



Hacking Windows NT (Using UNIX)


Hans Van de Looy
<hans@blackhats.org>



Preamble And Disclaimer

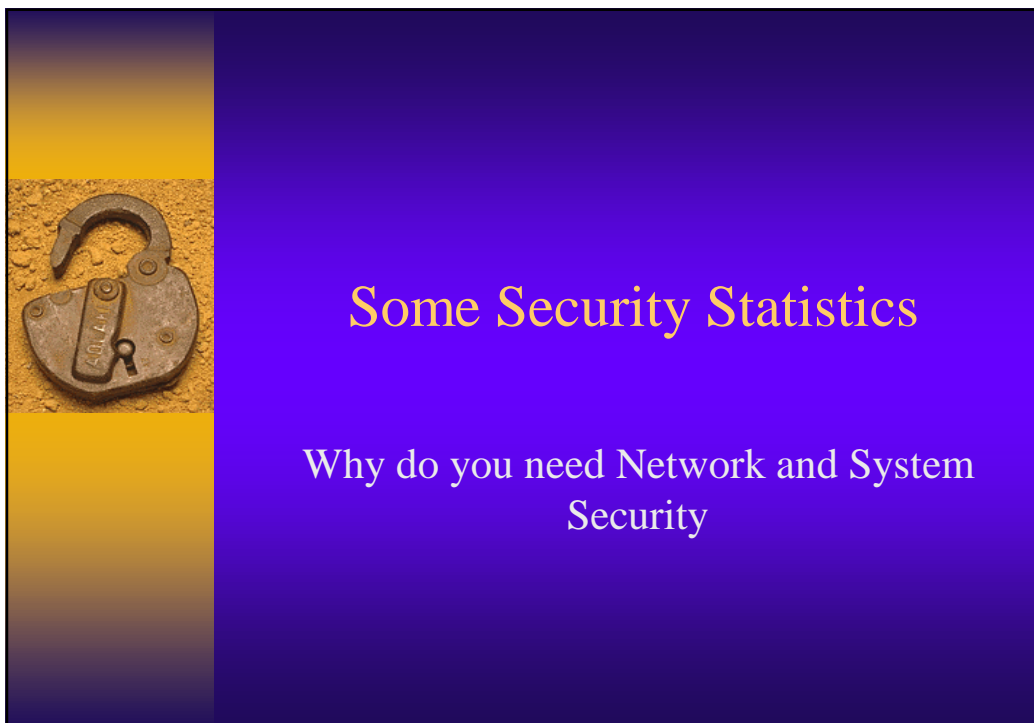
- ♦ A lot of the vulnerabilities described in this presentation can be fixed, but are still present in the world outside. Pointing these out to administrators is the only reason for including them in this presentation.
- ♦ Cracking may be a criminal offense and prosecuted by law in your country.





Contents

- ♦ Some Security Statistics
- ♦ No Holy Wars; Please!
- ♦ Windows NT Security Holes
- ♦ Well Known (UNIX) Tools
- ♦ Pitfall Avoidance
- ♦ Installing Baseline Security
- ♦ Internet References
- ♦ Conclusion





