secunet

Automated Information Collection in Windows NT Networks

Dirk Reimers

reimers@secunet.de

Overview

- Motivation
- Collecting information with automated tools
  - CASTInG NT
- Technical background
- Example data
- Questions & answers

Motivation

- Obtain as much information from “large scale“ NT networks as possible
  - user account information
  - host information
- Automatically generate nicely formatted reports
- Do it all for free!

Collection information

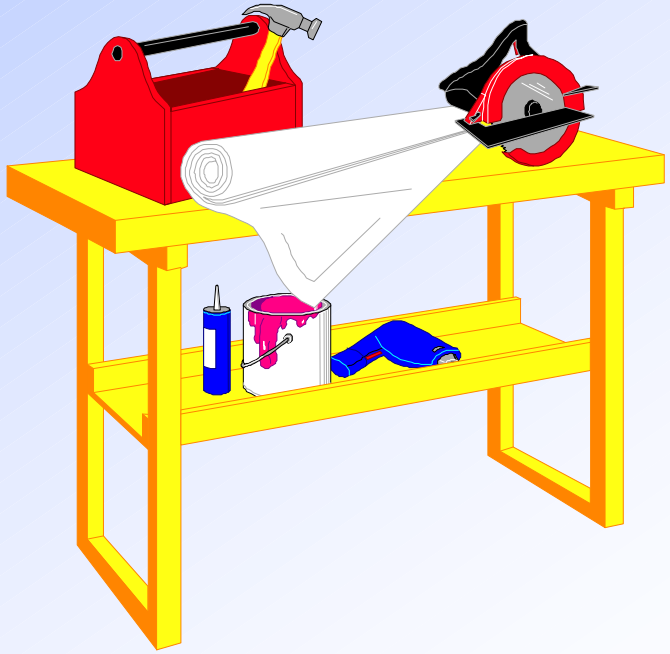
- Many tools available for Uni* systems
- Most Windows NT specific tools are commercial
  - ISS
  - NetSonar
  - etc.

Overview

- Motivation
- Collecting information with automated tools
  - CASTInG NT
- Technical background
- Example data
- Questions & answers

CASTInG NT

- **C**ollection of **A**utomated **S**cripts and **T**ools for **In**formation **G**athering within Windows **NT** networks



secunet

CASTInG NT (1)

- Minimal user interaction
- Report details information on
  - user accounts
  - hosts in a domain
  - common security threats
- Automatic generation of (Excel) reports
- Automatic conversion for WinWord documents

CASTInG NT (2)

- Implemented with VB-Script and VBCCE 5.0
- Collection of
  - VB-scripts
  - some ActiveX components
  - free libraries
  - free availiable tools
  - Excel VBA-macroes
- Different modules depending on access level

Overview

- Motivation
- Collecting information with automated tools
  - CASTInG NT
- Technical background
- Example data
- Questions & answers

Getting technical...

- Framework
  - Windows Scripting Host
  - VB-Script
  - VBCCE
- Components
  - Built in Windows NT tools
  - ActiveX components
  - Other components, e.g. executables

Windows Scripting Host (1)

- WSH included in
  - Windows 98
  - Windows NT 4.0 with Option Pack 4
  - Internet Explorer 5.0
- URL

  http://www.microsoft.com/scripting/

Windows Scripting Host (2)

- WSH controls ActiveX scripting engines
  - VB-Script
  - JavaScript
  - Perl
  - REXX
  - etc.
- Starts up as GUI or via shell command

Windows Scripting Host (3)

- Predefined objects for
  - filesystem handling
  - networking
  - object linking and embedding (OLE)
  - even Microsoft Agents ;-)
  - and much, much, more ...

VB-Script 5.0

- **Subset of Visual Basic 5.0**
- **complete programming language**
  - **subs and functions**
  - **variables, constants, arrays, types**
  - **conditional structures**
    - if..then..else
    - while..wend
    - select..case

VBCCE 5.0

- Visual Basic Control Creation Edition
- URL
  - http://www.microsoft.com/
- Complete Environment for builing ActiveX objects
  - .OCX files
- Subset of Visual Basic 5.0
  - but superset of VB-Script

Built in Windows NT tools (1)

- `net` command
  - `net view /domain` ➲ all availabe domains
  - `net use` ➲ check for weak admin passwords
- `ping` command
  - `ping reimers -n 1` ➲ get computer‘s IP-address

