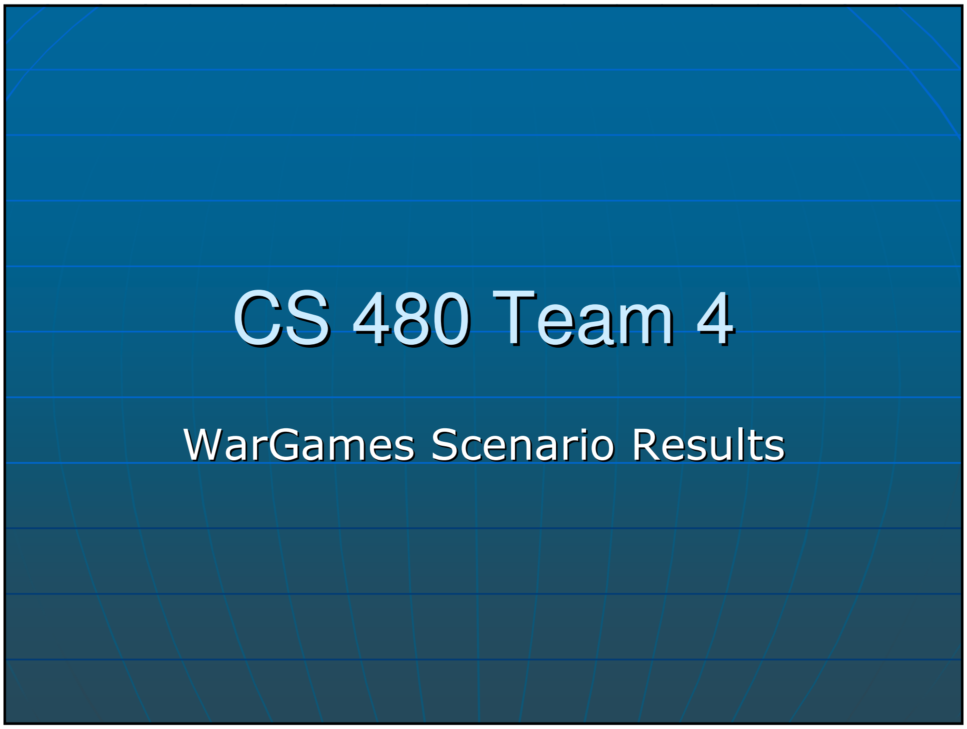
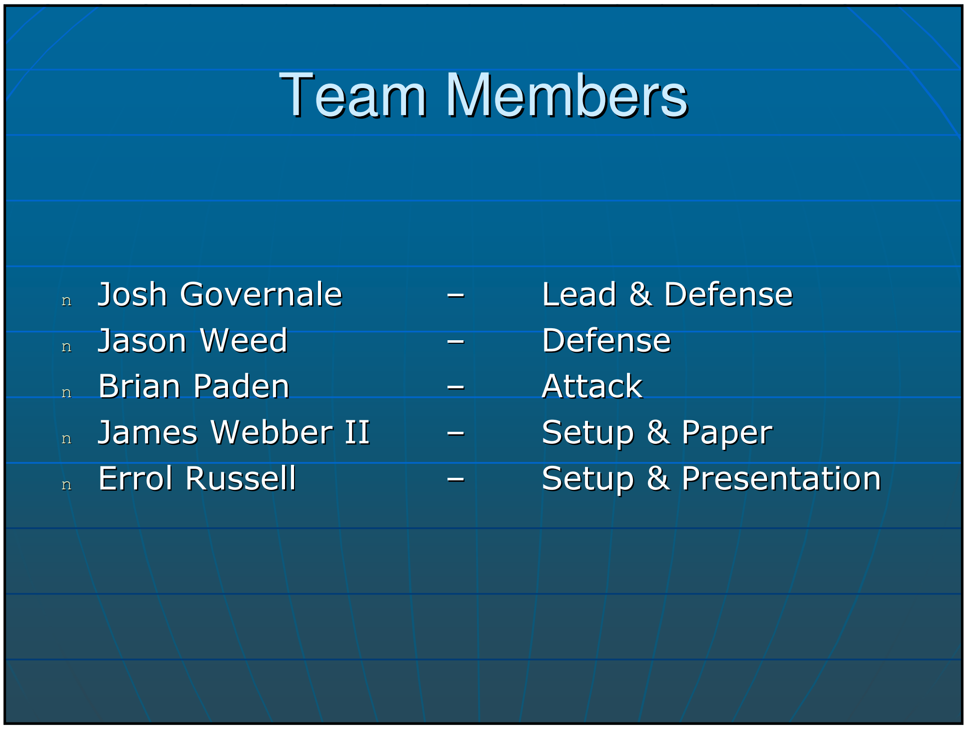


