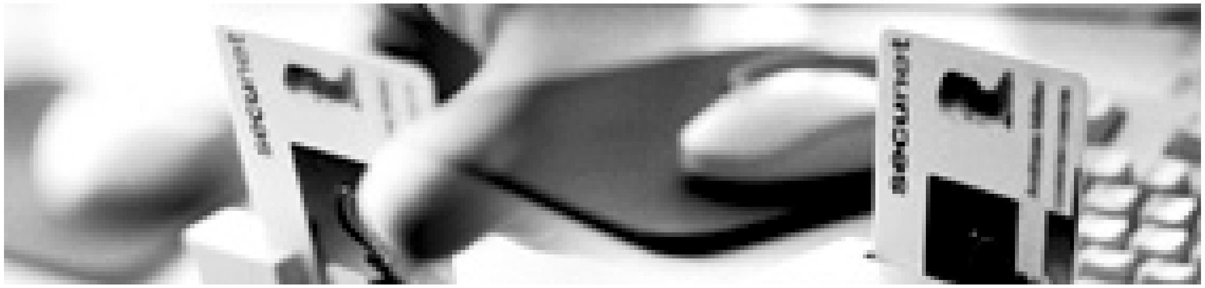
secunet



Stand and deliver
Essential Secutity Testing Tools

Nils Magnus

FIRST Technical Colloquium 2003
Uppsala, Sweden, February 10 - 11, 2003

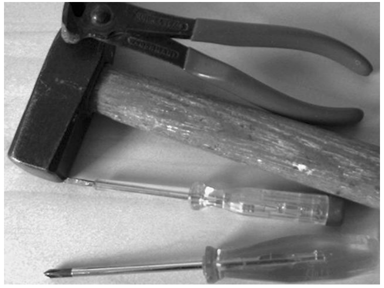
secunet Security Networks AG
The Trust Company

Overview and Motivation

- Incident handling is also Incident prevention
- Assessing your constituency‘s security status may be helpful
- Original motivation: Clients bugging me about „number of tools“
- Quite a lot security testing can be done with plain Unix tools
- There are other „schools“: Cisco/netflow, Windows/scanners

- Part 1: Introduction
- Part 2: Top 10 attacking tools
- (Part 3: Defending against most serious threats)
- Part 4: Discussion about your favourite tools

Hypothesis



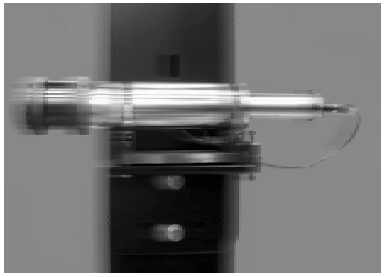
- Imagine you are going to Desert Island and you are allowed only

10 penetration testing tools

- My hypothesis: That´s all you need

- Presentation of my favorite TOP 10 tools
- What they do, how they work, where to get them, what they obsolete ...
- Discussion about your own favourites

Tool 1: nmap

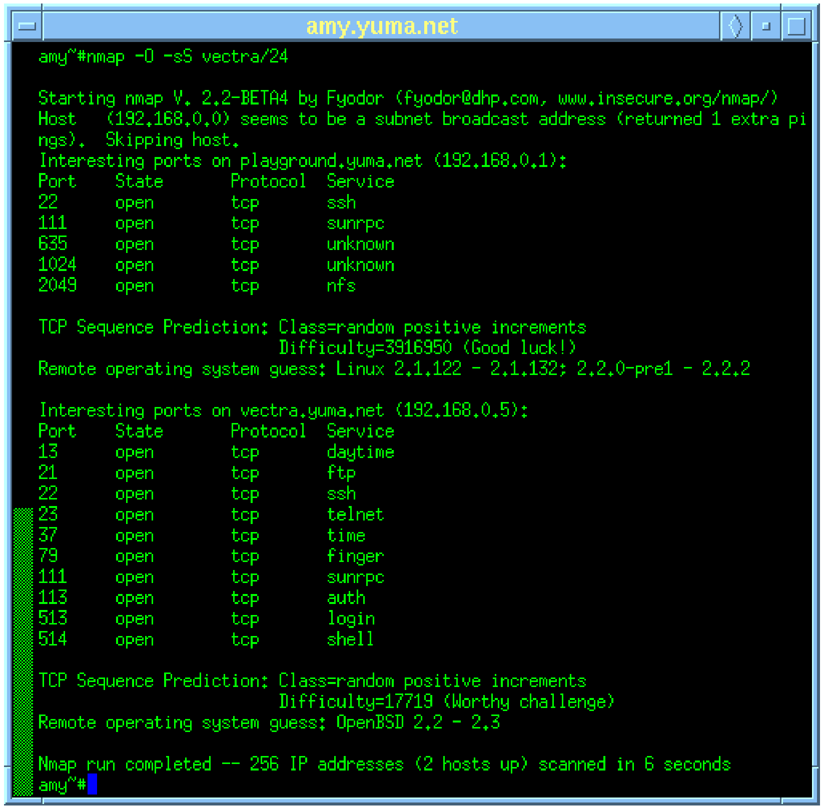


- The network mapper and scanner, OS detection
- written by Fyodor
- latest version: 2.54 beta 33 as of 28/04/2002
- Homepage: http://www.insecure.org/nmap/
- Typical use:

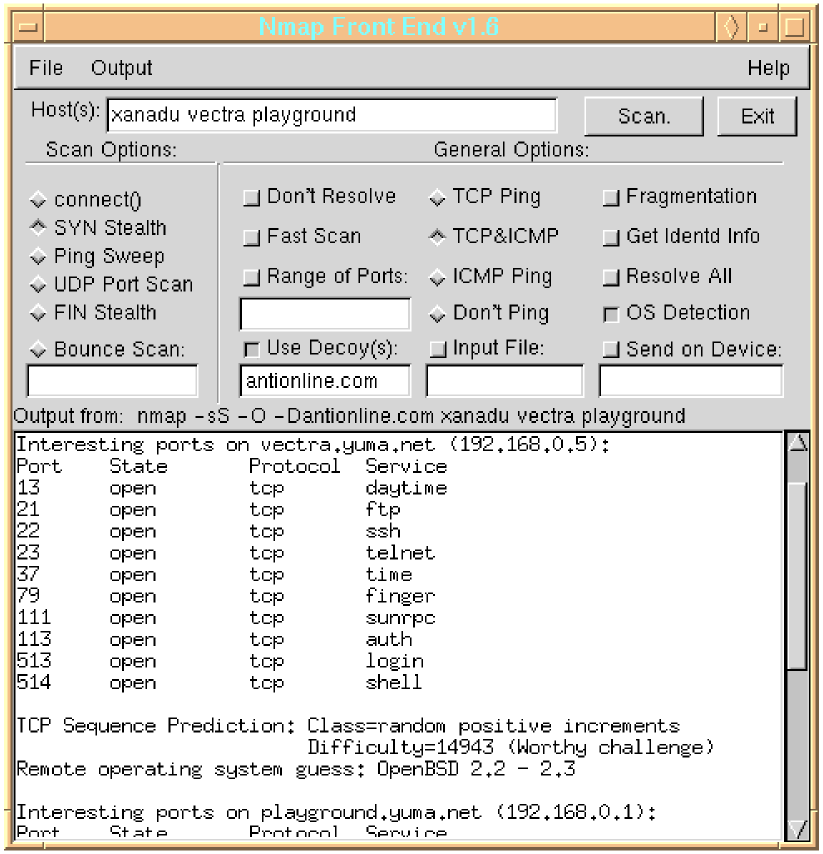
```
# nmap -v -sT -p80,139 -P0 \
       -o scan.txt -m scan.dat 192.168.13.192/29
```

- obsoletes: cheops, ftp-scanner, bind-scanner, webscanner, (sing), ...