Built in Windows NT tools (2)

- **`nbtstat` command**
  - **`nbtstat -a`**
    - ➲ get MAC-address
    - ➲ get current user
    - ➲ get computer type

ActiveX components (1)

- Active Directory Services Interface (ADSI)
  - access to user attributes
  - http://cwashington.netreach.net/downloads/files/adsiNT.zip
- ASPPing
  - using ping from within a VB-Script or ActiveX component
  - http://cwashington.netreach.net/downloads/ocx_controls/dsping.zip

ActiveX components (2)

- DajntADM
  - retrieves type of a computer
  - http://cwashington.netreach.net/downloads/ocx_controls/dajntadm.zip
- WSH LiteWeight Forms
  - building your own dialogboxes
  - http://cwashington.netreach.net/downloads/ocx_controls/wshLWform.zip

Other tools (1)

- **`dumpacl`**
  - **dumps permissions and audit settings for**
    - file system
    - registry
    - printers
    - shares
  - **http://www.systemtools.com/somarsoft/**
- **`user2sid`**
  - **getting SID for a known username**

Other tools (2)

- **NbtDump**
  - dumps NetBIOS information from Windows NT, Windows 2000 and *NIX Samba servers
    - shares
    - user accounts with comments
  - without an useraccount !
  - http://www.cerberus-infosec.co.uk/nbtdump.exe

Other tools (3)

- **Rpcdump**
  - dumps SUN RPC information
  - http://www.cerberus-infosec.co.uk/rpcdump.exe
- **Cerberus WebScan**
  - find known web server security issues
  - http://www.cerberus-infosec.co.uk/webscan.exe

Other tools (4)

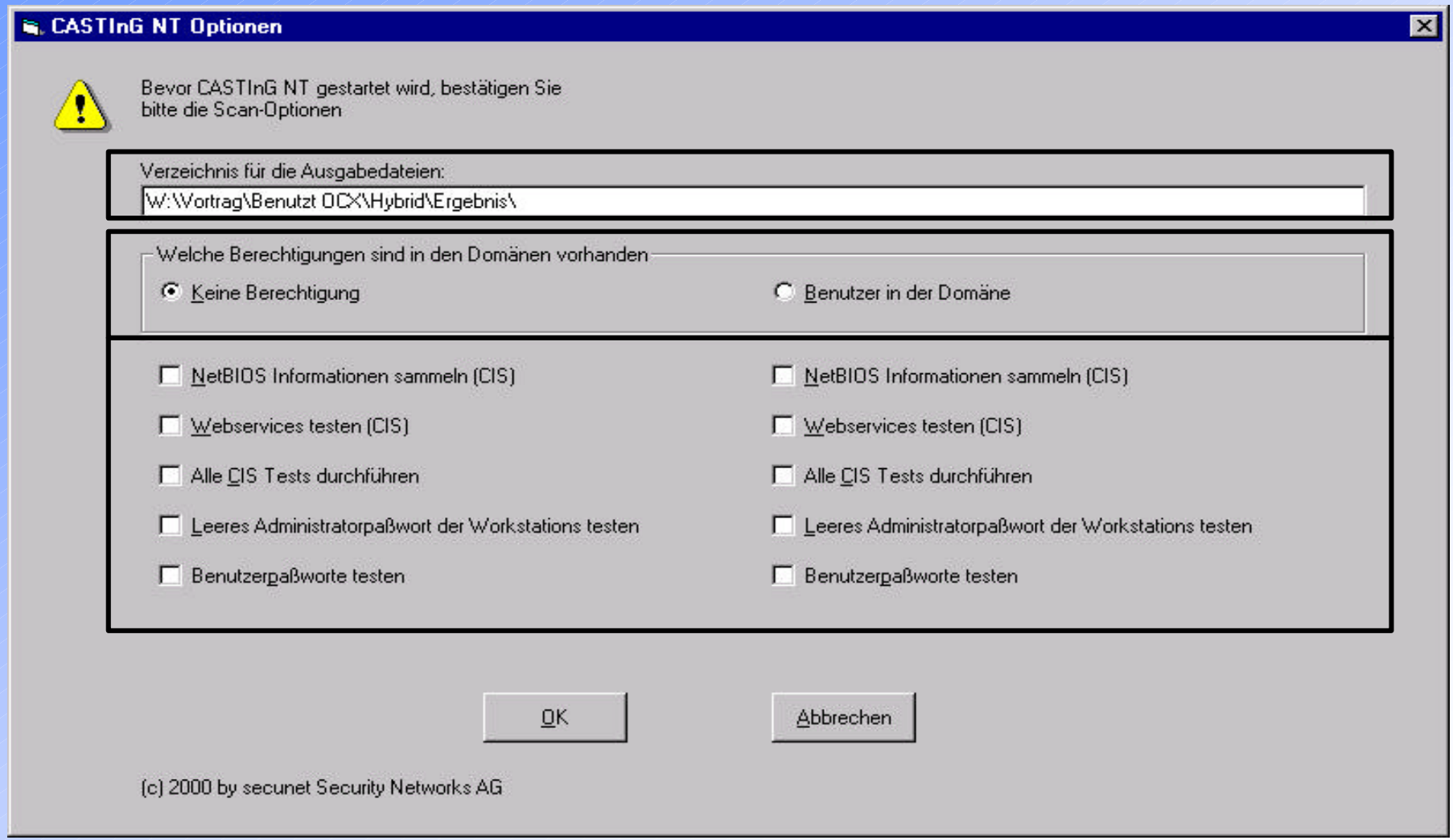
- `winfo`
  - retrieves a list of user accounts, workstation trust accounts, interdomain trust accounts, server trust accounts, and shares, from Windows NT.
  - shows all hidden shares.
  - http://ntsecurity.nu/toolbox/winfo/

