War Games Scenario

Team 3

Configured Machines: Win NT4 Services

- Gopher
- FTP
- Back Orifice
- SNMP
- RPC

Windows NT 4

- This was rather difficult to get up and running
- Turning off Event Logger was bad. Very bad.
- Disabled Plug and Play

CentOS Services

- SSH
- Sendmail
- Custom Webserver
- FTP

CentOS

- Uninstalled X.
- We added in a cron job that would delete and add a user named guest that had a UID of 0, and the password: 'password'.
- We also put in multiple Aliases, ls would go to ls .. etc.

Defensive Measures

- Nessus on our Machines
- Updated and Patched Services
- LanGuard

Windows:

- Firewall (ZoneAlarm)
- Patches (Offline Update)
- Deleted Users
- Anonymous Login VNC Server (Our weak link)
- LanGuard Again

CentOS

- Updated Apache

Offensive Measures: Tools

- Nessus
- LanGuard
- Metasploit
- EtherApe

Nessus

- We mainly used Nessus to look at vulnerabilities for both our own machines and other people's
- The most common vulnerabilities we found were DoS Attacks on Webservers.
- Found some vulnerabilities that included arbitrary code execution, but couldn't use them to our advantage.

LanGuard

- Surprisingly this worked almost like a LAN version of Nessus
- Found mostly the same vulnerabilities of Nessus
- Focused more on vulnerabilities because of older versions
- Found Black Diver(1985) on one machine

Metasploit

- Metasploit proved to be surprisingly useless.
- Sadly no “Exploit Now” button.
- Most of the exploits that Metasploit had did not affect most of the machines since most of them got patched quickly, or weren't using those vulnerable services.
- The ninja(autopwn) command was a bit of a misnomer

EtherApe

- EtherApe is a graphical Network Monitor
- Helped find some IP addresses since you could see who was on the LAN whenever traffic flowed between two IP addresses

Successfully Performed Attacks

Lessons Learned

- Attacking is far more difficult than we previously thought. The lack of network traffic was a bit of a hindrance as well.
- Defending happened to be easier than expected in some senses, because of how hard it was to attack.
- A checklist of things needed to be done on the machines would have helped (probably would have stopped our Windows box from being attacked)