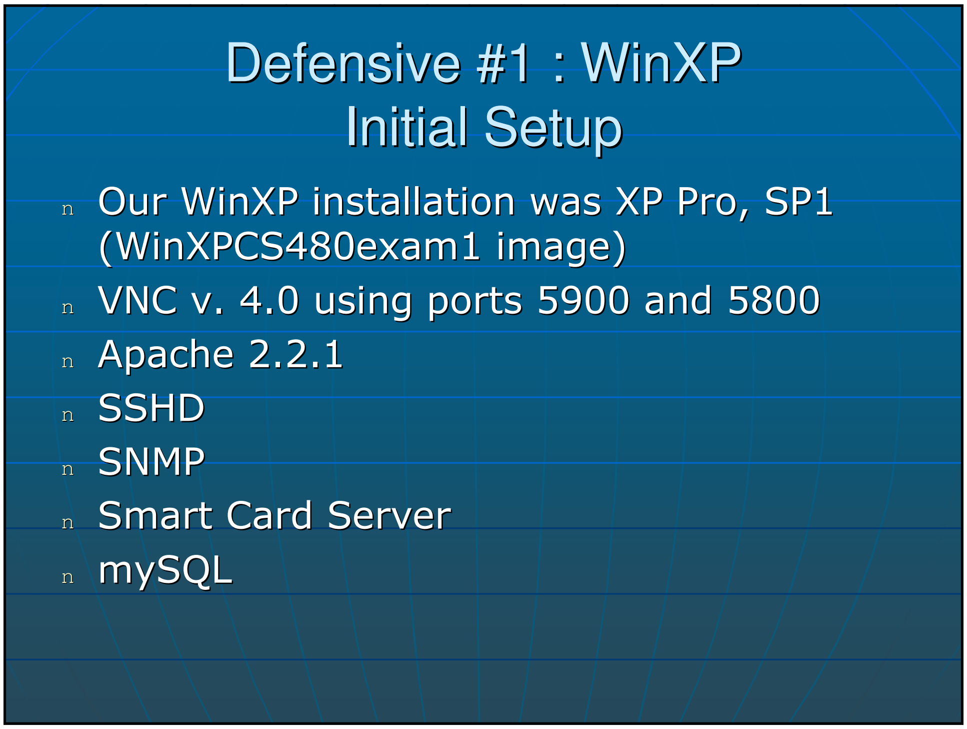
CS 480 Team 4

WarGames Scenario Results



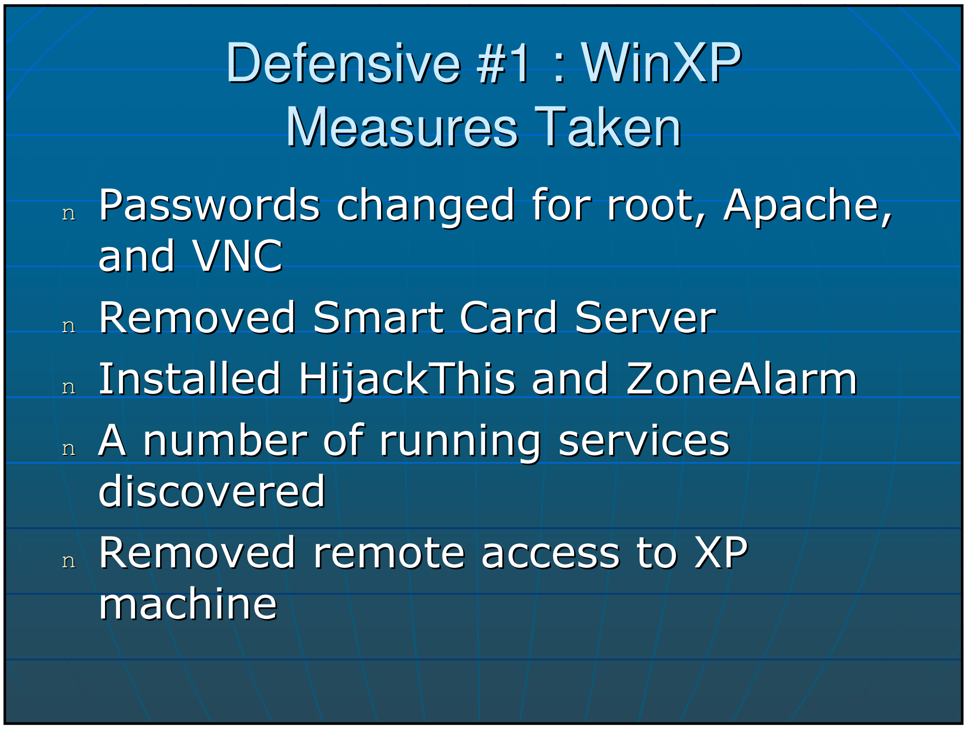
Team Members

Josh Governale	–	Lead & Defense
Jason Weed	–	Defense
Brian Paden	–	Attack
James Webber II	–	Setup & Paper
Errol Russell	–	Setup & Presentation



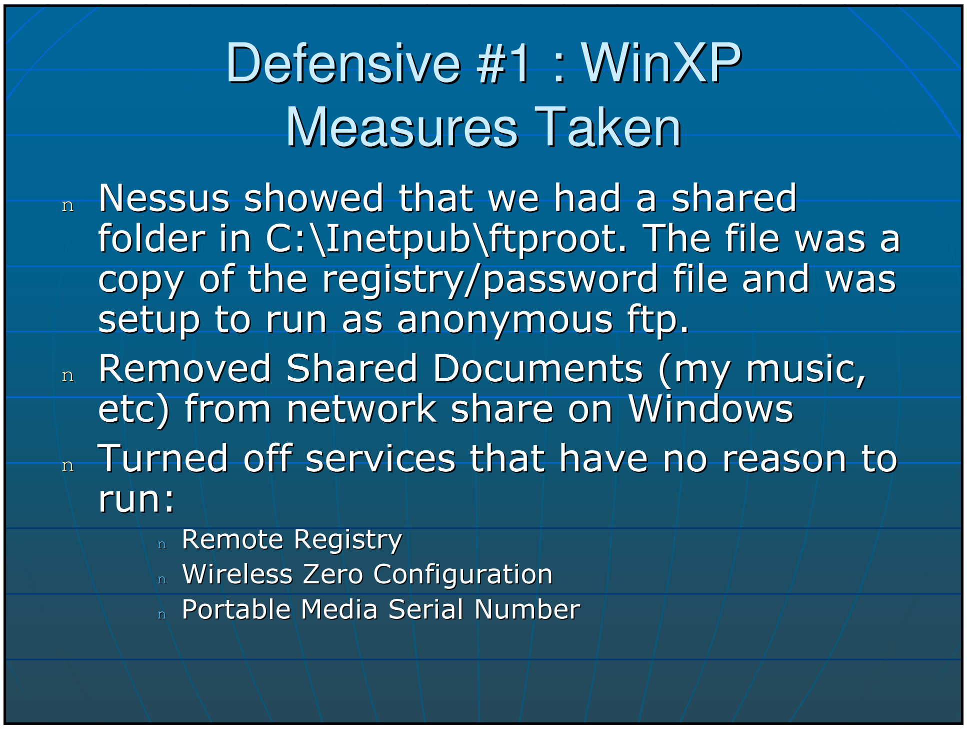
Defensive #1 : WinXP Initial Setup

- Our WinXP installation was XP Pro, SP1 (WinXPCS480exam1 image)
- VNC v. 4.0 using ports 5900 and 5800
- Apache 2.2.1
- SSHD
- SNMP
- Smart Card Server
- mySQL



