

A forum for experts to encourage discussion and share expertise in understanding the latest trends and security threats facing computer networks, systems and data.

AUTHENTICATION - Next Event **May 25th**
Downtown Toronto
6:00pm to 9:00pm

Visit & Register online at www.TASK.to



ATTACK!

Presenters
Brian Bourne, CISSP MCSE:Security
Christopher Diachok, MCSE

What we want to demonstrate today:

- Privilege Escalation
- Alternate Data Streams
- Hidden Rootkits
- Browser Exploitation

What is it?

- The obvious: upgrading your level of access. Usually “user” level to “administrator” level.

Where?

- User on local machine
- User on terminal server (or Citrix server)
- Local Admin to Domain Admin
- Domain Admin to Enterprise Admin

How?

- Discussion of alternate techniques
- Demonstration

DEMO

Example: F1 help exploit of local application

- Sending F1 key to a service/application via perl script
- System Level access gained
- User can elevate privilege to local administrator

DEFENCE

- Patch management
- Host based security / policy enforcement
- Group Policy
 - Software restriction policy
 - Restricted Groups

TOOLS/SOFTWARE FROM DEMO

- www.dell.ca - Dell TrueMobile 1400, TrueMobile 1300, TrueMobile 1300, Wireless 1350, Wireless 1450, Wireless 1370, v.3.100.35.1 / 3.100.41, A06 Driver Software
- www.perl.com - Perl v5.8.2 built for MSWin32-x86-multi-thread
- www.cqure.net - sendF1_towin version 1.2 by Ian Vitek

Alternate Data Streams

What?

- All versions of NTFS since 3.1 include the ability to store multiple streams of data.
- Basically a file attribute.

Why?

- Officially – to store extra information with a file
- Unofficially - A great way to hide data... and executables!

How?

- Demonstration

Details:

- Go to a DOS prompt
- Add text to file with:

```
echo <text> <file>:<stream>
```

- Retrieve with

```
more < <file>:<stream>
```

- Notice: No change in file size!

- Hide executables:

```
type "c:\windows\explorer.exe" > test.txt:hidden.exe  
start .\test.txt:hidden.exe
```

Why You Care

- This isn't new. Supported since 1993, IIS exploit in 1998, first virus (W2K.Stream) in 2000.
- More recently: Trojan.Comxt and Trojan.Comxt.B (Feb 05)
- Denial of service (fill up a drive)

Removal

- Delete the file / folder
- Make the stream null. Still there, but at least smaller.
- Copy to a non-NTFS file system, delete original, then copy it back.
- SysInternals "Stream" tool and others

References:

- How to use Alternate Data Streams:
<http://support.microsoft.com/default.aspx?scid=kb;en-us;105763>
- SysInternals “Streams”
<http://www.sysinternals.com/files/streams.zip>
- CrucialADS – GUI Scan Tool
<http://www.crucialsecurity.com/downloads.html>

Rootkits – A Teaser

What is a Rootkit?

- A root kit is a set of tools used by an intruder after cracking a computer system. These tools can help the attacker maintain his or her access to the system and use it for malicious purposes. Root kits exist for a variety of operating systems such as Linux, Solaris, and versions of Microsoft Windows.
Ref: en.wikipedia.org/wiki/Rootkit
- Functionality varies from kit to kit, but it's usually all bad.

What's new?

- Rootkits for Windows are becoming more “mainstream”
- Techniques used for hiding are increasingly advanced

