

The background of the image is a dark, star-filled space. In the upper right quadrant, the Earth is visible, showing its blue oceans and green continents against the black void. On the left side, the silhouettes of tall evergreen trees are visible against the dark sky.

PËÑËT®ÅTiØN TË\$TiÑG

βÅ\$ÌCØ\$

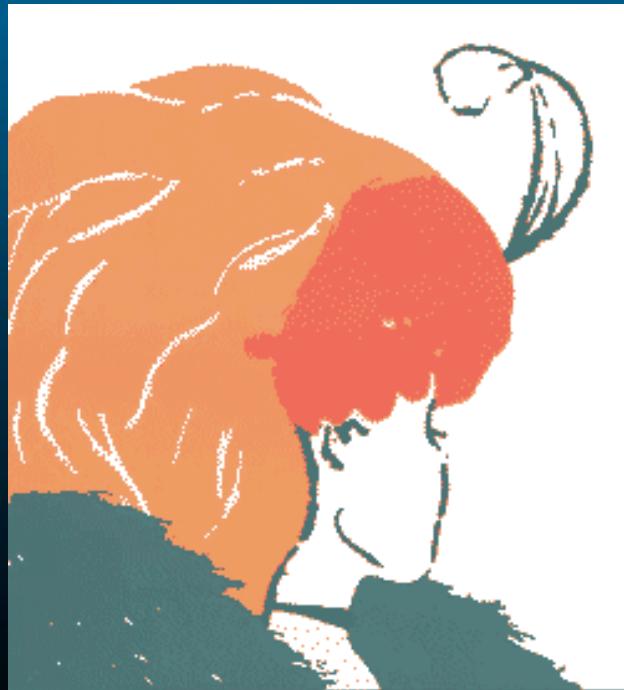
WHAT IS IT ?

- Often also called pen testing or 'ethical hacking"
- Methodology for identifying vulnerabilities of a particular system, application, network, or process
- Attempting to exploit those vulnerabilities to demonstrate that the security mechanisms can and will fail
- The non malicious usually get some small piece of proof and exit as quietly as they came

WHY DO WE DO IT ?

- Find poorly configured machines that you may have overlooked.
- Verify that your security mechanisms are working and test your incident response.
- Can be used to justify the need for an upgrade, bigger budget, or to validate risk assessments.

WHAT DO YOU SEE ?



- What you see is not always the truth
- KISS – Keep It Simple Stupid. Not always the most difficult route will get you in
- Know your Technologies as it will help