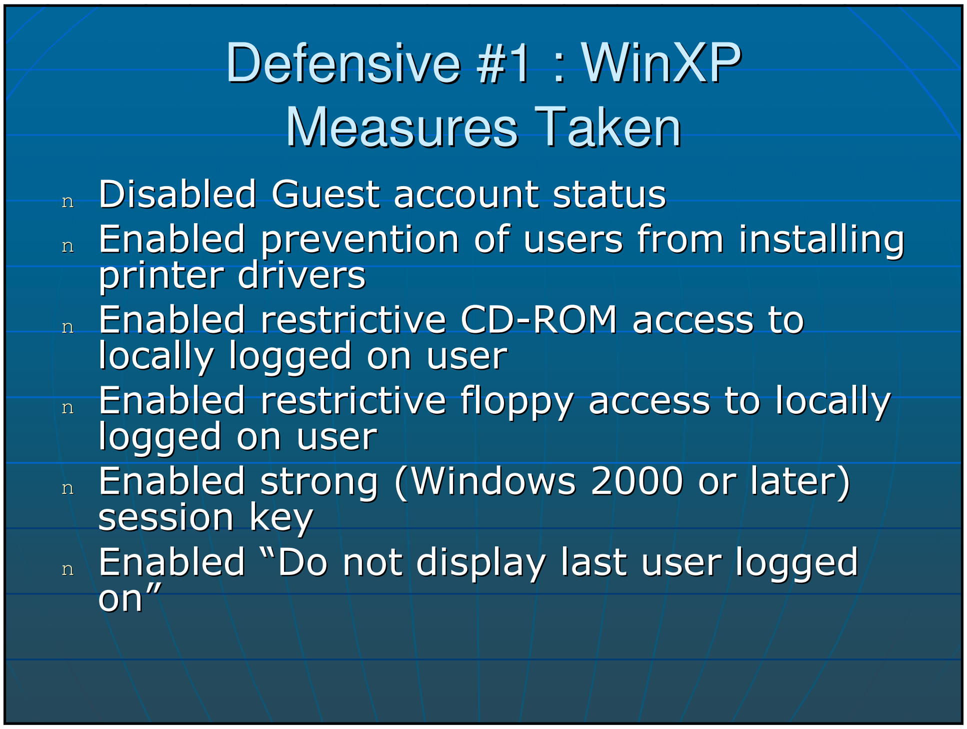
Defensive #1 : WinXP Measures Taken

- Passwords changed for root, Apache, and VNC
- Removed Smart Card Server
- Installed HijackThis and ZoneAlarm
- A number of running services discovered
- Removed remote access to XP machine



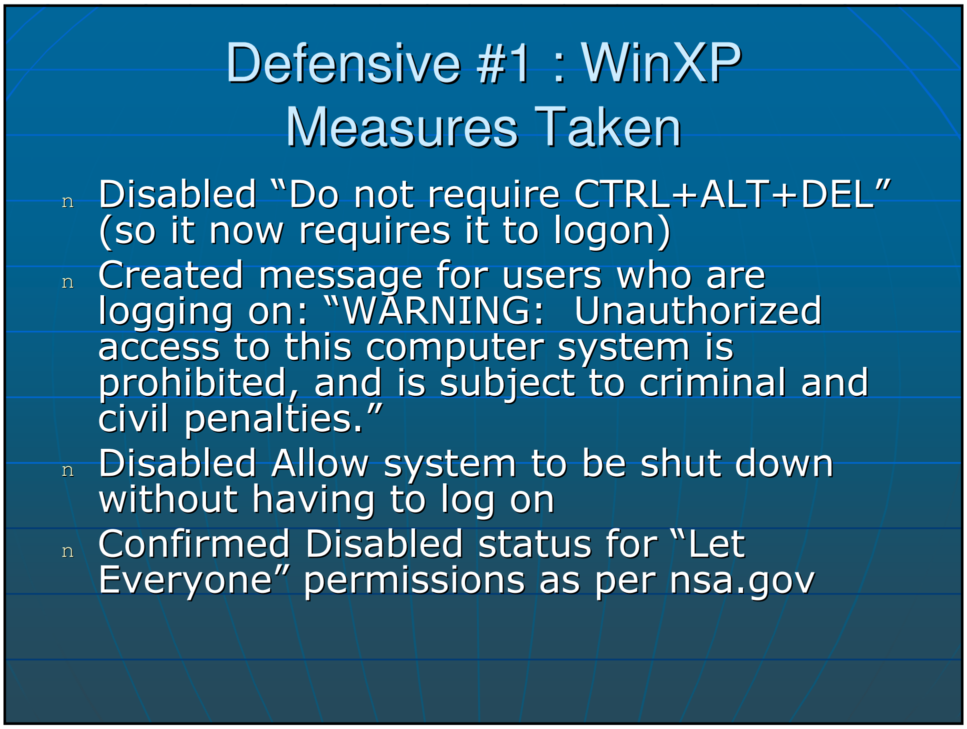
Defensive #1 : WinXP Measures Taken

- Nessus showed that we had a shared folder in C:\Inetpub\ftproot. The file was a copy of the registry/password file and was setup to run as anonymous ftp.
- Removed Shared Documents (my music, etc) from network share on Windows
- Turned off services that have no reason to run:
  - Remote Registry
  - Wireless Zero Configuration
  - Portable Media Serial Number



