
ÞËÑËTRÅTiØÑ TË$TiÑG
ßÅ$i©$
digitalblasphemy.com

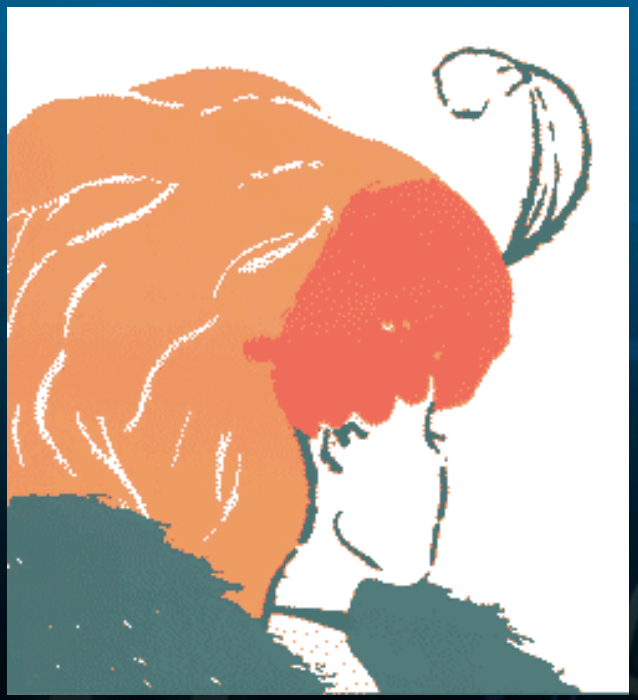
WHAT IS IT ?

- 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

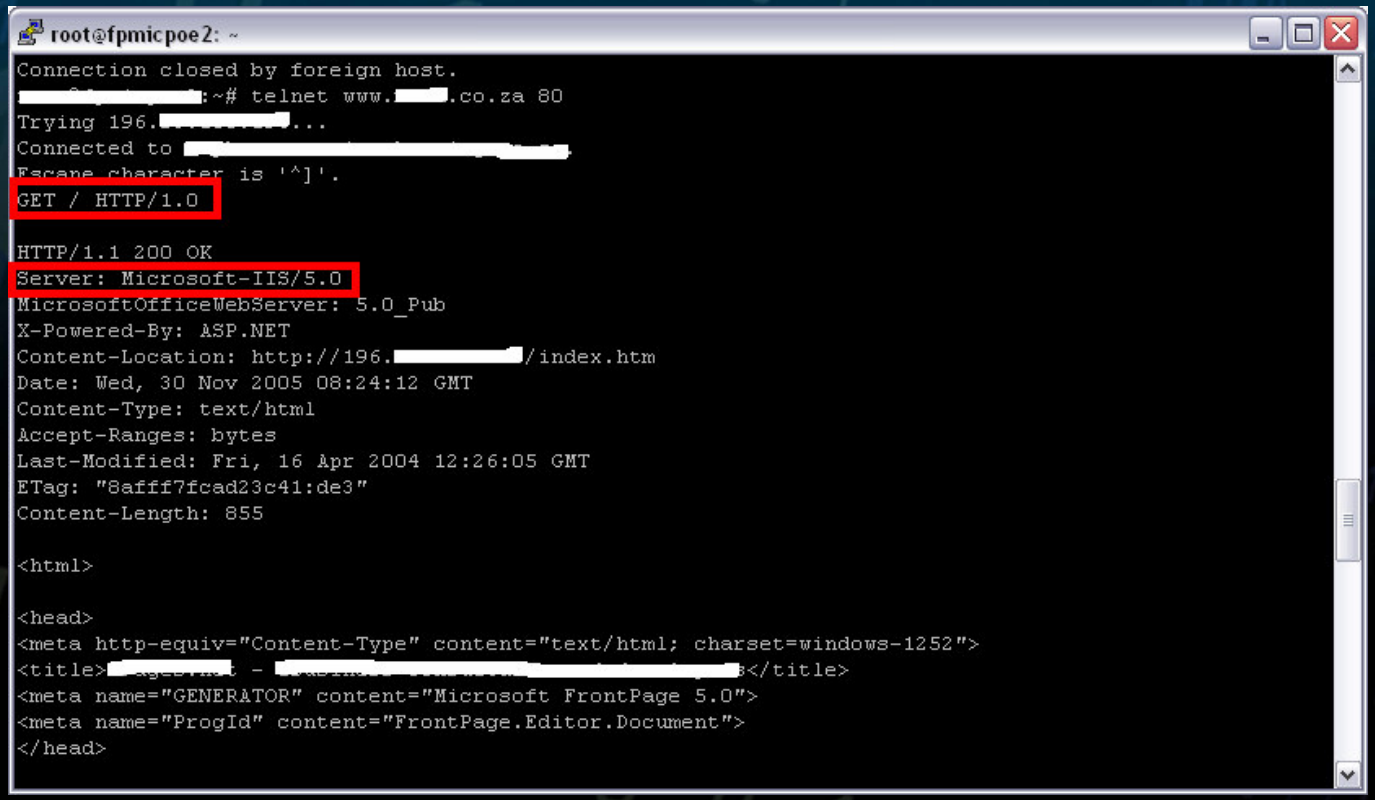
METHODOLOGY

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 vulnerabilies
  - Allows you to know what to look for



BANNER GRABBING

HTTPRINT

