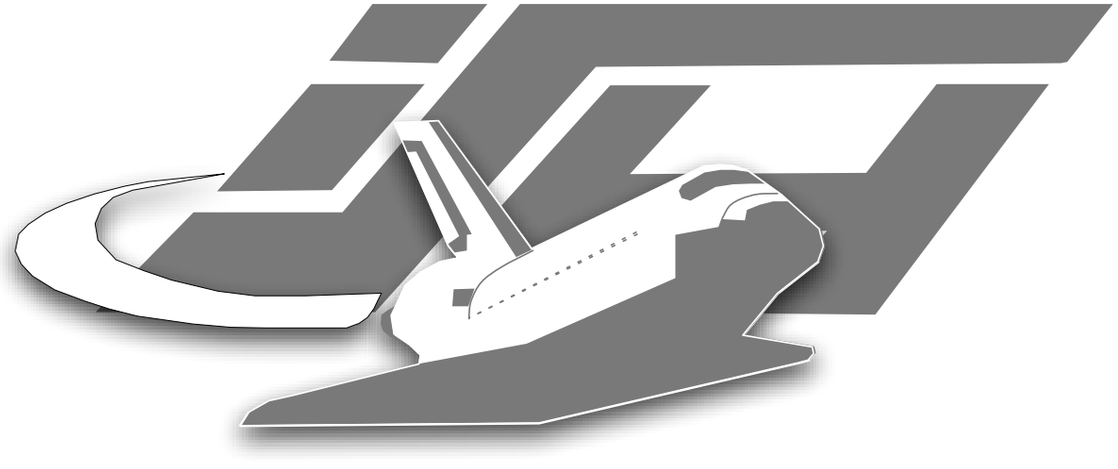
The Art of (Application) Fingerprinting

21. Chaos Communication Congress 2004

Ilja van Sprundel & Maximillian Dornseif
special guest:
psycho Dog from da <<< neo aRmY >>>

See http://md.hudora.de/presentations/#fingerprinting-21c3



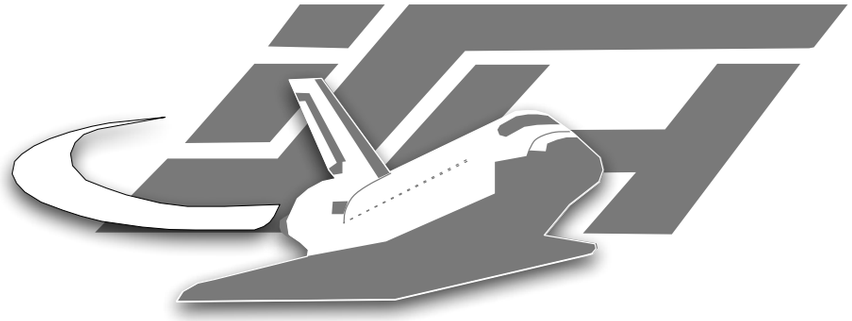
Laboratory for Dependable Distributed Systems

RHEINISCH-
WESTFÄLISCHE
TECHNISCHE
HOCHSCHULE
AACHEN

RWTH

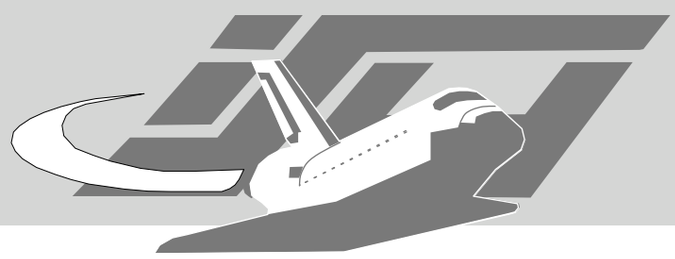
UNIVERSITY
OF TECHNOLOGY
AACHEN

Who we are



Laboratory for Dependable Distributed Systems

- Laboratory for Dependable Distributed Systems at RWTH-Aachen University
  - Founded in late 2003 for theoretical & practical security research, topics include:
    - Security Education
    - Honeypot technology
    - Sensor Networks
- Notable classes include “Hacker Seminar”, “Hacker Praktikum”, “Pen-Test Praktikum”, “Aachen Summerschool applied IT-Security”, “Computer Forensics”
- http://mail-i4.informatik.rwth-aachen.de/mailman/listinfo/lufgtalk/



Agenda

- What is fingerprinting?
- TCP/IP stack fingerprinting
  - well known, we had that an hour ago
- Application fingerprinting
  - more obscure, tools less well known
  - more fun

Fingerprinting

Fingerprinting

- People
- IP Stacks
- Applications

- Clients
- Servers

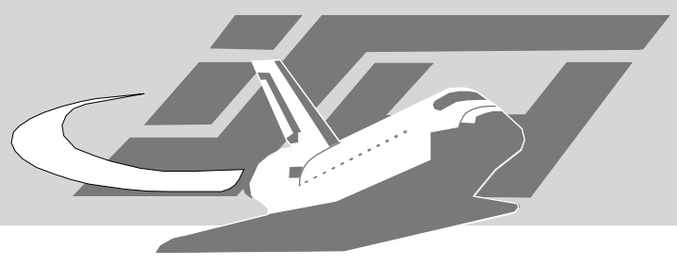
What is fingerprinting?

- comparing features which make something identifiable
- seldom exact
- the value of fingerprinting is in databases to match against

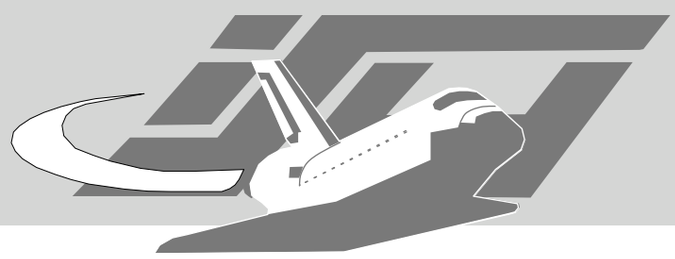
TCP/IP stack fingerprinting

...

Application Fingerprinting



- socat advertisement
  - http://www.dest-unreach.org/socat/
- Banner grabbing
- More interactive approaches



Banner Grabbing

- Connect, get response, disconnect
- Works lice a charm for many protocols

SSH

Terminal – RedTeam@RWTH

```
% socat - tcp4:deepblack.lolitacoders.org:22
SSH-1.99-OpenSSH_3.5p1 FreeBSD-20030924
^C
% socat - tcp4:untergrund.bewaff.net:22
SSH-1.99-OpenSSH_3.5p1 c0re
^C
% socat - tcp4:md.hudora.de:22
SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030924
^C
% socat - tcp4:koeln.ccc.de:22
SSH-2.0-OpenSSH_3.6.1p2 Debian 1:3.6.1p2-8
^C
% socat - tcp4:houston.informatik.rwth-aachen.de:22
SSH-2.0-OpenSSH_3.8.1p1 Debian 1:3.8.1p1-4
^C
% socat - tcp4:node21-gb.rhrz.uni-bonn.de:22
SSH-2.0-2.3.0 SSH Secure Shell (non-commercial)
^C
```

scanssh

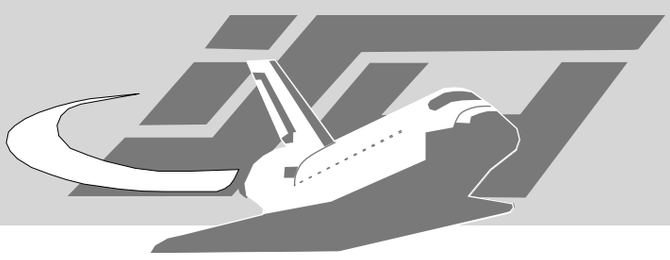
Terminal – RedTeam@RWTH

```
% sudo scanssh 213.221.87.0/24 | grep SSH
213.221.87.8 SSH-2.0-OpenSSH_3.4p1
213.221.87.81 SSH-1.99-OpenSSH_3.4p1
213.221.87.82 SSH-1.99-OpenSSH_3.0.2p1
213.221.87.83 SSH-2.0-OpenSSH_3.8p1
213.221.87.133 SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030924
213.221.87.134 SSH-1.99-OpenSSH_3.6.1p1 FreeBSD-20030924
213.221.87.179 SSH-1.99-OpenSSH_3.7.1p1_ASL
213.221.87.185 SSH-1.99-OpenSSH_3.7.1p1_ASL
213.221.87.195 SSH-1.5-SSH Protocol Compatible Server SCS 2.0
```

FTP

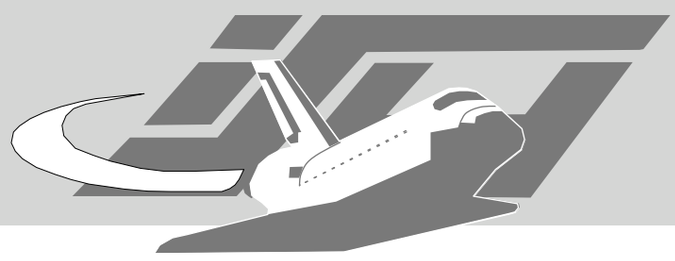
Terminal – RedTeam@RWTH

```
% socat - tcp4:ftp9.us.FreeBSD.org:21
220-osmirrors.cerias.purdue.edu.cerias.purdue.edu NcFTPd
Server (free educational license) ready.
220-          Welcome to the CERIAS Security FTP Archive
```



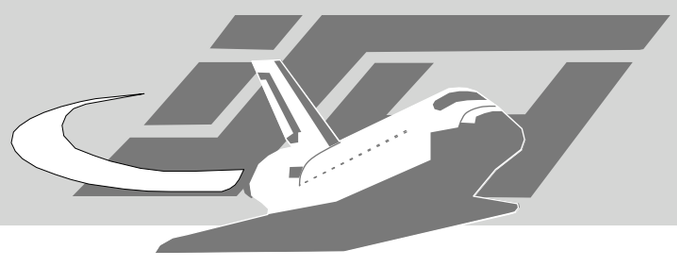
Terminal – RedTeam@RWTH

```
% socat - tcp4:131.220.15.211:21
220 f2node21 FTP server (Version 4.1 Mon Jun 4 14:21:11 CDT
2001) ready.
SYST
215 UNIX Type: L8 Version: BSD-44
```



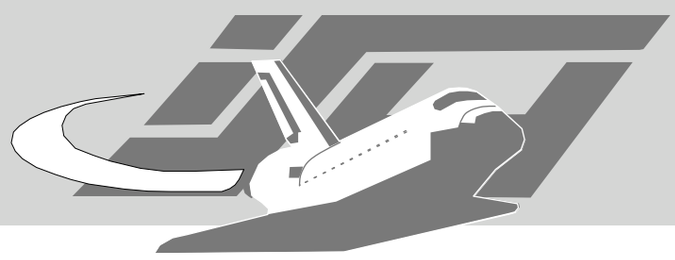
Terminal – RedTeam@RWTH

```
% (curl -s http://www.chalo.net/music/ftpservers.htm ; \
curl -s http://www.freebsd.org/doc/en_US.ISO8859-1/books/
handbook/mirrors-ftp.html ; \
curl -s http://www.geocities.com/TimesSquare/Alley/1557/
ftp.htm ; \
curl -s http://www.openbsd.org/ftp.html ; \
curl -s http://www.suse.de/en/private/download/ftp/
int_mirrors.html ; \
curl -s http://sanlab.kz.tsukuba.ac.jp/HTML/serverFTP.html ;
curl -s http://www.faqs.org/faqs/ftp-list/ ) | \
grep ftp:// | sort -u | \
perl -npe 's|.*ftp://([^"></]*).*|socat open:
ftptest,ignoreeof\\!\\!STDOUT  tcp4:$1:21,crnl|;' | sh
```



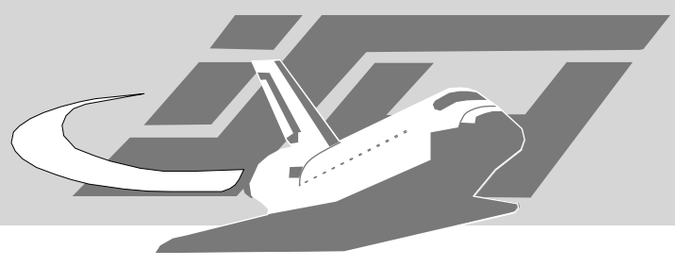
telnet

- ... much more complex than you thought
- from banner grabbing from to more complex fingerprinting



