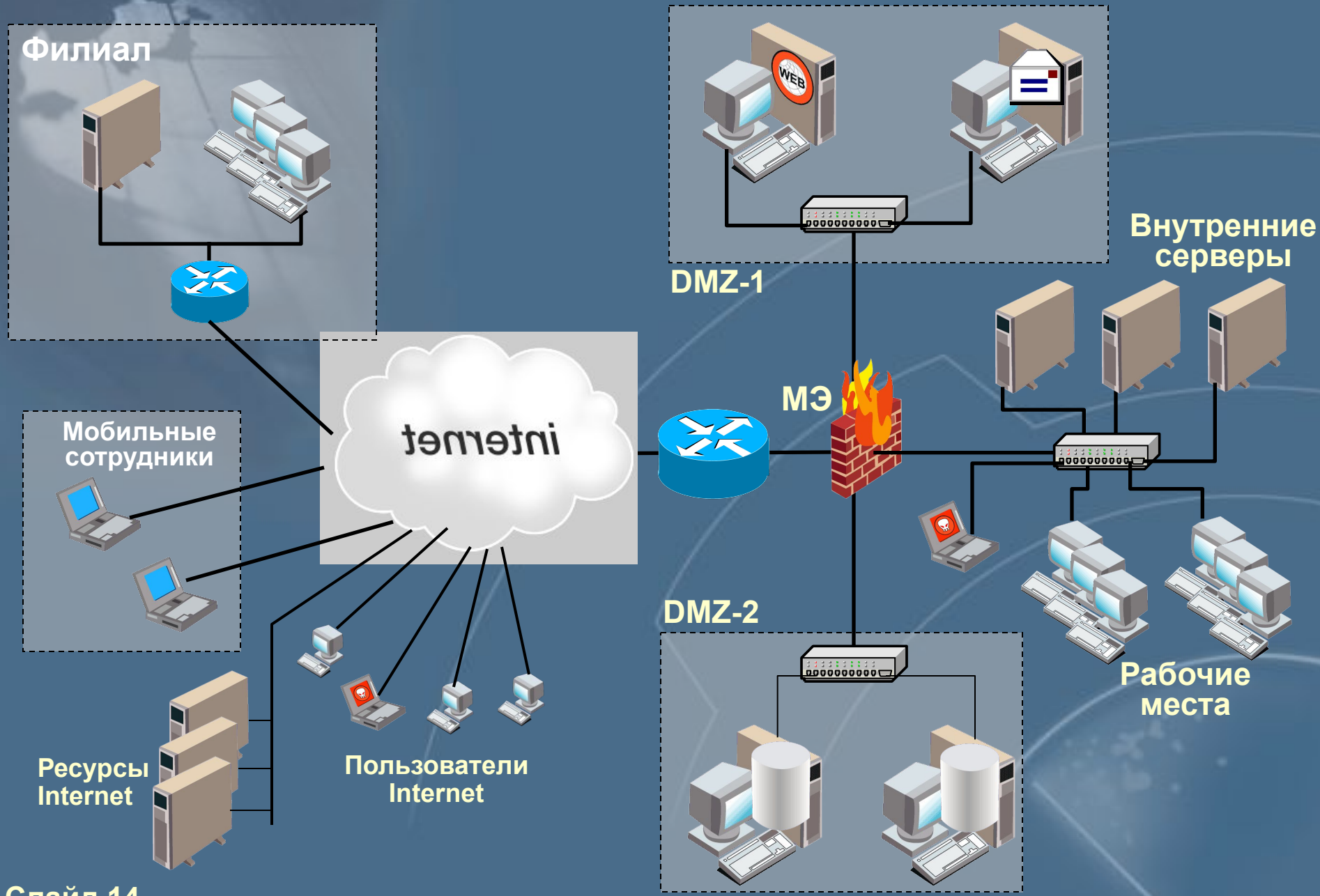
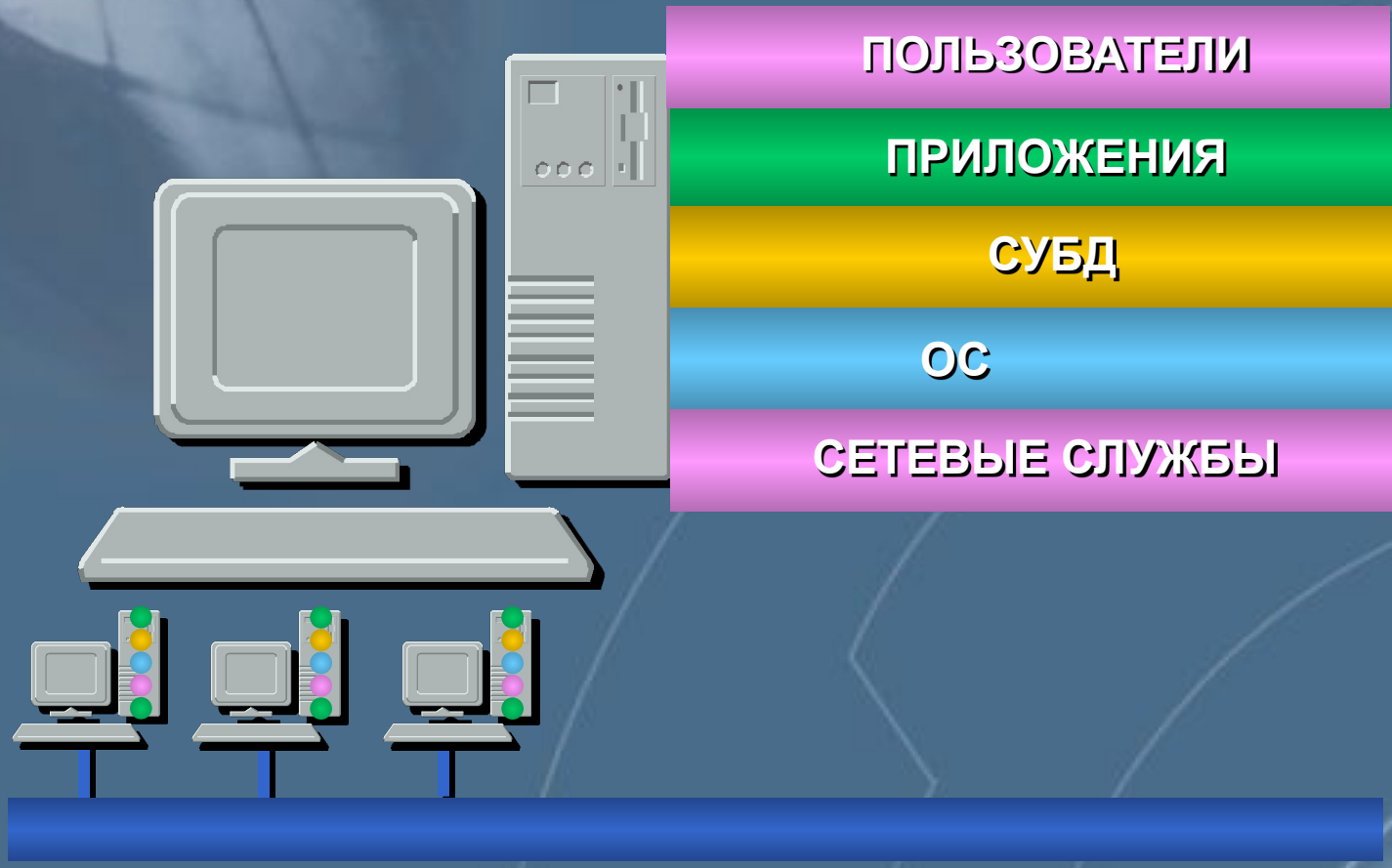
Типовая корпоративная сеть, понятие уязвимости и атаки