Overview

- Motivation
- Information gathering with automated tools
  - CASTInG NT
- Technical background
- Demo data
- Questions & answers

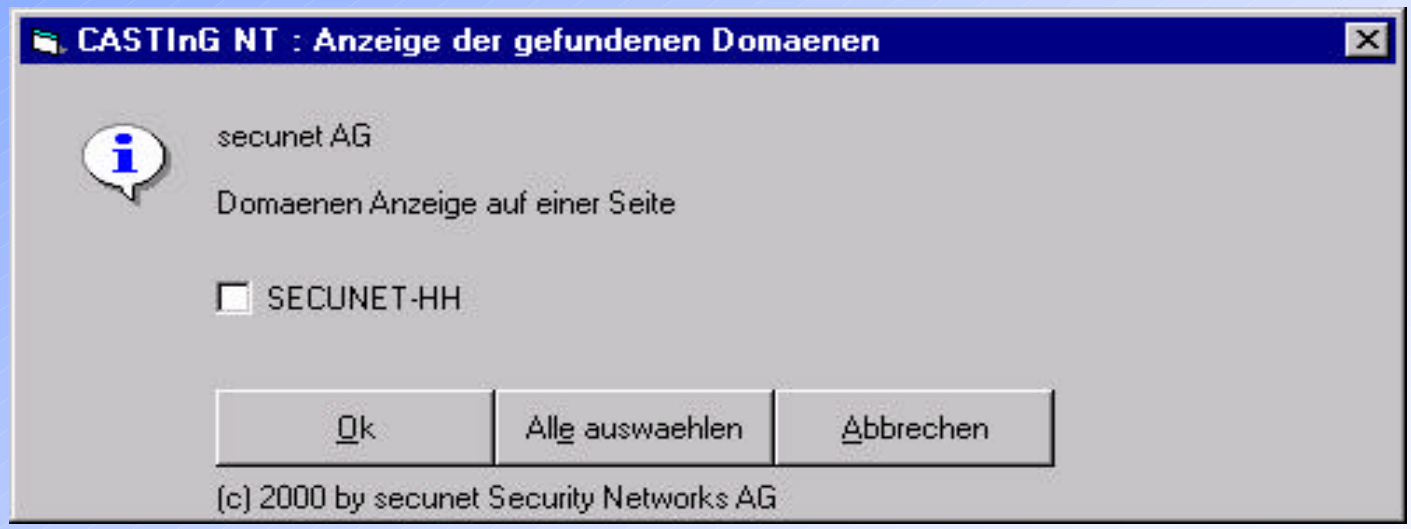
secunet

Select scan options



secunet

Select domains to be scanned



secunet

Some exemplary results: (1)
Users

Name	Realer Name	Kommentar	Gruppe	Pw Alter	Pw erloschen
Administrator		Built-in account for administering the computer/domain	513	93	Nein
Benutzer1		Benutzer mit Zugriff auf XY-Daten	513	0	Ja
Benutzer2			513	0	Ja
bethke	Sascha Bethke		513	30	Nein
Guest		Built-in account for guest access to the computer/domain	514	0	Nein
Herrmann	Dennis Herrmann	Praktikant	1035	4	Nein