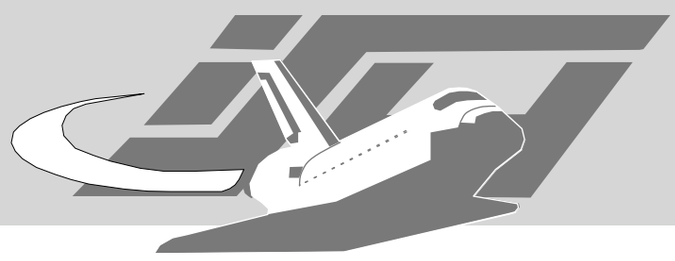
Terminal – RedTeam@RWTH

```
% socat - tcp4:131.220.15.211:23
??%??
^C
% telnet 131.220.15.211
Trying 131.220.15.211...
Connected to node21-gb.rhrz.uni-bonn.de.
Escape character is '^]'.
[...]
telnet (f2node21)
[...]
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: bla
bla's Password:
3004-007 You entered an invalid login name or password.
login: root
root's Password:
3004-007 You entered an invalid login name or password.
login: ^CConnection closed by foreign host.
```



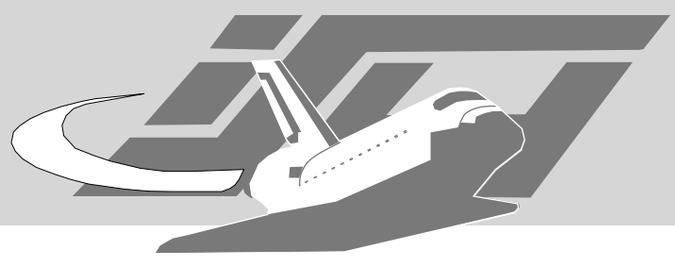
Terminal – RedTeam@RWTH

```
% socat - tcp4:213.221.0.153:23
???? ??#??'??$^C[c0ldcut:~] md% telnet 213.221.0.153
Trying 213.221.0.153...
Connected to 213.221.0.153.
Escape character is '^]'.

User Access VerificationPassword:
```



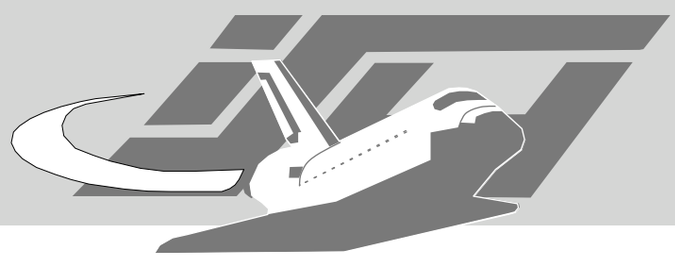
Terminal – RedTeam@RWTH

```
% telnet 213.221.4.225
Trying 213.221.4.225...
Connected to 213.221.4.225.
Escape character is '^]'.


User Access Verification

Password: Kerberos:     No default realm defined for
Kerberos!

% Password:  timeout expired!
Password:
% Password:  timeout expired!
Password:
% Password:  timeout expired!
% Bad passwords
Connection closed by foreign host.
```



Terminal – RedTeam@RWTH

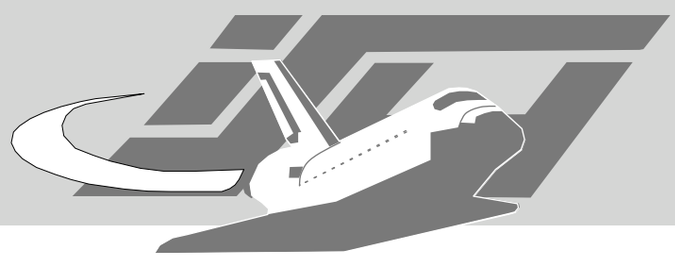
```
% telnet 213.221.11.1
Trying 213.221.11.1...
Connected to 213.221.11.1.
Escape character is '^]'.
[...]
!!! Welcome to Access TAINET WANpro 2000 !!!

username :
password :
Login incorrect
username :
password :
Login incorrect
username :
password :
Login incorrect
0Reject by server !!! Connection closed by foreign host.
```



telnet

Terminal – RedTeam@RWTH

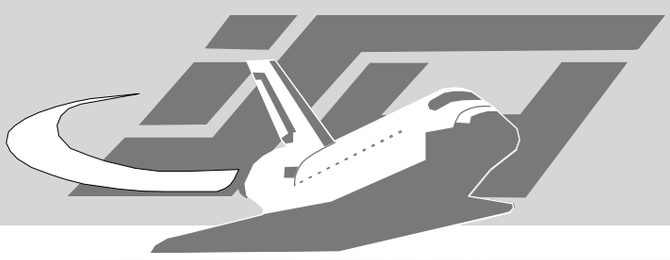
```
% telnet 213.221.0.153
Trying 213.221.0.153...
Connected to 213.221.0.153.
Escape character is '^]'.

User Access VerificationPassword:Client aborted login

telnet> quit
Connection closed.
```



telnet

Terminal – RedTeam@RWTH

```
telnet 213.221.113.125
Trying 213.221.113.125...
Connected to 213.221.113.125.
Escape character is '^]'.

Welcome. Type <return>, enter password at # prompt

#
```



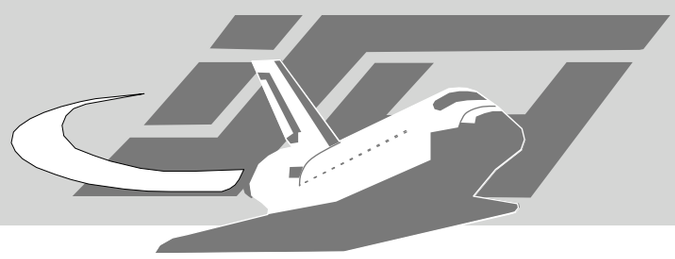
Terminal

File Edit View Terminal Go Help

Ouverture

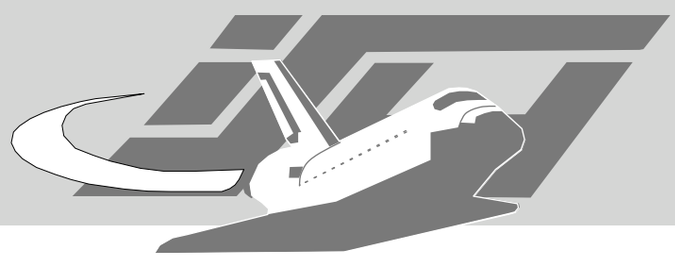
Syst□me . . . . . : ICOI
Sous-syst□me . . . : QBASE
Ecran . . . . . : QPADEV000P

Utilisateur . . . . . □_____
Mot de passe . . . . . .
Programme/proc□dure . . . . . _____
Menu . . . . . _____
Biblioth□que en cours . . . . . _____



telnet fingerprinting

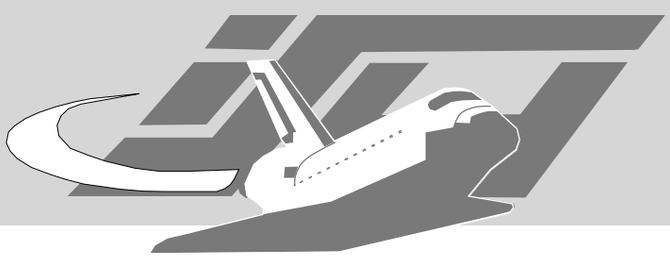
- Telnet has an handshake at the start of the communication which negotiates the options used in that connection
- WILL / WONT, DO / DONT
- This can be used for active and passive Fingerprinting (See Ben Doyle: “Passive Fingerprinting Utilizing the Telnet Protocol Negotiation data” - http://www.sans.org/resources/idfaq/fingerp_telnet.php)



telnetfp

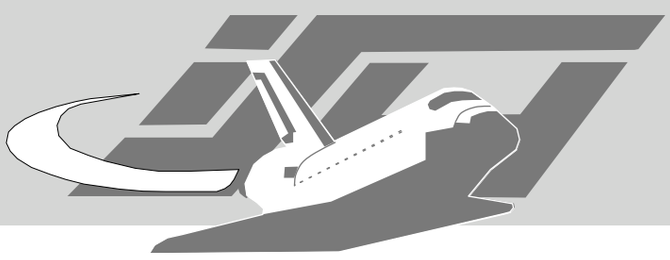
Terminal – RedTeam@RWTH

```
% ./telnetfp node21-gb.rhrz.uni-bonn.de
telnetfp0.1.2 by palmers / teso
DO:   255 254 37 255 253 24
DONT: 255 253 24 255 250 24 1 255 240

NOT FOUND!

please mail the following lines and OS/machine type to pa1mers@gmx.de:
DO:   255 254 37 255 253 24
DONT: 255 253 24 255 250 24 1 255 240

% nmap -sV -p 21-23 node21-gb.rhrz.uni-bonn.de

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-26 18:45 CEST
Interesting ports on node21-gb.rhrz.uni-bonn.de (131.220.15.211):
PORT   STATE SERVICE VERSION
21/tcp open  ftp     HP-UX 10.x ftpd 4.1
22/tcp open  ssh     F-Secure SSH Secure Shell 2.3.0 (protocol 2.0)
23/tcp open  telnet  AIX telnetd

Nmap run completed -- 1 IP address (1 host up) scanned in 1.707 seconds
```



Terminal – RedTeam@RWTH

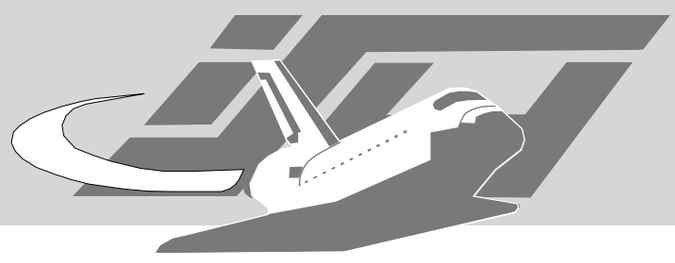
```
% telnet node21-gb.rhrz.uni-bonn.de
[...]
telnet (f2node21)
[...]
AIX Version 4
(C) Copyrights by IBM and by others 1982, 1996.
login: test
test's Password:
3004-007 You entered an invalid login name or password.
login:
login: test
test's Password:
3004-007 You entered an invalid login name or password.
login: root
root's Password:
3004-007 You entered an invalid login name or password.
Connection closed by foreign host.
```



Terminal – RedTeam@RWTH

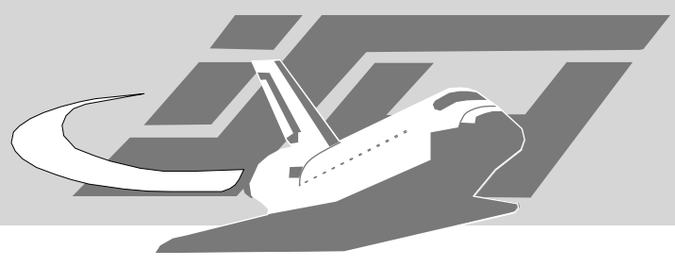
```
% ./telnetfp 213.221.0.153
telnetfp0.1.2 by palmers / teso
DO:   255 253 24 255 253 32 255 253 35 255 253 39 255 253 36
DONT:
255 250 32 1 255 240 255 250 35 1 255 240 255 250 39 1 255 240 255 250 24 1 255
240
Found matching finger print: FreeBSD
Digital Unix 4.0d/e
NetBSD 1.4.2
Tru64 UNIX V5.0A

% nmap -sV -p21-23 213.221.0.153

Starting nmap 3.55 ( http://www.insecure.org/nmap/ ) at 2004-09-26 18:58 CEST
Interesting ports on 213.221.0.153:
PORT   STATE  SERVICE VERSION
21/tcp closed ftp
22/tcp open   ssh     OpenSSH 3.4-j2 (protocol 1.99)
23/tcp open   telnet  Openwall GNU/*/Linux telnetd

Nmap run completed -- 1 IP address (1 host up) scanned in 1.697 seconds
```

```
% cat fps
#telnetfp fingerprints
#send more fingerprints to: pa1mers@gmx.de
# a '*' means: after this anything may follow
# a '?' represents no or any possible byte

DO:   255 253 24 255 253 32 255 253 35 255 253 39
DONT:
255 250 32 1 255 240 255 250 35 1 255 240 255 250 39 1 255 240 255 250 24 1 255 240
Linux

[...]

DO:   116 101 108 110 101 116 100 58 32 115 58 32 117 110 107 110 111 119 110 32 111 112
116 105 111 110 10 85 115 97
DONT:
103 101 58 32 116 101 108 110 101 116 100 32 91 45 100 101 98 117 103 93 32 91 45 68 32
40 111 112 116 105
Linux with support for SecurID cards enabled

DO:   116 101 108 110 101 116 100 58 32 *
DONT: *
probably Linux
```