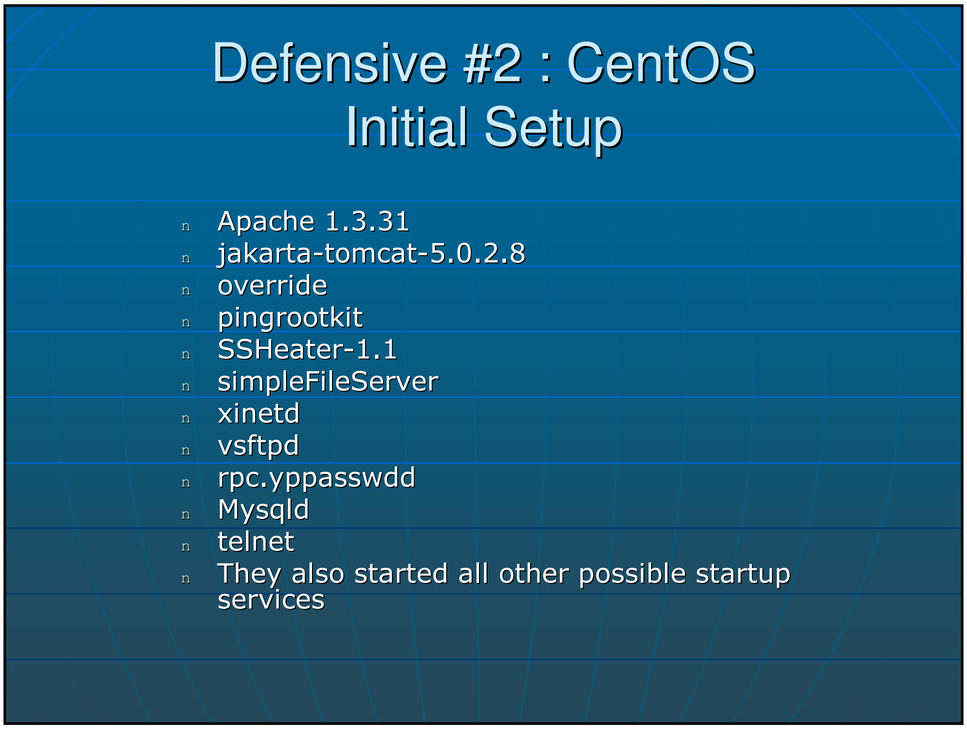
Defensive #1 : WinXP Measures Taken

- Disabled Guest account status
- Enabled prevention of users from installing printer drivers
- Enabled restrictive CD-ROM access to locally logged on user
- Enabled restrictive floppy access to locally logged on user
- Enabled strong (Windows 2000 or later) session key
- Enabled “Do not display last user logged on”



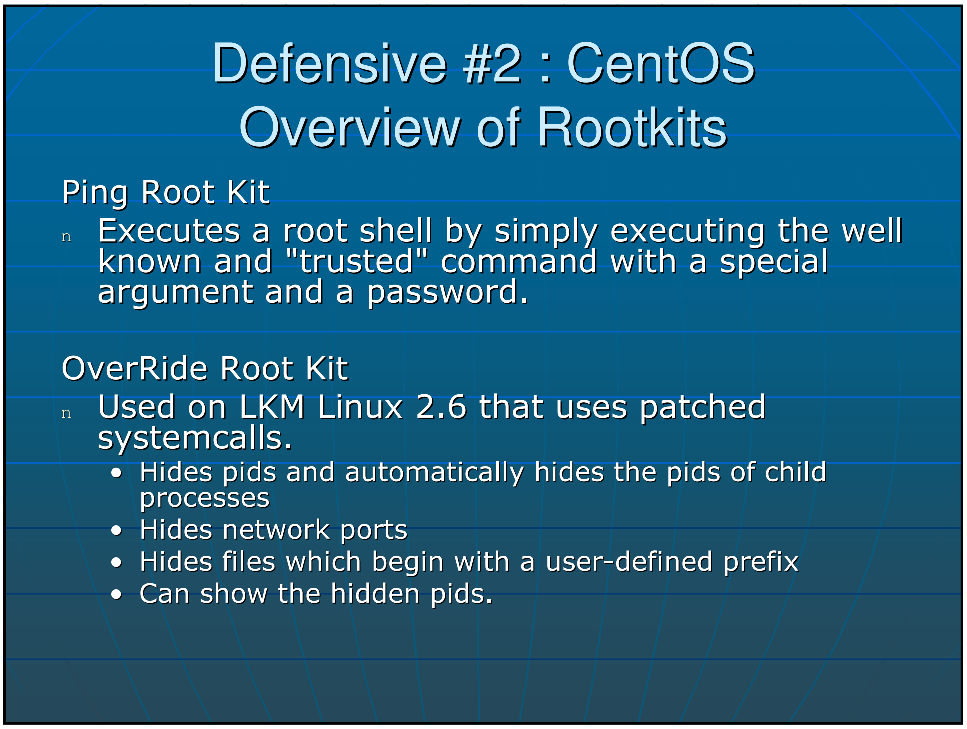
Defensive #1 : WinXP Measures Taken

- Disabled “Do not require CTRL+ALT+DEL” (so it now requires it to logon)
- Created message for users who are logging on: “WARNING: Unauthorized access to this computer system is prohibited, and is subject to criminal and civil penalties.”
- Disabled Allow system to be shut down without having to log on
- Confirmed Disabled status for “Let Everyone” permissions as per nsa.gov



