

Windows Server 2003/XP/Vista

Security Hardening II.

Jiří Hýzler, MCT, Security MVP

OKsystem s.r.o.

29/11/07

Obsah přednášky

- I. Díl Security hardening byl věnován „Baseline security“

 - Group Policy

 - Bezpečnostní šablony

 - Administrativní šablony


 - Security Configuration Wizard

 - Další bezpečnostní nastavení

- II. Díl je především věnován online/offline bezpečnostním scannerům a analyzérům, MRSK a desktop firewallům (bude méně slidů a více ukázek)

- Závěrem bude diskuse (snad 😊)

Získávání informací

- **Jednou z kategorií útoků je krádež informace**
 - **Aktivní** (přinucení internetové služby, aby vydala více informací než má, sociální inženýrství, phishing, ...)
 - **Pasivní** (odposlech sítě / telefonu, odpozorování hesla)
- **Kde útočník získává informace**
 - WHOIS, DNS, webové stránky, diskusní skupiny, IM, ...
 - Port scanning
 - Sniffing
 - ...
- **Existuje ale mnohem jednodušší cesta  donutit k tomu uživatele !**

Otevření TCP na portu 80 == povolení jen HTTP ???



Tunneling

HTTP-Tunnel - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites Media Print Mail Wordpad Links Enter the search term Go

Address <http://www.http-tunnel.com/html/solutions/overview.asp> Go

Overview
HTTP-Tunnel Client
HTTP-Tunnel Server
HTTP-Tunnel ActiveX Control
Corporate Messenger (VCM)

HTTP-Tunnel Technology

HTTP-Tunnel technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls. This is made possible by sending data through HTTP (port 80). Additionally, HTTP-Tunnel technology is very secure, making it indispensable for both average and business communications.

The **HTTP-Tunnel Client** is an application that runs in your system tray acting as a SOCKS server, managing all data transmissions between the computer and the network.

```
graph TD; U1[Users use HTTP-Tunnel to send data through the firewall] --- R1[Router / Firewall]; U2[Users use HTTP-Tunnel to receive data through the firewall] --- R2[Router / Firewall]; R1 --- S[HTTP-Tunnel Corporate Server, receives and relays the data.]; R2 --- S;
```

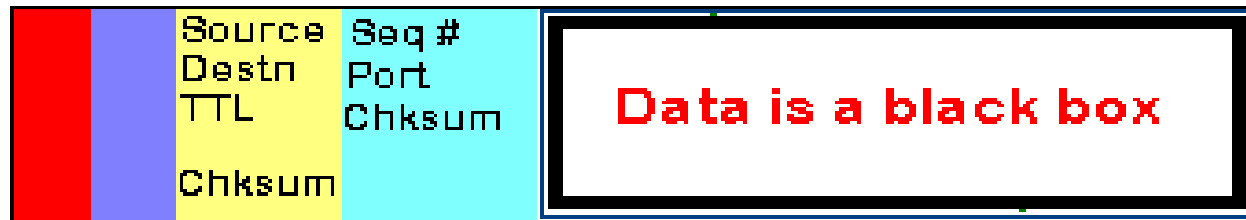
The **HTTP-Tunnel Server** is a customizable server software solution for both personal and corporate networks.

The **HTTP-Tunnel ActiveX Control** allows developers to incorporate HTTP-Tunnel technology into their software applications.

Done Internet

Proč může TCP 80 == All IP traffic ?

Physical Network

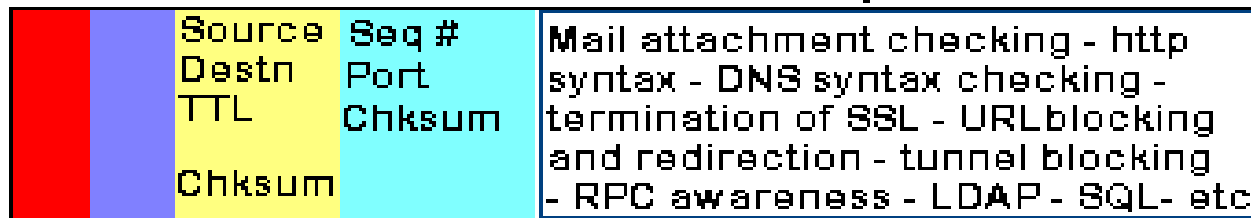


Standard
Firewall

Datalink Transport

Physical Network

Data is inspected



App
Inspection
Firewall

Datalink Transport

Co dělat, když už jste na svoje PC „něco chytli“

● Online (Live) nástroje



● <http://safety.live.com>

● **Kaspersky Online Scanner**

<http://www.kaspersky.com/kos/eng/partner/default/kavwebscan.html>

● **McAfee FreeScan**

<http://us.mcafee.com/root/mfs/default.asp?affid=294>

● **Symantec Security Check**

<http://security.norton.com/sscv6/default.asp?langid=ie&venid=sym>

● **Trend Micro HouseCall**

<http://housecall.trendmicro.com>

● **VirusTotal**

<http://www.virustotal.com/cs/>

● ...