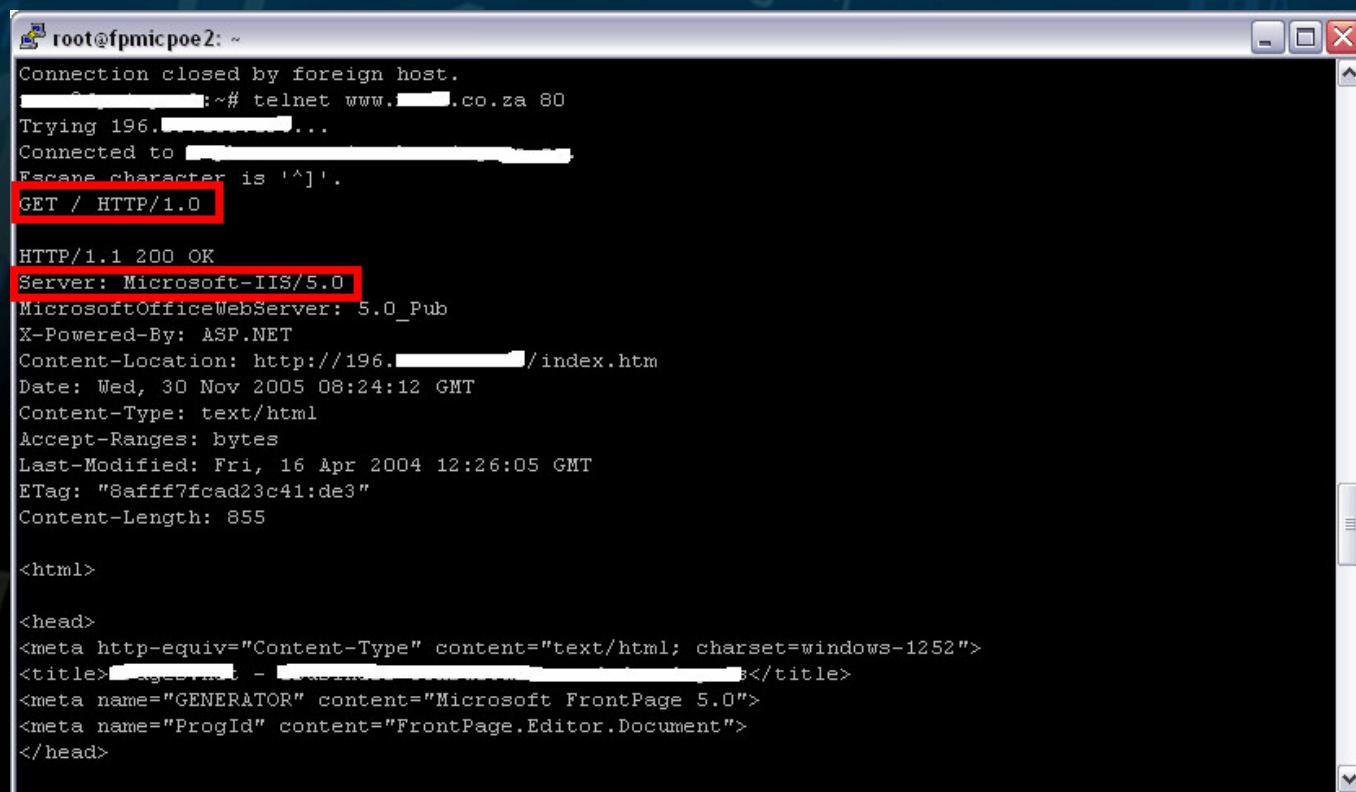
METHODOLOGY

The following are some of the major steps conducted during your testing

- Document **EVERYTHING**
- Recon / Foot printing
- Scanning
 - Enumeration
- Exploiting / Penetrating
 - Privilege escalation as required
- Data collection aka 'limited pillaging'
- Cleaning-Up
- Prepare & Deliver Report / Presentation

BANNER GRABBING

- Also know as Foot Printing
- Know the Platform you are attacking
 - Able to Google for vulnerabilities
 - Allows you to know what to look for



```
root@fpmicpoe2: ~
Connection closed by foreign host.
[REDACTED]:~# telnet www.[REDACTED].co.za 80
Trying 196.[REDACTED]...
Connected to [REDACTED]
Escape character is '^]'.
GET / HTTP/1.0

HTTP/1.1 200 OK
Server: Microsoft-IIS/5.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
Content-Location: http://196.[REDACTED]/index.htm
Date: Wed, 30 Nov 2005 08:24:12 GMT
Content-Type: text/html
Accept-Ranges: bytes
Last-Modified: Fri, 16 Apr 2004 12:26:05 GMT
ETag: "8afff7fcad23c41:de3"
Content-Length: 855

<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>[REDACTED] - [REDACTED]</title>
<meta name="GENERATOR" content="Microsoft FrontPage 5.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
</head>
```

BANNER GRABBING

HTTPPRINT

```
C:\>httpprint -h www.████.za -s signatures.txt
httpprint v0.200 (beta) - web server fingerprinting tool
(c) 2003, net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httpprint/
httpprint@net-square.com

Host: www.████.za is alive...
Finger Printing on http://www.████.za:80/
Derived Signature:
Microsoft-IIS/5.0
CD2698FD6ED3C295E4B1653082C10D64050C5D2594DF1BD04276E4BB630A04DB
0D7645B5811C9DC52A200B4C9D69031D6014C217811C9DC5811C9DC52655F350
FCCC535BE2CE69232E2CE69232FCD861AE2CE69272576B769E2CE6926CD2698FD
6ED3C295E2CE6920811C9DC5811C9DC568D17AAE68D17AAE2CE6923
6ED3C29568D17AAE732F670E2CE692768D17AAE

Banner Reported: Microsoft-IIS/5.0
Banner Deduced: Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/5.1
Scores:
Microsoft-IIS/5.0 ASP.NET: 144 86.75
Microsoft-IIS/5.1: 144 86.75
Microsoft-IIS/5.0: 139 77.11
Microsoft-IIS/4.0: 92 18.48
```

BANNER GRABBING

HTTPPRINT

The screenshot shows a Microsoft Internet Explorer window titled "httpprint web server fingerprinting report". The address bar shows the file path "C:\[REDACTED]\httpprintoutput.html". The title bar has a back button, forward button, stop button, and a search field with "Google" in it. Below the title bar is a menu bar with File, Edit, View, Favorites, Tools, and Help. The main content area features a logo on the left with the text "httpPrint" over a fingerprint pattern, and the text "web server fingerprinting report" on the right. Below this is a table with the following data:

host	port	ssl	banner reported	banner deduced	icon	confidence
www.[REDACTED].co.za	80		Microsoft-IIS/5.0	Microsoft-IIS/5.0 ASP.NET, Microsoft-IIS/5.1		<div style="width: 80%; height: 10px; background-color: blue;"></div>

At the bottom of the window, there is a footer bar with the "httpprint © 2003 net-square" logo.