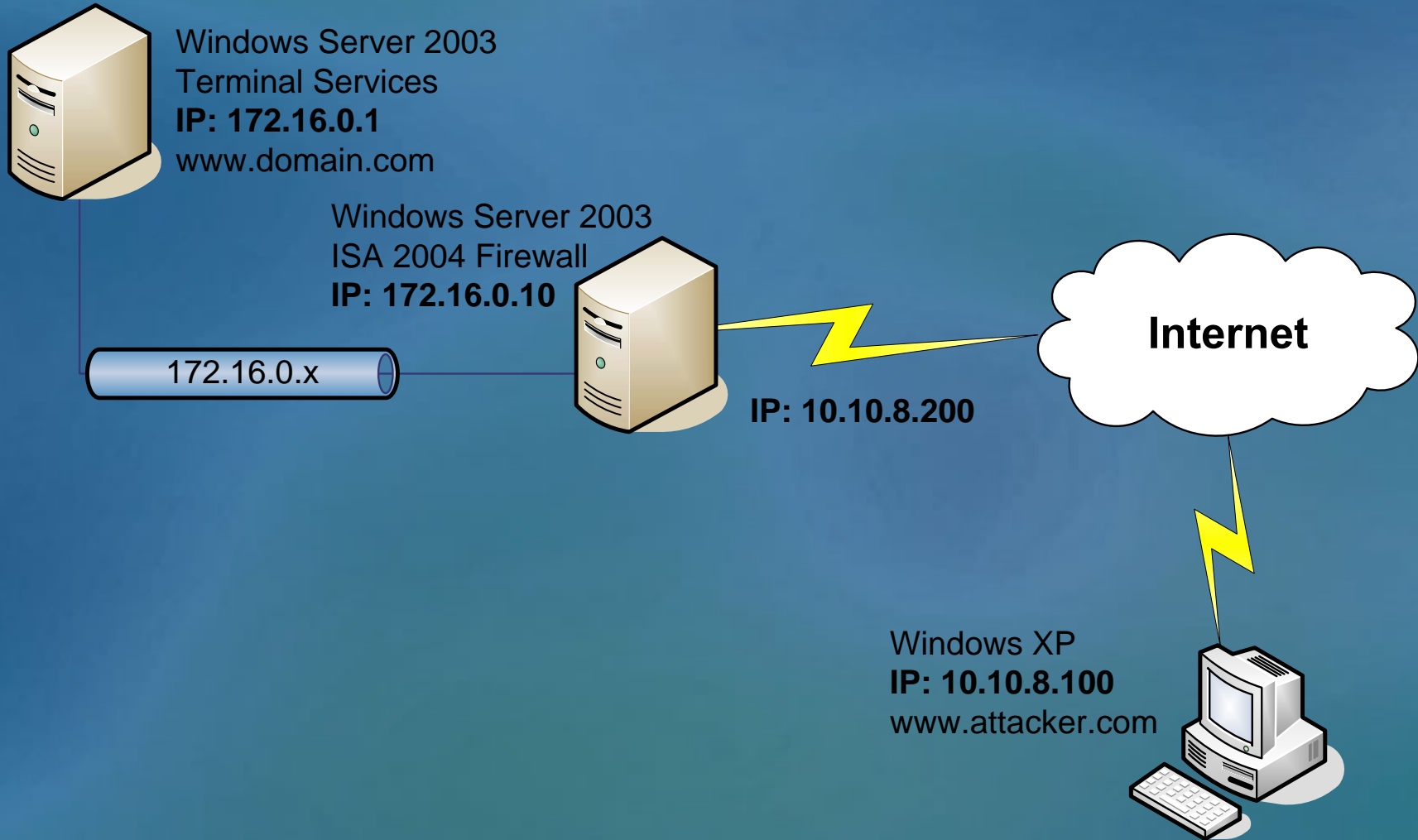
How does it get there?!?

- Short answer: the usual methods for installing any code!
- EG:
 - Brute force password attacks
 - Known Exploits (remote code execution)
 - Malware (Trojan, Browser Exploit, etc)
 - Social Engineering - User tricked into running it.

LET'S SEE ONE!

* Detailed presentation will be shown at InfoSecurity Canada.

Network Topology



Rootkit Demo Summary

* THIS SLIDE INCLUDED IF YOU DIDN'T SEE THE DEMO

- Port scan www.domain.com
- Web site information gathering
- RDP 3389: Tsgrinder (brute force) – admin account access
 - Other methods could be: pop3, web (http), vpn, telnet, etc...
- Plant hacker defender rootkit
 - Hides ports, registry keys, files/folders, processes & services

Golden Hacker Defender includes (Cost @\$1,000 CAD)

- protection against all AV, unique version and source code for both main module and driver module
- separation between hidden processes and hidden files in inifile
- outbound TCP connection hiding
- Rootkit Detector 0.61, 0.62 antidection
- modern detectors anti-detection engine with anti-detection against
 - F-Secure BlackLight 1.0.1017.0, 1.2.1003.0, 1.3.1015
 - F-Secure BlackLight console 1.25.1006.0, 1.28.1006.0
 - Sysinternals RootkitRevealer v1.00, v1.01, v1.10, v1.20, v1.31, v1.32, v1.33, v1.40
 - UnHackMe 1.0, 2.0, 2.5 beta
 - RootKit Shark 3.11
 - Malicious Software Removal Tool 05/04/12
 - Find Hidden Service 1.0, 1.1
 - Kernel SC 1.3
 - Kernel PS 0.4, 1.0
 - Klister 0.4
 - Process Magic 1.0
 - KProcCheck 0.2-beta1
 - TaskInfo 6.0.1.134

Protection

- The constant answer: Defence in Depth!

Removal / Detection

- Boot to safe mode (sometimes works)
- WinPE, Knoppix, etc
- Detection tools (sometimes works)
- Rollback technology / software
- **FORMAT!**
- See InfoSec Presentation!