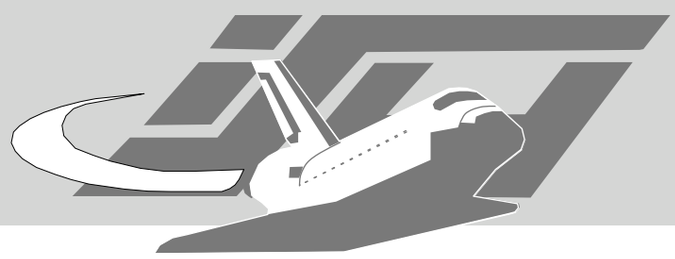
ident

- the lost tool
- identfp - http://www.synnergy.net/Archives/Utilities/dethy/identfp.tar.gz
- ldistfp - http://packetstormsecurity.org/UNIX/misc/ldistfp-0.1.4.tar.gz



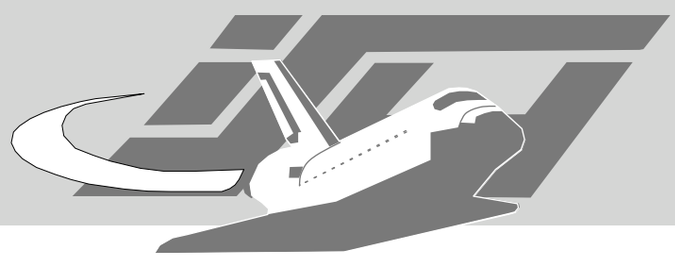
Terminal – RedTeam@RWTH

```
% socat - tcp4:213.221.113.111:113,crnl
VERSION
0 , 0 : ERROR : INVALID-PORT
% socat - tcp4:212.202.56.115:113
VERSION
0 , 0 : ERROR : INVALID-PORT
% socat - tcp4:212.202.56.14:113,crnl
VERSION
 : USERID : UNIX : fceykeund
^C
% socat - tcp4:212.202.56.68:113,crnl
VERSION
VERSION : USERID : UNIX : D47815
% socat - tcp4:www.chemie.fu-berlin.de:113
VERSION
0 , 0 : X-VERSION : pidentd 3.0.7 for IRIX64 6.5 (Sep 15 1999 11:21:21)
^C
% socat - tcp4:mail.oih.RWTH-Aachen.DE:113,crnl
VERSION
0 , 0 : X-VERSION : pidentd 3.0.12 for Linux 2.4.9-686-smp (Sep  2 2001 11:26:
57)
^C
% socat - tcp4:perplex.lbb.RWTH-Aachen.DE:113,crnl
VERSION
```



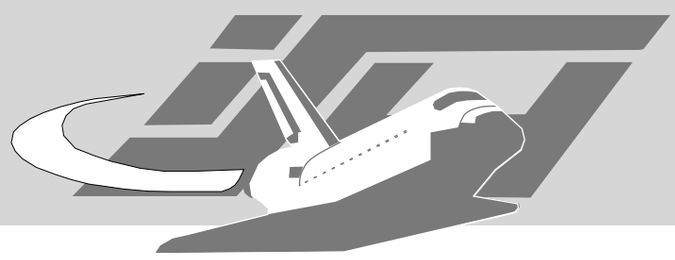
ftpmap

- Written by the PureFTPD author as a proof of concept.



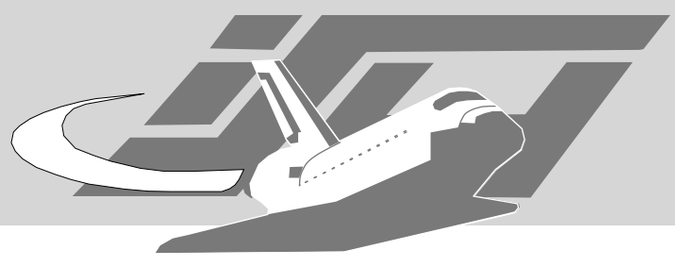
Terminal – RedTeam@RWTH

```
% ftpmap -s 213.221.113.125
*** Scanning IP : [213.221.113.125]

*** Fingerprint :

2642,1701,2642,2642,2642,2483,1726,1701,1726,2642,2642,2642,3305,2219,2642,2642,2642,2442,2442,2315,23
15,2642,2906,2642,2642,2642,2219,2219,2219,2642,2642,2642,2642,2642,2642,2642,2219,2219,2219,2642,2642
,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,1701,1701,1701,1701,1701,2642,2
642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,264
2,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,
2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,26
42,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,
2642,1701,2642,2642,2642,2483,1726,1701,1726,2642,2642,2642,3308,2219,2642,2642,2642,2442,2442,2315,23
15,2642,2906,2642,2642,2642,2219,2219,2219,2642,2642,2642,2642,2642,2642,2642,2219,2219,2219,2642,2642
,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,1701,1701,1701,1701,1701,2642,2
642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,264
2,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,
2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,26
42,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,2642,

*** This may be running :
[Pure-FTPd 1.0.1]       (error=6.3848 %)
[Pure-FTPd 1.0.12 (french)]     (error=6.41013 %)
[Pure-FTPd 0.98.5 (french)]     (error=6.68998 %)

*** Unable to determine FTP port sequence numbers

If you know the name of the FTP server you just scanned, please
contribute to this program by sending the fingerprint and the
name of the server software to : ftpmap@pureftpd.org
```



Terminal – RedTeam@RWTH

```
% ftpmap -s untergrund.bewaff.net
*** Scanning IP : [62.143.76.82]

*** Fingerprint :

2933,2450,2933,2945,2933,2933,3124,2933,2933,2974,2933,2933,3805,2933,2964,2933,2933,2933,2933,3097,29
33,2933,2933,2933,2933,2933,2933,2933,2933,2933,2933,2967,2933,2933,2933,3146,2933,2931,2933,2933,2933
,2977,2933,2933,2933,2943,2933,2933,2933,2933,2933,2933,2869,2933,2933,2933,2933,2876,2933,3076,2933,2
964,2933,2933,2933,3066,2933,2933,2933,2933,2942,2933,3037,2933,2933,2983,2933,3078,2933,3098,2942,302
3,2933,2955,2933,2933,2933,2964,2933,2933,2933,2933,2933,2933,2933,2972,2933,2933,2933,2933,2933,2933,
2933,2933,2933,2933,2933,2933,2933,2969,3047,3174,3225,3675,3048,3071,2958,5527,2120,2933,2933,3402,2933,29
33,2933,3353,2933,3479,2933,2933,3487,2933,2933,4185,2933,2933,2933,3427,2933,2933,3586,2933,3712,
2433,2450,2945,2088,3124,2647,2974,2732,3805,2964,2732,2774,3334,3097,3941,3325,2981,2442,2442,2361,23
61,2361,2892,2892,2361,2361,2966,1870,1869,2967,5488,5542,3146,2931,2766,2892,2977,1725,2235,2943,1725
,2235,2980,2722,2848,2869,1722,2232,2957,1722,2876,1722,3076,2964,1722,2971,3066,3093,1385,1393,2942,3
037,905,2983,3078,3098,2942,3023,2955,1869,1870,2846,1181,1181,3347,2964,1869,1870,2892,1181,1181,3393
,2961,3930,2892,1181,1181,3393,3930,2972,2532,2532,1181,1181,2532,2532,1435,1403,1403,1181,1181,1403,1
403,2969,3047,3174,3043,3225,3675,3048,2937,3071,2958,3287,3636,3276,3402,3410,3614,3353,3479,3433,348
7,4059,4185,4139,4193,3427,3553,3507,3561,3586,3712,3666,3724,3590,3716,3670,3724,2551,2965,2950,

*** This may be running :
[WuFTPd 2.6]    (error=7.3169 %)
[Microsoft FTPd 5]      (error=7.64757 %)
[SunOS 4.1 FTPd]        (error=7.66973 %)

*** FTP port sequence numbers : 63528 37355 51861 47658 54960
    Difficulty = 13046 (Worthy challenge)


If you know the name of the FTP server you just scanned, please
contribute to this program by sending the fingerprint and the
name of the server software to : ftpmap@pureftpd.org
```

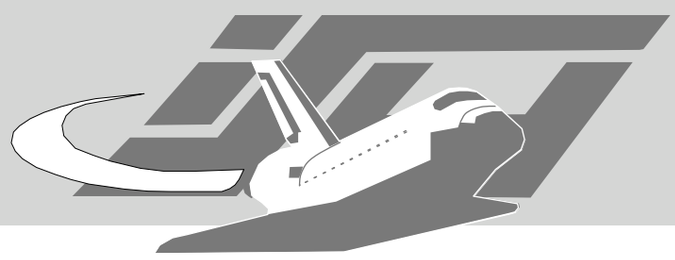


datastructures

Terminal – RedTeam@RWTH

```
typedef struct FP_ {
    unsigned long err;
    const char *software;
    unsigned long testcase[148 * 2];
} FP;

static FP fingerprints[] = {
    {
        0UL, "Pure-FTPd 0.97pre5" , {
3945,673,673,673,673,1203,2644,4689,2644,2644,3747,2644,3405,3406,3302,3303,474,2767,2767,2521,2521,2521,5223,
[...] 8,3708,3708,3708,3708,3708,1723,0,
3945,673,673,673,673,1203,2644,4689,2644,2644,3747,2644,3410,3411,3298,3299,470,2767,2767,2521,2521,2521,5223,
[...] 8,3708,3708,3708,3708,3708,1723,0,
        }
    },
    {
        0UL, "Pure-FTPd 0.97pre5 (romanian)" , {
2214,1161,1161,1161,1161,1203,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,2214,
[...] 4,2214,2214,2214,2214,2214,2214,2954,0,
5940,1161,1161,1161,1161,1203,2924,5381,2924,2924,2910,2924,3163,3205,3296,3256,462,2992,2992,2724,2724,2724,5
[...] ,5691,5691,5691,5691,2954,0,
        }
    },
```