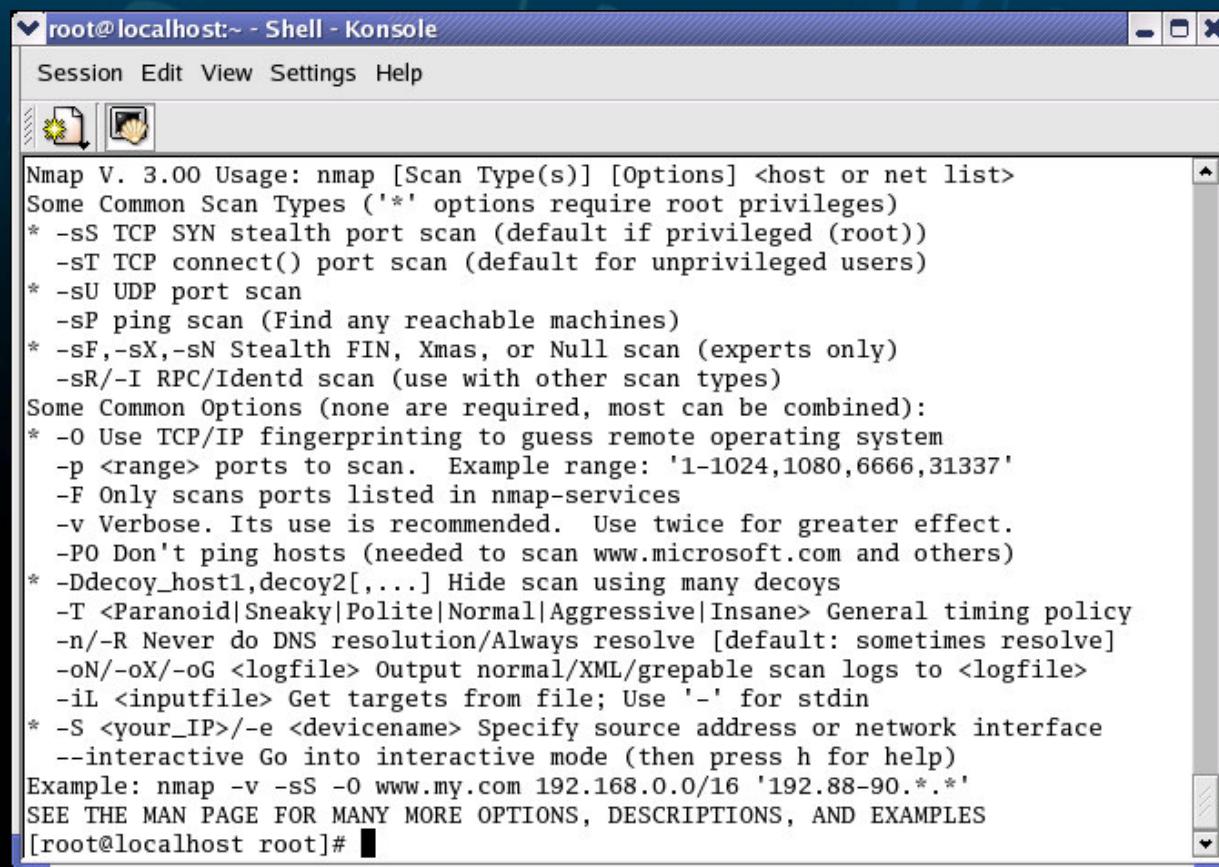
SMTP

```
[REDACTED]:~# telnet [REDACTED] 25
Trying 1[REDACTED]...
Connected to [REDACTED].
Escape character is '^]'.
220 [REDACTED] Microsoft ESMTP MAIL Service, Version: 6.0.3790.0 ready at Wed, 30 Nov 2005
10:52:32 +0200
```

TOOLS

Nmap

Sending a series of specially crafted packets to a target to identify open or listening UDP/TCP ports