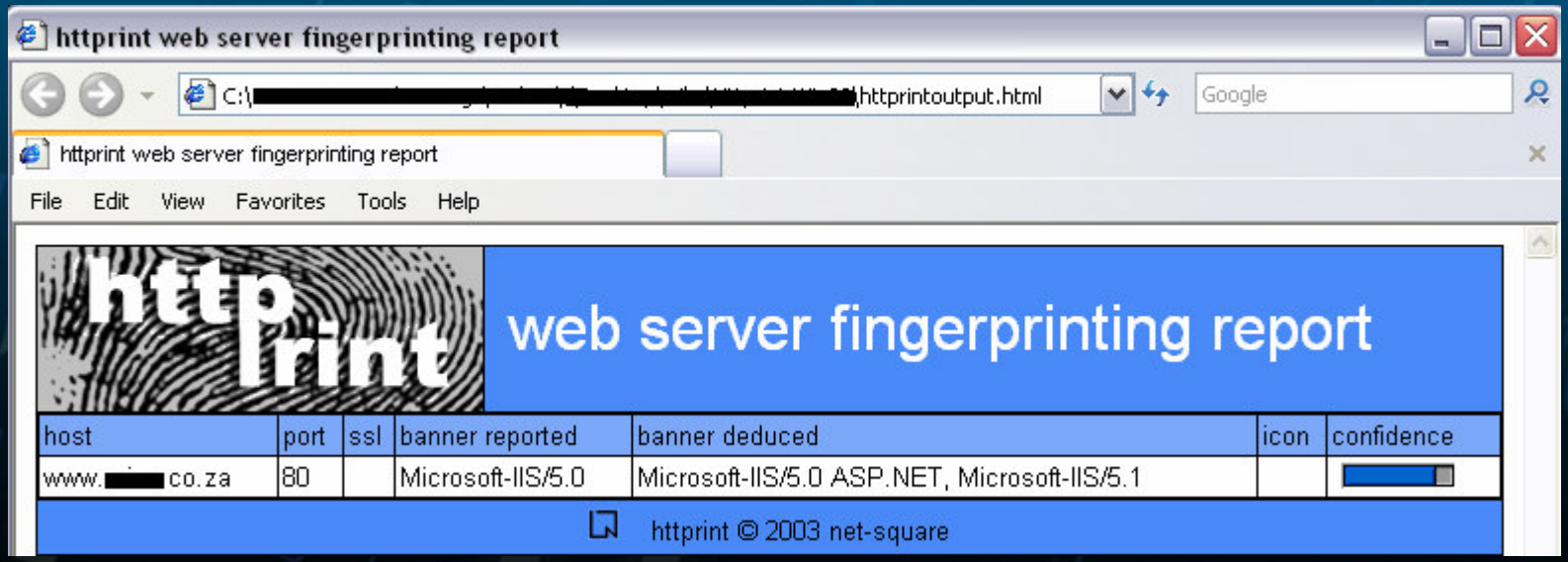
```
C:\[redacted]>httprint -h www.[redacted].za -s signatures.txt
httprint v0.200 (beta) - web server fingerprinting tool
(c) 2003, net-square solutions pvt. ltd. - see readme.txt
http://net-square.com/httprint/
httprint@net-square.com

---------------------------------------------------
Host: www.[redacted]co.za is alive...