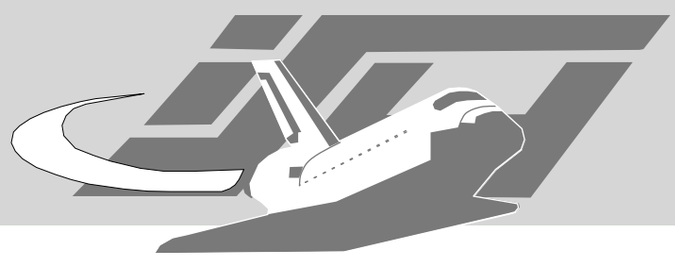
ftpmap-0.4 fingerprints.h



Terminal – RedTeam@RWTH

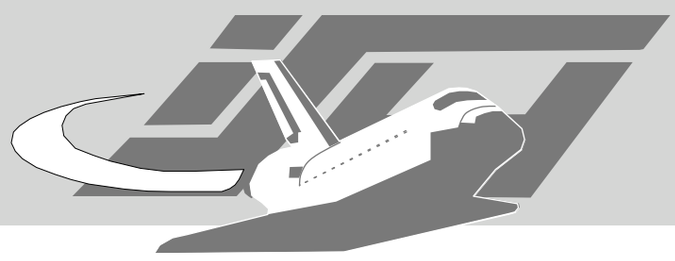
```
static const char *testcmds[] = {
        "ABOR" FTP_CRLF,
        "NOOP" FTP_CRLF,
        "ALLO" FTP_CRLF,
        "ALLO 42" FTP_CRLF,
        "ALLO -42" FTP_CRLF,
        "SYST" FTP_CRLF,
        "PORT" FTP_CRLF,
        "PORT 1,2,3,4,5,6" FTP_CRLF,
        "PORT -1,-2,-3,-4,-5,-6" FTP_CRLF,
        "EPRT" FTP_CRLF,
        "EPRT |1|2.3.4.5|6|" FTP_CRLF,
        "EPRT |-1|-2.-3.-4.-5|-6|" FTP_CRLF,
        "PASV" FTP_CRLF,
        "PASV 42" FTP_CRLF,
        "EPSV" FTP_CRLF,
        "EPSV 42" FTP_CRLF,
        "SPSV" FTP_CRLF,
        "PWD" FTP_CRLF,
        "XPWD" FTP_CRLF,
        "CWD" FTP_CRLF,
        "CWD /" FTP_CRLF,
        "XCWD /" FTP_CRLF,
        "CWD ~/" FTP_CRLF,
        "XCWD ~/" FTP_CRLF,
        "CDUP" FTP_CRLF,
        "XCUP" FTP_CRLF,
        "RETR" FTP_CRLF,
        "RETR /" FTP_CRLF,
        "RETR ." FTP_CRLF,
ftpmap-0.4
```

ftpmap-0.4 testcmds.h



ftpmap 0.5

- uses a database instead of hardcoded stuff
- check if we can't log in
- choose if you want to use IPv4 or IPv6
- support of multihosted servers
- better output
- updated fingerprints
- bugs fixed
- available in N minutes at http://ilja.netric.org/files/

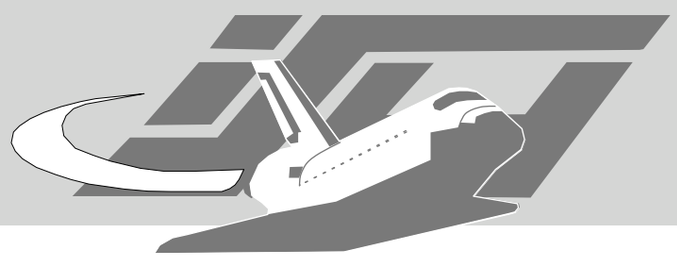


smtpscan

- Julien Bordet: Remote SMTP Server detection - http://www.greyhats.org/outils/smtpscan/remote_smtp_detect.pdf

Terminal – RedTeam@RWTH

```
% smtpscan tosses.info lolitacoders.org
smtpscan version 0.5
  15 tests available
  3184 fingerprints in the database
Scanning tosses.info (80.190.253.213) port 25
 15/15
Result --
250:250:250:250:250:250:250:214:252:502:502:502:502:250:250
Banner :
220 ipx11001.ipxserver.de ESMTP
SMTP server corresponding :
  - Qmail 1.0.3
Scanning lolitacoders.org (213.221.113.35) port 25
30/151555555555555
Result --
250:401:401:250:401:250:450:402:252:402:402:402:402:250:250
Banner :
220 beebop.23.nu ESMTP
SMTP server corresponding :
  - Postfix
```



fingerprints database

Terminal – RedTeam@RWTH

```
4D WebSTAR -0-:501:250:501:250:501:250:250:214:550:550:500:500:500:250:250
4D WebSTAR -1-:501:220:501:250:501:250:250:214:500:500:500:500:500:250:250
4D WebSTAR -2-:501:250:501:250:501:250:250:214:250:250:500:500:500:250:250
4D WebSTAR -3-:501:250:501:250:501:250:250:214:550:500:500:500:500:250:250
4D WebSTAR -4-:501:250:501:250:501:250:250:214:500:500:500:500:500:250:250
4D WebSTAR V Mail (5.2.4) -0-:503:250:500:250:500:250:500:500:250:250:500:500:500:250:250
4D WebSTAR V Mail (5.2.4) -1-:503:250:500:250:500:250:500:500:500:500:500:500:500:250:250
602Pro LAN SUITE v. 2000:501:250:501:250:501:250:501:214:502:502:502:250:250:250:250
AMOS Mail version 5.1:503:250:501:250:250:250:550:214:252:502:502:502:502:250:250
Abbing Mailserver v9.5:250:501:501:250:501:501:550:214:502:502:500:250:250:250:250
ArGoSoft Pro Version 1.8 -0-:550:250:502:250:550:550:550:214:502:550:502:502:502:250:250
[...]
Avirt 4.2:250:250:500:250:250:250:250:214:250:250:500:500:500:220:500
BMR ErlangTM/OTP (3.1/3.3) -0-:503:501:501:250:501:451:550:214:252:500:500:500:500:250:250
BMR ErlangTM/OTP (3.1/3.3) -1-:503:501:501:250:501:451:250:214:252:500:500:500:500:250:250
CSC-Sendmail:503:250:501:250:553:250:550:214:252:502:502:502:502:250:250
Canon IR2200i Printer:550:501:501:250:250:250:250:500:500:500:500:500:500:250:250
CheckPoint FireWall-1 secure SMTP server -0-:501:250:501:501:501:250:501:214:502:502:500:500:500:220:250
[...]
Exim 4.10:250:250:500:250:501:250:501:214:252:550:500:500:500:250:250
F-secure Anti-Virus for Internet Mail -0-:250:250:500:250:250:250:553:502:553:502:502:502:502:250:250
F-secure Anti-Virus for Internet Mail -1-:250:250:500:250:553:250:553:502:553:502:502:502:502:250:250
FTGate -0-:550:250:500:250:250:250:500:550:550:550:550:550:550:250:250
[...]
InterScan VirusWall 3.52 -1-:250:250:501:250:501:250:553:214:502:502:500:250:250:250:250
IntraStore TurboSendmail -0-:250:250:501:250:250:250:501:500:252:550:500:500:500:250:250
IntraStore TurboSendmail -1-:250:250:501:250:250:250:551:500:252:252:500:500:500:250:250
M>Wall 5.0:503:500:501:250:553:250:501:500:501:501:500:500:500:250:250
MAILsweeper 4.3 -0-:503:250:250:250:250:250:553:500:252:500:500:500:500:250:250
MAILsweeper 4.3 -1-:503:250:250:250:250:250:250:500:252:500:500:500:500:250:250
MAILsweeper 4.3.1.0:503:250:250:250:550:250:503:500:252:500:500:500:500:250:250
MAILsweeper 4.3.6.0:503:250:501:501:250:250:250:500:252:500:500:500:500:250:250
MDaemon 3.5.0 -0-:503:220:550:250:250:250:250:214:502:502:502:250:250:250:250
```

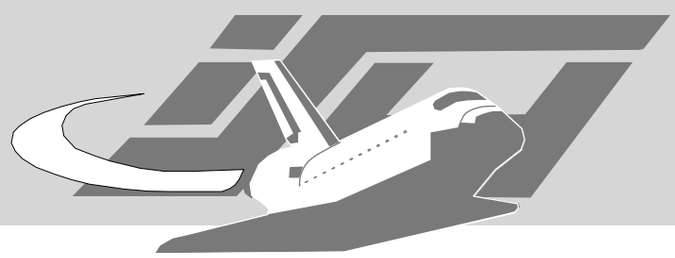
smtpscan-0.5 fingerprints

tests database

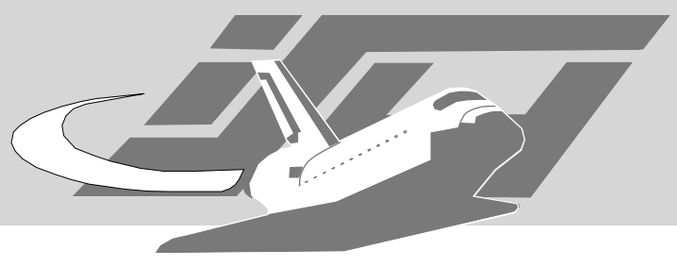
Terminal – RedTeam@RWTH

```
MAIL FROM: $VALID_SOURCE
HELO
HELO $MY_DOMAIN->MAIL FROM test
HELO $MY_DOMAIN->MAIL FROM: <>
HELO $MY_DOMAIN->MAIL FROM: <$VALID_SOURCE
HELO $MY_DOMAIN->MAIL FROM: <$INVALID_SOURCE>
HELO $MY_DOMAIN->MAIL FROM: <$VALID_SOURCE>->RCPT TO: test
HELO $MY_DOMAIN->HELP
HELO $MY_DOMAIN->VRFY root
HELO $MY_DOMAIN->EXPN root
HELO $MY_DOMAIN->TURN
HELO $MY_DOMAIN->SOML FROM: <$VALID_SOURCE>
HELO $MY_DOMAIN->SAML FROM: <$VALID_SOURCE>
HELO $MY_DOMAIN->NOOP
EHLO $MY_DOMAIN
#HELO $MY_DOMAIN->ETRN test
#HELO $MY_DOMAIN->MAIL FROM: <$VALID_SOURCE>->RCPT TO:
<$TARGET_DOMAIN:$VALID_SOURCE>
```

smtpscan-0.5 tests

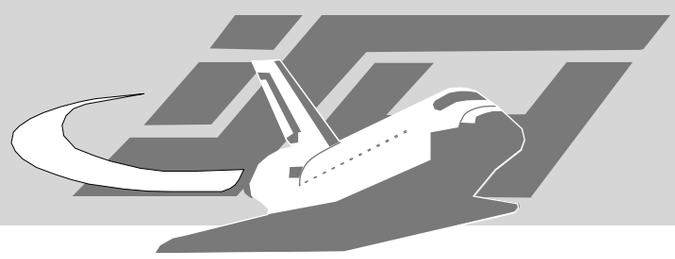


- smtpscan seems to have been integrated in nessus
- the nessus version claims to have much more fingerprints
- See http://cvsweb.nessus.org/cgi-bin/cvsweb.cgi/~checkout~/nessus-plugins/scripts/smtpscan.nasl?content-type=text/plain



lpd fingerprinting

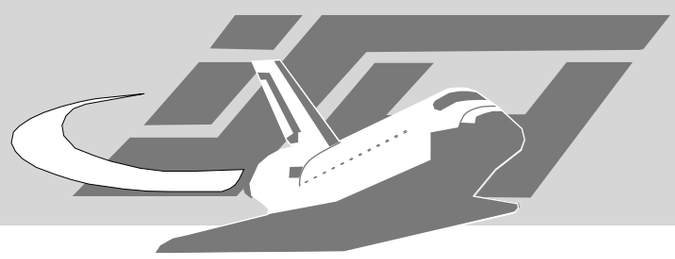
- f0bic: “Examining Remote OS Detection using LPD Querying” - http://packetstormsecurity.org/papers/os-detection/osdetect-lpd.txt



Terminal – RedTeam@RWTH

```
#
# LPDFP Fingerprints Database File
#
# Operating System                  Fingerprint
#
FreeBSD, OpenBSD                    lpd: Your host does not have line printer access
FreeBSD                             lpd: Host name for your address
AIX                                 ill-formed FROM address(.*)
OpenVMS                             Your host does not have printer access
OpenVMS                             Your host does not have line printer access
ConvexOS                            \/usr\/lib\/lpd: Malformed from address
SGI IRIX                            \/usr\/etc\/lpd: (.*):(.*)
Linux                               \/usr\/sbin\/lpd:(.*): Malformed from address
Linux                               lpd:(.*): Malformed from address
Linux                               no connect permissions
SunOS/Solaris (Possibly 5.6)        (.*)\/lpd: Malformed from address
NetBSD, Linux                       lpd: Malformed from address
SunOS/Solaris                       Invalid protocol request(.*)
SCO UnixWare, UNIX System V Release 4      (.*)Illegal service request(.*)
```

lpdfp.db



Terminal – RedTeam@RWTH

```
% ./lpdfp localhost
 -- Line Printer Daemon OS Fingerprinting
 -- by f0bic@low-level.net
 -- [lpd/fp] connected to localhost
    [Unknown Fingerprint]
    An unknown fingerprint has been gathered!
    Please submit the  following  information
    to f0bic@low-level.net :

       * Fingerprint -->

       * Host        --> localhost
       * Date        --> Sun Sep 26 20:56:54 CEST 2004

[c0ldcut:private/AppScan/lpdfp] md% ./lpdfp 213.221.113.125
 -- Line Printer Daemon OS Fingerprinting
 -- by f0bic@low-level.net
 -- [lpd/fp] connected to 213.221.113.125
^C
```