nmap



```
amy^#nmap -O -sS vectra/24

Starting nmap V. 2.2-BETA4 by Fyodor (fyodor@dhp.com, www.insecure.org/nmap/)
Host   (192.168.0.0) seems to be a subnet broadcast address (returned 1 extra pi
ngs).  Skipping host.
Interesting ports on playground.yuma.net (192.168.0.1):
Port    State       Protocol  Service
22      open        tcp       ssh
111     open        tcp       sunrpc
635     open        tcp       unknown
1024    open        tcp       unknown
2049    open        tcp       nfs

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=3916950 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.1.132; 2.2.0-pre1 - 2.2.2

Interesting ports on vectra.yuma.net (192.168.0.5):
Port    State       Protocol  Service
13      open        tcp       daytime
21      open        tcp       ftp
22      open        tcp       ssh
23      open        tcp       telnet
37      open        tcp       time
79      open        tcp       finger
111     open        tcp       sunrpc
113     open        tcp       auth
513     open        tcp       login
514     open        tcp       shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=17719 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Nmap run completed -- 256 IP addresses (2 hosts up) scanned in 6 seconds
amy^#
```



Host(s): xanadu vectra playground

Scan Options:

- ◇ connect()
- ◆ SYN Stealth
- ◇ Ping Sweep
- ◇ UDP Port Scan
- ◇ FIN Stealth
- ◇ Bounce Scan:

General Options:

- □ Don't Resolve
- □ Fast Scan
- □ Range of Ports:
- ☑ Use Decoy(s): antionline.com
- ◇ TCP Ping
- ◆ TCP&ICMP
- ◇ ICMP Ping
- ◇ Don't Ping
- □ Input File:
- □ Fragmentation
- □ Get Identd Info
- □ Resolve All
- ☑ OS Detection
- □ Send on Device:

Output from: nmap -sS -O -Dantionline.com xanadu vectra playground

```
Interesting ports on vectra.yuma.net (192.168.0.5):
Port     State       Protocol  Service
13       open        tcp       daytime
21       open        tcp       ftp
22       open        tcp       ssh
23       open        tcp       telnet
37       open        tcp       time
79       open        tcp       finger
111      open        tcp       sunrpc
113      open        tcp       auth
513      open        tcp       login
514      open        tcp       shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net (192.168.0.1):
Port     State       Protocol  Service
```

Tool 2: dig (or host)

Tells you all about DNS entries. Query hosts and bind versions. Date of installation. Zone transfers. Is an improvement of nslookup which is unusable.	
written by	ISC Internet Software Consortium
latest version:	bundeled with bind
Homepage:	http://www.isc.org/products/BIND/
Typical use:	

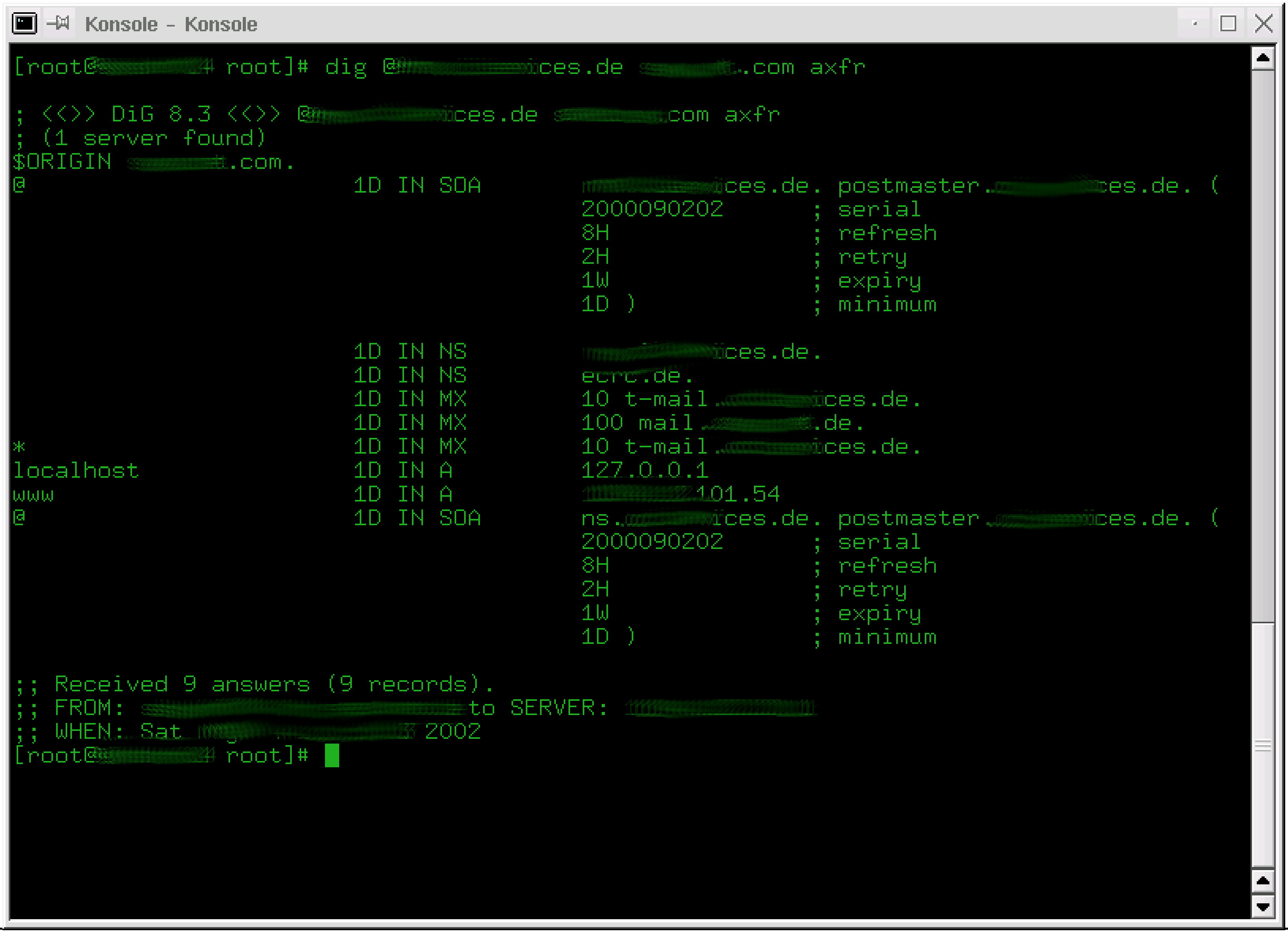
```
# dig @131.246.9.116 linuxtag.org axfr
```

- obsoletes: host, nslookup, dnsscan

secunet

dig

Getting a DNS zone



```
[root@[redacted] root]# dig @[redacted]ices.de [redacted].com axfr

; <<>> DiG 8.3 <<>> @[redacted]ices.de [redacted]com axfr
; (1 server found)
$ORIGIN [redacted].com.
@                       1D IN SOA       [redacted]ices.de. postmaster.[redacted]es.de. (
                                        2000090202      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

                        1D IN NS        [redacted]ices.de.
                        1D IN NS        ecrc.de.
                        1D IN MX        10 t-mail.[redacted]ices.de.
                        1D IN MX        100 mail.[redacted].de.
*                       1D IN MX        10 t-mail.[redacted]ices.de.
localhost               1D IN A         127.0.0.1
www                     1D IN A         [redacted]101.54
@                       1D IN SOA       ns.[redacted]ices.de. postmaster.[redacted]ces.de. (
                                        2000090202      ; serial
                                        8H              ; refresh
                                        2H              ; retry
                                        1W              ; expiry
                                        1D )            ; minimum

;; Received 9 answers (9 records).
;; FROM: [redacted] to SERVER: [redacted]
;; WHEN: Sat [redacted] 2002
[root@[redacted] root]# 
```

Tool 3: netcat

- Multipurpose tcp stream sender and receiver. Programmable „telnet“. Bannergrabbing. Generic server.
- written by Hobbit of @stake
- latest version: 1.10 as of 20/03/1996
- Homepage: http://www.atstake.com/research/tools/
- Typical use:

```
# (echo HEAD / HTTP/1.0; echo) | \
       netcat www.linuxtag.org 80
```

- obsoletes: telnet, web browsers, ...

