

()

... ..
.
...
... ..

:

-
-
-
-
-
-
-
-

ISP

.

.

.

.

.

.

.



:

-

.

.

.

:

-

.

.

.

:

-

-

-

.

:

-

..

:

-

-

-
-

.

-

:

" " " "

-
-

-

:

-
-

:

-
-
-
-

Aims :

-

:

:

-

Auto Hide

" "

:

Start

-

Setting

Taskbar

-

"

"

-

OK

"

"

-

:

-

:

Read Only

-

-

" Reading Only

"

"

"

-

OK

-

Ctrl

Propereties

:

-

Help

:

Control Panle "

"

"

"

-

"Display "

"

Screen Saver

-

"

"

"

:

BIOS

:

CMOS

CTRL

F10

DEL

CMOS

Security

. Password

Options

...

Screen Luck

Screen Luck

:
www.shareware.com
WinZip

Option " Password

:

:

:

-

-

-

()

-

Compressed Folder

Tools

-

My Document

-

Folder Compressed

New

-

Enter

-

()

-

Encrypt

-

OK

()

-
-
-

aims.cjb.net :

Aims.net

:

-
-
-
-
-

Aims :

"

:

"

"

"

:()

"

"

...

Resume.doc

CV

: ...

"

"

Resume.doc

Game.doc Oldfile.doc

Budget.xls

Calendar.xls

doc

:

DLL

Rename

()

Enter

:

WINDOWS/SYSTEM/

:

" "

:

Hidden

OK

.

:

:

-

C

-

-

:

"

"

.

-

-

"

"

-

-

-

-

-

-

Encryption

-

(

m r
bit

bit

bit

bit

bit

bit

bit

ASCII

MIME, UUENCODE

Decryption, Uncryption

Decryption

Encryption

Pretty

[/http://aims.cjb.net](http://aims.cjb.net)

Aims.net

Good Privacy PGP

(

Zip

Aims.net

:
Norton Utilities 2000
Windows Washer
Remove-It

(

...

Port Scanning
Ports

Server

.

...

)

(

PWL

PWL

Ice Defender Black

WAPS

PWL

Aims.net

(

temp

windowstemp

;temp,.htm. ,doc. :

Aims :

-

.

.

.

.

:

-

:

-

-

-

-

:

:

:

-

-

-

:

-

Aims.net

[/http://aims.cjb.net](http://aims.cjb.net)

Setup

/http://aims.cjb.net Aims.net)

.(

:

-

)

(/http://aims.cjb.net Aims.net

:

-

:

Scanning
Setup

Aims.net

History

Aims.net

:

-

" "

" "

packets

packet-sinffing

:Spam

:

" "

"

"

:

:AOL

-

AOL

AOL

AOL

AOL

Personal Filing Cabinet

AOL

AOL

Preferences

My AOL

Password

Personal Filing Cabinet

Good

Times

Fares.net Aims.net

Aims.net

aims :

()

:

() (-)

() II

..

.

...

.

.

"

"

"

"

.

.

.

()

() II

Aims :

NT
pcAnywhere
NetBIOS

NetBIOS

host

FScan

NT

Ping
FScan

FScan

NetBIOS

FScan

pcAnywhere

telent
webping.pl

MDAC
Adminstartor

.pcAnywhere

John the
cif
ShoWin

cif/s *dir
TFTP

Pwdump
Ripper

pcAnywhere use-from-work

pcAnywhere
TFTP

Pulist.exe NT

kill.exe NTRK

PID

.NT kill

Aims Was Here

WinVNC

pcAnywehre

WinVNC

Kill Pulist

WinVAC

MDAC

MDAC

Pwdump Netcat

Rain Forest Puppy

MDAC

() II

Aims :

:

-

-

.

.

.

.

.

()

:

- Traceroute -
- Scanning -
- Enumeration -

Traceroute

-

IP

Remote

: Traceroute

(

:

-

-

-

IP

-

TCP

-

-

(snmp

)

-

(

(DecNET IPX IP

)

-

-

-

TCP/UDP

IP

-

-

-

-

)
(SNMP -

(
-
-
-
(
-
-
-
(

()

()

()

)

(

(

:

-

-

-

-

-

-

HTML

Wget

teleport UNIX ((ftp://gnkilux.ce.fer.hr/pub/unix/util/wget
http://www.tenmax.com/teleport/home.htm Pro

www.finance.yahoo.com

www.companysleuth.com

FerretPRO

www.ferretsoft.com

(

whois

/http://www.allwhois.com

whois

whois

IP

POC :

DNS

DNS

DNS

IP

DNS

.Zone Transfer

DNS

DNS

IP

IP

)

(

Intranet

Scanning (

()

whois

IP

DNS

IP

.scanning

ping

TCP (

ack, syn/ack, syn

tcp

tcp/syn (

syn

FIN

TCP FIN (

push, urg, fin

tcp xmas tree (

tcp null (

TCP Windows (

tcp

UNIX

TCP RCP (

RPC

TCP ACK (

SecureXpert
Telent DOS (

/http://www.securexpert.com
Microsoft Telent Service

NetBIOS DOS (

/http://www.nai.com COVERT
NetBIOS

NetBIOS Name Service
NetBIOS

NetBIOS

ping (

t ping

SuprScan (

http://keir.net/software.html

IP TCP

IP Scan

WinScan (

/http://www.prosolve.com

TCP

Class C

WUPS (

ups

/http://ntsecurity.nu

Pinger (

ftp://ftp.technotronic.com/rhino9- :

products/pinger.zip

ZdNet (

/http://www.zd.net ZdNet

portscan

http://www.zdnet.com/downloads/stories/info/0,,68981,.html .