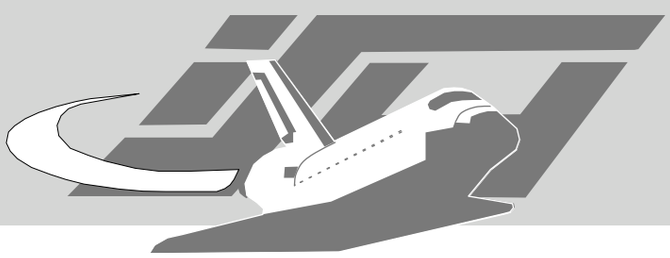
DNS

Terminal – RedTeam@RWTH

```
% dig @f.root-servers.net version.bind chaos txt

; <<>> DiG 9.2.2 <<>> @f.root-servers.net version.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32016
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL:
0

;; QUESTION SECTION:
;version.bind.                  CH      TXT

;; ANSWER SECTION:
version.bind.           0       CH      TXT     "9.2.3"

;; Query time: 391 msec
;; SERVER: 192.5.5.241#53(f.root-servers.net)
;; WHEN: Sun Sep 26 22:11:54 2004
;; MSG SIZE  rcvd: 48
```

Terminal – RedTeam@RWTH

```
% dig @f.root-servers.net authors.bind chaos txt
; <<>> DiG 9.2.2 <<>> @f.root-servers.net authors.bind chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8436
;; flags: qr aa rd; QUERY: 1, ANSWER: 12, AUTHORITY: 0, ADDITIONAL: 0
;; QUESTION SECTION:
;authors.bind.                  CH      TXT

;; ANSWER SECTION:
authors.bind.           0       CH      TXT     "Andreas Gustafsson"
authors.bind.           0       CH      TXT     "Bob Halley"
authors.bind.           0       CH      TXT     "Damien Neil"
authors.bind.           0       CH      TXT     "Danny Mayer"
authors.bind.           0       CH      TXT     "Matt Nelson"
authors.bind.           0       CH      TXT     "Ben Cottrell"
authors.bind.           0       CH      TXT     "Mark Andrews"
authors.bind.           0       CH      TXT     "James Brister"
authors.bind.           0       CH      TXT     "Michael Graff"
authors.bind.           0       CH      TXT     "David Lawrence"
authors.bind.           0       CH      TXT     "Michael Sawyer"
authors.bind.           0       CH      TXT     "Brian Wellington"

;; Query time: 368 msec
;; SERVER: 192.5.5.241#53(f.root-servers.net)
;; WHEN: Sun Sep 26 22:10:13 2004
;; MSG SIZE  rcvd: 341
```

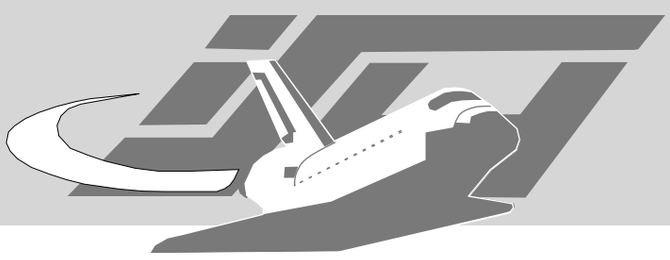


Terminal – RedTeam@RWTH

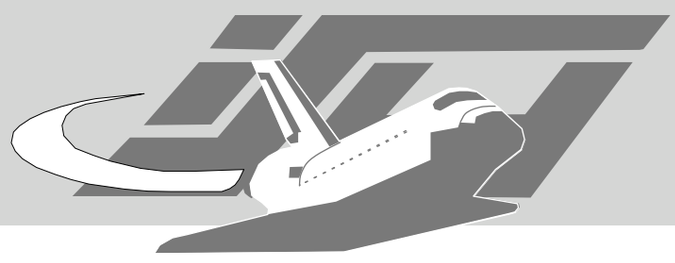
```
$ dig @k.root-servers.net version.server chaos txt

; <<>> DiG 9.2.1 <<>> @k.root-servers.net version.server chaos txt
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 39488
;; flags: qr; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;version.server.                        CH      TXT

;; ANSWER SECTION:
version.server.         0       CH      TXT     "NSD-1.0.2"

;; Query time: 37 msec
;; SERVER: 193.0.14.129#53(k.root-servers.net)
;; WHEN: Thu Jul 17 11:04:37 2003
;; MSG SIZE  rcvd: 54
```

Terminal – RedTeam@RWTH

```
% host in.gateway.23.tosses.info
in.gateway.23.tosses.info has address 194.77.77.142
in.gateway.23.tosses.info has address 194.77.77.142
```

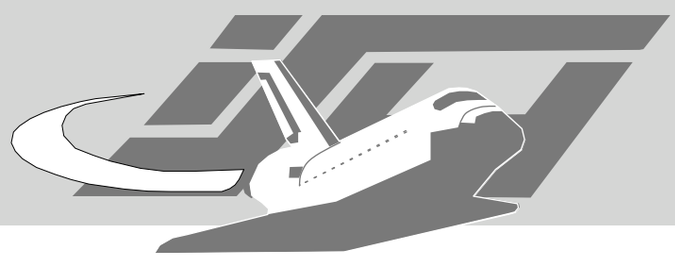


- Nice overview from Dan Bernstein - http://cr.yp.to/surveys/dns1.html
- Implemented in Nessus



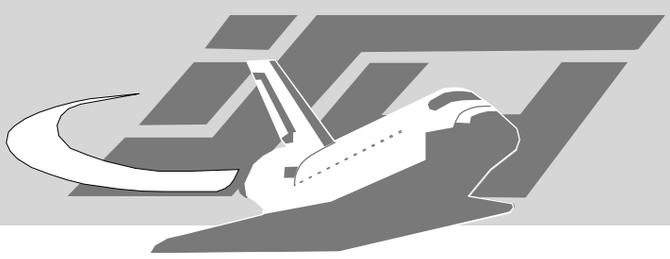
dnsfinger

- By "Nexus" <nexus@patrol.i-w>
- http://www.darklab.org/archive/msg00067.html
- See also THCbindinfo - http://www.thc.org/root/tools/THCbindinfo.c



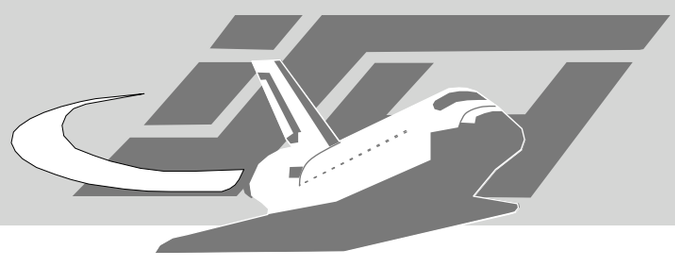
Terminal – RedTeam@RWTH

```
% ./dnsfinger xdsl-195-14-221-106.netcologne.de
DNS Fingerprint by Nexus <nexus@patrol.i-way.co.uk> Version 1.0

Sending version.bind...
Request OK, Version reported : .2.3(4x((((
RCODE = 0, No Error

Guess you have to trust it ;-)

Sending authors.bind...
RCODE = 0, No Error

Resolving 127.0.0.1...
Return Packet is 77 bytes
RCODE = 0, No Error

Resolving localhost...
Return Packet is 102 bytes
RCODE = 3, Name Error

All Done
% nmap -sV -p 53 xdsl-195-14-221-106.netcologne.de

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-09-26 21:48 CEST
Interesting ports on xdsl-195-14-221-106.netcologne.de (195.14.221.106):
PORT   STATE SERVICE VERSION
53/tcp open  domain  ISC Bind 9.2.3

Nmap run completed -- 1 IP address (1 host up) scanned in 6.003 seconds
```



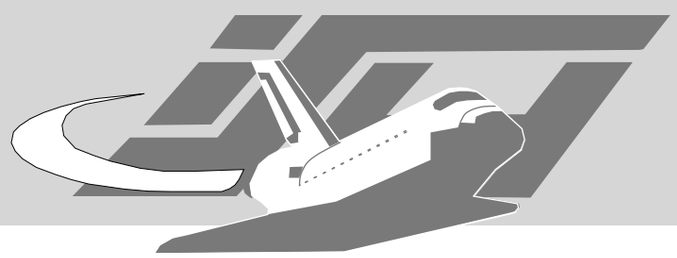
Terminal – RedTeam@RWTH

```
./dnsfinger xdsl-195-14-221-232.netcologne.de
DNS Fingerprint by Nexus <nexus@patrol.i-way.co.uk> Version 1.0

Sending version.bind...
Request OK, Version reported : NetCologne Nameserver V0.98rc2
RCODE = 0, No Error

Guess you have to trust it ;-)

Sending authors.bind...
RCODE = 2, Internal Server Error

Resolving 127.0.0.1...
Return Packet is 93 bytes
RCODE = 0, No Error

Resolving localhost...
Return Packet is 73 bytes
RCODE = 0, No Error



All Done
```



Terminal – RedTeam@RWTH

```
 ./dnsfinger 194.231.10.10
DNS Fingerprint by Nexus <nexus@patrol.i-way.co.uk> Version 1.0

Sending version.bind...
Request OK, Version reported : (((4x((((((((((((n(4(((@(((((H$(P(8(5LH5

[g|     &.8D^y4          (./
dnsfinger194.231.10.10STY=76895.ttyp0.titanTERM=screenTERMCAP=SC|screen|VT 100/ANSI X3.64
virtual terminal:\
        :DO=\E[%dB:LE=\E[%dD:RI=\E[%dC:UP=\E[%dA:bs:bt=\E[Z:\
        :cd=\E[J:ce=\E[K:cl=\E[H\E[J:cm=\E[%i%d;%dH:ct=\E[3g:\
        :do=^J:nd=\E[C:pt:rc=\E8:rs=\Ec:sc=\E7:st=\EH:up=\EM:\
        :le=^H:bl=^G:cr=^M:it#8:ho=\E[H:nw=\EE:ta=^I:is=\E)0:\
        :li#35:co#110:am:xn:xv:LP:sr=\EM:al=\E[L:AL=\E[%dL:\
        :cs=\E[%i%d;%dr:dl=\E[M:DL=\E[%dM:dc=\E[P:DC=\E[%dP:\
        :im=\E[4h:ei=\E[4l:mi:IC=\E[%d@:ks=\E[?1h\E=:\
        :ke=\E[?1l\E>:vi=\E[?25l:ve=\E[34h\E[?25h:vs=\E[34l:\
        :ti=\E[?1049h:te=\E[?1049l:us=\E[4m:ue=\E[24m:so=\E[3m:\
        :se=\E[23m:md=\E[1m:mr=\E[7m:me=\E[m:ms:\
        :Co#8:pa#64:AF=\E[3%dm:AB=\E[4%dm:op=\E[39;49m:AX:G0:\
        :as=\E(0:ae=\E(B:\
        :ac=\140\140aaffggjjkkllmmnnooppqqrrssttuuvvwwxxyyzz{{||}}~~..--++,,hhII00:\
        :k0=\E[10~:k1=\EOP:k2=\EOQ:k3=\EOR:k4=\EOS:k5=\E[15~:\
        :k6=\E[17~:k7=\E[18~:k8=\E[19~:k9=\E[20~:k;=\E[21~:\
        :F1=\E[23~:F2=\E[24~:kb=^H:kh=\E[1~:@1=\E[1~:kH=\E[4~:\
        :@7=\E[4~:kN=\E[6~:kP=\E[5~:kI=\E[2~:kD=\E[3~:ku=\EOA:\
Bus error (core dumped)
```

