- Deral Heiland
- Email dwotds@yahoo.com
- IT for 10 years SSCP,CCWS,CNE
  - Network Security Analyst
  - Network Administrator
  - Network Field Engineer

The Insecure Workstation

The Results of Poorly Defined and Deployed Group Policies

Focus on Client Group Policies

- This is not an attack on Microsoft®
- This is an informative look at poorly conceived and deployed Microsoft group policies
- Group policies are meant as a means to centralize control of users and computers

Areas of Discussion

- Where (policies are used)
- What (policies control)
- Why (policies are used)
- Exploiting for fun and entertainment
- Conclusions

Where to Use Group Policies

- Industrial control systems
  - Run manufacturing equipment
  - Data gathering systems
  - Kiosk systems
  - Citrix

Where to Use Group Policies

- Standard business desktops
- Public access terminals
  - Schools
  - Libraries
  - Kiosk systems

What to Secure or Restrict

- Applications
  - Restrict access to configurations tools
  - Restriction functionality of certain applications
    1. Internet Explorer
    2. Any applications that have features that can be controlled with registry entries can be configured with group policies
  - Preventing users from running certain applications

What to Secure or Restrict

- File systems
  - Hide drive Icons
  - Prevent file system browsing

Why Secure or Restrict?

- Prevent users from screwing up the workstations
- Prevent users from accessing (something?)
- Stop hackers
- If you really not sure why it needs secured then maybe it doesn't

Big Misconceptions

- If I can’t get around it it must be secure
- They aren’t hackers they won’t figure away around it
- So they break out of it. That don’t matter (There is nothing important there)
- Group policies work?

Exploit Basics

Hackers don't need fancy tools or scripts

- Use the tools you have in front of you
  - IE
  - Notepad
  - Help screens
  - Command line
- Give a resourceful man notepad and he will rule the world

Exploit Basics

Hackers don't need fancy tools or scripts

- **Know your environment**
  - **OS file structure (You cant exploit if cant find it)**
  - **OS command line tools**
- **XP, Win2000, 2003, and yes even win95**

Cheap Pet Tricks to Torment and Frustrate Your Group Policy Designers

- Help screens
- Loop back 127.0.0.1 to shares
- USB memory drives
- Older versions applications(backward compatible)
- Trigger errors (debug, memory overruns, Dr watson)
- Security alert popups
- Non associated extension

Group Policy Tricks

- Group policy cache
- Group policy server DNS resolution
- Read-Exclusive mode

Examples

- Launching IE
  - This is easily done with any application that provides access to the windows help menu
  - Shell folder vulnerability

Examples

- Using shell folder directory traversal vulnerability on IE to get access

  shell:appdata\+..\..\..\..\..\windows\systems32\cmd.exe

  If cmd.exe is locked out, try command.com… It wont be

- Using shell folder directory traversal vulnerability on IE to get access to USB drives

  shell:appdata\+..\..\..\..\..\d:\file.exe

Examples

- Copying files to the desktop
  - Any application that gives you browse access to a file system
  - Remember: Microsoft gave you a clipboard
- Non-associated extensions

Examples

- REG.EXE
  - Certain registry entries can be modified
  - The registry is a wealth of information.
    - Dump it for future exploit info
    - Extract user id password info off kiosk systems that auto login
- ?

Conclusions – Why?

- Take a closer look at why you are using a policy and its purpose
  - Hackers amongst us
    1. Weekend warriors
    2. Bored employees
  - Inept users

"If they had two sticks to rub together, they would poke there eye out."

Conclusions - What?

- If you don't want users running an application remove it from the workstation
- If you lockout cmd.exe don't forget command.com
- If you don't want users screwing with the registry, don't forget to lockout reg.exe
- Take a good look at USB devices
- If you don't want users accessing files, secure it with file system rights. Don't try to secure it with policies
  1. Smoke and mirrors never works
  2. File systems are better secured with file system rights

Solutions for Better Security

- Better security starts with correctly securing the file system
- When policies fall short look at 3rd party solutions
  - Solution that prevent any application not installed by administrator from running
  - Solution that let you control any and every application on the system

Questions ?

- No
- Yes
- Maybe
- If the price is right