Defensive #2 : CentOS Initial Setup

- Apache 1.3.31
- jakarta-tomcat-5.0.2.8
- override
- pingrootkit
- SSHeater-1.1
- simpleFileServer
- xinetd
- vsftpd
- rpc.yppasswdd
- Mysqld
- telnet
- They also started all other possible startup services



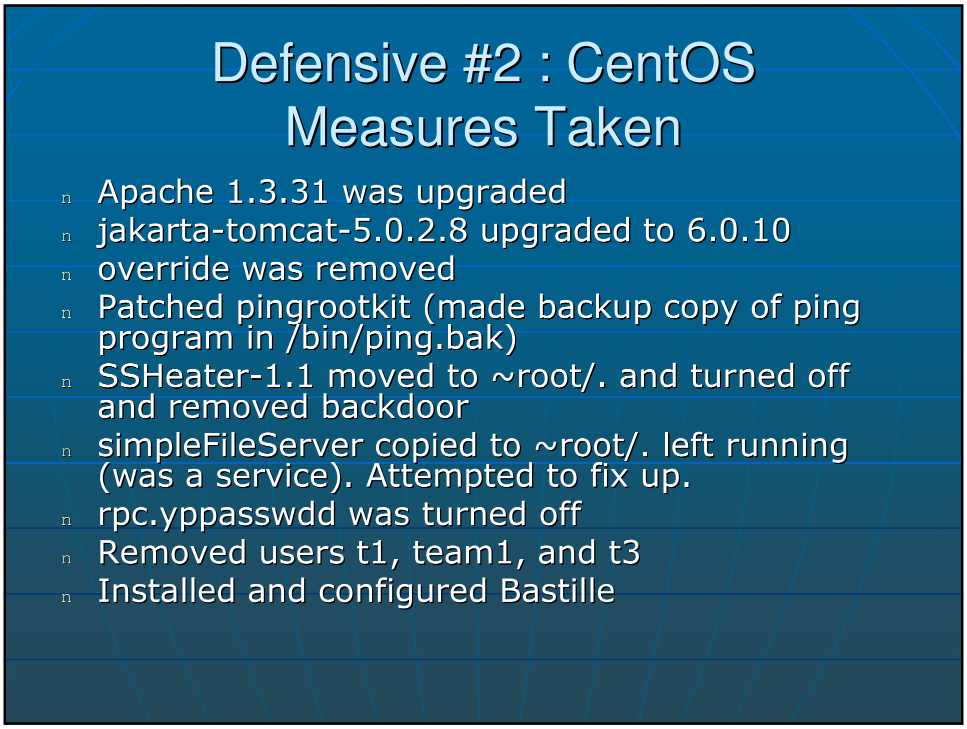
Defensive #2 : CentOS
Overview of Rootkits

Ping Root Kit

- Executes a root shell by simply executing the well known and "trusted" command with a special argument and a password.

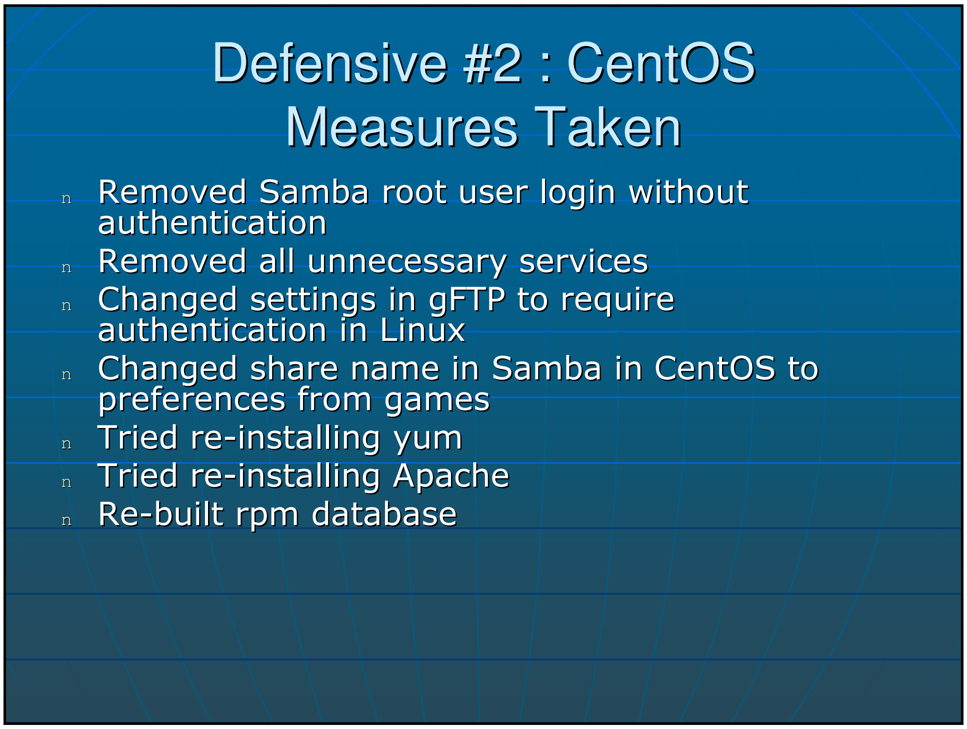
OverRide Root Kit

- Used on LKM Linux 2.6 that uses patched systemcalls.
  - Hides pids and automatically hides the pids of child processes
  - Hides network ports
  - Hides files which begin with a user-defined prefix
  - Can show the hidden pids.