Recent Security Statistics

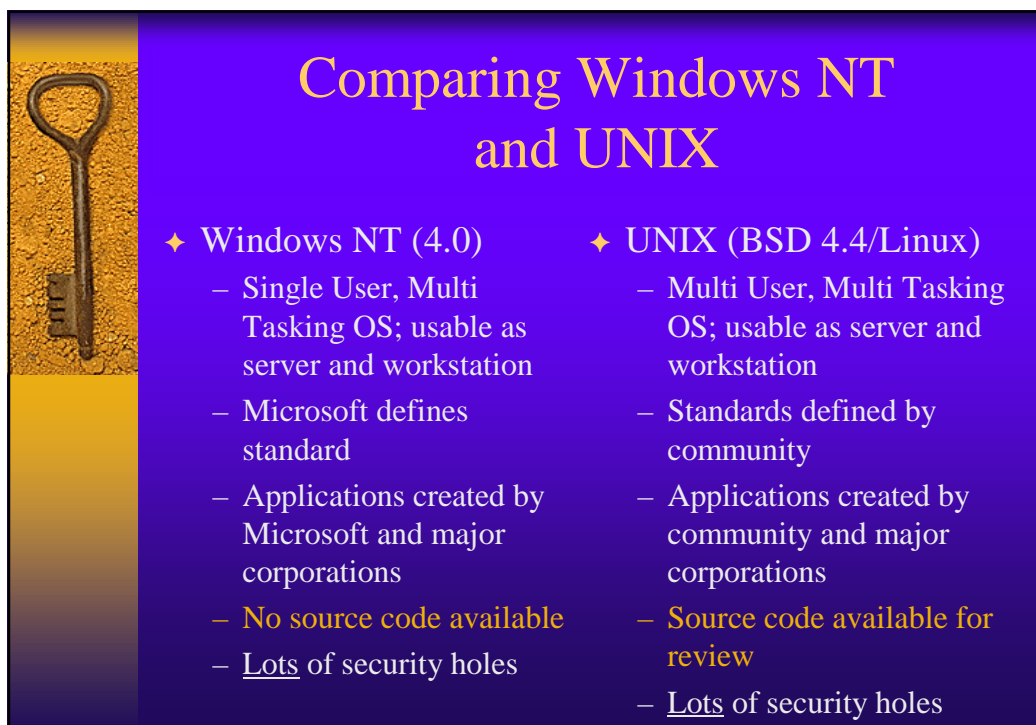
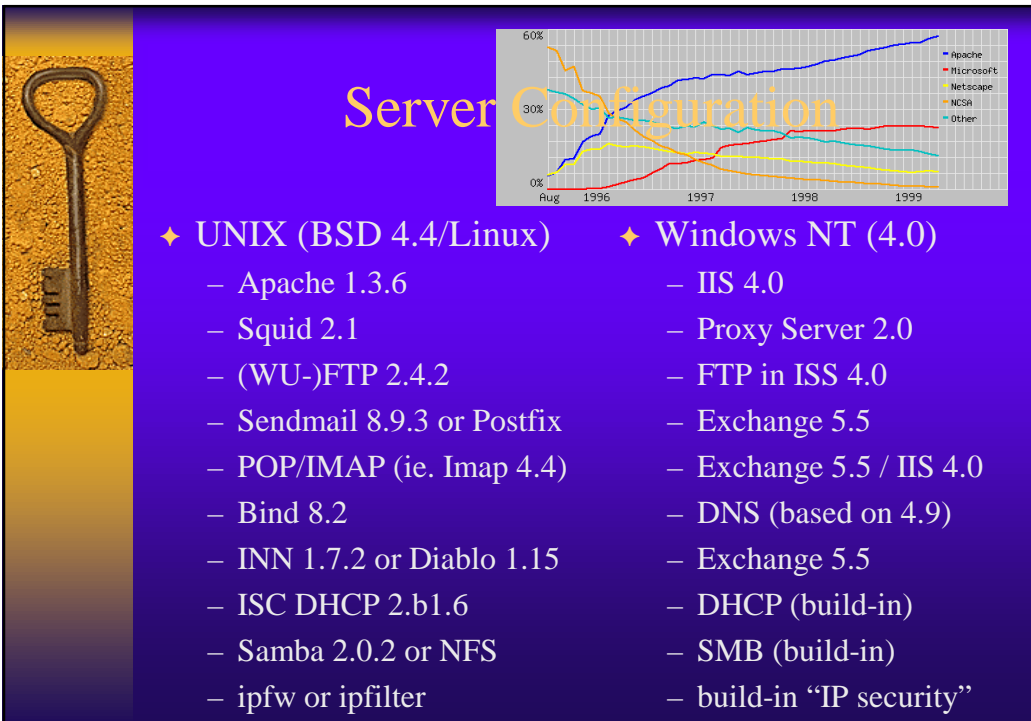
- ♦ Network Security is a serious issue for most organisations
 - 30% of respondents reported system penetration by outsiders
 - 55% of organisations surveyed report increased attacks by “insiders”
 - 32% of respondents reported serious incidents to law enforcement - *previously only 17%*
 - 20% increase in attacks from the outside since 1996 thanks to e-commerce

Source 1999 CSI/FBI Computer Crime and Security Survey



No Holy Wars; Please!