Tool 4: whisker

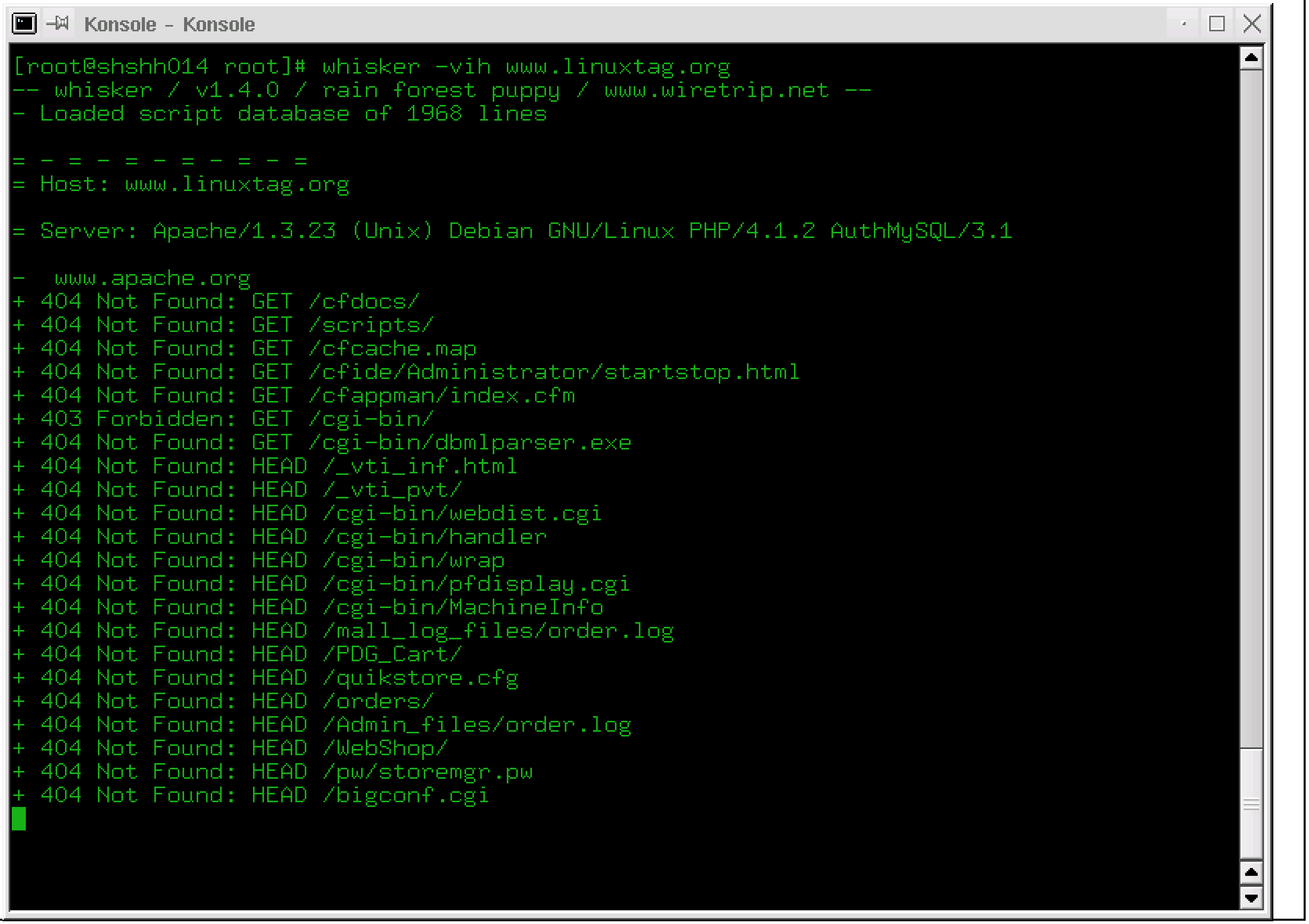
- Convenience tool to detect common vulnerabilities of web servers. Nice database of built-in patterns. Sensible scanning instead of brute force trial.
- written by Rain Forest Puppy
- latest version: 1.4 as of 03/08/2001
- Homepage: http://www.wiretrip.net/rfp/
- Typical use:

```
# whisker -vih www.linuxtag.org
```

- obsoletes: web browsers, specific scanner

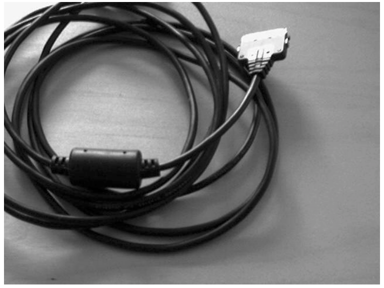
whisker

Scan web servers



```
[root@shshh014 root]# whisker -vih www.linuxtag.org
-- whisker / v1.4.0 / rain forest puppy / www.wiretrip.net --
- Loaded script database of 1968 lines

= - = - = - = - = - =
= Host: www.linuxtag.org

= Server: Apache/1.3.23 (Unix) Debian GNU/Linux PHP/4.1.2 AuthMySQL/3.1

-  www.apache.org
+ 404 Not Found: GET /cfdocs/
+ 404 Not Found: GET /scripts/
+ 404 Not Found: GET /cfcache.map
+ 404 Not Found: GET /cfide/Administrator/startstop.html
+ 404 Not Found: GET /cfappman/index.cfm
+ 403 Forbidden: GET /cgi-bin/
+ 404 Not Found: GET /cgi-bin/dbmlparser.exe
+ 404 Not Found: HEAD /_vti_inf.html
+ 404 Not Found: HEAD /_vti_pvt/
+ 404 Not Found: HEAD /cgi-bin/webdist.cgi
+ 404 Not Found: HEAD /cgi-bin/handler
+ 404 Not Found: HEAD /cgi-bin/wrap
+ 404 Not Found: HEAD /cgi-bin/pfdisplay.cgi
+ 404 Not Found: HEAD /cgi-bin/MachineInfo
+ 404 Not Found: HEAD /mall_log_files/order.log
+ 404 Not Found: HEAD /PDG_Cart/
+ 404 Not Found: HEAD /quikstore.cfg
+ 404 Not Found: HEAD /orders/
+ 404 Not Found: HEAD /Admin_files/order.log
+ 404 Not Found: HEAD /WebShop/
+ 404 Not Found: HEAD /pw/storemgr.pw
+ 404 Not Found: HEAD /bigconf.cgi
```

Tool 5: Ethereal (with tcpdump)