Раздел 1 – Тема 2

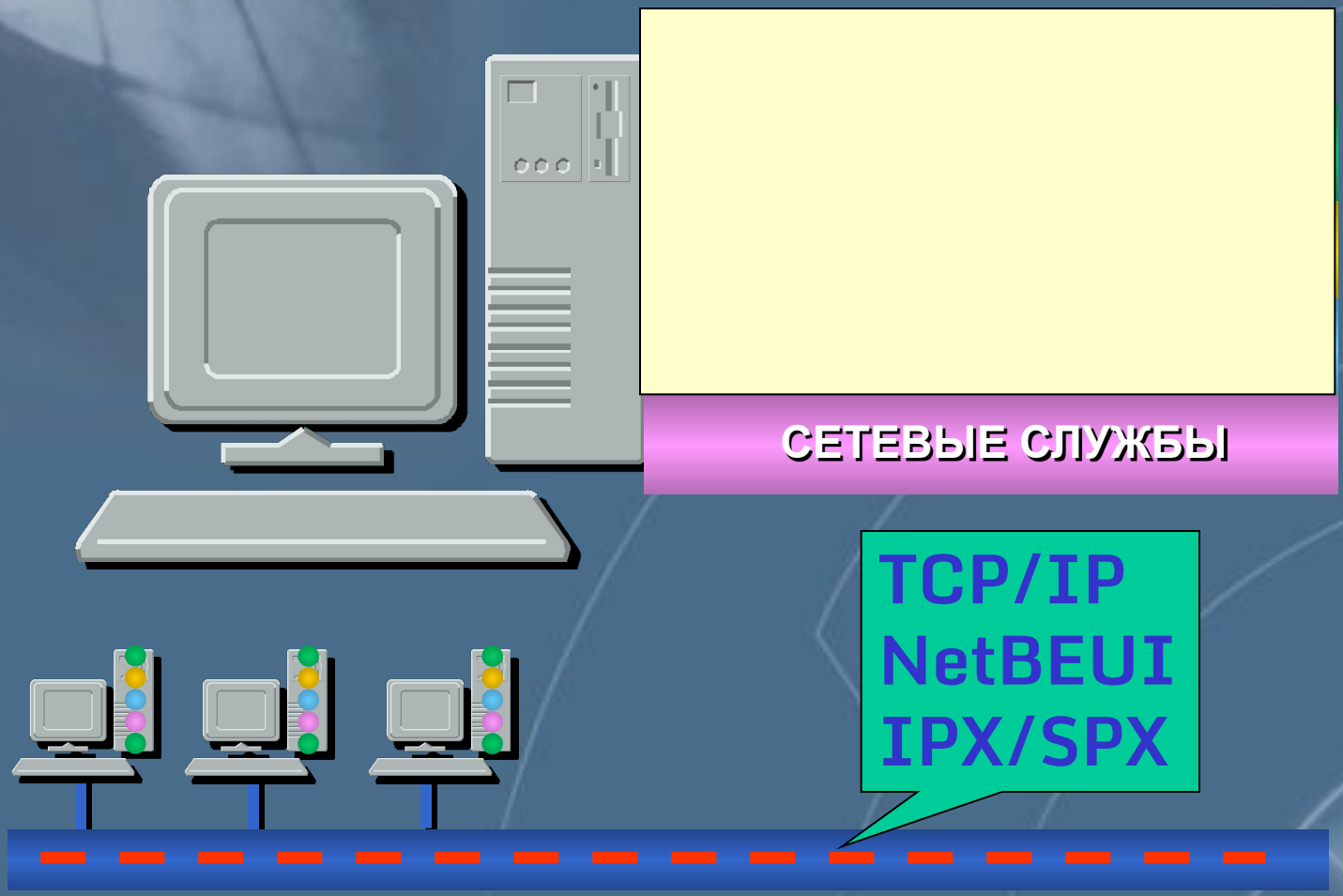
Типовая корпоративная сеть



Уровни информационной инфраструктуры