Strengths and weaknesses of
Windows NT and UNIX





Availability Of Source Code

- ♦ Enables peer review of “Features”
- ♦ History reveals a lot of security holes found
- ♦ Unavailability (Security-through-Obscurity) does not guarantee more security
- ♦ Who has studied every piece of source code from a major Operating System kernel (i.e. Linux or BSD) or Application (i.e. PGP)?



Let's Talk About Marketing

Lies, Damned Lies and Marketing



How To Manipulate The Truth With Marketing

♦ C2 Security

- Windows NT 3.51 is C2 certified as an Operating System, NOT as a Trusted Network Component (orange book, not red book)¹

♦ Microsoft is becoming more Security Aware

- Microsoft has needed to recall several security patches in the past due to the problems they created

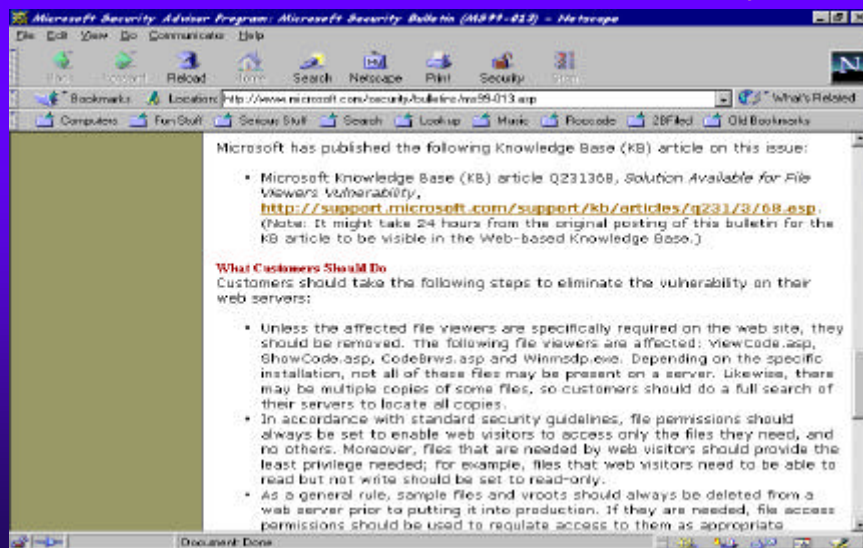
¹ Hot News: At InfoSecurity NT 4.0 received UK E3/FC-2 certification