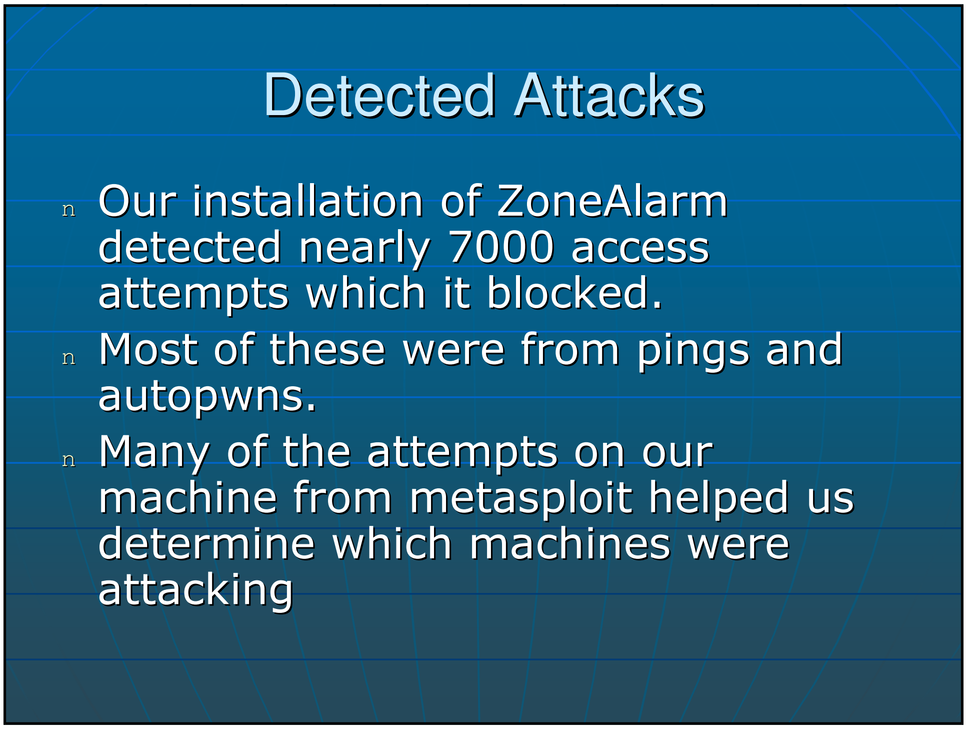
Defensive #2 : CentOS
Measures Taken

- Apache 1.3.31 was upgraded
- jakarta-tomcat-5.0.2.8 upgraded to 6.0.10
- override was removed
- Patched pingrootkit (made backup copy of ping program in /bin/ping.bak)
- SSHeater-1.1 moved to ~root/. and turned off and removed backdoor
- simpleFileServer copied to ~root/. left running (was a service). Attempted to fix up.
- rpc.yppasswdd was turned off
- Removed users t1, team1, and t3
- Installed and configured Bastille



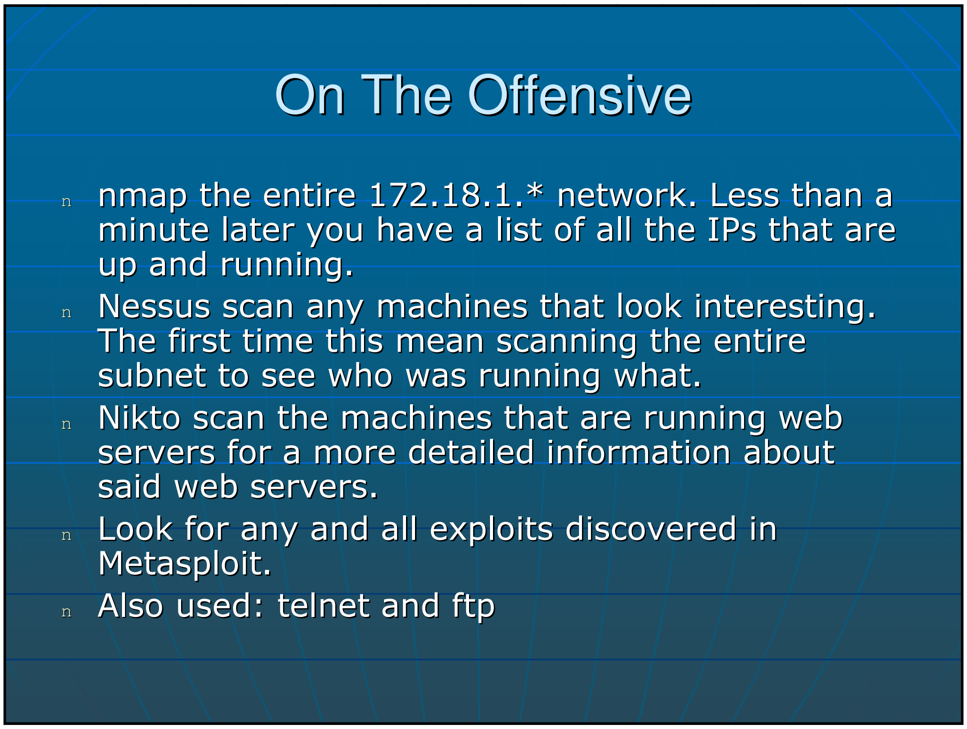
Defensive #2 : CentOS Measures Taken

- Removed Samba root user login without authentication
- Removed all unnecessary services
- Changed settings in gFTP to require authentication in Linux
- Changed share name in Samba in CentOS to preferences from games
- Tried re-installing yum
- Tried re-installing Apache
- Re-built rpm database



