The Insecure Workstation II

Bob Reloaded

When not having access qualifies as a disability…

Its not my fault, trust me!

- The information provided in this presentation is for educational purposes only. I am in no way responsible for any damage that is the result of the use or misuse of the information provided in this presentation

Today's presentation

- This presentation has two parts:
  - Rights escalation using API call vulnerabilities
  - Subverting Windows logon
- Key take-aways
  - Better understanding of simple desktop/console vulnerabilities
  - Protecting information assets with layered defense
  - Subverting desktop security for fun and entertainment!

What is your opinion?

- You will be asked to participate at the end of this presentation:
  - What methods do you use to secure your environment?
  - Do you follow defense in depth principles?
  - What would you do different?

Help API vulnerability

- What is a “help API” vulnerability?

  A vulnerability that is exposed when an application running with system level rights makes a API call to the help viewer and does not drop any privileges before invoking the help viewer.

  A user can then us the help viewer to access other application which will execute at system level.

- Bugtraq report

  Bugtraq ID 8884 Oct 24th 2003 Brett Moore

  http://www.securityfocus.com/bid/8884

Help API vulnerability

- How wide spread is this vulnerability?
- Why do vendors continue down this path?
  - Money
  - Beat competitors to market – cutting corners
  - Vendors presume that users will not abuse their product – security through obscurity
  - Sell first, fix later – make the customer pay to fix flaws

Help API vulnerability

- Demonstration
  - Netware Zenworks remote desktop manager
    - Novell quickly released a security patch
  - Spysweeper anti spyware enterprise version
    - Help API fixed, but application still runs at system level and interacts with desktop
  - Mcafee AV 4.51
    - This was reported in Sep 15 2004 Bugtraq #11181
    - A different exploit point

Help API vulnerability

- How do I tell if my system is vulnerable?
  - What is running with system rights?
    - Taskmgr (take a close look)
    - What icons are in the tray?
  - What applications need higher rights to function correctly?
    - Antivirus
    - Anti Spyware
    - Remote management tools
    - Auditing tools and application

Help API vulnerability

- How do we protect ourselves from a Help API Vulnerability?
  - Group policy (maybe)
  - Remove icons from the system tray
  - Test all new applications before deployment

This years project

Subverting Windows logon

Subverting Windows logon

- This year's research project and what we learned
- Credit for all the hard work
- Three rules that drove the research:
  - It must be simple
  - It needs to fit in my pocket if not in my head
  - Must be able to easily protect against it

Bypassing Windows logon

- What, Why, Were, When and How
  - Can Windows logon be subverted?
  - Curiosity “Just because its there”
  - XP, W2K3 , etc
  - Bob is back on the job
  - How
    - Methodology - “the attack process”
    - Programmatically -“the attack application”

Exploit part 1 “Utility Manager”

- What is Utility Manager?
- How does it work and how do we access it?
- Why is it such a problem?
  - Local System
  - User controlled

Exploit part 2 “ Logon Screen”

- User interface objects are managed using Windows stations and desktops
  - Winsta0
  - Multiple desktops in Windows
    - Default
    - Screen Saver
    - Winlogon

Exploit Part 3 “Delivery”

- Admin access
- API vulnerabilities
- Bit level modification of hard disk
- Maintenance boot disk

Exploit part 4 “The code”

- This code poses no security issues by itself
- Basically we are just setting the CreateProcess thread to run under the winlogon desktop
- The security breakdown is how it is used. We are taking advantage of an architecture design issue within Microsoft
- The code is extremely simple!

Exploit part 4 “ The code”

```
#include <windows.h>

int WINAPI WinMain(HINSTANCE hInst, HINSTANCE hPrevInst, LPSTR lpCmdLine,
      int nShowCmd) {

      STARTUPINFO si;
      PROCESS_INFORMATION pi;
      memset( &si, 0, sizeof(si) );
      memset( &pi, 0, sizeof(pi) );
      si.cb = sizeof(STARTUPINFO);
      si.lpDesktop = "Winsta0\\Winlogon";
      CreateProcess("C:\\windows\\system32\\cmd.exe", NULL, NULL, NULL, false, NULL,
      NULL, NULL, &si, &pi);

      return 0;
}
```

BOB RELOADED

When not having access qualifies as a disability…

BOB RELOADED

- Install exploit code using maintenance disk
  - Open back door at Winlogon desktop with osk.exe
    - Limited resources XP
    - taskmgr
    - Network access
    - Using memory tools “Password grab”
  - CreateProcessAsUser and Impersonating the security context of a logged on user.

BOB RELOADED

- Open back door at Winlogon desktop on W2K3 server
  - Resources
  - Run explorer “full desktop”
- There is more than one way to use this:
  - Create LocalSystem shell on Default desktop with Magnifier

Exploit "Is this real?"

- Is this a real threat?
  - Why it is…
  - Potential impact to security
  - Possible real word scenarios
  - Other exploits could follow this same method
- Unknown exploits are stopped with Defense in Depth tactics

Basic Protection

- How do I protect my systems from this exploit?
  - Group policy (maybe)
  - Remove or disable utilmgr
  - Disable boot CDROM - lock BIOS
  - Host IDS on servers

"The Big Picture"

- Preventing back door exploits by employees:
  - Policies
  - Separation of duties
  - Application, system verification and testing before deployment

“The Big Picture”

- Preventing non-employee access
  - Who is that maintenance man and what do you really know about the night janitors?
  - Using social engineering to gain physical access “security awareness training”
  - Contractual agreements with contractors and outsourcers “whether it’s janitorial or application development”

"The Big Picture"

- Defense in Depth "The only effective method to defend your network"
  - Combination of people, processes and technology
  - Applied at each layer. If one layer is compromised your entire organization is not compromised
  - Policy, physical, perimeter, internal network, host, application and data

Now its your turn…

- What methods do you use to secure your environment?
- Do you follow defense in depth principles?
- What would you do different?

Remember Bob may be working for you.

Contact information:

- Email: dh@layereddefense.com
- Web Site: www.layereddefense.com