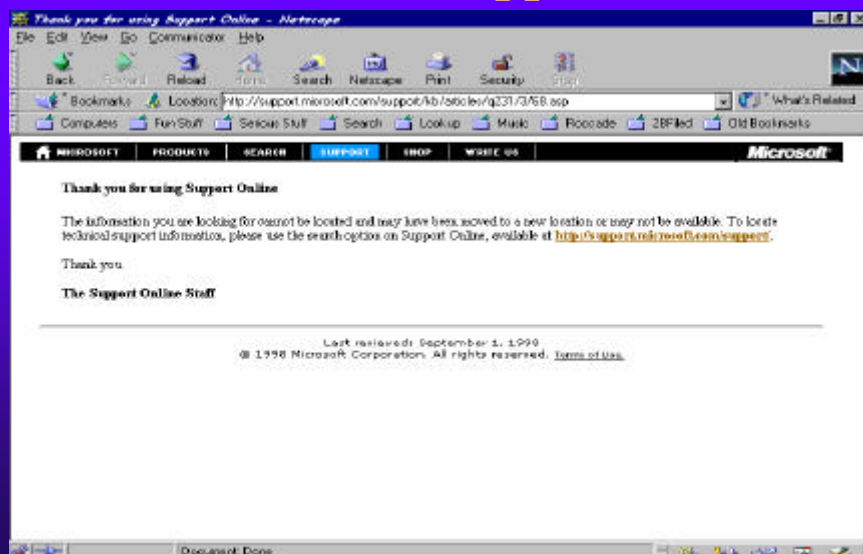
HackerNews Reaction

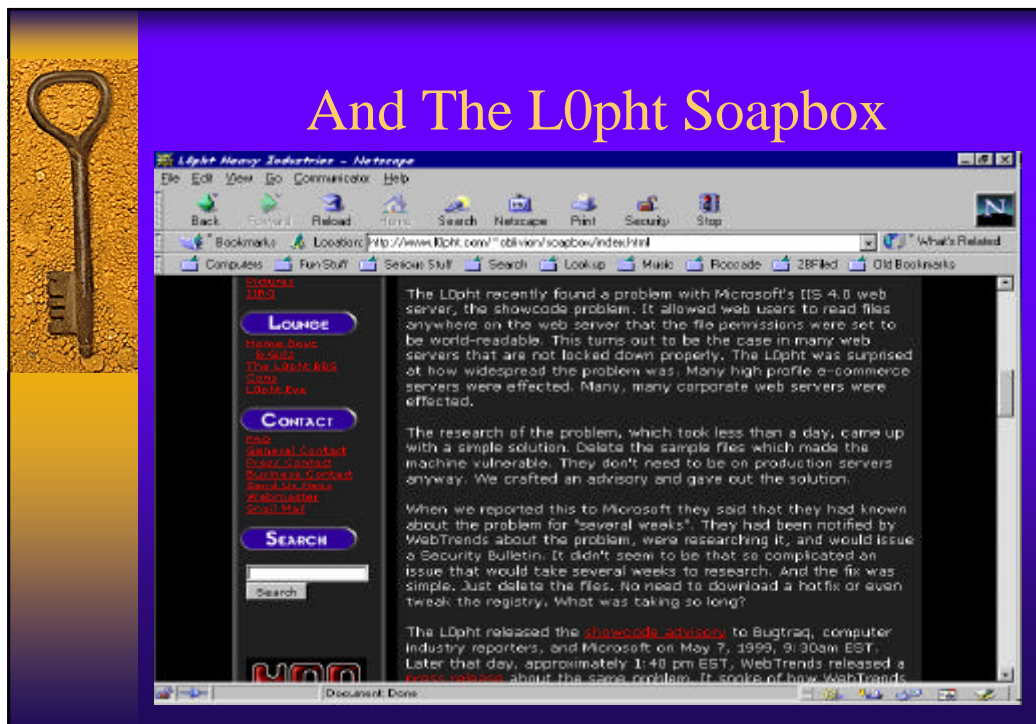



Recent Microsoft Advisory



So Much For Support Online








Windows NT Security Holes

- ♦ Denial Of Service
- ♦ Local Exploits
- ♦ Gaining Administrator Rights
- ♦ Password Cracking
- ♦ Network Vulnerabilities
- ♦ Remote Exploits
- ♦ Known Microsoft Software Vulnerabilities (IIS, Exchange, PPTP, Macro's ...)




Denial Of Service

Lame (but effective) Attacks




Denial Of Service (1)

- ♦ Ping O'Dead (Packet-size ≥ 65510 bytes)
- ♦ SYN Flooding
- ♦ LAND (SYN where source = destination)
- ♦ Fraggle (UDP Broadcast)
- ♦ Smurf (TCP/IP Broadcast)
- ♦ ICMP-DoS (ICMP Echo Reply Flood info)
- ♦ Teardrop (IP Fragment Overlap Bug)




Ping O'Dead

- ♦ Aliases/Variations: FatPing, SSPing, Jolt, IceNewk
- ♦ Description: Sends series of (highly fragmented) oversized (size ≥ 65510 bytes) ICMP_ECHO packets over the connection.
- ♦ Result: The system cannot re-assemble them fast enough and locks up




WinNuke

- ♦ Aliases/Variations: OOBNuke
- ♦ Description: Sends a packet with an URGENT flag set and pointing to Out of Band data.
- ♦ Result: Blue Screen (virtual device driver)




Nuke

- ♦ Aliases/Variations: Click, ICMP Nuke, WinFreeze
- ♦ Description: This attack tries to convince your computer that it has lost its connection. The computer then disconnects from the port specified.
- ♦ Result: Connection reset by peer, Connection refused or Host unreachable




Bonk

- ♦ Aliases/Variations: Boink, Newtear, Teardrop2
- ♦ Description: This attack sends IP fragments resulting in a malformed UDP header packet.
- ♦ Result: Systems crashes with Blue Screen of Dead




Teardrop

- ♦ Aliases/Variations: Tear, TCP/IP Fragment overlap, Nestea (for Linux)
- ♦ Description: This attack sends overlapping IP fragments that the system cannot re-assemble.
- ♦ Result: System will enter Catatonic State or Crash and Reboot




Land

- ♦ Aliases/Variations: Latierra
- ♦ Description: Sends a SYN packet where source address equals destination address so the victim will try to respond to itself.
- ♦ Result: Extreme Slowdown, Enter Catatonic State.