Finger Printing on http://www.[redacted]co.za:80/
Derived Signature:
Microsoft-IIS/5.0
CD2698FD6ED3C295E4B1653082C10D64050C5D2594DF1BD04276E4BB630A04DB
0D7645B5811C9DC52A200B4C9D69031D6014C217811C9DC5811C9DC52655F350
FCCC535BE2CE6923E2CE69232FCD861AE2CE69272576B769E2CE6926CD2698FD
6ED3C295E2CE6920811C9DC5811C9DC5811C9DC568D17AAE68D17AAEE2CE6923
6ED3C29568D17AAEA732F670E2CE692768D17AAE

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

HTTPRINT

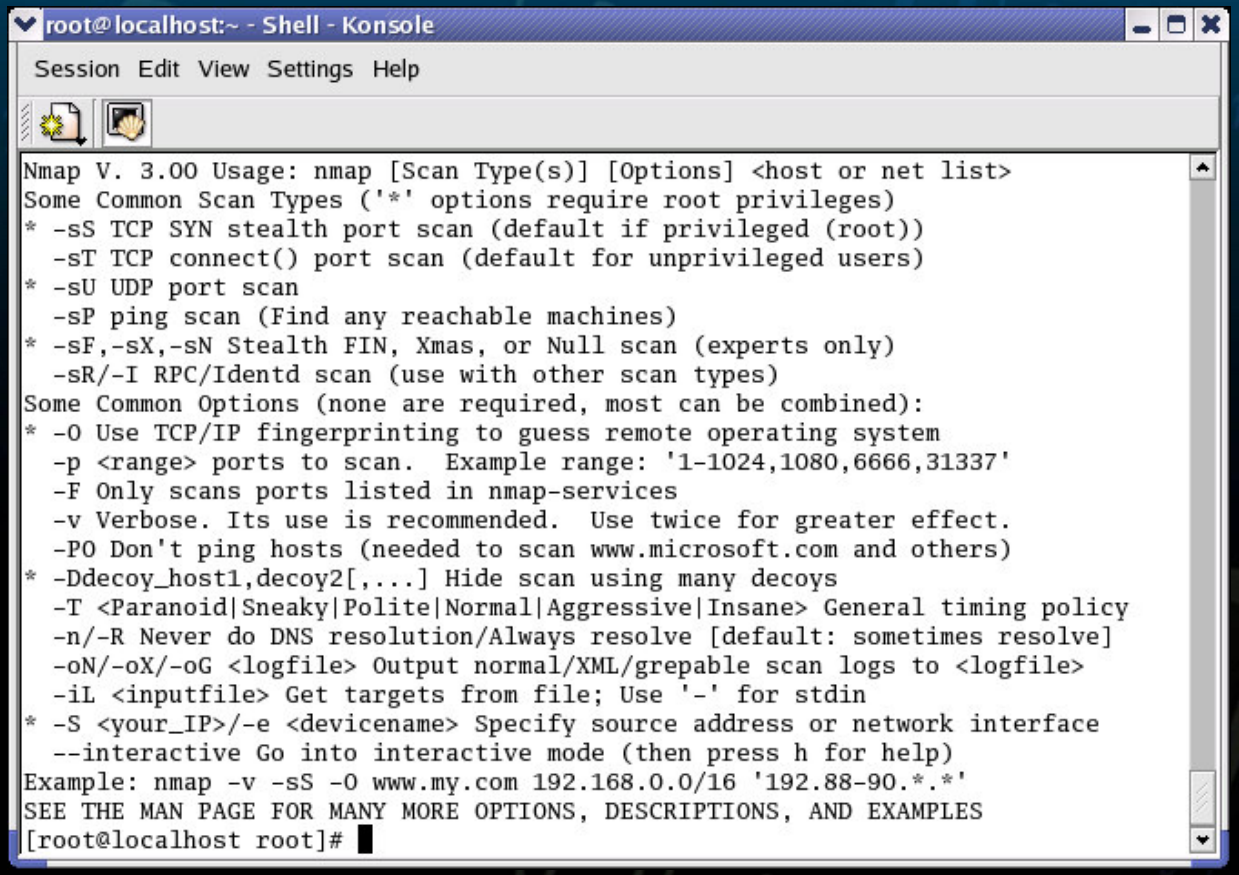


SMTP

TOOLS

Nmap

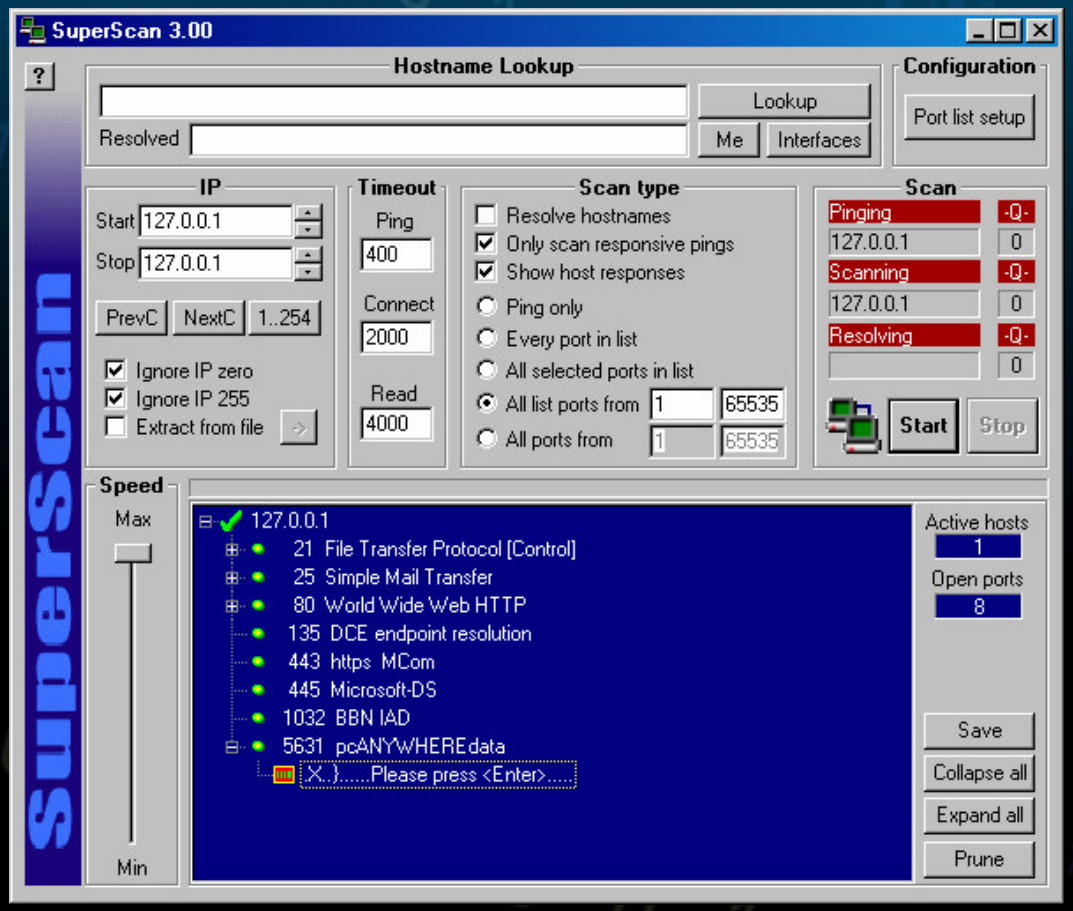
