



## Windows Attacks and Defenses

Jesper M. Johansson, Ph.D.  
Trustworthy Computing Team  
Microsoft Corporation




## Windows Can be Secured: PC Week [www.hacknt.com](http://www.hacknt.com)

- ◆ System placed behind firewall
- ◆ Port filtering enabled as if firewall failed
- ◆ Server service, DCOM disabled
- ◆ Essential command-line tools not executable by web server
  
- ◆ It emerged unscathed!




## Anatomy of an Attack

- ◆ Information gathering
- ◆ Establishing a beachhead
- ◆ Escalating privilege
- ◆ Maintaining position




## OS Fingerprinting

- ◆ Matches low-level TCP responses to database of known behaviors
- ◆ Often possible to identify operating system down to service pack level
- ◆ HTTP, FTP, and SMTP banners are often helpful to your opponent




## Firewalking

- ◆ A traceroute depends on setting a “hop count”
- ◆ Traceroutes can be performed using ANY type of packet – TCP, UDP, ICMP
- ◆ A careful and methodical attacker can determine where your defenses are




## Information Gathering – Win32 API Level

- ◆ Depends on ports 137-139,445 TCP/UDP
- ◆ Can deliver version, service pack, running services, users, groups, number of adapters
- ◆ A pure Windows 2000 network can be locked down more tightly
  - RestrictAnonymous = 2



## Initial Attacks

- ◆ Password guessing
- ◆ Web server attacks
  - Unpatched web servers
    - Web servers are often the first point of attack
  - Improper FrontPage permissions
    - Especially on author.dll and admin.dll
- ◆ SQL Server command shell
  - Poor sa passwords
  - Unpatched buffer overflows
- ◆ Terminal Server



## Common IIS Attack Vectors

- ◆ Missing patches
- ◆ Missing patches
- ◆ Missing patches
- ◆ Misconfigured/missing permissions
- ◆ Hosting web site on boot partition
- ◆ Running in low isolation
- ◆ SQL command insertion
  
- ◆ Run the IIS Lockdown Tool!



## Escalation of Privilege

- ◆ Password cracking
- ◆ Service users
- ◆ Files with embedded passwords
  - asp, inc, asa files
- ◆ Trojans
- ◆ AutoAdminLogon
  - Credentials available remotely



## Maintaining Position

- ◆ Backdoors and rootkits
- ◆ Compromised accounts



## Defending your Network

- ◆ Keep informed
  - [www.microsoft.com/security](http://www.microsoft.com/security)
  - Subscribe to security bulletin notification mailing list
- ◆ Know your weaknesses
- ◆ Have an *enforceable* security policy
- ◆ Manage security



## Know Your Enemy

*Know your enemy as you know yourself and success will be assured*

- ◆ Stay current on mailing lists
  - NTBUGTRAQ ([www.ntbugtraq.com](http://www.ntbugtraq.com))
  - BUGTRAQ ([www.securityfocus.com](http://www.securityfocus.com))
  - Firewall Wizards ([www.nfr.net](http://www.nfr.net))
  - NT Security ([www.ntsecurity.net](http://www.ntsecurity.net))
- ◆ Read other forums
  - Slashdot (<http://www.slashdot.com>)
  - Packetstorm (<http://packetstormsecurity.nl>)




## Know Yourself

- ◆ Use security auditing tools regularly
  - Know where your weaknesses are
- ◆ Design your network with security in mind



## Security Policies

- ◆ An unenforceable policy is as bad as no policy
- ◆ High-level buy-in
  - Information security needs leverage over operations



## Defense in Depth

- ◆ Design for security fault-tolerance
- ◆ Assume that failures will occur
- ◆ Use multiple layers at every step

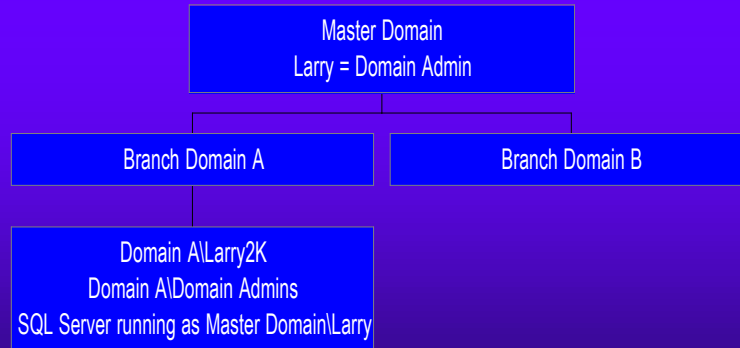


## Managing Security

- ◆ Know your critical systems
- ◆ Plan for security hotfixes
  - Hotfixes are painful and expensive, therefore they are only created for critical problems
- ◆ Roll fixes into the build process



## Understanding Security Dependencies




Any local admin can execute code under the context of any other user logged on locally



## Following Dependency Chains




- ◆ Shep mis-configures Test-Host
- ◆ Moe's account is compromised
- ◆ Crit-Serv3 now compromises Larry
  - Attacker is now a domain admin!
- ◆ Crit-Serv2 compromises \_Svc
- ◆ Crit-Serv1 compromises Curly



## Limit Dependencies

- ◆ Limit Admin-Level accounts
- ◆ Know where administrators log on
- ◆ Avoid using domain accounts for services
  - Domain admin accounts for services means any local admin is a domain admin




## Limit Privileges

- ◆ Debug privilege is the most dangerous privilege there is
- ◆ Users with Backup privilege can read *any* file
  - You do not need Restore
- ◆ Use privileges to restrict logons
  - “Prevent” your Domain Administrators from logging on to workstations



## Recovering From an Attack

- ◆ Restore from trusted media
- ◆ Baseline your data
- ◆ Reset ALL admin-level passwords
- ◆ Plan for the worst-case



## Conclusions

- ◆ Think like your enemy in order to defeat them
- ◆ Use a layered, fault-tolerant defense strategy
- ◆ Understand your network security infrastructure
- ◆ Conduct frequent security audits