Smurf

- ♦ Aliases/Variations: ICMP Flood, Ping flood, Fraggle, Pong, PapaSmurf
- ♦ Description: Perpetrator sends a large amount of ICMP_ECHO traffic at broadcast addresses, all having spoofed source addresses of Victim. Traffic will be multiplied by hosts on that IP network.
- ♦ Result: Connections dropped, Enter Catatonic State



SYN Flooding

- ♦ Aliases/Variations:
- ♦ Description: Connections are opened in rapid succession, but handshake is not completed, thus filling up queues.
- ♦ Result: Extreme Slowdown / Enter Catatonic State



Denial Of Service (2)

- ♦ CPU Attack (Telnet to port to be confused)
 - DNS (53 - 1 character + CR)
 - RPCSS (135 - ±10 characters + disconnect)
 - INETINFO (1031)
- ♦ DNS DoS
 - Send it a DNS response when it did not make a query and DNS will crash.
- ♦ ISS Crash (GET ../../.)
 - and another one (still works with SP4):
\$ telnet localhost chargen | nc your-iis-host http




Denial Of Service (3)

- ♦ System Call Insecurity
 - Kernel located in NTOSKRNL.EXE
 - KERNEL32.DLL just like “libc” in UNIX
 - NTDLL.DLL used by KERNEL32.DLL (Simple functions to perform actual Syscalls)
- ♦ Invalid parameters result in BSOD, thus users can crash the whole system and may gain additional rights!
- ♦ Source: Solar Designer message to NTBUGTRAQ




Local Exploits

What to do with console access




Local Exploits

- ♦ NTFS C:\WINNT default permissions are Full Control for Everyone, while most subdirectories have Change Control
- ♦ Administrator account (always SID 500) has full control over complete system
- ♦ Security Account Manager (SAM) contains all user account information
- ♦ Service Pack 3 solved a lot (but not all) of security related problems (Need **SP-5** now!)




Security Access Manager

- ♦ Contains both the LanManager (DES) and the Windows/NT (MD4) hash values
- ♦ Normally stored in:
C:\WINNT\system32\config\Sam
(Locked during normal operation)
- ♦ Backup made during creation of an Emergency Repair Disk at location:
C:\WINNT\repair\sam._
- ♦ Also available on the ERD




SAM Replacement

- ♦ Rename WINNT/system32/LOGON.SCR
- ♦ Copy MUSRMGR.EXE to LOGON.SCR
- ♦ Wait for screensaver to kick in... (usermanager will allow you to change any passwords)
- ♦ Replace LOGON.SCR to normal location




Administrator Rights

- ♦ **GetAdmin** written by Konstantin Sobolev attaches to the WinLogon process to give an account Administrator rights
 - **Crash4.exe** will allow GetAdmin to work on SP3 patched machines by rearranging a few things on the stack to allow GetAdmin to work
- ♦ **Sechole** modifies OpenProcess API and successfully requests Debug rights to give Administrator rights (tested under **SP4**)



Password Cracking

- ♦ Since Microsoft does not salt during hash generation, once a potential password has generated a hash, it can be checked against ALL accounts
- ♦ All current NT crackers take advantage of this
- ♦ Several freeware and shareware products are available on the Internet



Some Password Crackers

- ♦ **L0phtcrack 2.5**
 - Gather and crack NT password hashes directly through SAM (database or backup) or by monitoring SMB network activity
 - Beware: 8 character password = one 7 character passwords and a one letter password
- ♦ **John the Ripper 1.7 / Crack 5.x**
 - UNIX password crackers that can also handle Windows NT passwords (when “dumped” in right format)




KnownDLLs List (1)

- ♦ Core OS DLLs are kept in virtual memory and shared between the programs running on the system
- ♦ OS references a data structure called the KnownDLLs list to determine the location of the DLL in virtual memory
- ♦ Windows NT protects in-memory DLLs against modification, but allows all users to read from and write to the KnownDLLs list



KnownDLLs List (2)


- ♦ Load into memory a malicious DLL that has the same name as a system DLL, then change the entry in the KnownDLLs list to point to the malicious copy
- ♦ Programs that request the system DLL will instead be directed to the malicious copy
- ♦ When called by a program with sufficiently high privileges, it could take any desired action