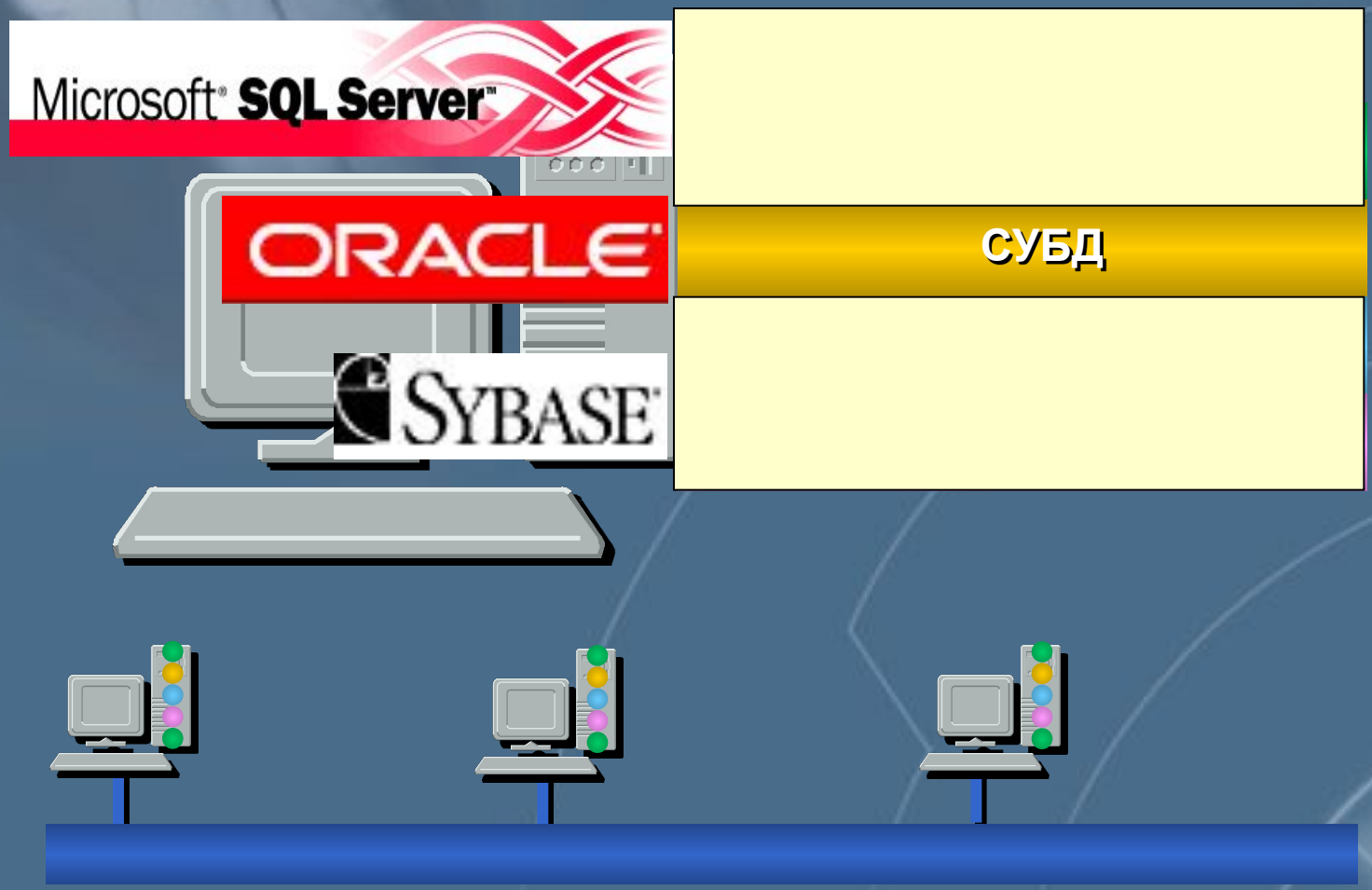


Уровни информационной инфраструктуры

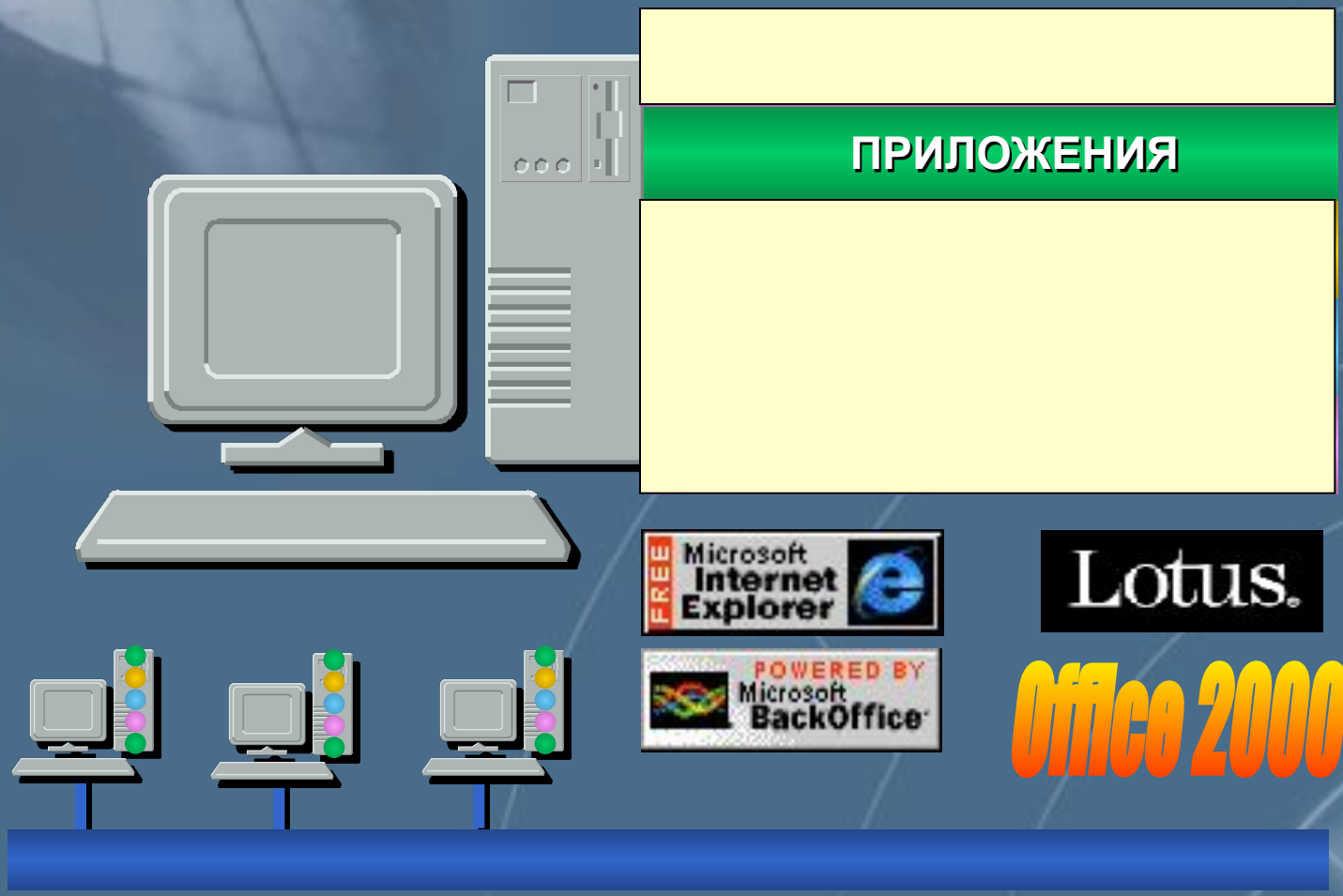