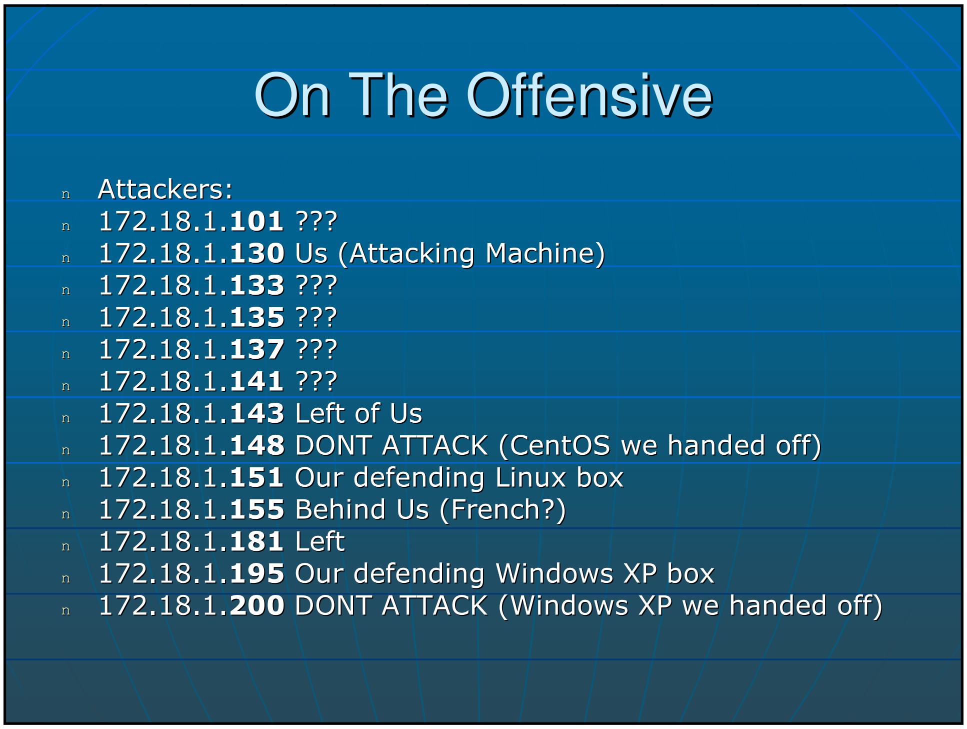
Detected Attacks

- Our installation of ZoneAlarm detected nearly 7000 access attempts which it blocked.
- Most of these were from pings and autopwns.
- Many of the attempts on our machine from metasploit helped us determine which machines were attacking



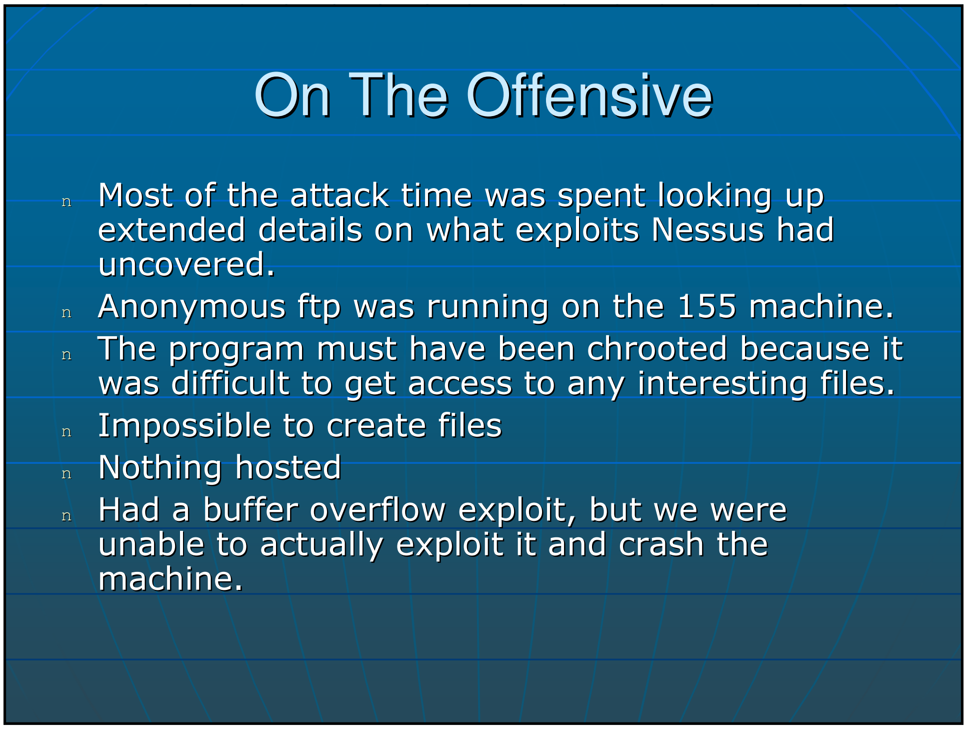
On The Offensive

- nmap the entire 172.18.1.* network. Less than a minute later you have a list of all the IPs that are up and running.
- Nessus scan any machines that look interesting. The first time this mean scanning the entire subnet to see who was running what.
- Nikto scan the machines that are running web servers for a more detailed information about said web servers.
- Look for any and all exploits discovered in Metasploit.
- Also used: telnet and ftp