Buffer Overflows (1)

- ♦ Became “popular” on UNIX after articles published by Aleph1 and Mudge
- ♦ David Litchfield (*a.k.a. mnemonix*) published “*RAS Buffer Overrun Exploit and Tutorial*” and “*Winhlp32 Buffer Overrun Exploit and Analysis*”

<http://www.infowar.co.uk/mnemonix/ntbufferoverruns.htm>



Buffer Overflows (2)

- ♦ Dildog (cDc) wrote “*The Tao of Windows Buffer Overflow*”
(http://www.cultdeadcow.com/cDc_files/cDc-351/)
 - A complete picture of buffer overflows, how they work, and how to code your own exploits for Microsoft operating systems
- ♦ Assumption: This will be the “next craze”




Remote Exploits

Secure Networking is an art




C2Myazz

- ♦ Another computer spoofs the client into sending a clear-text password to the server, bypassing all password encryption
 - The software listens for SMB negotiations, and upon detecting one, sends a single packet to the client instructing it to downgrade its connection attempt to a clear text level
 - Password is retrieved while the client is successfully connected to the NT server




How To Use LanManager Hash

- ♦ LanManager hash is a password equivalent in a challenge-response protocol
- ♦ A modified (Samba) client with access to uncracked NT password database can use this information to authenticate to the server




Man In The Middle Attack

- ♦ Nmap provides the following comment:
 - TCP Sequence Prediction: Class=trivial time dependency
Difficulty=0 (Trivial joke)
Remote operating system guess: Windows NT4/Win95/Win98
- ♦ SMB Hijacking should be possible, but no known exploits (Yet...)
 - Complex spoofing job
 - the session has to be hijacked at the transport level (getting all of the ACK/NACK numbering correct)
 - the Tree ID (TID) and User ID (UID) would have to be spoofed as well (at redirector and server level)




Microsoft's Implementation of PPTP

- ♦ PPTP can be used for the creation of VPNs
- ♦ Bruce Schneier and Mudge published "*Cryptanalysis of Microsoft's Point-to-Point Tunneling Protocol*"
- ♦ The paper did not find flaws with PPTP, only Microsoft's implementation of it
- ♦ Phrack 53 contained another paper by Aleph1 entitled "*The Crumbling Tunnel*"




Microsoft's PPTP Flaws

- ♦ The security flaws allow sniffing passwords across the network and breaking the encryption that protects the tunneling protocol
- ♦ Recommendation by Schneier: Use IPSec (or 3rd party implementation of PPTP) instead



Microsoft's Remaining PPTP Issues (1)

- ♦ The entire session and/or packet is not encrypted
- ♦ There are still "pieces" visible to sniffing, such as DNS server addresses
 - This is partially due to the fact that the entire negotiation process is "on the wire"
 - Control of the encrypted session is handled via this separate connections



Microsoft's Remaining PPTP Issues (2)

- ♦ The connection that "controls" the session is not authenticated, making it vulnerable to Denial of Service
 - The concern here is that we do not have control over the client configuration at all times, and that the session could be interrupted followed by some spoofing to "dummy down" to MS-CHAPv1 with its weaker encryption a la LanMan hashes as the client attempts to re-connect



Microsoft's Remaining PPTP Issues (3)

- ♦ The nature of the challenge-response still places all of the material used during the generation of session keys onto the wire (Keyspace is less than 128 bits)
 - Only the password is protected in this sense, so the key is only as strong as the password
 - This means that offline cryptanalysis of a session could reveal the user password
 - To further the theory an entire encrypted session could be "decrypted" offline



Scanners

Point and Click Tools from the Internet



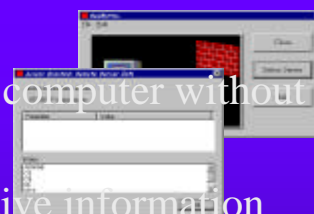
Remote Scanners



- ♦ OGRE (Rhino9 Team)
 - Simple Port and Vulnerability Scanner
- ♦ NAT (Andrew Tridgell)
 - Brute Force NetBIOS Auditing Tool
- ♦ NTIS (David Litchfield)
 - Great NT Information Scanner
- ♦ RedButton (Midwestern Commerce, Inc.)
 - NetBIOS Auditing Tool