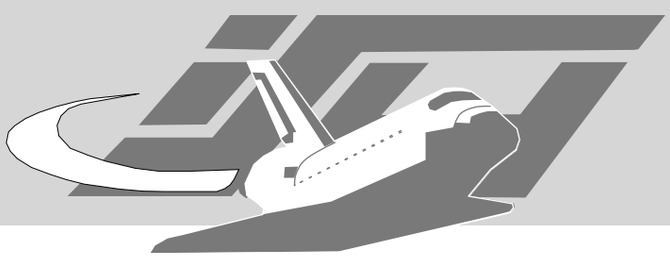


fpdns

- Seems still maintained
- Decision Tree - hardcoded
- http://www.rfc.se/fpdns/

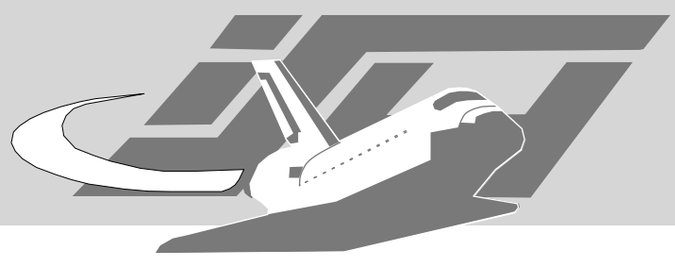
Terminal – RedTeam@RWTH

```
% perl5.8.5 fpdns.pl 213.221.113.105
fingerprint (213.221.113.105, 213.221.113.105): q0tq0tq7tq6r?query timed out
% perl5.8.5 fpdns.pl b.23.nu
% perl5.8.5 fpdns.pl afingerprint (b.23.nu, 213.221.87.134): q0tq0tq7tq6r?query timed
out
% perl5.8.5 fpdns.pl a.ns.tosses.info
fingerprint (a.ns.tosses.info, 80.190.253.213): TinyDNS 1.05
% perl5.8.5 fpdns.pl server-charta.charta.de
fingerprint (server-charta.charta.de, 194.231.10.10): q0tq0tq7tq6r?query timed out
% perl5.8.5 fpdns.pl PCE-net5.ffm.revmap.vianetworks.de
fingerprint (PCE-net5.ffm.revmap.vianetworks.de, 194.231.12.5): BIND 9.2.3rc1 -- 9.4.0a0
% perl5.8.5 fpdns.pl xdsl-195-14-221-219.netcologne.de
fingerprint (xdsl-195-14-221-219.netcologne.de, 195.14.221.219): BIND 8.3.0-RC1 -- 8.4.4
[recursion enabled]
% perl5.8.5 fpdns.pl -f xdsl-195-14-221-219.netcologne.de
fingerprint (xdsl-195-14-221-219.netcologne.de, 195.14.221.219): BIND 8.3.0-RC1 -- 8.4.4
[recursion enabled] id: "NetCologne Nameserver V0.98rc2"
% perl5.8.5 fpdns.pl -fd xdsl-195-14-221-219.netcologne.de
fingerprint (xdsl-195-14-221-219.netcologne.de, 195.14.221.219): BIND 8.3.0-RC1 -- 8.4.4
[recursion enabled] id: "NetCologne Nameserver V0.98rc2"
% perl5.8.5 fpdns.pl 194.231.15.8
fingerprint (194.231.15.8, 194.231.15.8): BIND 4.9.3 -- 4.9.11
% perl5.8.5 fpdns.pl -f 194.231.14.74
fingerprint (194.231.14.74, 194.231.14.74): BIND 9.1.0 -- 9.1.3 [recursion enabled] id:
"1.0a"
% perl5.8.5 fpdns.pl -f 194.231.15.8
fingerprint (194.231.15.8, 194.231.15.8): BIND 4.9.3 -- 4.9.11 id unavailable (SERVFAIL)
```



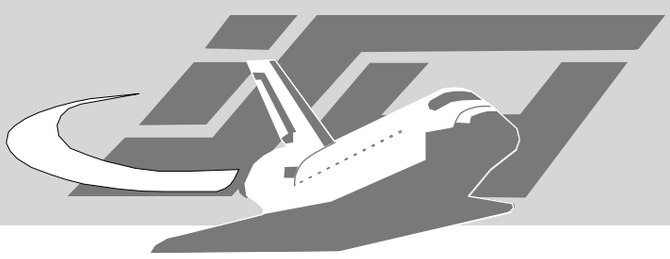
Multicast DNS

- mDNS, Zeroconf, Rendezvous, IPv4ll
- Overview at http://www.dotlocal.org/



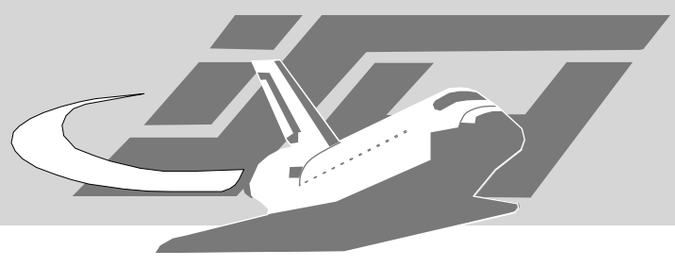
Terminal – RedTeam@RWTH

```
% dig @127.0.0.1 -p 5353 c0ldcut.local ANY

; <<>> DiG 9.2.2 <<>> @127.0.0.1 -p 5353 c0ldcut.local ANY
;; global options:  printcmd
;; connection timed out; no servers could be reached
```



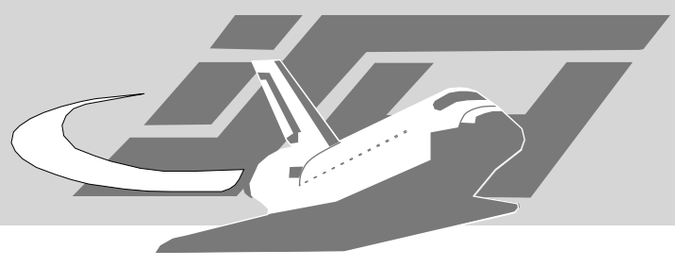
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 c0ldcut.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 c0ldcut.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51530
;; flags: qr aa; QUERY: 1, ANSWER: 4, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;c0ldcut.local.                 IN      ANY

;; ANSWER SECTION:
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      HINFO   "PowerBook3,5" "Mac OS X 10.3.5
(7M34), mDNSResponder-58.8 (Apr 24 2004 20:38:40)"
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:
3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

;; Query time: 10 msec
;; SERVER: 213.221.113.110#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:14:32 2004
;; MSG SIZE  rcvd: 194
```



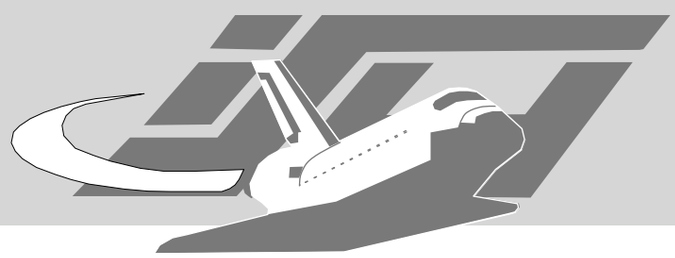
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _ssh._tcp.local ANY
[...]
;; ANSWER SECTION:
_ssh._tcp.local.        10      IN      PTR     c0ldcut._ssh._tcp.local.

;; ADDITIONAL SECTION:
c0ldcut._ssh._tcp.local. 10     IN      SRV     0 0 22 c0ldcut.local.
c0ldcut._ssh._tcp.local. 10     IN      TXT     ""
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110
[...]

% dig @224.0.0.251 -p 5353 _workstation._tcp.local ANY
[...]
;; ANSWER SECTION:
_workstation._tcp.local. 10     IN      PTR     c0ldcut\032[00:0a:95:74:c8:
6c]._workstation._tcp.local.

;; ADDITIONAL SECTION:
c0ldcut\032[00:0a:95:74:c8:6c]._workstation._tcp.local. 10 IN SRV 0 0 9 c0ldcut.local.
c0ldcut\032[00:0a:95:74:c8:6c]._workstation._tcp.local. 10 IN TXT ""
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110
[...]
```



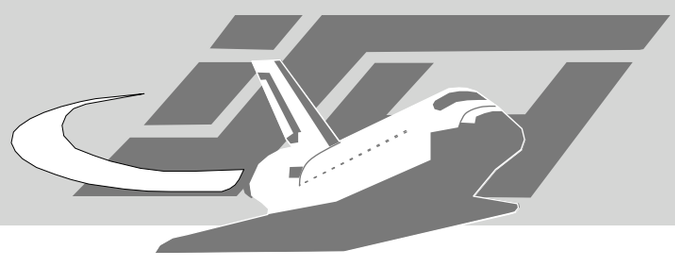
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _daap._tcp.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 _daap._tcp.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 35886
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;_daap._tcp.local.              IN      ANY

;; ANSWER SECTION:
_daap._tcp.local.       10      IN      PTR     c0recut._daap._tcp.local.

;; ADDITIONAL SECTION:
c0recut._daap._tcp.local. 10    IN      SRV     0 0 3689 c0ldcut.local.
c0recut._daap._tcp.local. 10    IN      TXT     "txtvers=1" "Version=196608" "iTSh
Version=131073" "Machine ID=7A4A0823922E" "Database ID=0C31E560278D9926" "Machine
Name=c0recut" "Password=false"
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

;; Query time: 56 msec
;; SERVER: 213.221.113.110#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:26:40 2004
;; MSG SIZE  rcvd: 302
```



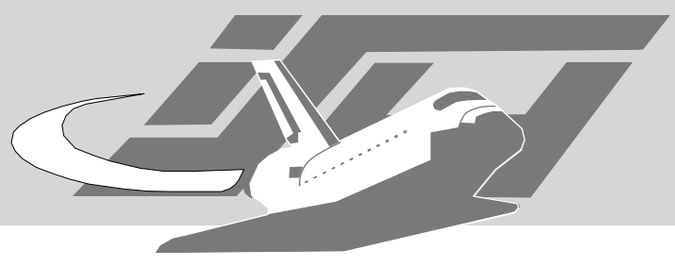
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _see._tcp.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 _see._tcp.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56258
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;_see._tcp.local.               IN      ANY

;; ANSWER SECTION:
_see._tcp.local.        10      IN      PTR     md\@c0ldcut._see._tcp.local.

;; ADDITIONAL SECTION:
md\@c0ldcut._see._tcp.local. 10 IN      SRV     0 0 6942 c0ldcut.local.
md\@c0ldcut._see._tcp.local. 10 IN      TXT     "txtvers=1" "name=Maximillian Dornseif"
"userid=79CD5CC7-C880-11D8-B621-000A9574C86C" "version=2"
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

;; Query time: 114 msec
;; SERVER: 213.221.113.110#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:33:00 2004
;; MSG SIZE  rcvd: 260
```



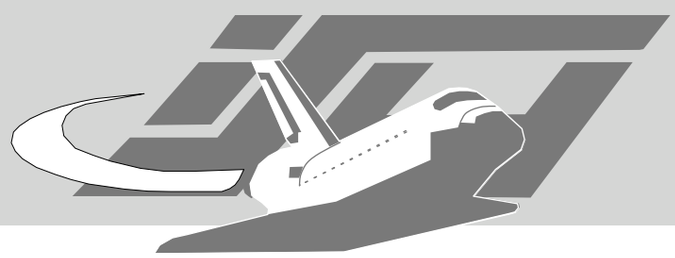
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _raop._tcp.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 _raop._tcp.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28064
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 3

;; QUESTION SECTION:
;_raop._tcp.local.              IN      ANY

;; ANSWER SECTION:
_raop._tcp.local.       10      IN      PTR     00112404FE57\@Mathilde._raop._tcp.local.

