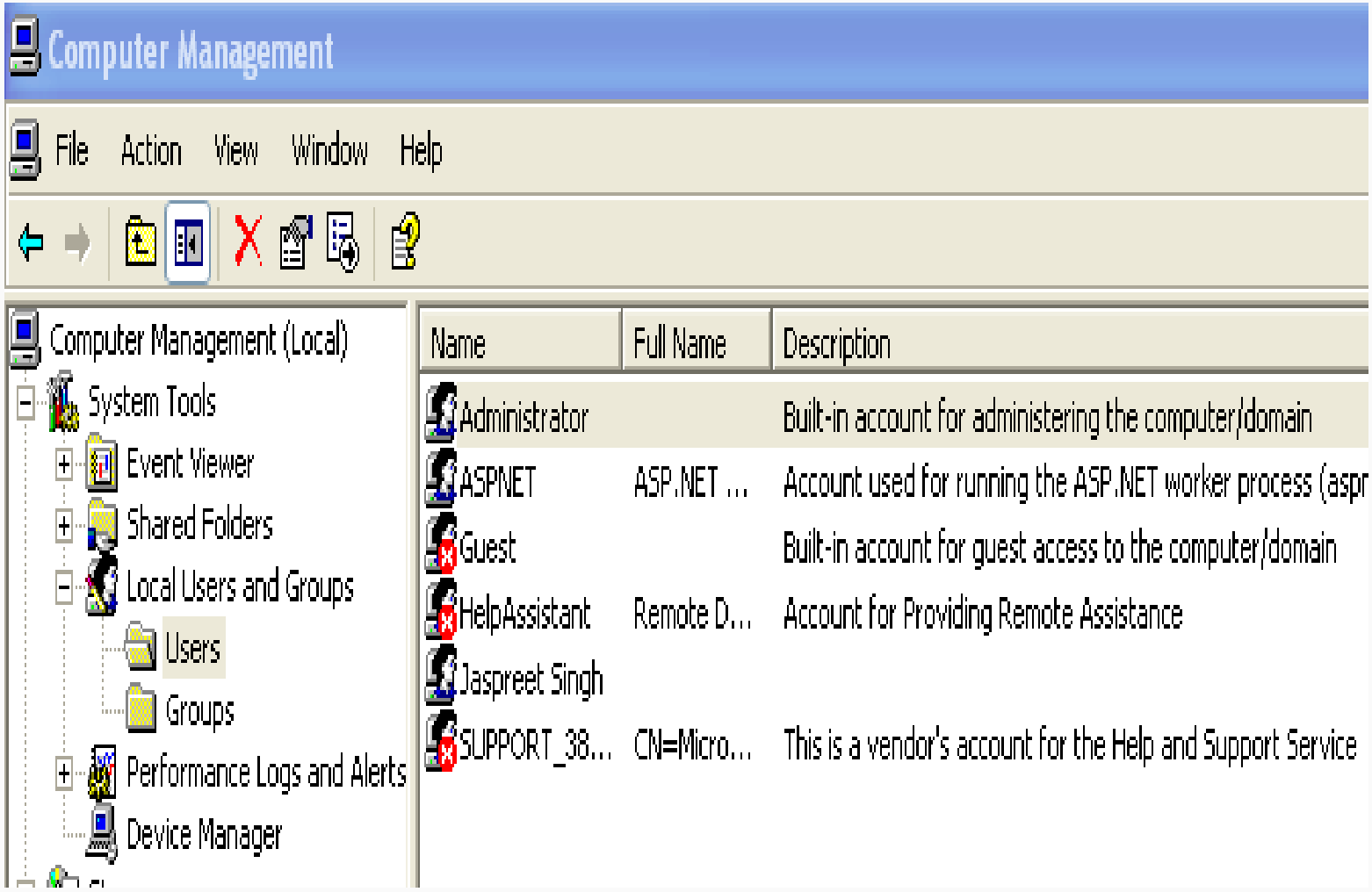




Computer Accounts

- For our purposes, there are two types of accounts on a system:
  - Administrator (or root)
  - User (or non-privileged user)
- Administrator accounts have unlimited power
  - With great power comes great responsibility
  - Administrator accounts are needed to install new software, configure network settings, install printers, etc.
  - Malicious websites and programs take advantage of that power to compromise your system
- “User” or “non-privileged” accounts
  - Generally can’t install software and cant make changes to firewall, AV and other critical system components.