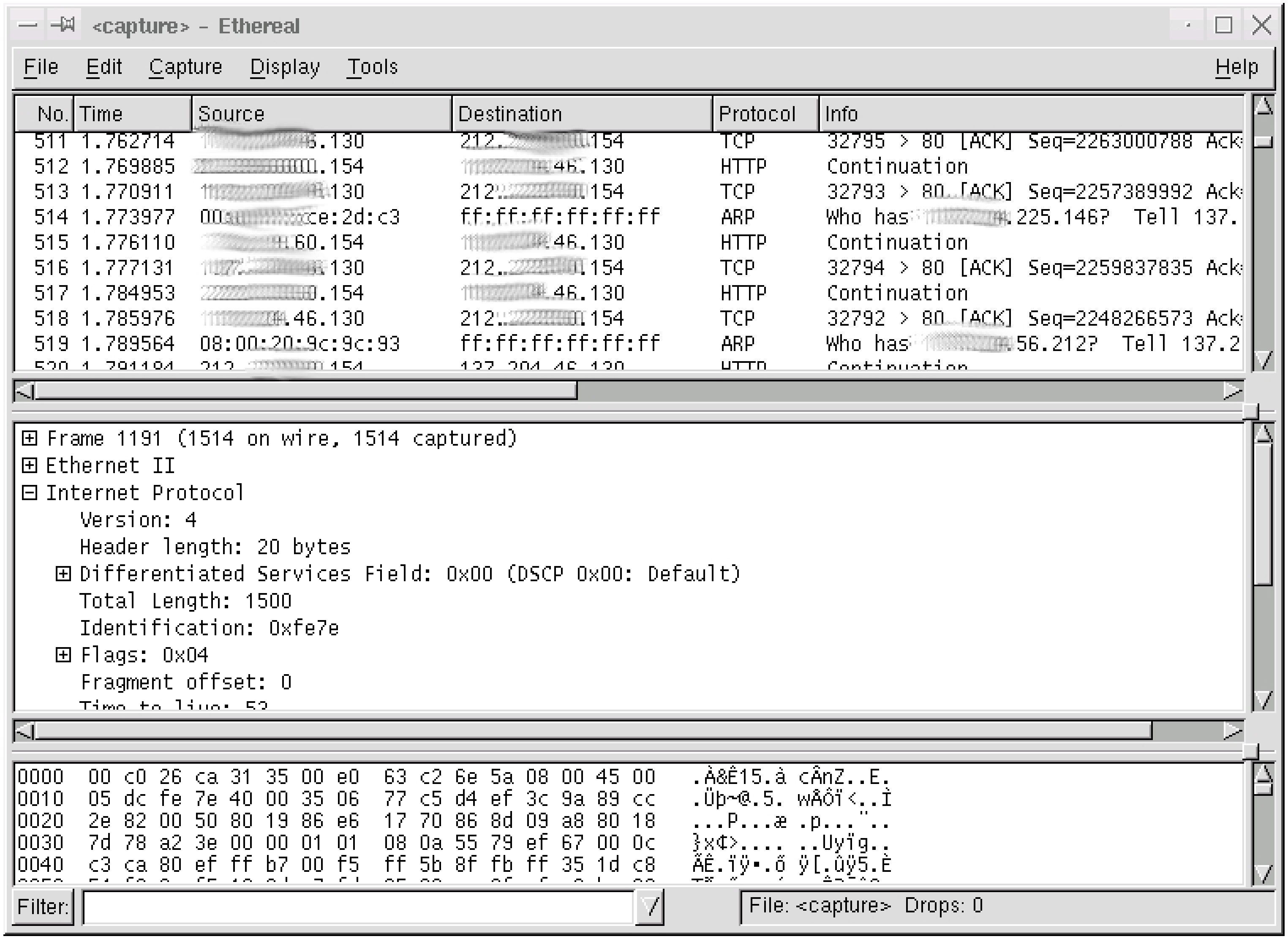


- Network sniffer, filtering, advanced protocol disassembly, TCP packet reassembly
- written by Gerald Combs and team
- latest version: 0.9.3 as of 30/03/2002
- Homepage: http://www.ethereal.com/
- Is based on the powerful pcap library, has both GUI and text frontend
- obsoletes: (tcpdump), sniffit, several custom scanners, ...

secunet

Ethereal

Sniff and visualize



```
No. Time      Source                Destination          Protocol  Info
511 1.762714  [redacted]6.130       212.[redacted]154    TCP       32795 > 80 [ACK] Seq=2263000788 Ack
512 1.769885  [redacted].154        [redacted]46.130     HTTP      Continuation
513 1.770911  [redacted].130        212[redacted]154     TCP       32793 > 80 [ACK] Seq=2257389992 Ack
514 1.773977  00[redacted]ce:2d:c3  ff:ff:ff:ff:ff:ff    ARP       Who has [redacted].225.146?  Tell 137.
515 1.776110  [redacted].60.154     [redacted].46.130    HTTP      Continuation
516 1.777131  [redacted].130        212.[redacted].154   TCP       32794 > 80 [ACK] Seq=2259837835 Ack
517 1.784953  [redacted].154        [redacted].46.130    HTTP      Continuation
518 1.785976  [redacted].46.130     212.[redacted].154   TCP       32792 > 80 [ACK] Seq=2248266573 Ack
519 1.789564  08:00:20:9c:9c:93     ff:ff:ff:ff:ff:ff    ARP       Who has [redacted]56.212?  Tell 137.2
520 1.791184  212.[redacted].154    137.204.46.130       HTTP      Continuation
```

```
⊞ Frame 1191 (1514 on wire, 1514 captured)
⊞ Ethernet II
⊟ Internet Protocol
    Version: 4
    Header length: 20 bytes
  ⊞ Differentiated Services Field: 0x00 (DSCP 0x00: Default)
    Total Length: 1500
    Identification: 0xfe7e
  ⊞ Flags: 0x04
    Fragment offset: 0
    Time to live: 53
```

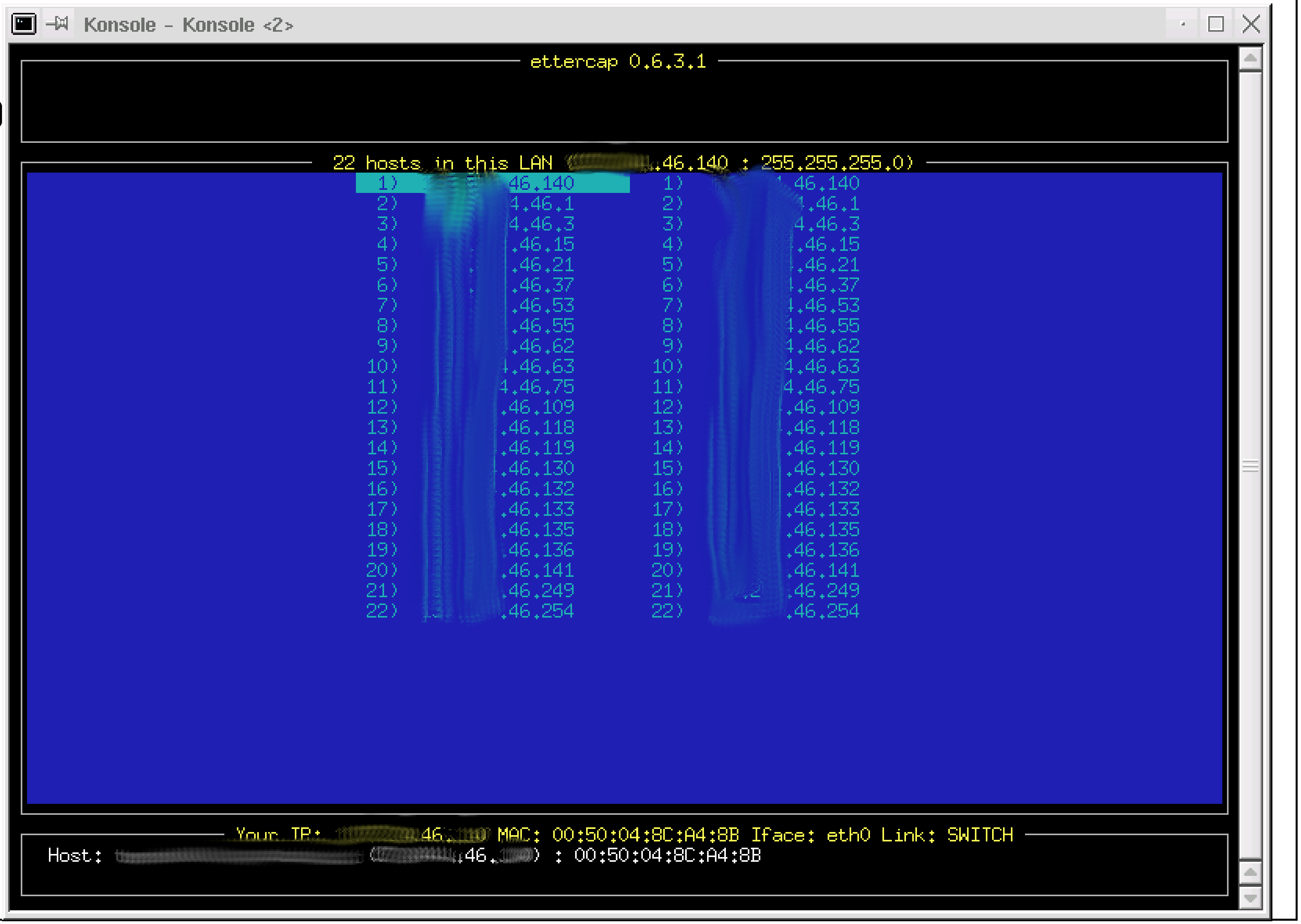
```
0000  00 c0 26 ca 31 35 00 e0  63 c2 6e 5a 08 00 45 00   .À&Ê15.à cÂnZ..E.
0010  05 dc fe 7e 40 00 35 06  77 c5 d4 ef 3c 9a 89 cc   .Üþ~@.5. wÅÔï<..Ì
0020  2e 82 00 50 80 19 86 e6  17 70 86 8d 09 a8 80 18   ...P...æ .p....¨..
0030  7d 78 a2 3e 00 00 01 01  08 0a 55 79 ef 67 00 0c   }x¢>.... ..Uyïg..
0040  c3 ca 80 ef ff b7 00 f5  ff 5b 8f fb ff 35 1d c8   ÃÊ.ïÿ·.õ ÿ[.ûÿ5.È
```