RedButton


- ♦ Logs on remotely to a Target computer without User Name/Password
- ♦ Unauthorized access to sensitive information stored in file system and registry available to Everyone group can be obtained
- ♦ Determines current name of Built -in Administrator account
- ♦ Reads several registry entries
- ♦ Lists all shares (including the hidden ones)






NetBus Pro 2.0

- ♦ According to the author (Carl-Fredrik Neikter) NetBus Pro is a easy-to-use remote administration and spy tool
- ♦ Features for remote administration include:
 - File manager, Registry manager and Application Redirect
- ♦ Spying features include:
 - Capture screen, Listen keyboard, Capture camera image and Record sound




Macro's and Some Other Vulnerabilities

User Friendly or Cracker Friendly



Macro's

- ♦ Various applications contain a **very** powerful MACRO language capable of doing file-I/O and calling Win32 APIs
- ♦ Perfect for writing virii / worms (Anyone heard of Melissa or PrettyPark?)
- ♦ Windows Help files (.HLP) are capable of running DLLs




Other Vulnerabilities

- ♦ RAS and RRAS Vulnerability
 - User credentials are cached in Registry regardless of whether checkbox is selected or deselected.
(Lisa O'Connor, Martin Dolphin, and Joe Greene)
- ♦ Interesting special key-combinations usable on a locked-down system:
 - Ctrl-Shift-ESC starts Task Manager (like Ctrl-Alt-Del)
 - Alt-TAB to choose Active Window




Using (UNIX) Tools

To hack Windows NT systems




Alternate Operating System

- ♦ Floppy-disk (or bootable CDROM) can be used to boot alternative Operating System (Trinux or PicoBSD)
- ♦ **Offline NT Password Editor** by Petter Nordahl-Hagen; available as Linux bootdisk containing a script that leads you through the complete process



NetCat

- ♦ Swiss Army Knife of Hacker Tools (can act both as client and as listener)
- ♦ NT version can bind to ports in front of processes already listening (Cracker can filter interesting data before passing it on)
- ♦ Also useful for Administrators




Samba

- ♦ Another fine tool developed by Andy Tridgell
- ♦ Samba talks SMB; integrates UNIX and NT in a LanManager environment
- ♦ A tool like Samba and information from “*CIFS: Common Insecurities Fail Scrutiny*” by Hobbit (L0pht) will guide you to Enlightenment




Pitfall Avoidance

Keeping your system (more) secure




Basic Security (Confuse The Wannabe's)

- ♦ Set BIOS Password
- ♦ Boot from C:
not from A: or CD-ROM
- ♦ Disable or remove floppy drive from system
- ♦ If possible remove CDROM drives
- ♦ Not REAL Security! Use it just to filter the anklebiters from the experts




File System Security

- ♦ Use NTFS wherever possible
 - Allows use of Access Control Lists
 - Is more robust during crashes
- ♦ FAT provides no protection at all (i.e. delete SAM database and reboot)
- ♦ There are tools that allow access to NTFS from DOS (ntfsdos.exe) or UNIX (Linux ntfs)




Watch Those File Permissions

- ♦ Copying lets a file *inherit* the permissions from the destination directory (use SCOPY instead)
- ♦ Moving a file preserves the existing file permissions
- ♦ This may result in “full control” access for “everybody” when this is not wanted