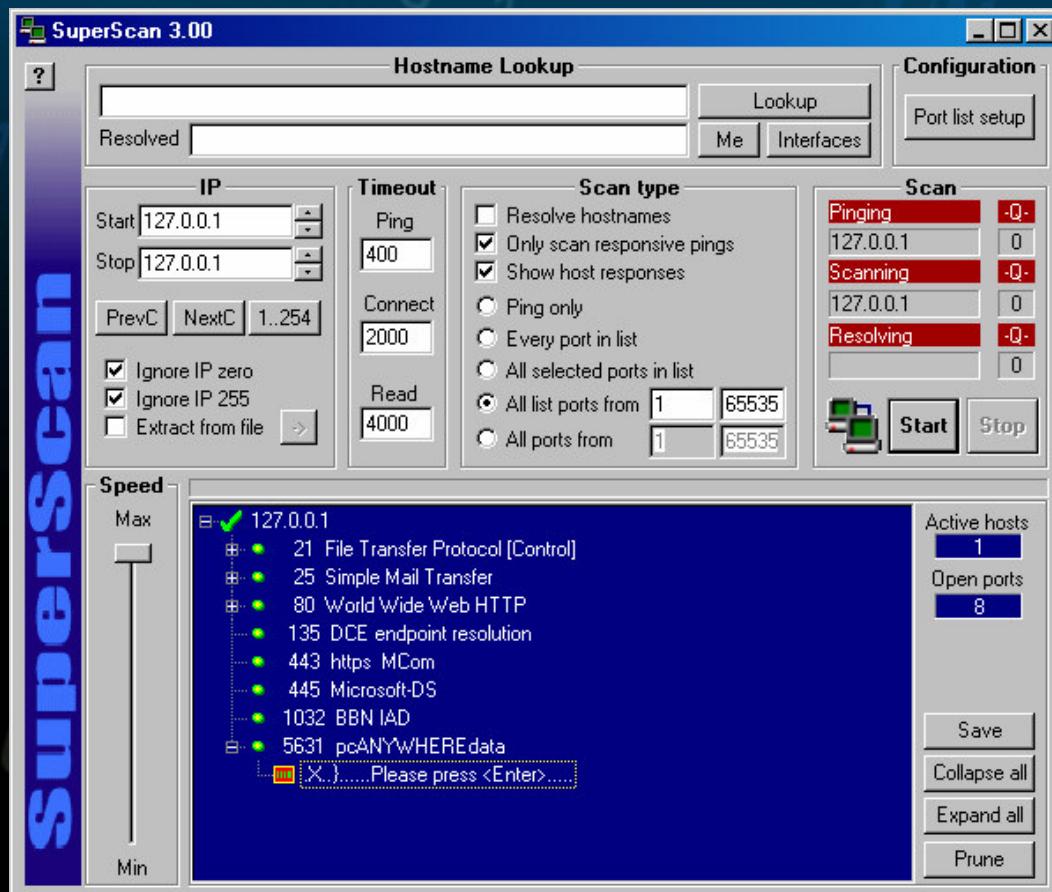


```
Nmap V. 3.00 Usage: nmap [Scan Type(s)] [Options] <host or net list>
Some Common Scan Types ('*' options require root privileges)
* -sS TCP SYN stealth port scan (default if privileged (root))
  -sT TCP connect() port scan (default for unprivileged users)
* -sU UDP port scan
  -sP ping scan (Find any reachable machines)
* -sF,-sX,-sN Stealth FIN, Xmas, or Null scan (experts only)
  -sR/-I RPC/Identd scan (use with other scan types)
Some Common Options (none are required, most can be combined):
* -O Use TCP/IP fingerprinting to guess remote operating system
  -p <range> ports to scan. Example range: '1-1024,1080,6666,31337'
  -F Only scans ports listed in nmap-services
  -v Verbose. Its use is recommended. Use twice for greater effect.
  -PO Don't ping hosts (needed to scan www.microsoft.com and others)
* -Ddecoy_host1,decoy2[,...] Hide scan using many decoys
  -T <Paranoid|Sneaky|Polite|Normal|Aggressive|Insane> General timing policy
  -n/-R Never do DNS resolution/Always resolve [default: sometimes resolve]
  -oN/-oX/-oG <logfile> Output normal/XML/grepable scan logs to <logfile>
  -iL <inputfile> Get targets from file; Use '-' for stdin
* -S <your_IP>/-e <devicename> Specify source address or network interface
  --interactive Go into interactive mode (then press h for help)
Example: nmap -v -sS -O www.my.com 192.168.0.0/16 '192.88-90.*.*'
SEE THE MAN PAGE FOR MANY MORE OPTIONS, DESCRIPTIONS, AND EXAMPLES
[root@localhost root]#
```