Tool 6: ettercap

- Allround tool for spoofing, sniffing and hijacking. Has both passive and active modes. Allows injection of own data in communication streams. Man-in-the-middle-attacks. Password collection for several protocols.
- written by ALoR and NaGA
- latest version: 0.6.5 as of 23/04/2002
- Homepage: http://ettercap.sourceforge.net/
- Typical use:
  Use ettercap to redirect traffic through your machine in a switched network and use Ethereal to read the passwords out of the streams.
- obsoletes: cheops, ftp-scanner, bind-scanner, webscanner, ...

ettercap

Target Selection

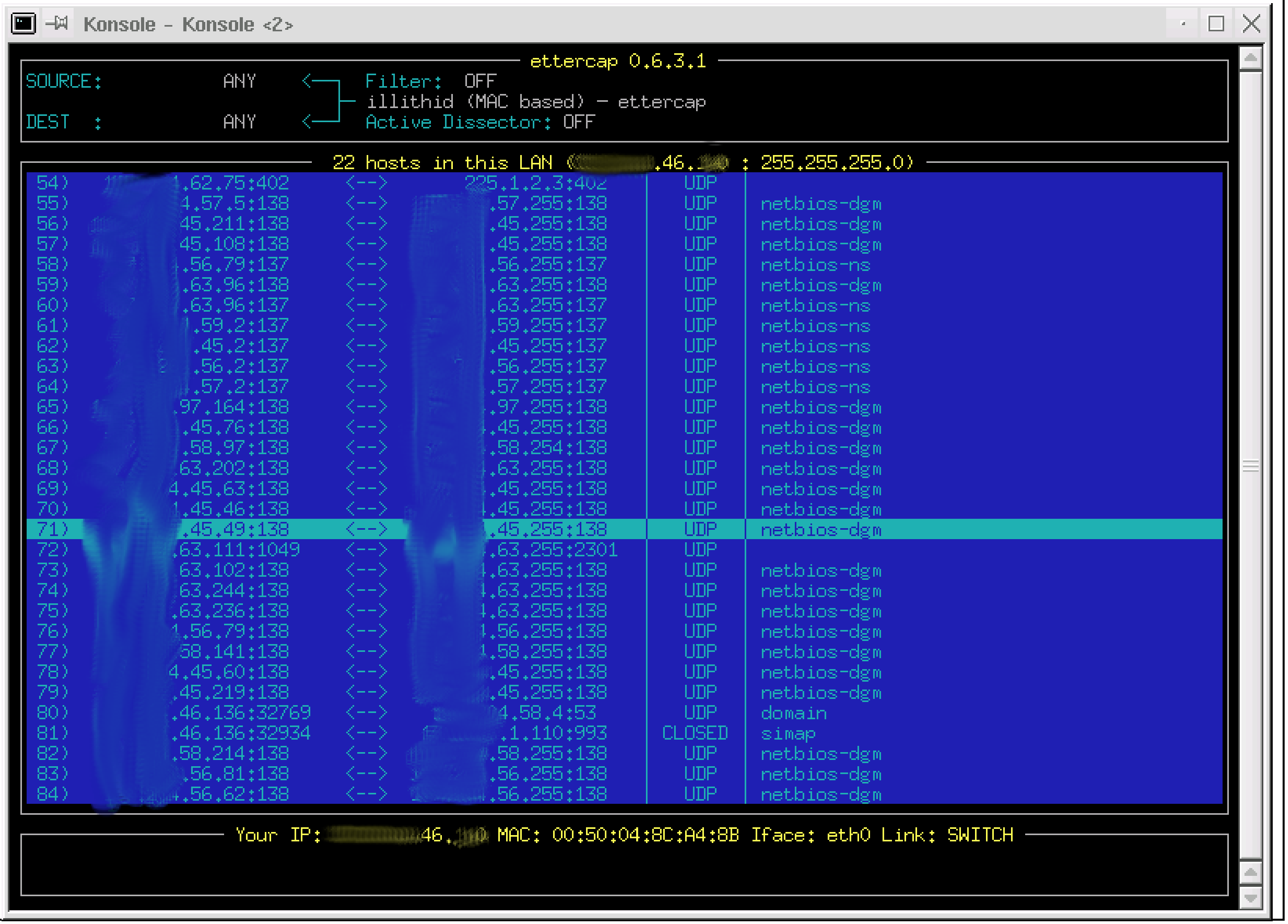


```
                         ettercap 0.6.3.1

        22 hosts in this LAN ([redacted].46.140 : 255.255.255.0)
         1) [redacted].46.140           1) [redacted].46.140
         2) [redacted].46.1             2) [redacted].46.1
         3) [redacted].46.3             3) [redacted].46.3
         4) [redacted].46.15            4) [redacted].46.15
         5) [redacted].46.21            5) [redacted].46.21
         6) [redacted].46.37            6) [redacted].46.37
         7) [redacted].46.53            7) [redacted].46.53
         8) [redacted].46.55            8) [redacted].46.55
         9) [redacted].46.62            9) [redacted].46.62
        10) [redacted].46.63           10) [redacted].46.63
        11) [redacted].46.75           11) [redacted].46.75
        12) [redacted].46.109          12) [redacted].46.109
        13) [redacted].46.118          13) [redacted].46.118
        14) [redacted].46.119          14) [redacted].46.119
        15) [redacted].46.130          15) [redacted].46.130
        16) [redacted].46.132          16) [redacted].46.132
        17) [redacted].46.133          17) [redacted].46.133
        18) [redacted].46.135          18) [redacted].46.135
        19) [redacted].46.136          19) [redacted].46.136
        20) [redacted].46.141          20) [redacted].46.141
        21) [redacted].46.249          21) [redacted].46.249
        22) [redacted].46.254          22) [redacted].46.254

   Your IP: [redacted]46.[redacted] MAC: 00:50:04:8C:A4:8B Iface: eth0 Link: SWITCH
 Host: [redacted] ([redacted].46.[redacted]) : 00:50:04:8C:A4:8B
```