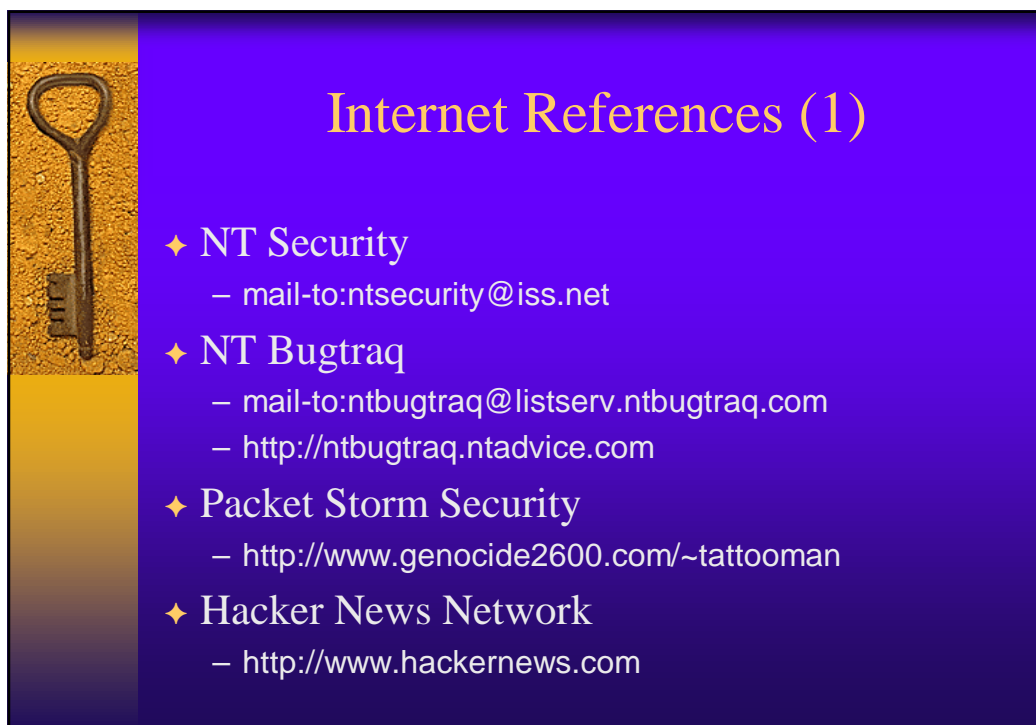
Some NT Administration Tools

- ♦ Chronicle v1.0 (Rhino9 Team)
 - Service Pack and Hot Fix Scanner
- ♦ NTInfoScan (David Litchfield a.k.a.. Mnemonic)
 - Security Scanner (SATAN) for NT Servers
- ♦ ScanNT (MWC)
 - Simple NT Password Checker
 - User needs extra privileges: Act as part of the OS, Replace a process level token, Increase quotas



Windows NT Security 101

- ♦ These Fine Documents Will Be Of Great Help:
 - Windows NT Wardoc by Rhino9 Team
 - Also available in handy 3Com Palm Doc format
 - NSA Windows NT Security Guidelines
 - SANS Institute NT Security Step By Step



Internet References (1)

- ♦ NT Security
 - mail-to:ntsecurity@iss.net
- ♦ NT Bugtraq
 - mail-to:ntbugtraq@listserv.ntbugtraq.com
 - <http://ntbugtraq.ntadvice.com>
- ♦ Packet Storm Security
 - <http://www.genocide2600.com/~tattooman>
- ♦ Hacker News Network
 - <http://www.hackernews.com>




Internet References (2)

- ♦ L0ht Heavy Industries
 - <http://www.l0pht.com>
- ♦ Computer Emergency Response Team
 - <http://www.cert.org>
- ♦ Microsoft Corporation
 - <http://www.microsoft.com/security>
- ♦ Hack FAQ
 - <http://www.genocide2600.com/~tattooman/hacking-textfiles/hack-faq/index.html> (no direct access ;-)




Conclusion

Keep Security In Mind



Windows NT Security...

- ♦ Is definitively not as good as Microsoft wants us to believe
- ♦ Is at best as good as security on a UNIX system
- ♦ Vulnerabilities found every week in spite of Microsoft's Security Through Obscurity Strategy



The “Best” Is Still To Come...

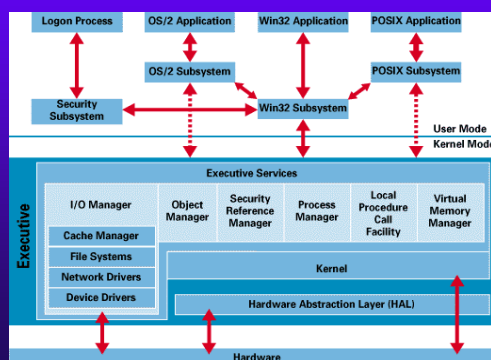
- ♦ Windows 2000 will consist of more than 27 million lines of code (and lots of changes)

Think about it!

☺

Linux 2.0 consists of 1.5 million lines of code

NT 3.5 had about 5 million lines of code





THANK YOU!

Any Questions?