Sending a series of specially crafted packets to a target to identify open or listening UDP/TCP ports



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] [-1buSRHUdqv] [[-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

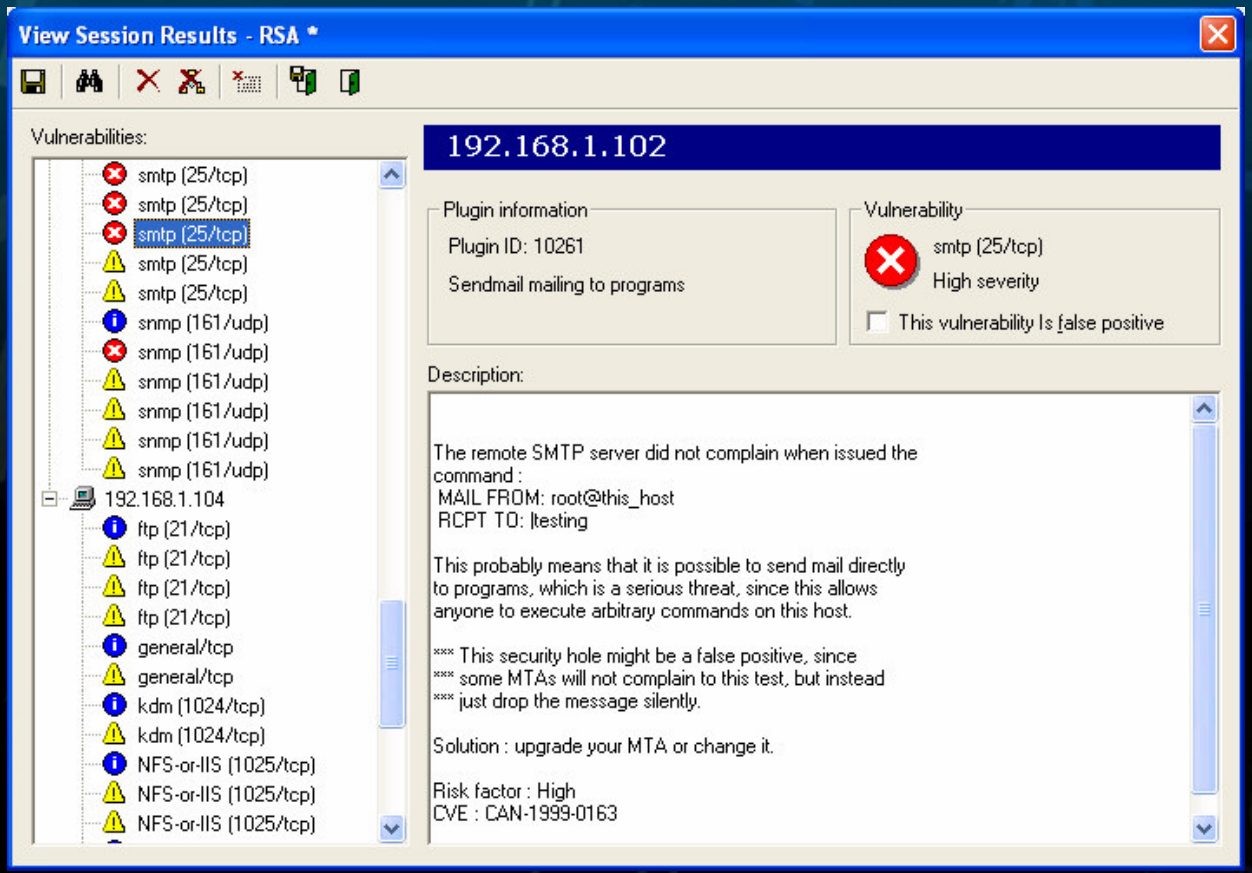