secunet

ettercap

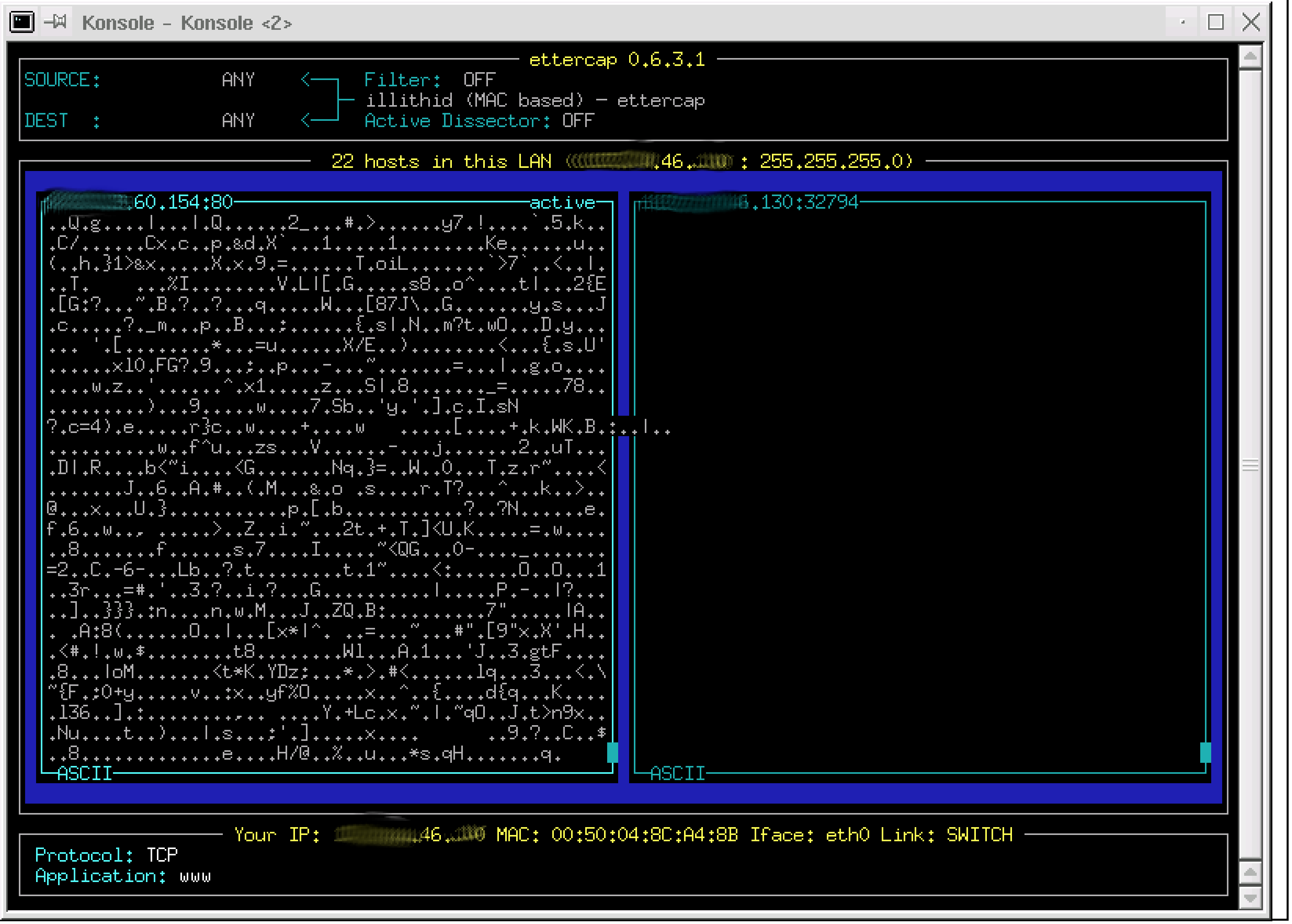
Passive Scanning



```
ettercap 0.6.3.1
SOURCE:          ANY    <--+  Filter:  OFF
                           |- illithid (MAC based) - ettercap
DEST  :          ANY    <--+  Active Dissector: OFF

22 hosts in this LAN ([redacted].46.[redacted] : 255.255.255.0)
54) [redacted].62.75:402     <-->  225.1.2.3:402          UDP
55) [redacted].57.5:138      <-->  [redacted].57.255:138  UDP     netbios-dgm
56) [redacted]45.211:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
57) [redacted]45.108:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
58) [redacted].56.79:137     <-->  [redacted].56.255:137  UDP     netbios-ns
59) [redacted].63.96:138     <-->  [redacted].63.255:138  UDP     netbios-dgm
60) [redacted].63.96:137     <-->  [redacted].63.255:137  UDP     netbios-ns
61) [redacted].59.2:137      <-->  [redacted].59.255:137  UDP     netbios-ns
62) [redacted].45.2:137      <-->  [redacted].45.255:137  UDP     netbios-ns
63) [redacted].56.2:137      <-->  [redacted].56.255:137  UDP     netbios-ns
64) [redacted].57.2:137      <-->  [redacted].57.255:137  UDP     netbios-ns
65) [redacted].97.164:138    <-->  [redacted].97.255:138  UDP     netbios-dgm
66) [redacted].45.76:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
67) [redacted].58.97:138     <-->  [redacted].58.254:138  UDP     netbios-dgm
68) [redacted]63.202:138     <-->  [redacted].63.255:138  UDP     netbios-dgm
69) [redacted].45.63:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
70) [redacted].45.46:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
71) [redacted].45.49:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
72) [redacted].63.111:1049   <-->  [redacted].63.255:2301 UDP
73) [redacted]63.102:138     <-->  [redacted].63.255:138  UDP     netbios-dgm
74) [redacted]63.244:138     <-->  [redacted].63.255:138  UDP     netbios-dgm
75) [redacted].63.236:138    <-->  [redacted].63.255:138  UDP     netbios-dgm
76) [redacted].56.79:138     <-->  [redacted].56.255:138  UDP     netbios-dgm
77) [redacted]58.141:138     <-->  [redacted].58.255:138  UDP     netbios-dgm
78) [redacted].45.60:138     <-->  [redacted].45.255:138  UDP     netbios-dgm
79) [redacted].45.219:138    <-->  [redacted].45.255:138  UDP     netbios-dgm
80) [redacted].46.136:32769  <-->  [redacted].58.4:53     UDP     domain
81) [redacted].46.136:32934  <-->  [redacted].1.110:993   CLOSED  simap
82) [redacted].58.214:138    <-->  [redacted].58.255:138  UDP     netbios-dgm
83) [redacted].56.81:138     <-->  [redacted].56.255:138  UDP     netbios-dgm
84) [redacted].56.62:138     <-->  [redacted].56.255:138  UDP     netbios-dgm

Your IP: [redacted].46.[redacted] MAC: 00:50:04:8C:A4:8B Iface: eth0 Link: SWITCH
```

ettercap

Live Sniffing



```
ettercap 0.6.3.1
SOURCE:          ANY     <-┐  Filter:  OFF
                           ├─ illithid (MAC based) - ettercap
DEST  :          ANY     <-┘  Active Dissector: OFF

22 hosts in this LAN ([redacted].46.[redacted] : 255.255.255.0)

[redacted].60.154:80                                  active    [redacted].130:32794
..Q.g....|...|.Q......2_....#.>......y7.!....`.5.k..
.C/......Cx.c..p.&d.X`...1.....1........Ke......u..
(..h.}1>&x.....X.x.9.=.......T.oiL........`>7`..<..|.
..T.     ...%I.........V.LI[.G.....s8..o^....t|...2{E
.[G:?...^.B.?..?...q......W...[87J\..G........y.s...J
.c......?._m...p..B...;........{.s|.N..m?t.wO...D.y...
...  '.[.........*...=u.......X/E..).........<....{.s.U'
.......x1O.FG?.9...;..p...-...~.........=...|..g.o.....
....w.z..'.......^.x1......z...S|.8........_=......78..
..........)...9......w....7.Sb..'y.'.].c.I.sN
?.c=4).e......r}c..w.....+.....w    ......[.....+.k.WK.B.:...|..
...........w..f^u...zs...V........-...j........2..uT...
.D|.R....b<~i.....<G.........Nq.}=..W..O....T.z.r~.....<
........J..6..A.#..(.M...&.o .s.....r.T?....^....k..>..
@...x...U.}..............p.[.b..............?..?N.......e.
f.6..w...  ......>..Z..i.~....2t.+.T.]<U.K......=.w....
..8.........f........s.7.....I......~<QG....O-...._........
=2..C.-6-....Lb..?.t...........t.1~.....<:.........O..O...1
..3r....=#.'..3.?..i.?...G..............|......P.-..|?...
..]..}}}.:n.....n.w.M....J..ZQ.B:...........7"......|A..
.  .A:8(........O..|....[x*|^.  ..=....~....#".[9"x.X'.H..
.<#.!.w.$.........t8..........Wl....A.1....'J..3.gtF.....
.8....|oM.........<t*K.YDz:....*.>.#<........1q....3....<.\
~{F.;O+y......v..:x..yf%O.......x..^..{.....d{q....K.....
.136..].:............  .....Y.+Lc.x.~.|.~qO..J.t>n9x...
.Nu....t..)....|.s...;'.].......x.....         ..9.?..C..$
..8................e.....H/@..%..u....*s.qH..........q.
ASCII                                                              ASCII

Your IP: [redacted].46.[redacted] MAC: 00:50:04:8C:A4:8B Iface: eth0 Link: SWITCH
Protocol: TCP
Application: www
```

Tool 7: spak

- Generate custom packets of various network layers: Set strange TCP-Flags, Send UDP packets with bogus data boundaries. Forge source routed IP packets, with source routing and more.
- written by Karyl F. Stein
- latest version: 0.6b as of 02/03/1998
- Homepage: http://www.cs.purdue.edu/homes/steinfk/software/
- Typical use:

```
# maketcp $SRC $SRCP $DST $DSTP -ss -of
  ../sample_options |\ makeip $SRC $DST -i - -sd |
  sendpacket $DST -v
```

- obsoletes: arp-fun, nemesis, ...