TOOLS/SOFTWARE

- www.gfi.com - GFI Languard
- www.hammerofgod.com - TSGrinder
- hxdef.czweb.org - Hacker Defender
- <http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml>

Browser Exploitation

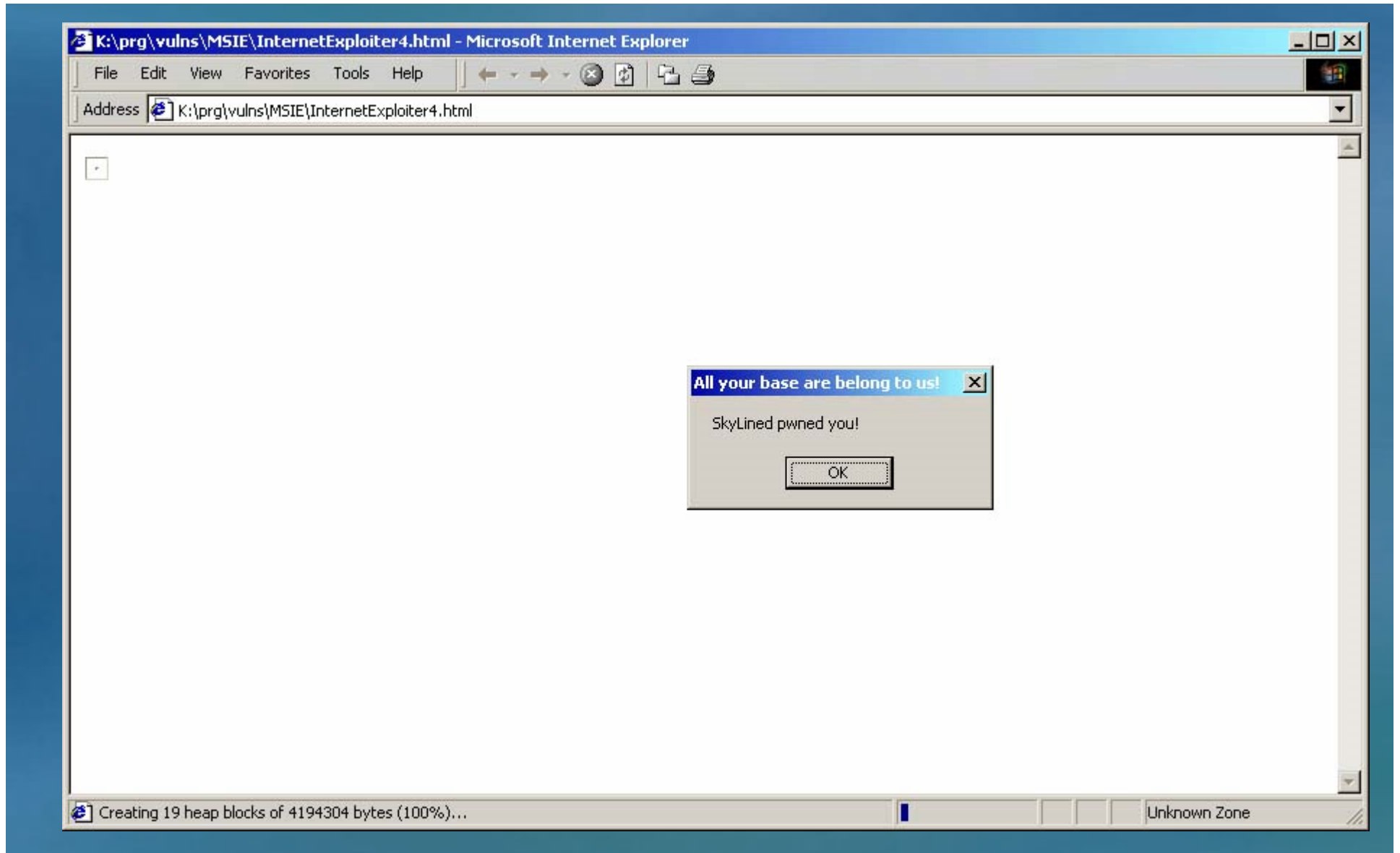
IE exploit to allow code execution (NOTE: not stable)

- Fictitious www.attack.com web site is visited
- Reverse shell (telnet) on port 28876 executes
- Runs in the user context of the currently logged on account

TOOLS/SOFTWARE

- www.microsoft.com - Internet Explorer (without the MS05-020 patch)
- www.edup.tudelft.nl/~bjwever - Internet Exploiter 2 v0.1
 - 2005-04-19 **MSIE**: Upcoming advisory - Internet Exploiter 4: a remote exploit for MSIE 0 day vulnerability

Internet Exploiter 4



Time to go learn more!

- Privilege Escalation
- Alternate Data Streams
- Hidden Rootkits
- Browser Exploitation

Contact Us

Use the TASK.TO forums!!!

On the forums as “Chris” and “Brian”.

Brian Bourne – brian@cms.ca

Christopher Diachok – christopher@cms.ca