Уровни информационной инфраструктуры

Уровни информационной инфраструктуры



Уровни информационной инфраструктуры



Уровни информационной инфраструктуры

Классификация уязвимостей и атак

Раздел 1 – Тема 3

Примерный сценарий атаки

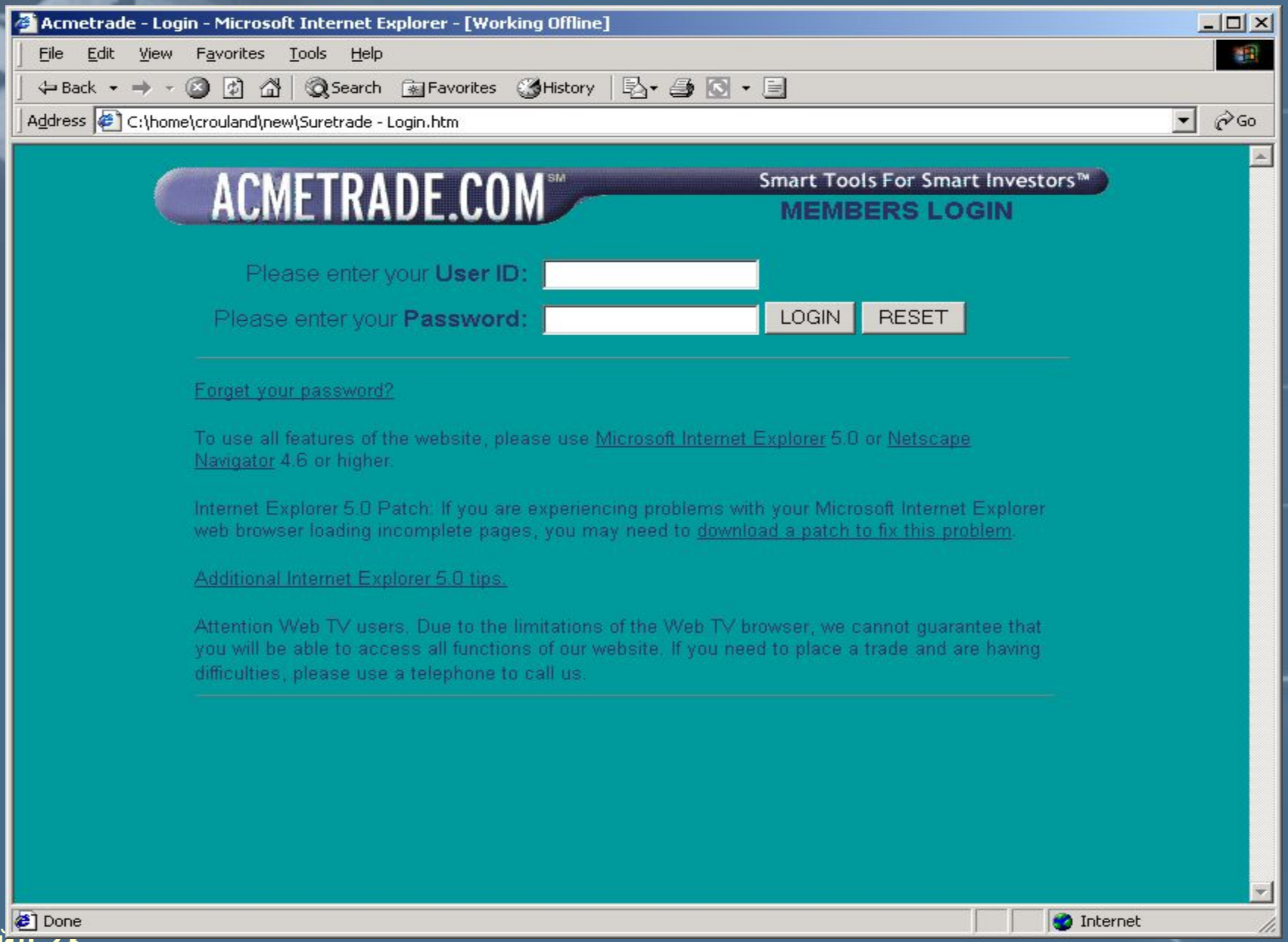
Сбор информации