TOOLS

- SuperScan

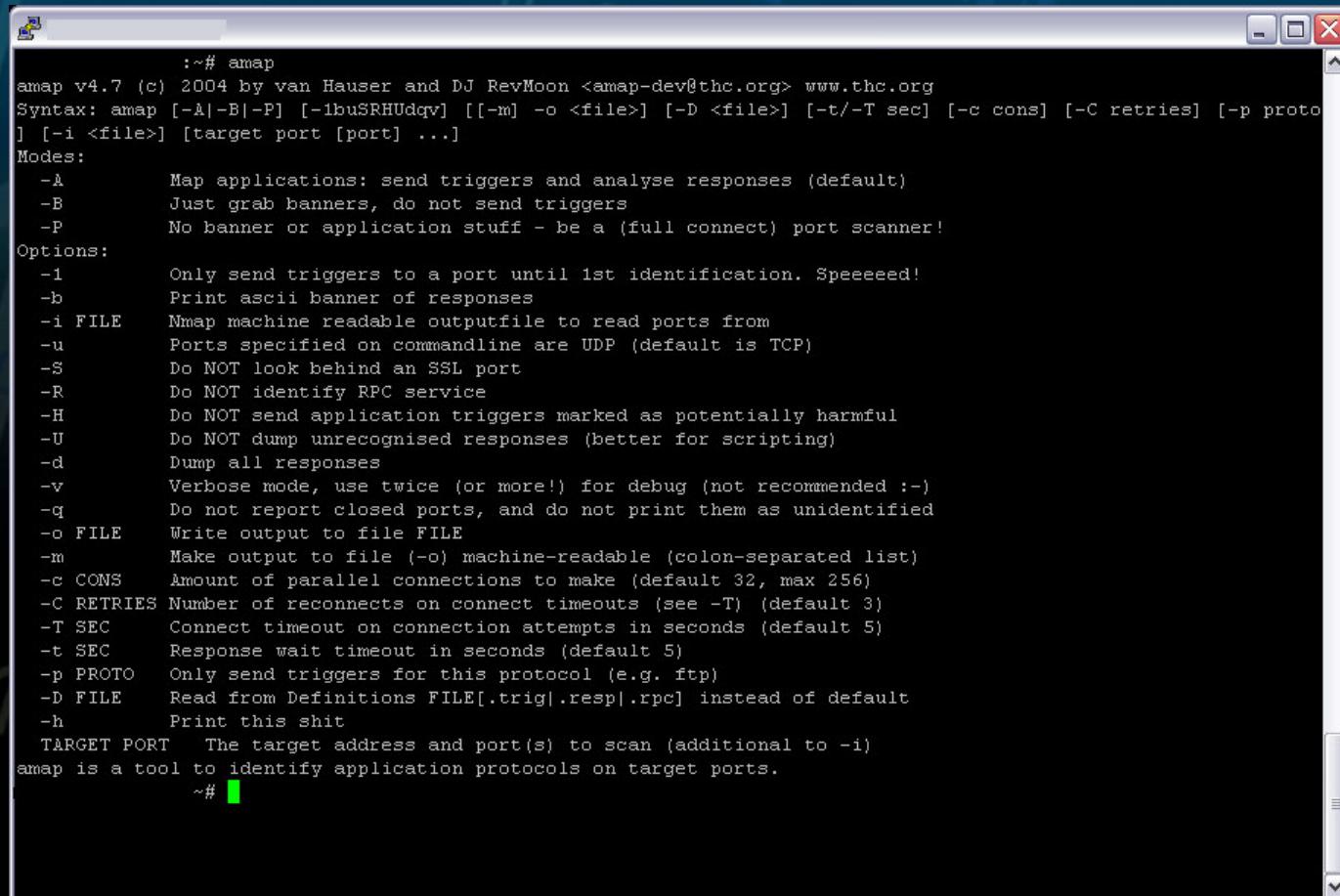
Microsoft Windows GUI



TOOLS

Amap

Can be used to help identify ports that have been changed. By specifying the port it can help identify the application associated to it.



```
:~# amap
amap v4.7 (c) 2004 by van Hauser and DJ RevMoon <amap-dev@thc.org> www.thc.org
Syntax: amap [-A|-B|-P] [-1buSRHUbqy] [[-m] -o <file>] [-D <file>] [-t/-T sec] [-c cons] [-C retries] [-p proto]
] [-i <file>] [target port [port] ...]
Modes:
-A      Map applications: send triggers and analyse responses (default)
-B      Just grab banners, do not send triggers
-P      No banner or application stuff - be a (full connect) port scanner!
Options:
-1      Only send triggers to a port until 1st identification. Speeeeed!
-b      Print ascii banner of responses
-i FILE Nmap machine readable outputfile to read ports from
-u      Ports specified on commandline are UDP (default is TCP)
-S      Do NOT look behind an SSL port
-R      Do NOT identify RPC service
-H      Do NOT send application triggers marked as potentially harmful
-U      Do NOT dump unrecognised responses (better for scripting)
-d      Dump all responses
-v      Verbose mode, use twice (or more!) for debug (not recommended :--)
-q      Do not report closed ports, and do not print them as unidentified
-o FILE Write output to file FILE
-m      Make output to file (-o) machine-readable (colon-separated list)
-c CONS Amount of parallel connections to make (default 32, max 256)
-C RETRIES Number of reconnects on connect timeouts (see -T) (default 3)
-T SEC Connect timeout on connection attempts in seconds (default 5)
-t SEC Response wait timeout in seconds (default 5)
-p PROTO Only send triggers for this protocol (e.g. ftp)
-D FILE Read from Definitions FILE[.trig|.resp|.rpc] instead of default
-h      Print this shit
TARGET PORT  The target address and port(s) to scan (additional to -i)
amap is a tool to identify application protocols on target ports.
~#
```