Tool 8: John the ripper

- Multipurpose password cracker. Breaks old (DES) and new (MD5) Unix passwords, different types of Windows passwords from sam and from network sniffers, cisco passwords etc.
- written by Solar Designer
- latest version: 1.6.31-dev as of 03/03/2002
- Homepage: http://www.openwall.com/john/
- Typical use:

```
# john -resume passwd.grabbed
```

- obsoletes: crack, l0phtcrack, ciscocrack, ...

Tool 9: OpenSSL

- Create and fake certificates. Encrypt and decrypt DES, 3DES, Blowfish, IDEA, AES, ... Talk SSL/TLS to encrypted webservers.
- written by OpenSSL project team
- latest version: 0.9.6c as of 22/12/2001
- Homepage: http://www.openssl.org/
- Typical use:

```
# (echo HEAD / HTTP/1.0; echo) |\
  openssl s_client -connect www.linuxtag.org:443
```

- Library version is built into some tools like ettercap

Tool 10: Nessus

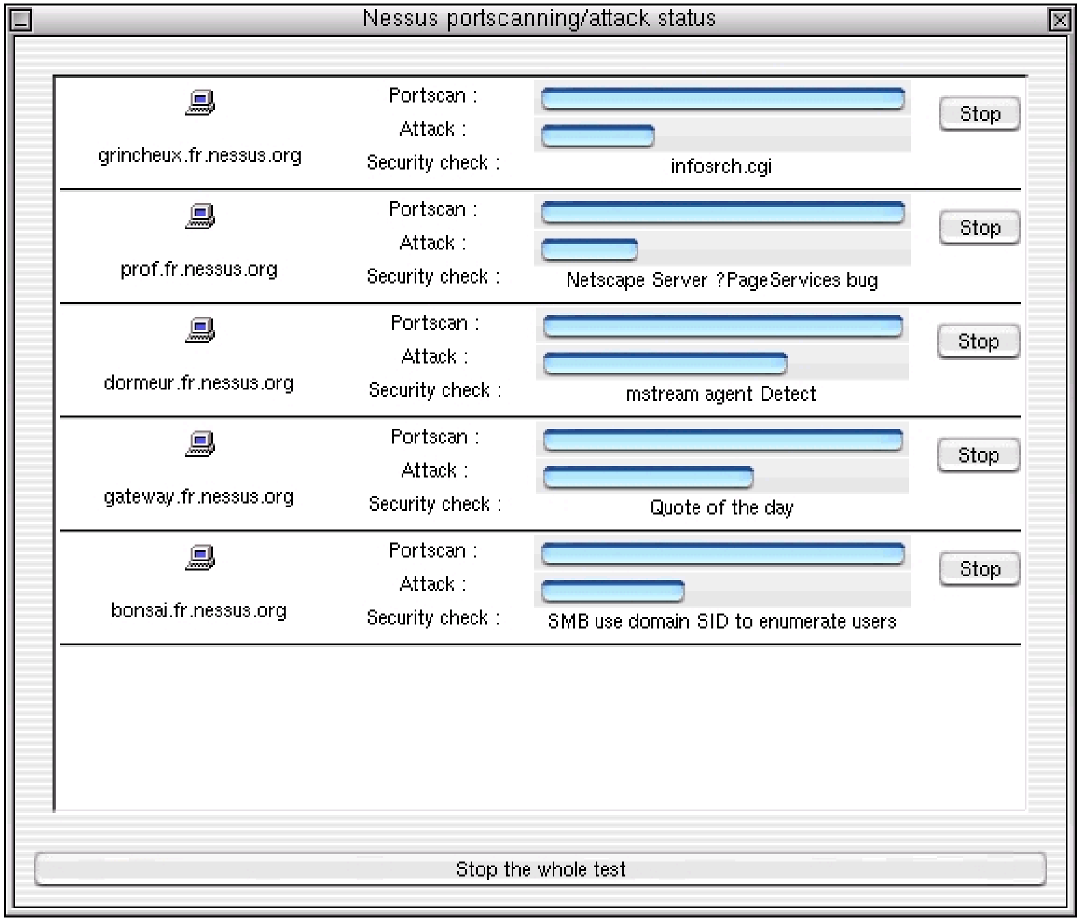
- Multi purpose, all-in-one integrated security scanner. Not really necessary, but convenient. Comes with graphical frontend. C/S-based. Can generate nifty reports and pie charts.

written by	Renaud Deraison and team
latest version:	1.2 as of 18/04/2002
Homepage:	http://www.nessus.org/

- Typical use:

  Get a first-glance overview of the security situation of a network. Beware of the dealing with lots of false positives and some negatives.
- obsoletes: (COPS), SATAN, Saint, Netsaint, SARA, ISS, ...

Nessus



Nessus portscanning/attack status

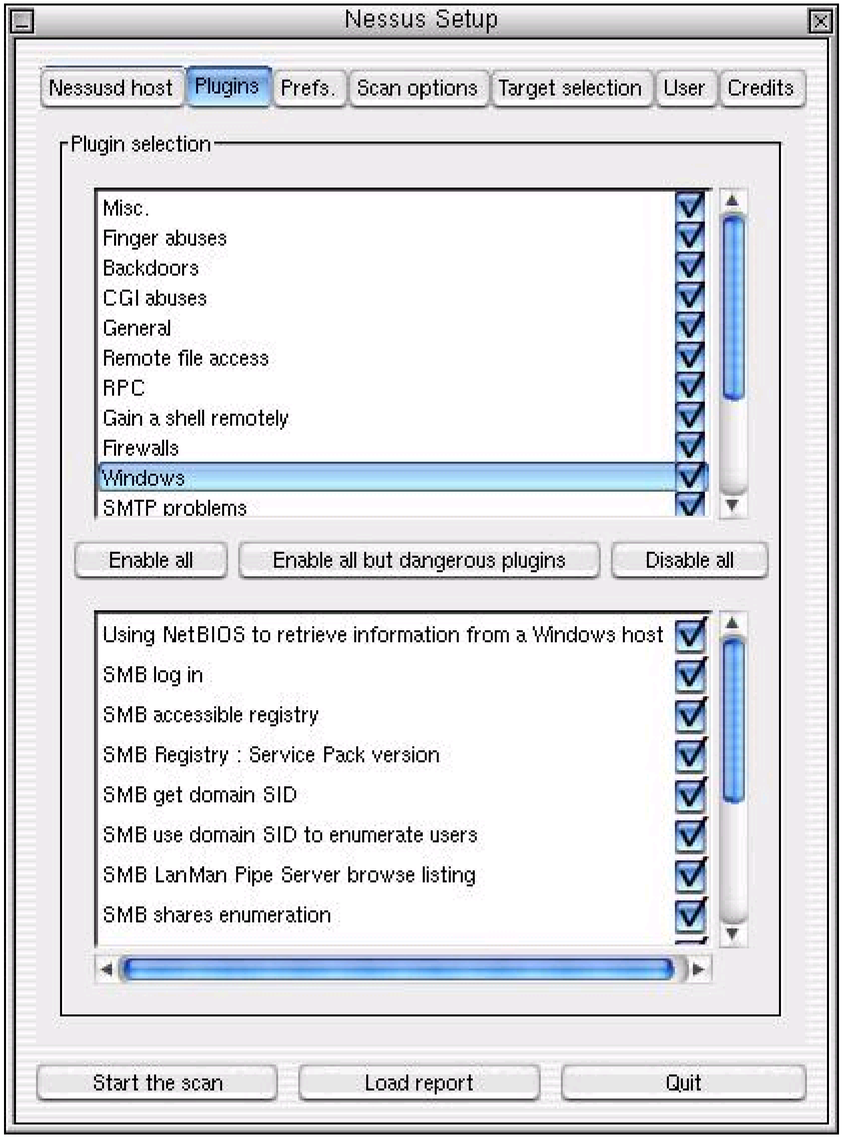
grincheux.fr.nessus.org
Portscan :
Attack :
Security check : infosrch.cgi

prof.fr.nessus.org
Portscan :
Attack :
Security check : Netscape Server ?PageServices bug

dormeur.fr.nessus.org
Portscan :
Attack :
Security check : mstream agent Detect

gateway.fr.nessus.org
Portscan :
Attack :
Security check : Quote of the day

bonsai.fr.nessus.org
Portscan :
Attack :
Security check : SMB use domain SID to enumerate users