secunet

Some exemplary results: (2)
Users

Gruppen	Flags
(Domain Admins) (Domain Users) (NSG) (Replica Backup)	S-1-5-21-1389432826-159778891-569397357-500
(Domain Users)	S-1-5-21-1389432826-159778891-569397357-1018
(Domain Users)	S-1-5-21-1389432826-159778891-569397357-1019
(Domain Users) (NSG) (secunet Hamburg)	S-1-5-21-1389432826-159778891-569397357-1023
(Domain Guests)	S-1-5-21-1389432826-159778891-569397357-501
(Domain Users) (secunet Hamburg)	Account has no flags set. User is active

secunet

Some exemplary results: (3)
Users

PW endet	falsche Pw	Letzter Login	Letzer Logout	AutoUnlock
23.09.99 08:35:04	0	12.11.99 13:38	12.11.99 13:38	1800
25.12.99 12:05:10	0	07.04.99 10:20	07.04.99 10:22	1800
25.12.99 12:05:10	0	07.04.99 10:22	07.04.99 10:20	1800
25.11.99 09:07:18	0	11.11.99 17:44	11.11.99 18:40	1800
25.12.99 12:05:11	0	niemals	niemals	1800
21.12.99 09:53:51	0	28.11.99 01:00	12.11.99 09:31	09.11.99 10:32:43

secunet

Some exemplary results: (4) Computers

XX-HH001	nicht erreichbar	nicht erreichbar	nicht erreichbar
XX-HH002	00-00-00-00-00-00	Mitarbeiter 1	Workstation
XX-HH003	nicht erreichbar	nicht erreichbar	nicht erreichbar
XX-HH004	00-00-00-00-00-00	Mitarbeiter 2	Workstation
XX-HH005	nicht erreichbar	nicht erreichbar	nicht erreichbar
XX-HH006	Host nicht gefunden	Host nicht gefunden	Error
XX-HH007	nicht erreichbar	nicht erreichbar	nicht erreichbar
XX-HH009	nicht erreichbar	nicht erreichbar	nicht erreichbar
XX-HH010	00-00-00-00-00-00	ADMINISTRATOR	Workstation
XX-HH012	Host nicht gefunden	Host nicht gefunden	Error
XX-HH013	Host nicht gefunden	Host nicht gefunden	Error

Some exemplary results: (5)
Shares

Share	lokales Verzeichnis	berechtigte Benutzer	Rechte
Share 1	C:\client (disktree)	Jeder	read
Share 1	C:\client (disktree)	Administratoren	all
Share 2	C:\eingang (disktree)	Jeder	all
Share 3	C:\gäste (disktree)	Jeder	read
Share 3	C:\gäste (disktree)	Benutzer 1	all
Share 3	C:\gäste (disktree)	Benutzer 2	read

secunet

Analysis of passwords

Paßwortalter (alle Accounts) :	
weniger als 30 Tage	10
zwischen 30 und 60 Tage	3
zwischen 60 und 90 Tage	1
zwischen 90 Tagen und 1/2 Jahr	1
zwischen 1/2 und 1 Jahr	1
mehr als 1 Jahr	1
Durchschnittliches Paßwortalter	36,125

Paßwortalter (aktive Accounts) :	
weniger als 30 Tage	6
zwischen 30 und 60 Tage	3
zwischen 60 und 90 Tage	0
zwischen 90 Tagen und 1/2 Jahr	1
zwischen 1/2 und 1 Jahr	0
mehr als 1 Jahr	0
Durchschnittliches Paßwortalter	23,7

secunet

Questions & Answers

Speaker

Dirk Reimers, Dipl.-Inform.
IT-Security Consultant

secunet
Security Networks AG
Osterbekstr. 90b
22083 Hamburg

Tel.: +49-40-696599-11
Fax: +49-40-696599-29
E-Mail: reimers@secunet.de
URL: www.secunet.de