TOOLS

Nessus



- Open Source Vulnerability Scanner
- Engine requires a Linux server, client can be Linux or Microsoft Windows based
- Intelligent, assumes little, but uses what it learns as it scans
- Vendor neutral, so nothing is 'sugar coated' and recommended fixes don't point you towards their products

TOOLS

Nessus



- Review of results through Nessus GUI

View Session Results - RSA *

Vulnerabilities:

- smtp (25/tcp)
- snmp (161/udp)
- 192.168.1.104
 - ftp (21/tcp)
 - ftp (21/tcp)
 - ftp (21/tcp)
 - ftp (21/tcp)
 - general/tcp
 - general/tcp
 - kdm (1024/tcp)
 - kdm (1024/tcp)
 - NFS-or-IIS (1025/tcp)
 - NFS-or-IIS (1025/tcp)
 - NFS-or-IIS (1025/tcp)

192.168.1.102

Plugin information

Plugin ID: 10261
Sendmail mailing to programs

Vulnerability

smtp (25/tcp)
High severity

This vulnerability is false positive

Description:

The remote SMTP server did not complain when issued the command:
MAIL FROM: root@this_host
RCPT TO: |testing

This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary commands on this host.

*** This security hole might be a false positive, since
*** some MTAs will not complain to this test, but instead
*** just drop the message silently.

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0163

TOOLS

Netcat

- Simple Netcat connection between a Linux and Microsoft Windows machine.

```
[root@localhost root]# nc 192.168.1.100 53
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\netcat>dir c:\windows\system32\restore
dir c:\windows\system32\restore
 Volume in drive C is DRIVE_C
 Volume Serial Number is 201B-3C11

 Directory of c:\windows\system32\restore

10/12/2002 12:02 PM    <DIR>      .
10/12/2002 12:02 PM    <DIR>      ..
10/11/2002  06:03 PM           78 MachineGuid.txt
08/29/2002  05:41 AM        370,688 rstrui.exe
08/23/2001  07:00 AM        47,104 srdiag.exe
08/23/2001  07:00 AM         984 srframe.mmf
          4 File(s)     418,854 bytes
          2 Dir(s)   61,233,397,760 bytes free

C:\netcat>net statistics
net statistics
Statistics are available for the following running services:

      Server
      Workstation

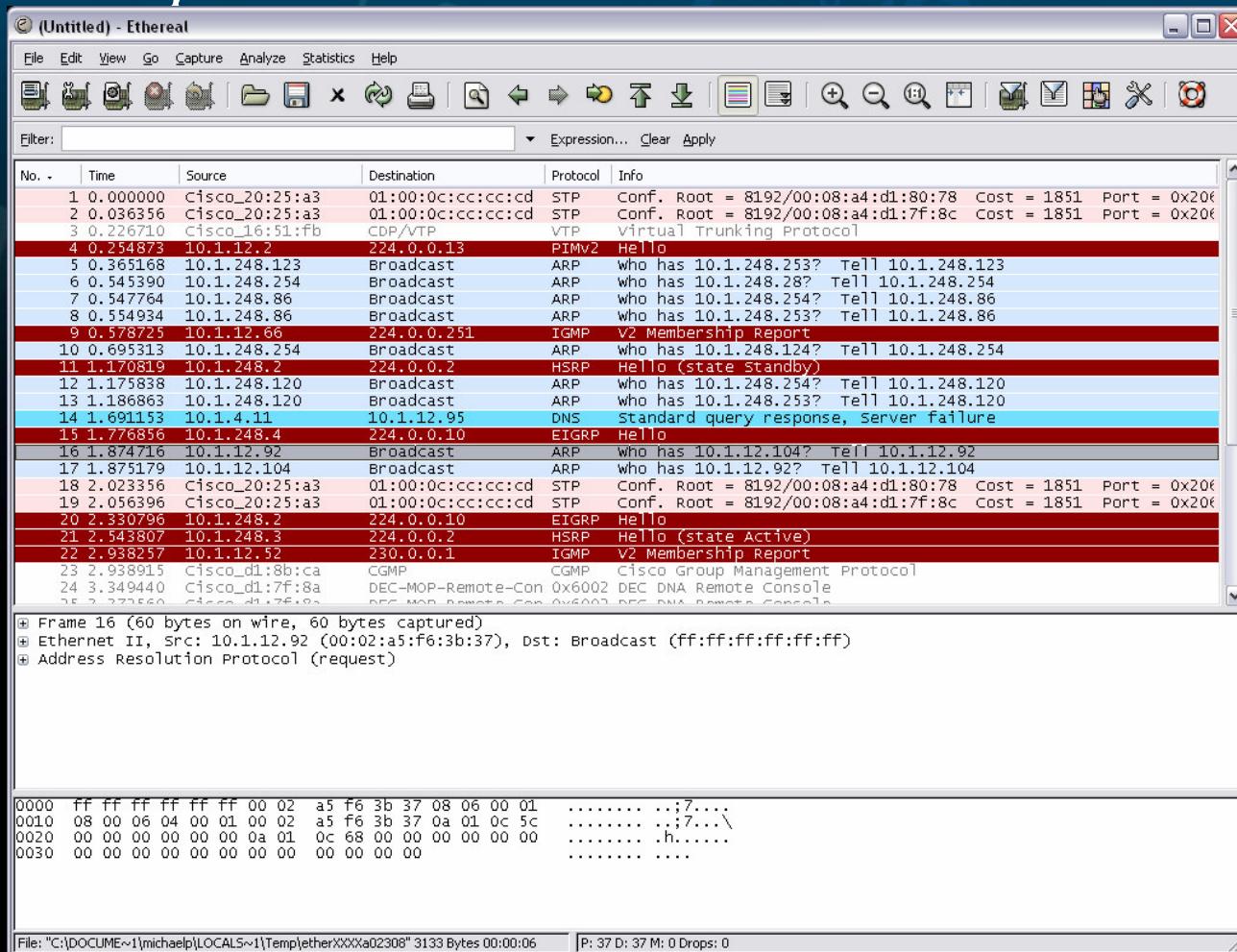
The command completed successfully.

C:\netcat>
```