Nessus

- 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

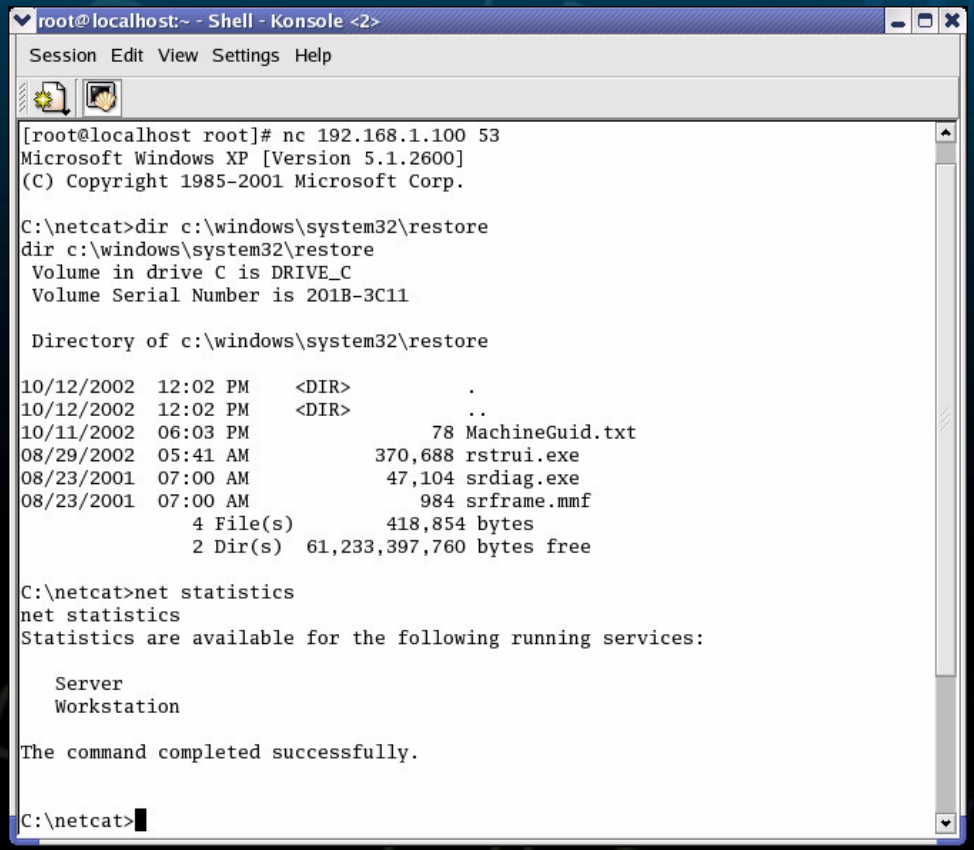
- Review of results through Nessus GUI



TOOLS

Netcat

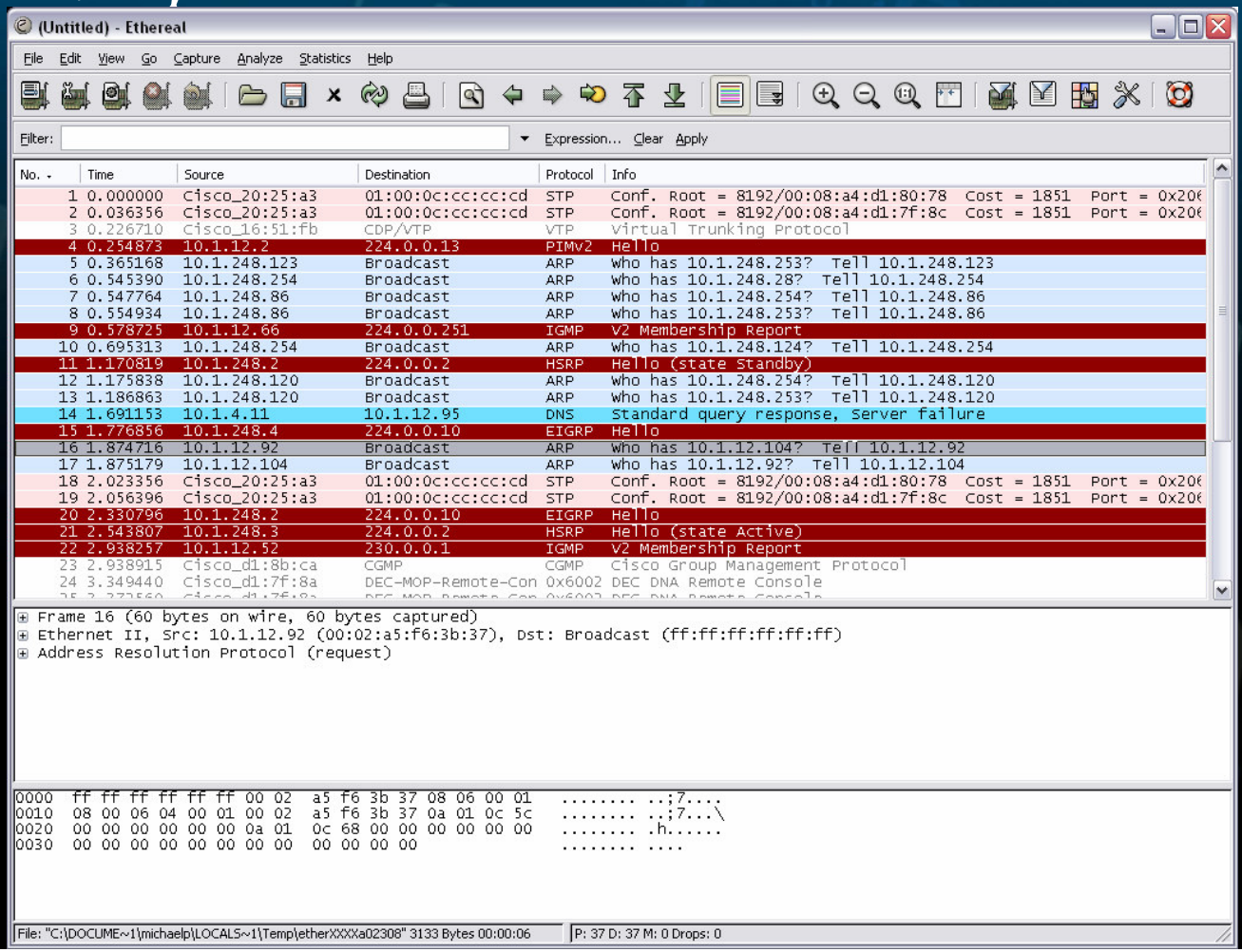
- Simple Netcat connection between a Linux and Microsoft Windows machine.