Nessus Setup

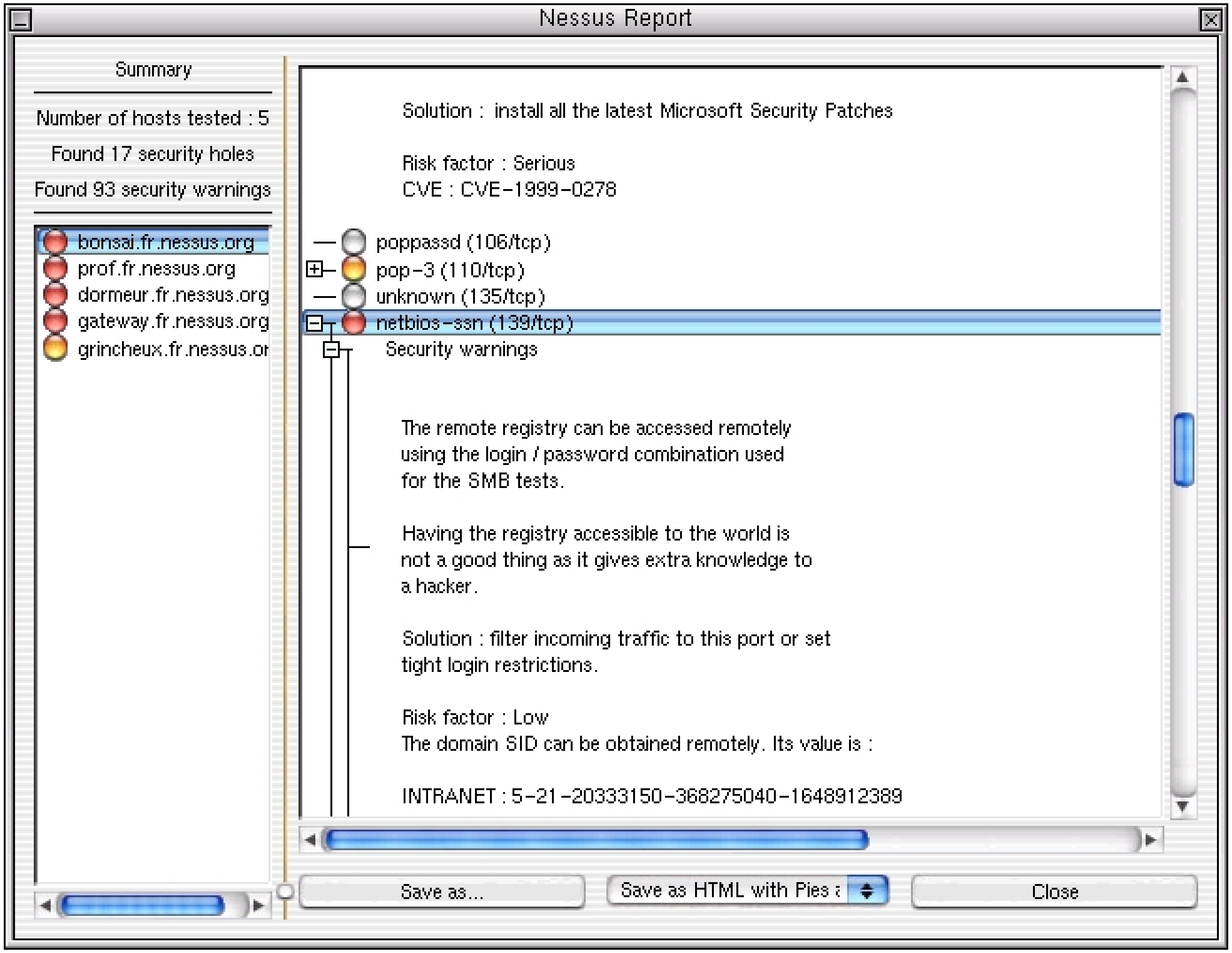
Plugin selection

- Misc. ☑
- Finger abuses ☑
- Backdoors ☑
- CGI abuses ☑
- General ☑
- Remote file access ☑
- RPC ☑
- Gain a shell remotely ☑
- Firewalls ☑
- Windows ☑
- SMTP problems ☑

- Using NetBIOS to retrieve information from a Windows host ☑
- SMB log in ☑
- SMB accessible registry ☑
- SMB Registry : Service Pack version ☑
- SMB get domain SID ☑
- SMB use domain SID to enumerate users ☑
- SMB LanMan Pipe Server browse listing ☑
- SMB shares enumeration ☑

Nessus

Nifty reports with suggestions for help



Number of hosts tested : 5
Found 17 security holes
Found 93 security warnings

- bonsai.fr.nessus.org
- prof.fr.nessus.org
- dormeur.fr.nessus.org
- gateway.fr.nessus.org
- grincheux.fr.nessus.or

Solution : install all the latest Microsoft Security Patches

Risk factor : Serious
CVE : CVE-1999-0278

- poppassd (106/tcp)
- pop-3 (110/tcp)
- unknown (135/tcp)
- netbios-ssn (139/tcp)
  - Security warnings

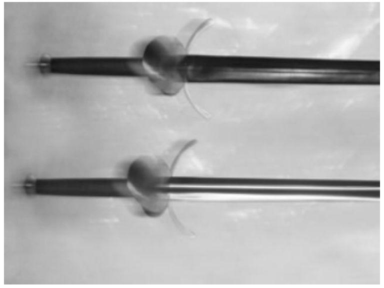
The remote registry can be accessed remotely
using the login / password combination used
for the SMB tests.

Having the registry accessible to the world is
not a good thing as it gives extra knowledge to
a hacker.

Solution : filter incoming traffic to this port or set
tight login restrictions.

Risk factor : Low
The domain SID can be obtained remotely. Its value is :

INTRANET : 5-21-20333150-368275040-1648912389



Summary of Linux attacking tools

nmap	Scan
dig	List
netcat	Send and Receive
whisker	Browse
Ethereal/tcpdump	Sniff
ettercap	Spoof and Hijack
spak	Generate
John the Ripper	Crack
openssl	Encrypt and Decrypt
Nessus	Summarize

My watchlist

Ok, ok, just ten items may be a little hard ...
... some of these tools might get on my list one day:

■ nagios	successor of Netsaint
■ snmp-Utilities	dumping Network Management data
■ netcat with SSL built-in	combines netcat and OpenSSL
■ argus	augments ethereal/tcpdump
■ airsnort	for detection and analyzing WLANs
■ babelweb	additional aproach to whisker

Questions,

Comments,

Discussion

LINUX
TAG
OPEN HORIZONS
VISIONARIUM
TECH TRACK
THE LINUXTAG 2003 CONFERENCE
JUNE 6 - 9 2002 - KARLSRUHE CONFERENCE CENTER
www.linuxtag.org

Hacker in charge

Dipl.-Inform. Nils Magnus
Senior-Consultant IT-Security

secunet
Security Networks AG
Osterbekstr. 90b
22083 Hamburg, Germany

Tel.: +49 40 69 65 99 - 13
Fax: +49 40 69 65 99 - 29
E-Mail: magnus@secunet.de
URL: www.secunet.com