:

TCP

Scanning

. ICMP

)

(

:

Enumeration

(

Enumeration (

:
(
(
(

. ()

(

NT

TCP/IP NetBIO
net view
. NT
nbtscan nbtstat

NT (

NT

- -

NetBIOS

NT

(

Enter

telnet

() II

[/http://www.aims.cjb.net](http://www.aims.cjb.net) Aims on Line

Aims :

:

:

"

...

"

"

"

.

() II

.

.

Aims :

()

:

-

()

:

:

<http://download.cnet.com/downloads/0-10106-108-63806.html?bt.37419.10014..dl-63806>

START

CHECK

t=onlinecheck&http://www.anti-trojan.net/at.asp?l=en

:

()

Aims :

on-line

()

ports

Read me

- ()

Hack Tracer
Black-ICE Defender

Aims :

:

Hack Tracer :

[/http://www.sharptechnology.com/hacktracer/demo-trial/demo](http://www.sharptechnology.com/hacktracer/demo-trial/demo)

: Hack Tracer

tool. It blocks Hack Tracer is an intrusion detection and prevention trace unwanted traffic, logs the contact, and allows you to easily the potential hacker back to the source. Hack Tracer also gives to a user community working together to defend itself you access .potential threats from hackers and other

Hack .Using Hack Tracer is very simple. You install it and go Tracer will block any unwanted traffic from reaching your system. lesser protection systems and 'evil port monitors' Hack Unlike only detect the traffic but also track it back to Tracer is able to not connections are destroyed before they get it's source. Unwanted total protection for you and to the Windows tcp/ip stack, meaning .internet 'stealth' mode when you are connected to the

Hack Tracer

Hack Tracer

Hack Tracer

.
:
<http://www.sharptechnology.com/bh-cons.htm>

:
Black-ICE Defender

Aims :

:

BlackICE Defender :

BlackICE Defender

" "

BlackICE Defender

BlackICE

ICE

Black

server

(

) client

Trojans

LAN

DSL

. dial-up

:

BlackICE Defender

:

:

. stealth

Intrusion Detection System

()

PC

:

:

www.networkice.com

:

:

[/http://www.ajeel.com](http://www.ajeel.com)

<http://www.cimos.com/TradNet.htm>

http://www.networkice.com/downloads/blackice_defender_exe.html
http://www.networkice.com/docs/BI_Defender_29_User_Guide.pdf
<http://www.networkice.com/products/firewalls.html>
http://www.networkice.com/products/networkice_guide.html
http://www.networkice.com/products/blackice_defender.html
http://www.networkice.com/products/blackice_agent.html

: " " ()
 BlackICE Defender
 : (

Tracking Down Intruders: Back Tracing
 connection back to Back tracing is the process of tracing a network its origin. When somebody connects to your computer via a network such as the Internet, your system and the intruder.s packets. Before an intruder.s packets reach your system exchange several routers. BlackICE can system they travel through and identify automatically read information from these packets ,each router the intruder.s packets traveled through. Eventually BlackICE can .hop. all the way back to the intruder.s system. trace information indirectly or directly. ! An BlackICE can back that do not make contact with the indirect trace uses protocols

indirectly from other intruder.s system, but collect information back sources along the path to the intruder.s system. Indirect tracing does not make contact with the intruder.s system, and does not acquire much information. Indirect traces are therefore lower-severity attacks. ! A direct trace goes all the best suited for system to collect information. Direct way back to the intruder.s intruder.s system and back tracing makes contact with the traces are therefore can acquire a lot of information. Direct back best for high- severity attacks, when you want as much about the intruder as possible. Intruders cannot detect information However, they can detect and block a direct .an indirect trace are not experienced enough to trace. Fortunately, most intruders to set the block direct traces. The Back Trace tab allows you threshold when an indirect or direct back trace is set off. The severity of the incoming event, not the address of the intruder, back trace. BlackICE shows all the back tracing triggers the about the intruder next to the Intruder information it has collected intruder it attempts to gather List. When BlackICE back traces an Name, Group the IP address, DNS name, NetBIOS name, Node name and MAC address. Savvy intruders will likely block BlackICE from acquiring this information. Back trace information is also standard text files in the Hosts folder in the directory stored in installed. Each file is prefixed with the intruder.s where BlackICE is .IP address

: Defender BlackICE

BlackICE Defender

:

about To control when and how BlackICE looks for information :intruders, follow these steps

Tools, then From the BlackICE Local Console Menu Bar, select .

.Edit BlackICE Settings

.window Select the Back Trace tab in the BlackICE Settings .

about Figure 32. Use the Back Trace tab to gather information .intruders

numeric In the Indirect Trace Threshold text box, type the . severity level at which BlackICE should initiate an indirect back

The default threshold for an indirect trace is 3. With this .trace with a severity of 3 or above triggers an indirect setting, any event explanation of the BlackICE severity levels, see back trace. For an .an Intrusion. on page 38 .Understanding the Severity of Select DNS Lookup to have BlackICE query Domain Name . Service servers for trace. DNS information about the intruder as part of an indirect .Lookup is enabled by default numeric In the Direct Trace Threshold text box, type the . severity level at which BlackICE should launch a direct trace. The default event severity for the direct trace threshold is 6. With this any event with a severity of 6 or above triggers a direct ,setting .back trace the Select NetBIOS nodestatus to have BlackICE find out . machine address of the intruder.s computer using a NetBIOS intruder.s system. NetBIOS Node Status is enabled lookup on the .by default

:
<http://www.networkice.com/press/awards.html>

Aims :
aims@mail2www.com

...

.

.

.

:

**Trojan
Server**

Client

.

.

Anti-Trojan Ad-Aware
:
t=onlinecheck&http://www.anti-trojan.net/at.asp?l=en

Aims
aimsonline@msn.com