;; ADDITIONAL SECTION:
00112404FE57\@Mathilde._raop._tcp.local. 10 IN SRV 0 0 5000 Mathilde.local.
00112404FE57\@Mathilde._raop._tcp.local. 10 IN TXT "txtvers=1" "vn=3" "pw=false" "sr=44100" "ss=16"
"ch=2" "cn=1" "et=1" "ek=1" "sv=false" "sm=false"
Mathilde.local.         10      IN      A       213.221.113.120

;; Query time: 85 msec
;; SERVER: 213.221.113.120#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:34:54 2004
;; MSG SIZE  rcvd: 204
```



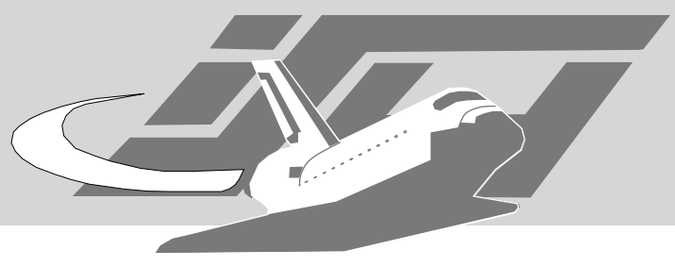
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _dpap._tcp.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 _dpap._tcp.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 24769
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;_dpap._tcp.local.              IN      ANY

;; ANSWER SECTION:
_dpap._tcp.local.       10      IN      PTR     Maximillian\032Dornseif's\032Photos._dpap._tcp.local.

;; ADDITIONAL SECTION:
Maximillian\032Dornseif's\032Photos._dpap._tcp.local. 10 IN SRV 0 0 8770 c0ldcut.local.
Maximillian\032Dornseif's\032Photos._dpap._tcp.local. 10 IN TXT "txtvers=1" "Version=65536" "Machine
Name=Maximillian Dornseif's Photos" "Password=true"
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

;; Query time: 40 msec
;; SERVER: 213.221.113.110#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:37:40 2004
;; MSG SIZE  rcvd: 271
```



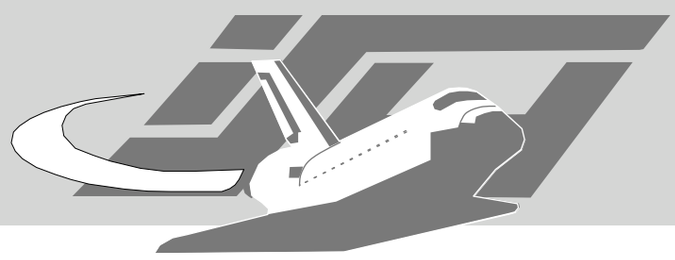
Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _netbios-ssn._tcp.local ANY | grep -v ";"
_netbios-ssn._tcp.local. 10     IN      PTR     c0ldcut._netbios-ssn._tcp.local.
c0ldcut._netbios-ssn._tcp.local. 10 IN  SRV     0 0 139 c0ldcut.local.
c0ldcut._netbios-ssn._tcp.local. 10 IN  TXT     ""
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

% dig @224.0.0.251 -p 5353 _ftp._tcp.local ANY | grep -v ";"
_ftp._tcp.local.        10      IN      PTR     c0ldcut._ftp._tcp.local.
c0ldcut._ftp._tcp.local. 10     IN      SRV     0 0 21 c0ldcut.local.
c0ldcut._ftp._tcp.local. 10     IN      TXT     ""
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

% dig @224.0.0.251 -p 5353 _eppc._tcp.local ANY | grep -v ";"
_eppc._tcp.local.       10      IN      PTR     c0ldcut._eppc._tcp.local.
c0ldcut._eppc._tcp.local. 10    IN      SRV     0 0 3031 c0ldcut.local.
c0ldcut._eppc._tcp.local. 10    IN      TXT     ""
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

% dig @224.0.0.251 -p 5353 _airport._tcp.local ANY | grep -v ";"
_airport._tcp.local.    10      IN      PTR     karl._airport._tcp.local.
karl._airport._tcp.local. 10    IN      SRV     0 0 5009 karl.local.
karl._airport._tcp.local. 10    IN      TXT     "waMA=00-03-93-E1-1C-0B,laMA=00-03-93-E1-1C
-0A,raMA=00-03-93-EC-24-06,syDs=Apple Base Station V5.1,syFl=0x00000000,syAP=3"
karl.local.             10      IN      A       213.221.113.116
```



Terminal – RedTeam@RWTH

```
% dig @224.0.0.251 -p 5353 _presence._tcp.local ANY

; <<>> DiG 9.2.2 <<>> @224.0.0.251 -p 5353 _presence._tcp.local ANY
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 28877
;; flags: qr aa; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 5

;; QUESTION SECTION:
;_presence._tcp.local.          IN      ANY

;; ANSWER SECTION:
_presence._tcp.local.   10      IN      PTR     md\@c0ldcut._presence._tcp.local.

;; ADDITIONAL SECTION:
md\@c0ldcut._presence._tcp.local. 10 IN SRV     0 0 5298 c0ldcut.local.
md\@c0ldcut._presence._tcp.local. 10 IN TXT     "txtvers=1" "last=Dornseif"
"phsh=b87277ed11f060039b0a83d2207a47437a4e94e3" "vc=A!" "1st=Maximillian"
"email=dornseif@informatik.rwth-aachen.de" "AIM=mdornseif@mac.com" "version=1" "msg=\226\143\142"
"status=avail" "port.p2pj=5298"
c0ldcut.local.          10      IN      AAAA    fe80::230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      AAAA    3ffe:bc0:861:1:230:65ff:fe0d:3bbb
c0ldcut.local.          10      IN      A       213.221.113.110

;; Query time: 30 msec
;; SERVER: 213.221.113.110#5353(224.0.0.251)
;; WHEN: Sun Sep 26 23:31:02 2004
;; MSG SIZE  rcvd: 376
```

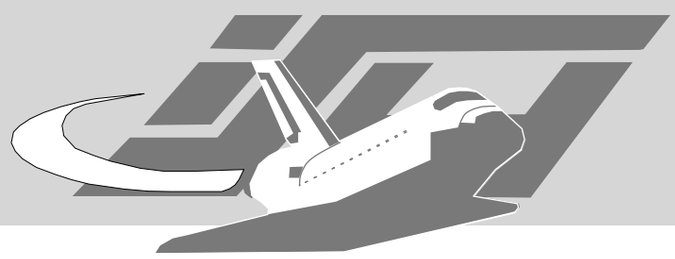


Internet Draft Multicast DNS 14th February 2004

4. IP TTL Checks

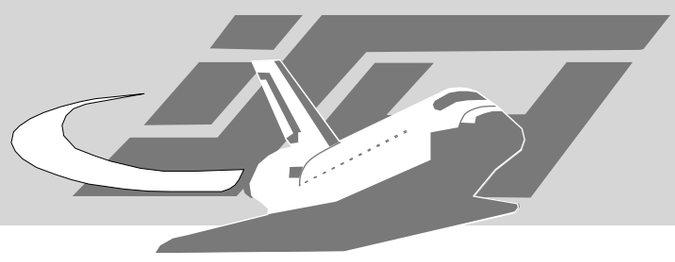
All Multicast DNS responses (including responses sent via unicast) MUST be sent with IP TTL set to 255.

A host sending Multicast DNS queries to a link-local destination address (including the 224.0.0.251 link-local multicast address) MUST verify that the IP TTL in response packets is 255, and silently discard any response packets where the IP TTL is not 255. Without this check, it could be possible for remote rogue hosts to send spoof answer packets (perhaps unicast to the victim host) which the receiving machine could misinterpret as having originated on the local link.



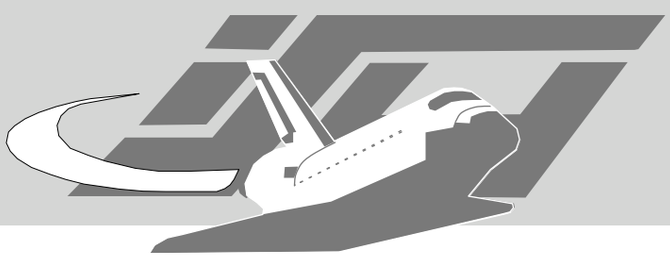
ike scan

- can identify certain firewalls
  - http://www.nta-monitor.com/ike-scan/



Conglomerates

- vmap - http://www.thc.org/download.php?t=r&f=vmap-0.6.tar.gz
  - http://c0re.23.nu/c0de/macosx/vmap-0.6-macosx.patch
- amap - http://www.thc.org/download.php?t=r&f=amap-4.7.tar.gz
- nmap - http://www.insecure.org/nmap/



amap

Terminal – RedTeam@RWTH

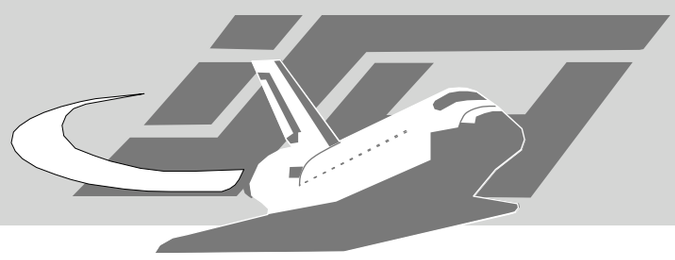
```
% amap untergrund.bewaff.net 21 22 25 80
amap v4.5 (www.thc.org) started at 2004-09-09 16:48:46 -
APPLICATION MAP mode

Protocol on 62.143.76.82:22/tcp matches ssh
Protocol on 62.143.76.82:22/tcp matches ssh-openssh
Protocol on 62.143.76.82:25/tcp matches nntp
Protocol on 62.143.76.82:25/tcp matches smtp
Protocol on 62.143.76.82:80/tcp matches http
Protocol on 62.143.76.82:80/tcp matches http-apache-2
Protocol on 62.143.76.82:21/tcp matches ftp
Protocol on 62.143.76.82:21/tcp matches smtp

Unidentified ports: none.

amap v4.5 finished at 2004-09-09 16:48:53
```

triggers

Terminal – RedTeam@RWTH

```
ftp:21:tcp:0:"USER AMAP\r\n"
ms-sql::udp:1:0x02
smtp:25:tcp:0:"HELO AMAP\r\n"
dns:53:udp:1:0x00 00 10 00 00 00 00 00 00 00 00 00 00
dns:53:tcp:1:0x00 0c 00 00 10 00 00 00 00 00 00 00 00 00
dns-bind:53:udp:1:
0x00 06 01 00 00 01 00 00 00 00 00 00 07 76 65 72 73 69 6f
6e 04 62 69 6e 64 00 00 10 00 03
ldap:389:tcp:1:0x30 0c 02 01 01 60 07 02 01 02 04 00 80 00
x-windows:6000:tcp:1:0x6c 00 0b
00 00 00 12 00 10 00 00 00 4d 49 54 2d 4d 41 47 49 43 2d
43 4f 4f 4b 49 45 2d  31 00 00 c6 17 34 b7 89 ed 65 c0 93 fd
d8 56 66 fa 52 40
```

from amap 4.6 - appdefs.trig



Terminal – RedTeam@RWTH

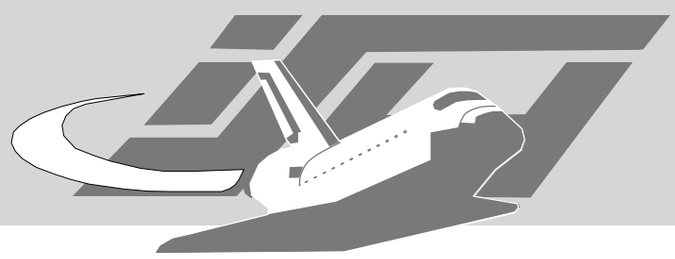
```
cvs::tcp::^cvs
cvs::tcp::cvs [pserver aborted]:
daytime-unix:::26:^[A-Z].* [A-Z].* [0-3].* [0-9][0-9]:[0-9][0-9]:[0-9][0-9] 200.\r\n
daytime-windows:::26-50:^[A-Z][a-z]+, [A-Z][a-z]+ [0-9]+, 200[0-9] [0-9]+:[0-9]+:[0-9]+\x0a\x00
daytime-unix:::20,36:^[A-Z][a-z]+ [A-Z][a-z]+ [0-9 ][0-9] [0-9]+:[0-9]+:[0-9]+ 200[0-9]\x0d\x0a
dns::::\x80\x81\x00
dns::::^\x00\x00\x90
dns-bind:dns:udp::^\x00\x00\x90\x01
dns-bind9:dns-bind:udp::^...[\x00-\x7e].........................\xc0
dns-bind8:dns-bind:udp::^...[\x00-\x7e].........................[^\xc0]
dns-djb:dns-bind:udp::^...[\x80-\x83].*version.bind
dns-djb::udp::^\x79\x08\x80\x80\x00\x01\x00\x00\x00\x0d
dns-ms:dns:udp::^\x00\x00\x90\x04
dns-ms:netbios-session:udp::^\x79\x08.*a.root-servers.net\x00
eggdropp::tcp::\(Eggdrop
finger::tcp::Line     User
finger::tcp::Login name:
finger::tcp::Login.*Name.*TTY.*Idle
finger::tcp::^No one logged on
finger::tcp::^\r\nWelcome
finger::tcp::^finger:
finger::tcp::^must provide username
finger::tcp::finger: GET:
ftp:ftp:tcp::^220.*\n331
ftp:ftp:tcp::^220.*\n530
ftp::tcp::^220.*FTP
ftp::tcp::^220 .* Microsoft .* FTP
http::tcp::^Invalid requested URL
http-apache-1::tcp::^HTTP/.*\nServer: Apache/1
http-apache-2::tcp::^HTTP/.*\nServer: Apache/2
http-cups::tcp::^HTTP/.*\nServer: CUPS/
http-hp-jet-direct::tcp::^HTTP/.*<title>Not supported</title>
```

from amap 4.6 - appdefs.resp

nmap

Terminal – RedTeam@RWTH

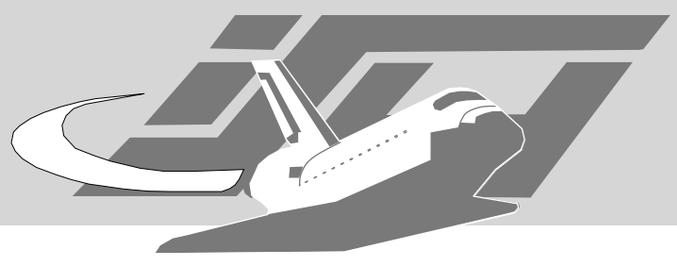
```
 nmap -sV -T4 untergrund.bewaff.net