USER ACCOUNTS



Computer Security

- Many security problems can be alleviated just by keeping your software up to date!
  - Enable Automatic Updates (Win) or System Update (Mac) to download and install automatically
  - Allow add-on programs like Adobe Reader and QuickTime to check for updates automatically
  - Security Patching in Linux
- Uninstall software you no longer use
  - Forgotten, unpatched software may make your machine more vulnerable

UPDATES


Windows Security Center
Security Center
Help protect your PC
Resources
Get the latest security and virus information from Microsoft
Check for the latest updates from Windows Update
Get support for security-related issues
Get help about Security Center
Change the way Security Center alerts me
Security essentials
Security Center helps you manage your Windows security settings. To help protect your computer, make sure the three security essentials are marked ON. If the settings are not ON, follow the recommendations. To return to the Security Center later, open Control Panel.
What's new in Windows to help protect my computer?
Firewall
ON
Automatic Updates
OFF
Automatic Updates is turned off. Your computer is more vulnerable to viruses and other security threats. Click Turn on Automatic Updates to have Windows automatically keep your computer current with important updates. How does Automatic Updates help protect my computer?
Turn on Automatic Updates
Virus Protection
NOT FOUND
Windows did not find antivirus software on this computer. Antivirus software helps protect your computer against viruses and other security threats. Click Recommendations for suggested actions you can take. How does antivirus software help protect my computer?
Note: Windows does not detect all antivirus programs.
Recommendations...
Manage security settings for:
At Microsoft, we care about your privacy. Please read our privacy statement.

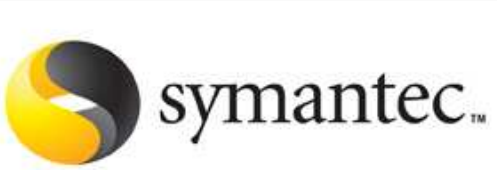
Computer Security: Firewalls

- Both Windows and Macintosh computers come with firewalls
  - Windows XP Service Pack 3 & Vista enable firewall by default
  - Mac OS X *may not* enable its firewall by default
- Linux also supports the firewall known as iptables.

Computer Security: Antivirus

- Corrective *at best*
- No computer should be without it
- Have you paid your subscription fee?
- Check for updates every 30 mins
- Never try to run more than one AV package at once!
- MS Security Essential is free for Windows 7.

Computer Security: Antivirus



Computer Security: Anti-spyware

- There are several excellent free anti-spyware tools available
- “Active protection” *may* conflict with your antivirus software
- “Passive protection” *shouldn’t* cause a problem
- Malwarebytes
- Spybot Search & Destroy
- Microsoft Windows Defender
- Ad-Aware
- Spyware Blaster

Computer Security: Other utilities

- HijackThis
  - Inspects browsers and OS settings to generate a log file of the current state of machine. Helps in removing unwanted settings and files.
- Ccleaner
  - Cleans internet history, orphaned registry entry and delete other unused files.
- TrendMicro Housecall
  - It features an intuitive interface and the ability to perform fast scans that target critical system areas and active malware.