Co dělat, když už jste na svoje PC „něco chytili“

● Offline nástroje

● Autoruns

<http://www.microsoft.com/technet/sysinternals/Security/Autoruns.mspx>

● Process Explorer

<http://www.microsoft.com/technet/sysinternals/utilities/processexplorer.mspx>

● RootKit Revealer

<http://www.microsoft.com/technet/sysinternals/Security/RootkitRevealer.mspx>

● Malicious Software Removal Tool

<http://www.microsoft.com/security/malwareremove/default.mspx>

● Sigcheck

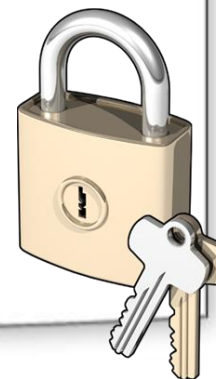
<http://www.microsoft.com/technet/sysinternals/Security/Sigcheck.mspx>

● avast! Virus Cleaner http://www.avast.com/eng/down_cleaner.html

● McAfee AVERT Stinger <http://vil.nai.com/vil/stinger/>

● Spybot – Search & Destroy

<http://www.spybot.info/en/download/index.html>



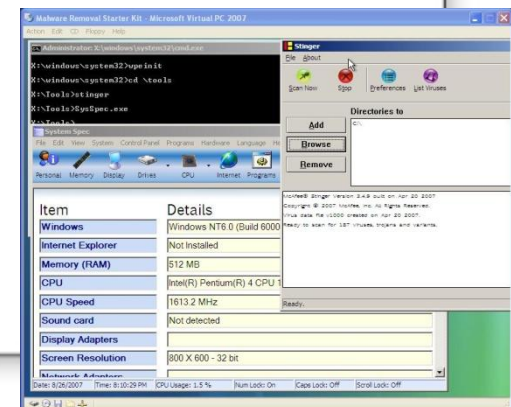
Malware Removal Starter Kit

- **Požadavky pro vytvoření CD s kitem:**

- Windows Vista, Windows XP SP2 s KB926044 nebo Windows Server 2003 SP2 (popř. SP1 s KB926044)
- DVD vypalovací mechanika a software pro vypalování .img/.iso souborů
- 992 MB volného místa na HDD pro stažení Windows PE .img souboru (Windows Automated Installation Kit) plus dalších 800 MB na vytvoření boot image pomocí skriptů kitu.
- [Microsoft .NET Framework Version 2.0](#) (instalační soubor je také součástí Windows Automated Installation Kitu)
- [Microsoft Core XML Services \(MSXML\) 6.0](#) (instalační soubor je také součástí Windows Automated Installation Kitu)

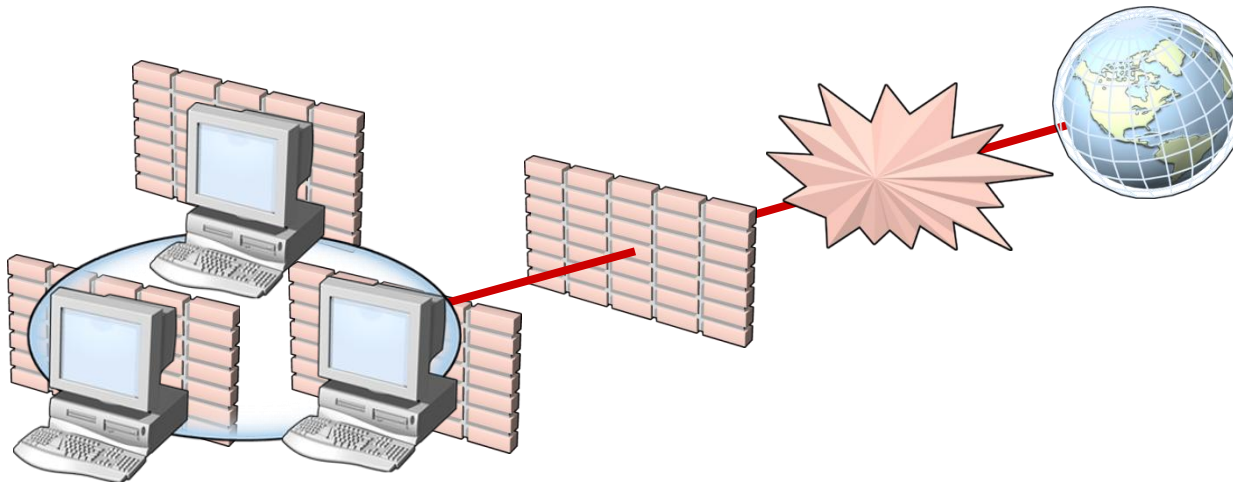
- **Více v článku:**

<http://www.microsoft.com/cze/technet/clanky/malware.mspx>



Prevence – dobrý firewall / antivir / antispypware je základ

- Microsoft Forefront Client Security: <http://www.microsoft.com/forefront/clientsecurity/default.aspx>
- Windows Defender: <http://www.microsoft.com/athome/security/spyware/software/default.aspx>
- Windows Firewall: <http://technet.microsoft.com/en-us/network/bb545423.aspx>



Odkazy

- ShieldsUP a LeakTest:
<http://www.grc.com/default.htm>
- Firehole (simulátor trojského koně):
<http://keir.net/firehole.html>
- O Rootkitech: <http://www.rootkit.com>
- Microsoft Malware Protection Center:
<http://www.microsoft.com/security/portal/default.aspx>
- Microsoft Security Home Page:
<http://www.microsoft.com/security/default.mspx>
- Windows Security Home Page:
<http://www.microsoft.com/windows/security/default.mspx>

Diskuse

- **Otázky ?**

- **Můžete se těšit na další díly:**

17.1. 2008 - **Security hardening III** – šifrování (Bitlocker, EFS, SSL, IPSec, S/MIME, ..)

Květen - **Security hardening IV** – karantény a tunely (NAP, SSTP, VPN s ISA 2006)

- **Další informace najdete na:**

<http://www.microsoft.com/cze/technet/default.msp>

<http://blogs.technet.com/technetczsk/>

<http://support.microsoft.com/newsgroups/>

Školení 2823: Implementace a administrace ve Windows Server 2003 síti



OKsystem

Microsoft
Small Business
Specialist

Microsoft
GOLD CERTIFIED
Partner

Learning Solutions
Networking Infrastructure Solutions