Starting nmap 3.70 ( http://www.insecure.org/nmap/ ) at 2004-09-27 01:36 CEST
Interesting ports on ip82.76.1311A-CUD12K-01.ish.de (62.143.76.82):
(The 1652 ports scanned but not shown below are in state: closed)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              WU-FTPD 6.00LS
22/tcp    open  ssh              OpenSSH 3.5p1 (protocol 1.99)
25/tcp    open  smtp             qmail smtpd
80/tcp    open  http             Apache httpd 2.0.50 ((FreeBSD) DAV/2)
113/tcp   open  auth?
4000/tcp  open  remoteanything?
8080/tcp  open  http             Jetty httpd 4.1.4 (FreeBSD 4.10-STABLE i386)
31337/tcp open  Elite?
```



- Fyodor: “nmap Version Scanning” - http://www.insecure.org/nmap/versionscan.html

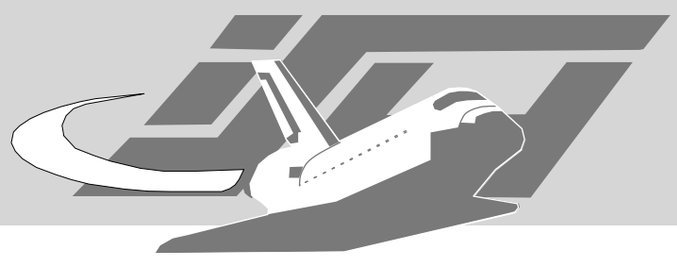
```
# This is the NULL probe that just compares any banners given to us
##############################NEXT PROBE##############################
Probe TCP NULL q||
# Wait for at least 5 seconds for data.  Otherwise an Nmap default is used.
totalwaitms 5000

match aim m|^\*\x01..\0\x04\0\0\0\x01$|s v/Pyboticide AIM chat filter///
# arkstats (part of arkeia-light 5.1.12 Backup server) on Linux 2.4.20
match arkstats m|^\0`\0\x03\0\0\0\x1810\x000\x000\x00852224\0\0\0\0\0\0\0\0\0\0| v/
Arkeia arkstats///
match backdoorjeam m|^220 jeem\.mail\.pv ESMTP\r\n| v/Jeem backdoor//**BACKDOOR**/
# Bittorrent Client 3.2.1b on Linux 2.4.X
match bittorent m|^\x13BitTorrent protocol\0\0\0\0\0\0\0\0| v/Bittorrent P2P client///

match ftp m/^220.*Welcome to PureFTPd (\d\S+)/ v/PureFTPd/$1//
match ssh m/^SSH-([.\d]+)-OpenSSH_(\S+)/ v/OpenSSH/$2/protocol $1/
match mysql m/^.\0\0\0\n(4\.[-.\w]+)\0...\0/s v/MySQL/$1//
match ssc-agent m|^\0\x1e\0\x06\0\t\0\0$| v/Novell Netware ssc-agent///
match chargen m|@ABCDEFGHIJKLMNOPQRSTUVWXYZ

softmatch ftp m/^220 [-.\w ]+ftp.*\r\n$/i
softmatch smtp m|^220 [-.\w ]+SMTP.*\r\n|
softmatch pop3 m|^\+OK [-\[\]\(\)!,/+:<>@.\w ]+\r\n$
```

```
Probe TCP GetRequest q|GET / HTTP/1.0\r\n\r\n|
ports 70,79,80-85,88,113,139,143,280,497,515,540,554,631,783,993,995,1220,1503,2030,3052,3128,3372,3531,3689,5
000,5432,5800,5900,6699,7070,8000-8010,8080-8085,8888-8888,9090,9999,10000,10005,11371,13722,15000,40193,4711
sslports 443

# Kerio PF 4.0.11 unregistered - Service process (Port 44xxx?) on MS W2K SP4+
match keriopfservice m|^(HTTP/1\.0) 200 OK\r\nServer: Kerio Personal Firewall\r\n| v/Kerio PF 4 Service//$1/

match backupexecra m|^\xf6\xff\xff\xff\x10\0\0\0\0\0\0\0\0\0\0$| v/Veritas BackupExec Remote Agent///

match dantzretrospect m|^\0\xca\0\0\0\0\0\x04\0\0\0\0$| v/Dantz Retrospect/6.0//
match dnet-keyproxy m|^HTTP/1\.0 302 Found\r\nLocation: http://www\.distributed\.net/\r\n\r\n$| v/Distributed.

Probe TCP RTSPRequest q|OPTIONS / RTSP/1.0\r\n\r\n|
match rtsp m|^RTSP/1\.0 200 OK\r\nCSeq: 0\r\nDate: .*\r\nServer: RealServer Version (\d[-.\w]+) \(win32\)\r\n| v/
Realserver RTSP/$1/win32/
match rtsp m|^RTSP/1\.0 200 OK\r\n.*Server: RealMedia EncoderServer Version (\d[-.\w]+) \(win32\)\r\n|s v/
RealMedia EncoderServer/$1/win32/
match rtsp m|^RTSP/1\.0 200 OK\r\n.*Server: RealServer Version (\d[-.\w]+) \(([-.+\w]+)\)\r\n|s v/RealOne Server/
$1/platform: $2/
Net HTTP Keyproxy///
```



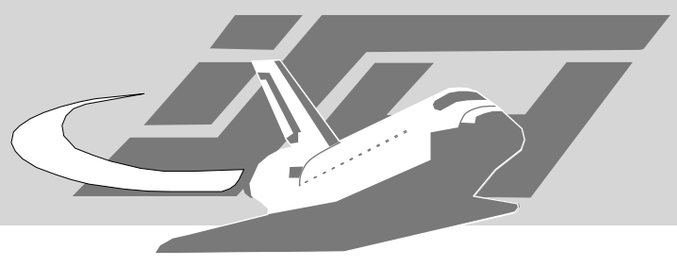
- User Enumeration
  - can lead to fingerprinting
  - helpful for brute forcing
- Vulnerability Assessment Tools
  - Nessus
  - Nikto

Fingerprinting
Fingerprinting



honeyd

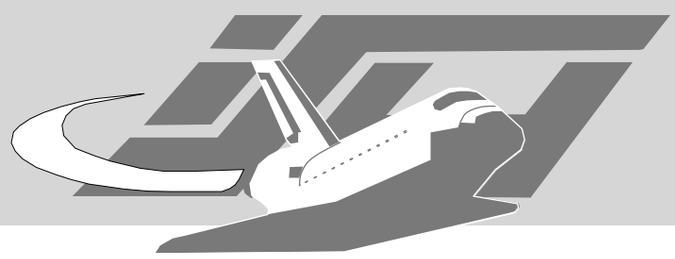
- IP stack simulator
- uses the databases fingerprinting tools to emulate IP-stacks
  - nmap, xprobe and p0f



honeyd xMAP

- Hacked by Thomas Apell
- Application emulation for for honeyd
- Using honeyd's Python plugins
- uses the databases of fingerprinting tools
  - vmap
  - amap, nmap are harder ...
- http://c0re.23.nu/c0de/misc/honeyd-vmap.py

Rethinking Fingerprinting

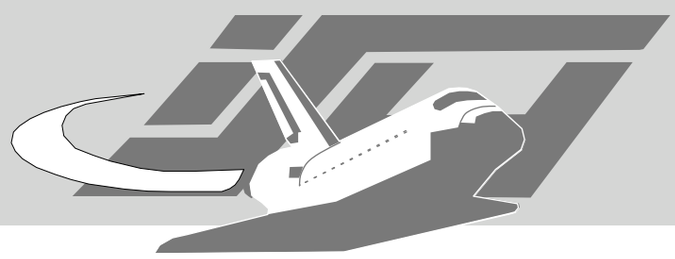


- fingerprints are more or less handcrafted
- learn from others who fingerprint:
  - e.g. people attacking anonymity systems
- George Danezis put his code, where his mouth is: http://c0re.23.nu/c0de/snap/xc0rr-snap-2004-12-29.tar.gz

```
% python xcorr.py -d headers/ ./test.txt
691 training files found
loading names... No /Users/md/Desktop/xcorr/headers/names.pbi name file found.
Building names database... done
Loading features ... [Errno 2] No such file or directory: '/Users/md/Desktop/xcorr/headers/
features.pbi'
No /Users/md/Desktop/xcorr/headers/features.pbi file found.
Building.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................finished
done
loading vectors ... No /Users/md/Desktop/xcorr/headers/vectors.pbi file found.
Building Vectors
database.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................................................
.....................................done
[...]
```

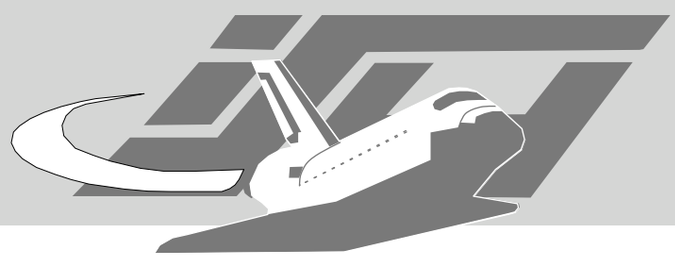
Terminal – RedTeam@RWTH

```
Top 20 features:
Content-Length: 13 - 7.23128700433
Server: Microsoft-IIS/6.0 - 6.14609773599
Set-Cookie: ASPSESSIONID - 5.88755225763
Cache-control: private - 5.77903467542
X-Powered-By: ASP.NET - 5.50512481759
Date: Mon, 27 Sep 2004 14:4 - 5.4519500551
Set-Cookie: ASP - 5.37498901396
[...]
Top 20 matches:
0.999280678295 - Microsoft-IIS/6.0 (xcorr/headers/out-199.txt)
0.849102347347 - Microsoft-IIS/6.0 (xcorr/headers/out-110.txt)
0.764737916816 - Microsoft-IIS/6.0 (xcorr/headers/out-1465.txt)
0.695353199053 - Microsoft-IIS/6.0 (xcorr/headers/out-1157.txt)
0.693628101034 - Microsoft-IIS/5.0 (xcorr/headers/out-105.txt)
0.686729823284 - Microsoft-IIS/6.0 (xcorr/headers/out-1343.txt)
0.680819650667 - Microsoft-IIS/5.0 (xcorr/headers/out-133.txt)
[...]
```



Things that broke while developmentt

- Minix ftpd
- Viking II DSL Router
- StupidFTPD
- atphttpd
- ...



Links

- http://del.icio.us/tag/fingerprinting