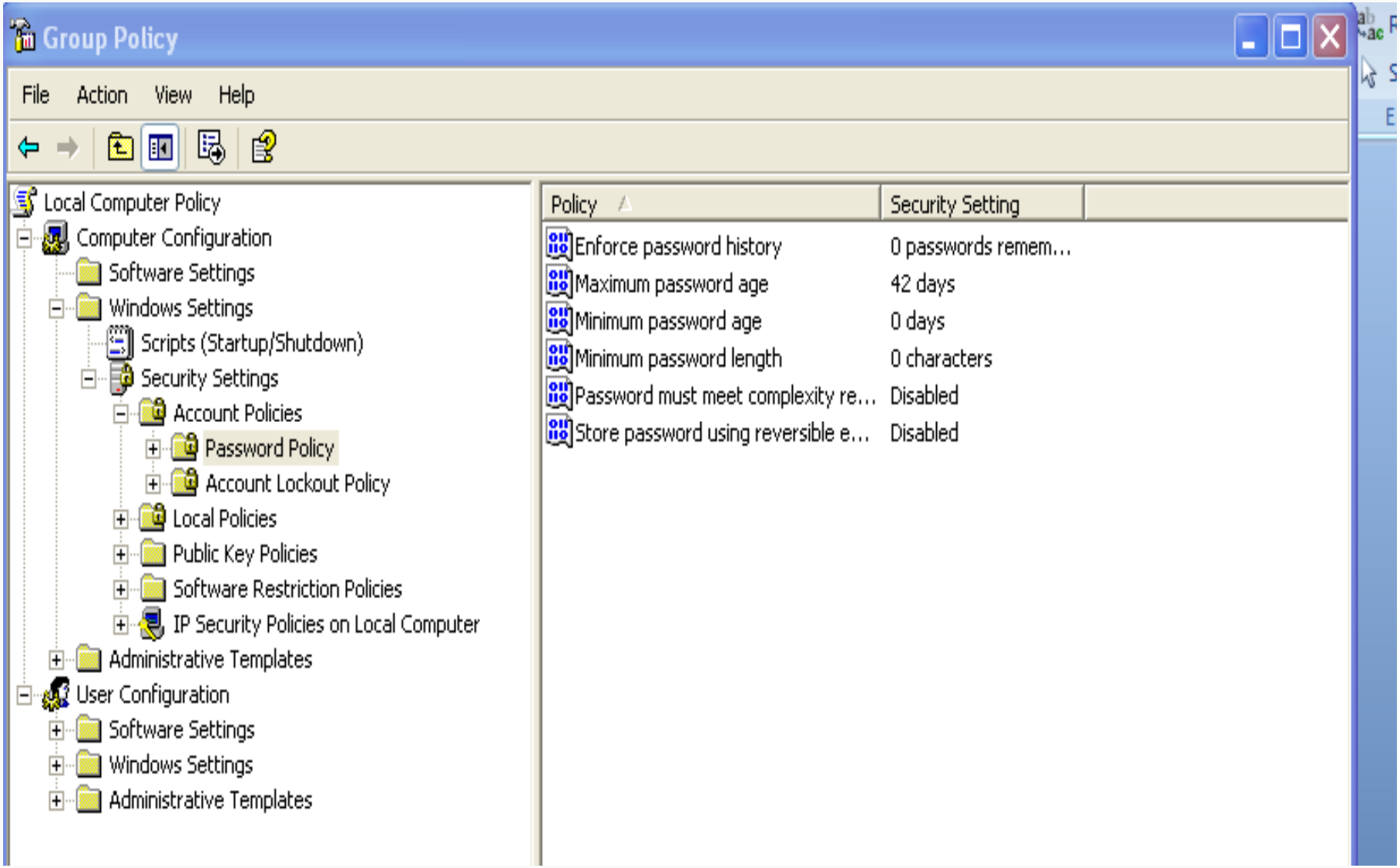
Application Hardening

- Basic Assumption : default installation is insecure
- Pay close attention on every installation steps
  - No typical, full installation
  - Choice custom installation
  - Install the components you need
- Applied patches
- Get a list of what files have been installed (try your best)

Sample Password Policy

- Account Lockout : **3 times**
- Password Uniqueness : **history of 2**
- Create a password with a combination of letters and numbers, use upper and lower case
- Change your password on a regular basis **- eg every 30 days (compulsory)**
- Cannot use password with anything personal such as birthdays, names, phone numbers or other familiar words
- Should not be User id or part of it.

PASSWORD POLICY



File Sharing

- Remove hidden share in windows.
  - Controlling access through File sharing wizard.
- *nux

  - File permissions must be taken in account.

  - # ls –l will show the permissions.

  - # chmod will set permissions
- -- *nux = Linux, Unix based systems

- Must Review …

Top 10 Windows Vulnerabilities

- *Web Servers* - misconfigurations, product bugs, default installations, and third-party products such as php can introduce vulnerabilities.
- *Microsoft SQL Server* - vulnerabilities allow remote attackers to obtain sensitive information, alter database content, and compromise SQL servers and server hosts.
- *Passwords* - user accounts may have weak, nonexistent, or unprotected passwords. The operating system or third-party applications may create accounts with weak or nonexistent passwords.
- *Workstations* - requests to access resources such as files and printers without any bounds checking can lead to vulnerabilities. Overflows can be exploited by an unauthenticated remote attacker executing code on the vulnerable device.
- *Remote Access* - users can unknowingly open their systems to hackers when they allow remote access to their systems.

Top 10 Windows Vulnerabilities

- *Browsers* – accessing cloud computing services puts an organization at risk when users have unpatched browsers. Browser features such as Active X and Active Scripting can bypass security controls.
- *File Sharing* - peer to peer vulnerabilities include technical vulnerabilities, social media, and altering.
- *E-mail* – by opening a message a recipient can activate security threats such as viruses, spyware, Trojan horse programs, and worms.
- *Instant Messaging* - vulnerabilities typically arise from outdated ActiveX controls in MSN Messenger, Yahoo! Voice Chat, buffer overflows, and others.
- *USB Devices* - plug and play devices can create risks when they are automatically recognized and immediately accessible by Windows operating systems.

Top 10 Unix Vulnerable objects

- Remote Procedure Calls (RPC) - RPC is the tool that allows a program on one computer to run software on a remote computer
- BIND Domain Name System - BIND is critical because it's by far the most popular DNS in use around the world and is, therefore, a popular target for hackers wanting to trigger a Denial of Service (DoS) event.
- Apache Web Server - Don't run Apache as root & Disable any scripting languages you don't really need.\
- Clear Text Services - Sniffer attacks are common, and the fact that many Linux/UNIX services such as FTP don't encrypt any part of the session, even the logon information, makes this a popular attack vector
- General Unix Authentication -- Accounts with No Passwords or Weak Passwords

Top 10 Unix Vulnerable objects

- Sendmail - The widespread use of Sendmail as a mail transfer agent means that known vulnerabilities in older or unpatched versions are a common target.
- Simple Network Management Protocol (SNMP) - Since SNMP is often enabled by default, it's one of those services that must be maintained if you can't disable it.
- Secure Shell (SSH) - SSH is an important security tool, but many installations of it aren't being properly maintained or configured.
- Misconfiguration of Enterprise Services NIS/NFS - The main threat here is probably the fact that this is often enabled by default, whether it is needed or not, and is, therefore, rarely maintained effectively.
- Open Secure Sockets Layer (SSL) - here are a lot of holes in older OpenSSL libraries and, because it is often used by other services such as Apache or even Sendmail, it may not be maintained properly.

Harden your OS

- **Question: How can you implement your security setting in numerous computers at one go????**
- ***Answer: Security Template***

Thank You

The information provided is concise for presentation purpose. It is not meant to be complete. If you need more detailed information please refer to books and Internet wikis.