TOOLS

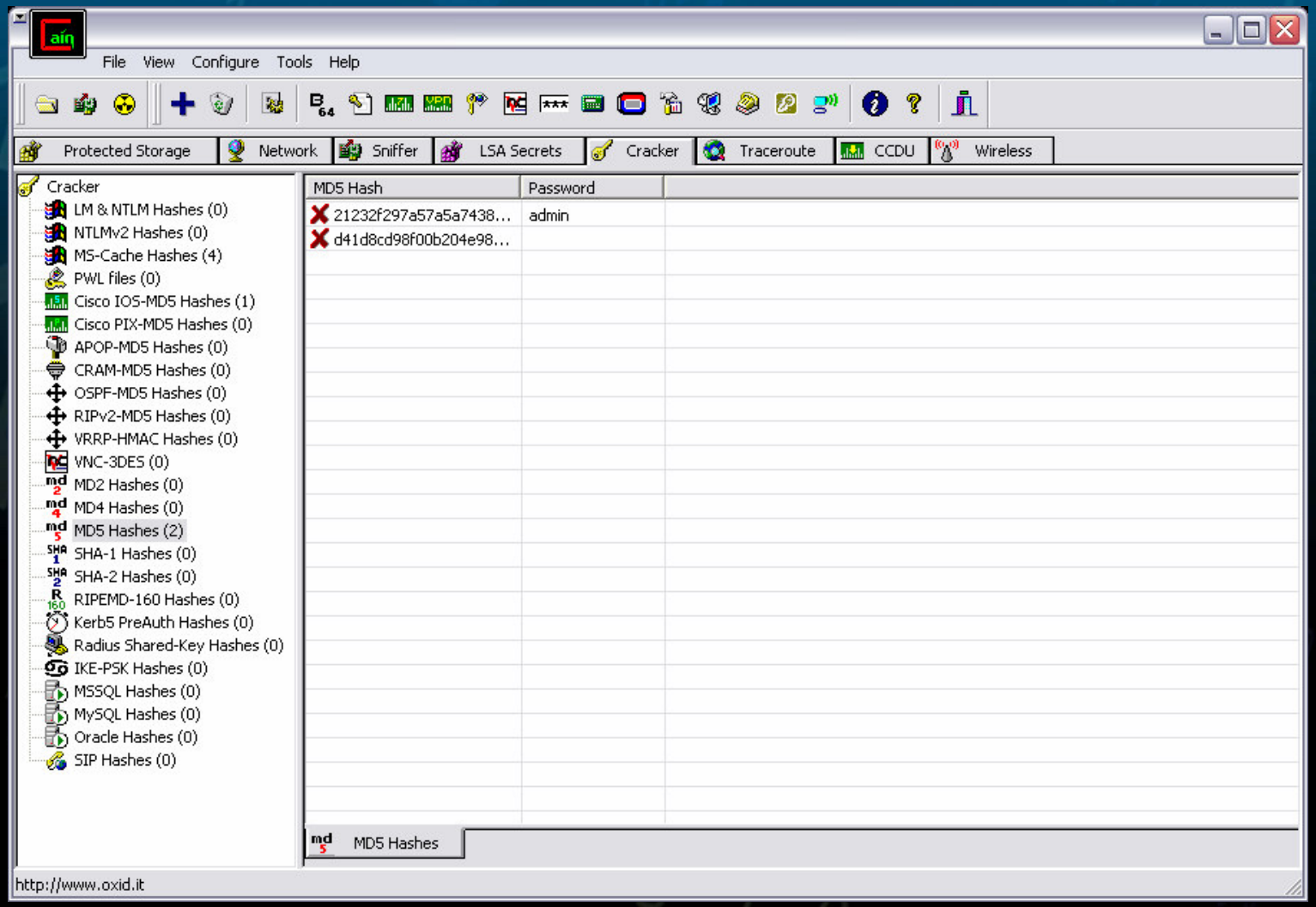
EtherReal

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



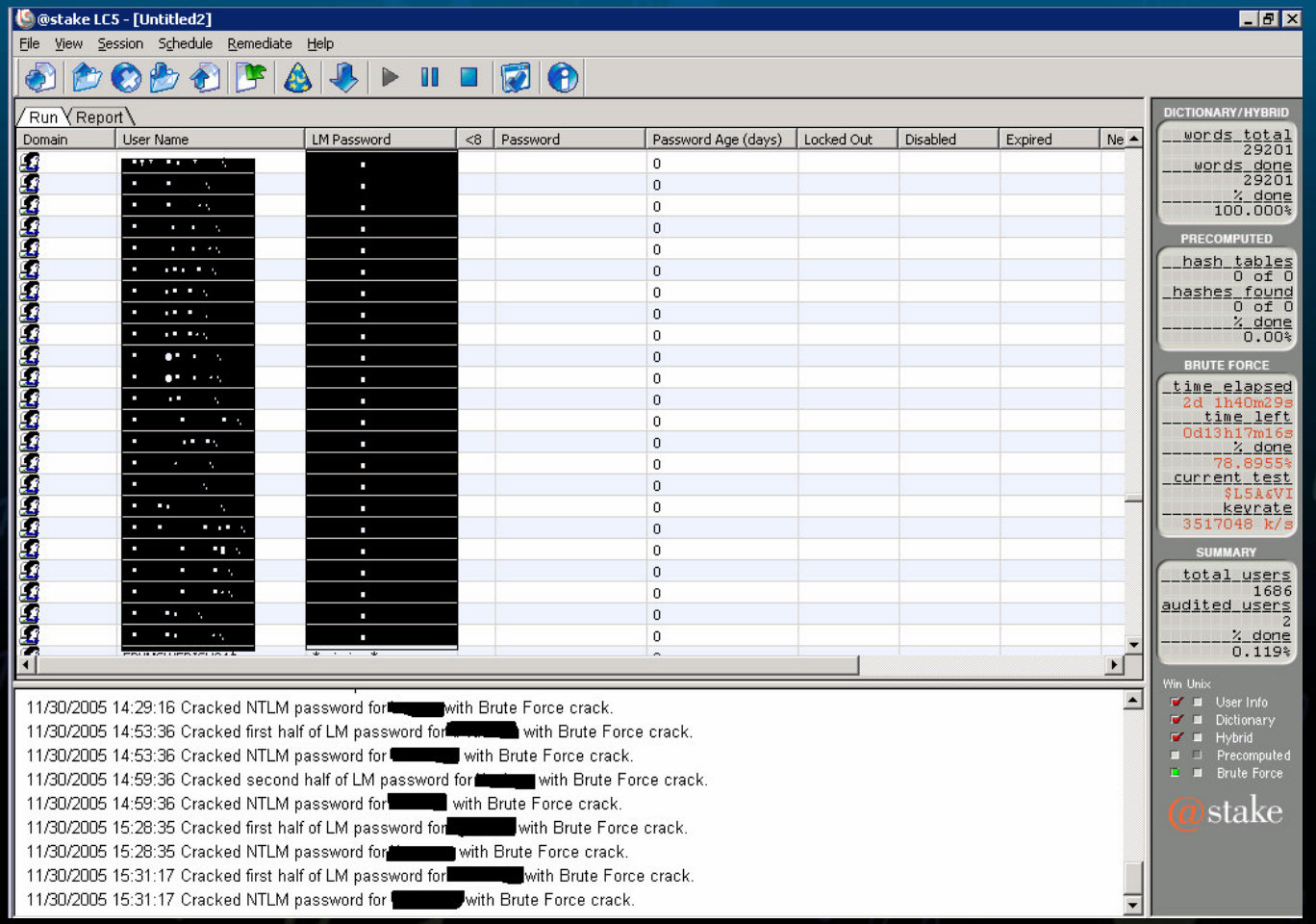
PASSWORD TOOLS

Cain and Abel



PASSWORD TOOLS

LophtCrack



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 mechanism's 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