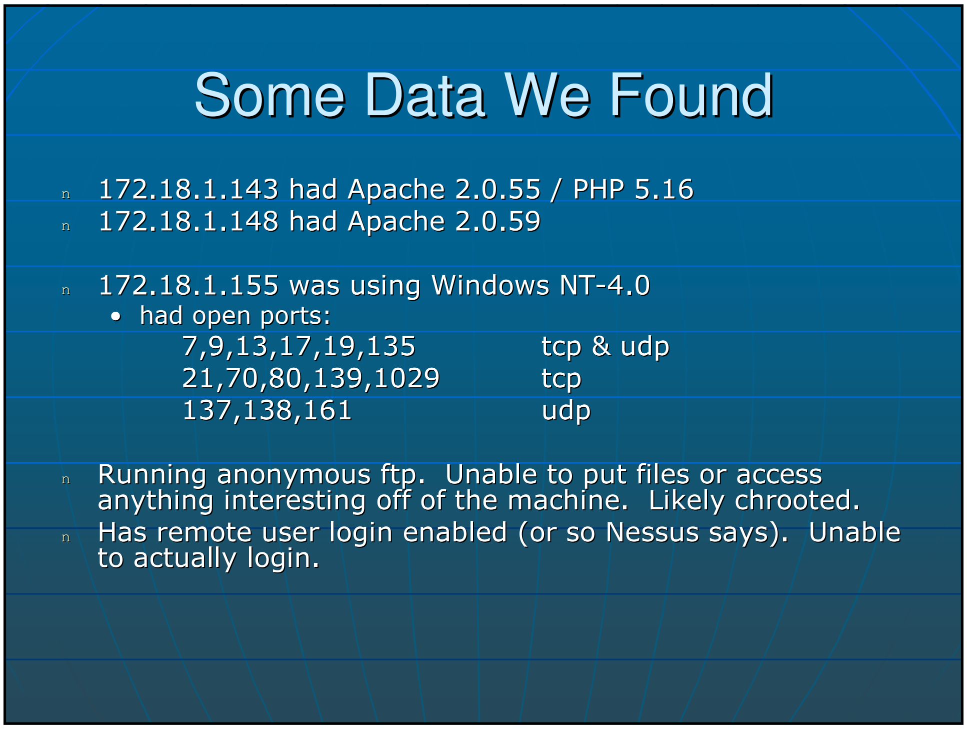
On The Offensive

- Attackers:
- 172.18.1.**101** ???
- 172.18.1.**130** Us (Attacking Machine)
- 172.18.1.**133** ???
- 172.18.1.**135** ???
- 172.18.1.**137** ???
- 172.18.1.**141** ???
- 172.18.1.**143** Left of Us
- 172.18.1.**148** DONT ATTACK (CentOS we handed off)
- 172.18.1.**151** Our defending Linux box
- 172.18.1.**155** Behind Us (French?)
- 172.18.1.**181** Left
- 172.18.1.**195** Our defending Windows XP box
- 172.18.1.**200** DONT ATTACK (Windows XP we handed off)



On The Offensive

- Most of the attack time was spent looking up extended details on what exploits Nessus had uncovered.
- Anonymous ftp was running on the 155 machine.
- The program must have been chrooted because it was difficult to get access to any interesting files.
- Impossible to create files
- Nothing hosted
- Had a buffer overflow exploit, but we were unable to actually exploit it and crash the machine.



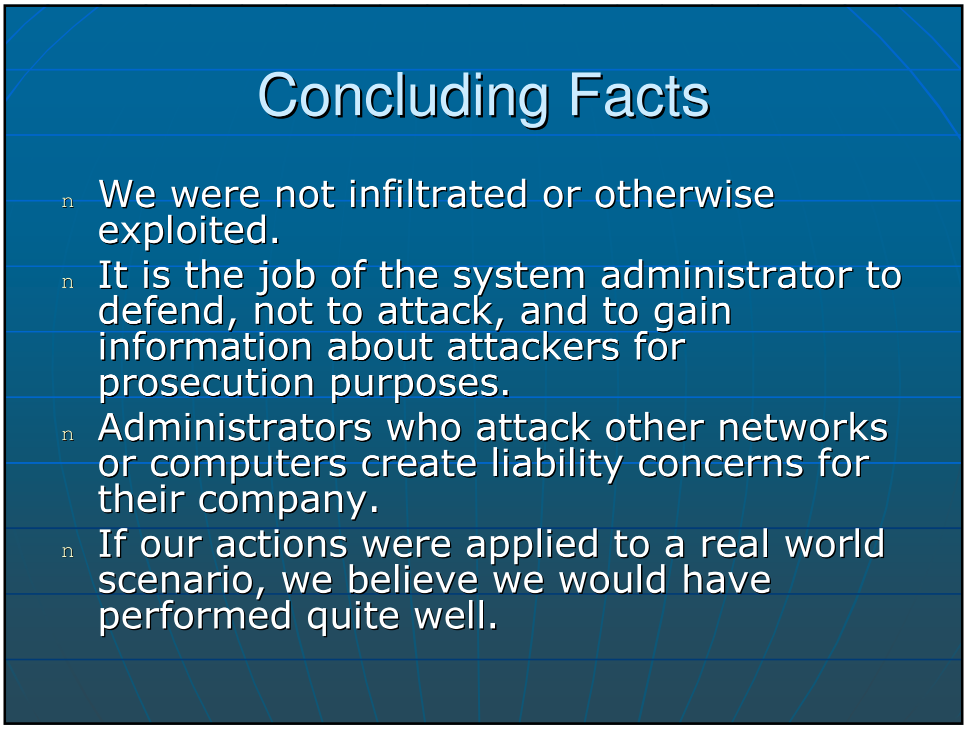
Some Data We Found

- 172.18.1.143 had Apache 2.0.55 / PHP 5.16
- 172.18.1.148 had Apache 2.0.59

- 172.18.1.155 was using Windows NT-4.0
  - had open ports:

7,9,13,17,19,135	tcp & udp
21,70,80,139,1029	tcp
137,138,161	udp

- Running anonymous ftp. Unable to put files or access anything interesting off of the machine. Likely chrooted.
- Has remote user login enabled (or so Nessus says). Unable to actually login.



Concluding Facts

- We were not infiltrated or otherwise exploited.
- It is the job of the system administrator to defend, not to attack, and to gain information about attackers for prosecution purposes.
- Administrators who attack other networks or computers create liability concerns for their company.
- If our actions were applied to a real world scenario, we believe we would have performed quite well.