TOOLS

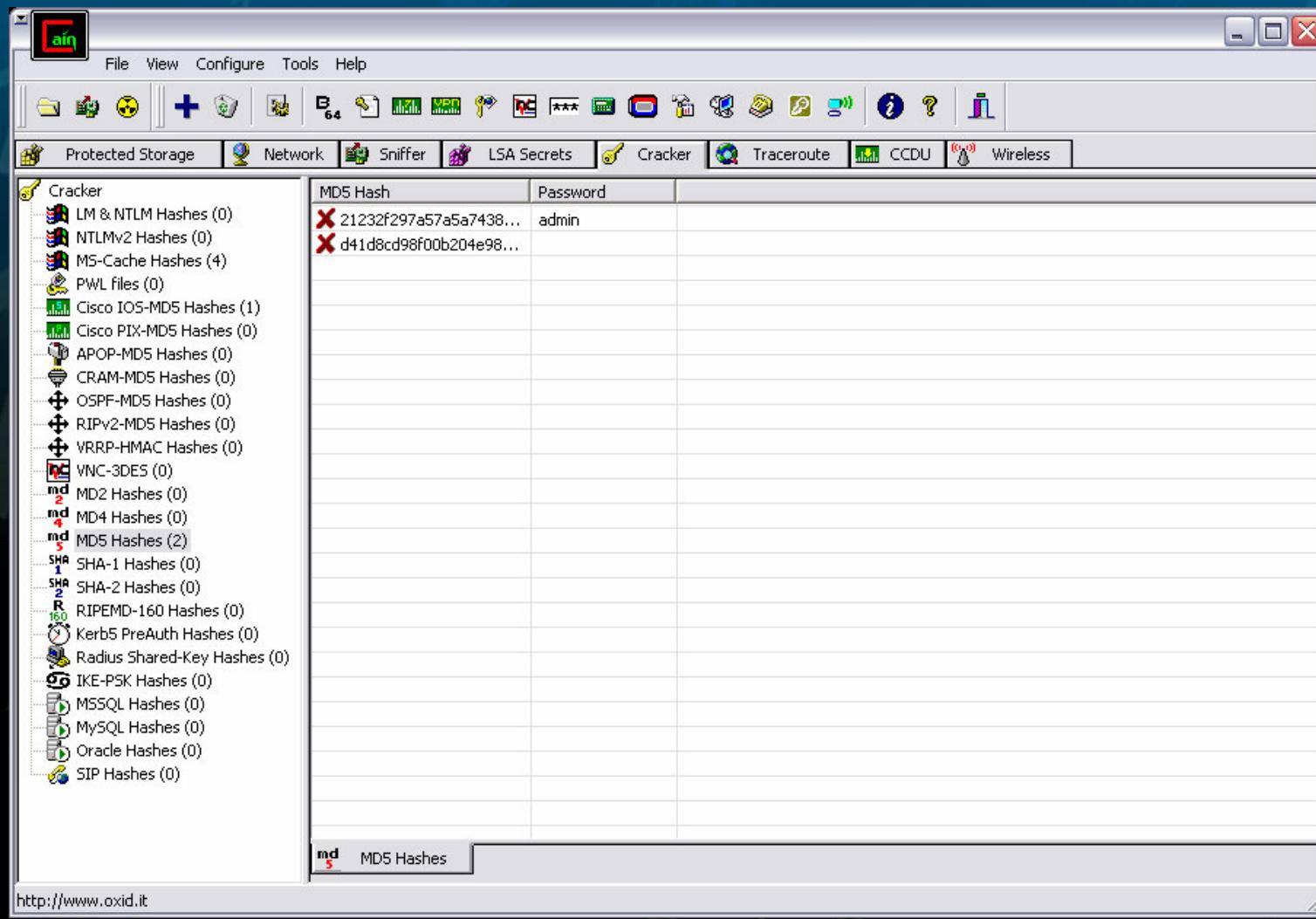
EtherReal

- Don't Believe what you see always get hands on and dirty



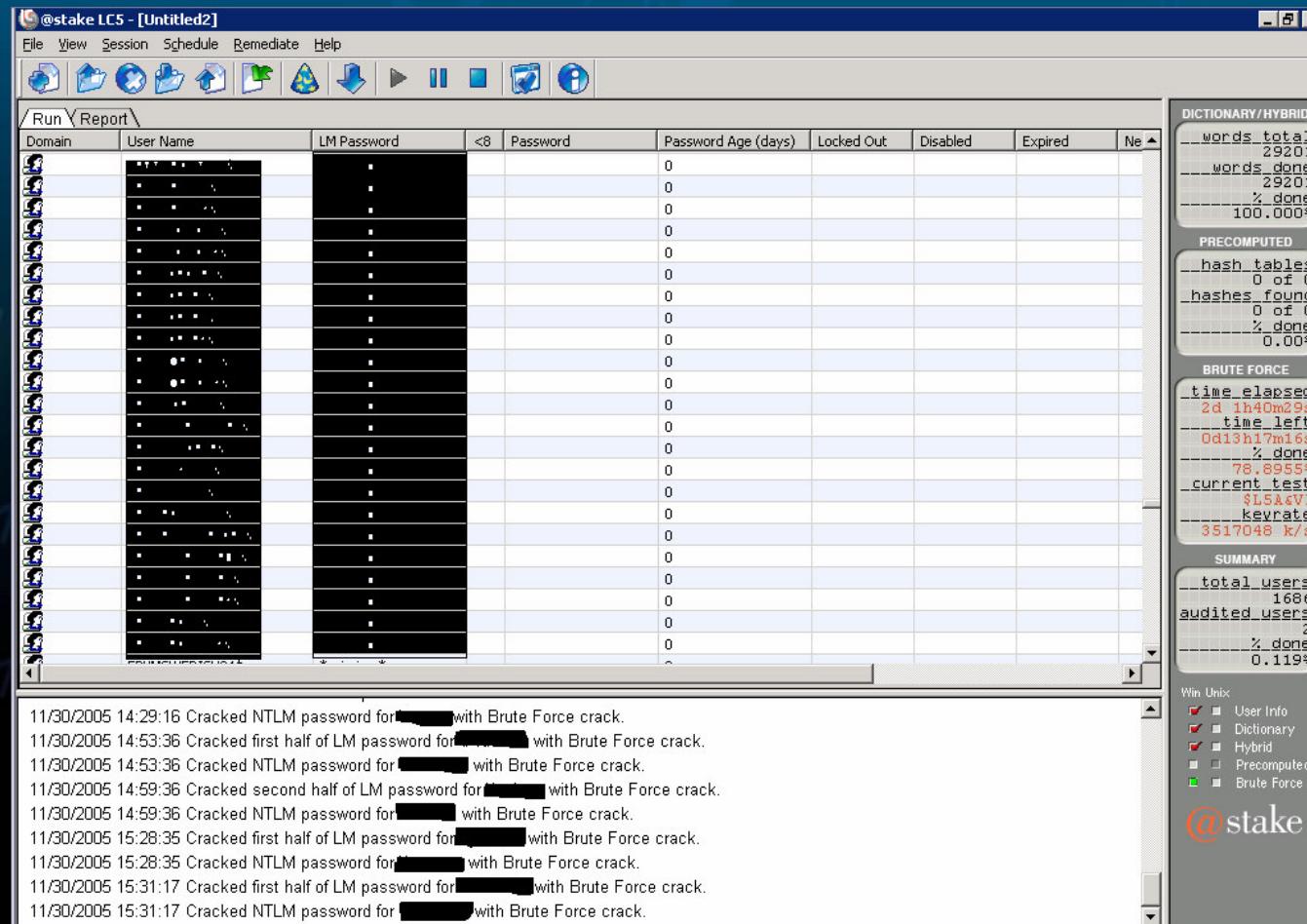
PASSWORD TOOLS

Cain and Abel



PASSWORD TOOLS

LophCrack



DEFINITION

Penetration Tests

A penetration test subjects a system to the real-world attacks selected and conducted by the testing personnel.

The benefit of a penetration test is to identify the extent to which a system can be compromised before the attack is identified and assess the response mechanisms effectiveness.

Penetration tests generally are not a comprehensive test of the system's security and should be combined with other independent diagnostic tests to validate the effectiveness of the security process.

QUESTIONS