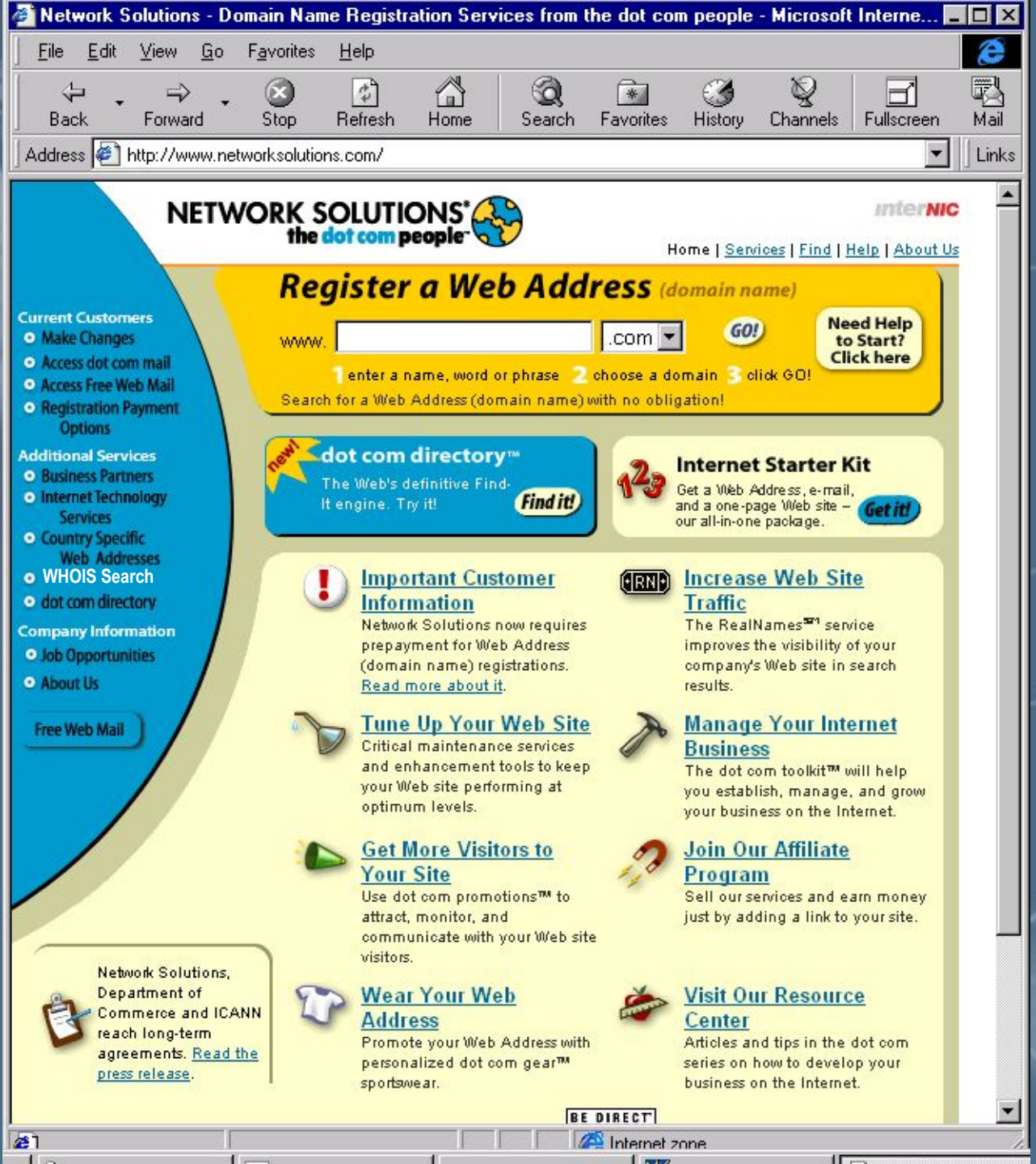
Получение доступа к наименее защищённому узлу
(возможно с минимальными привилегиями)

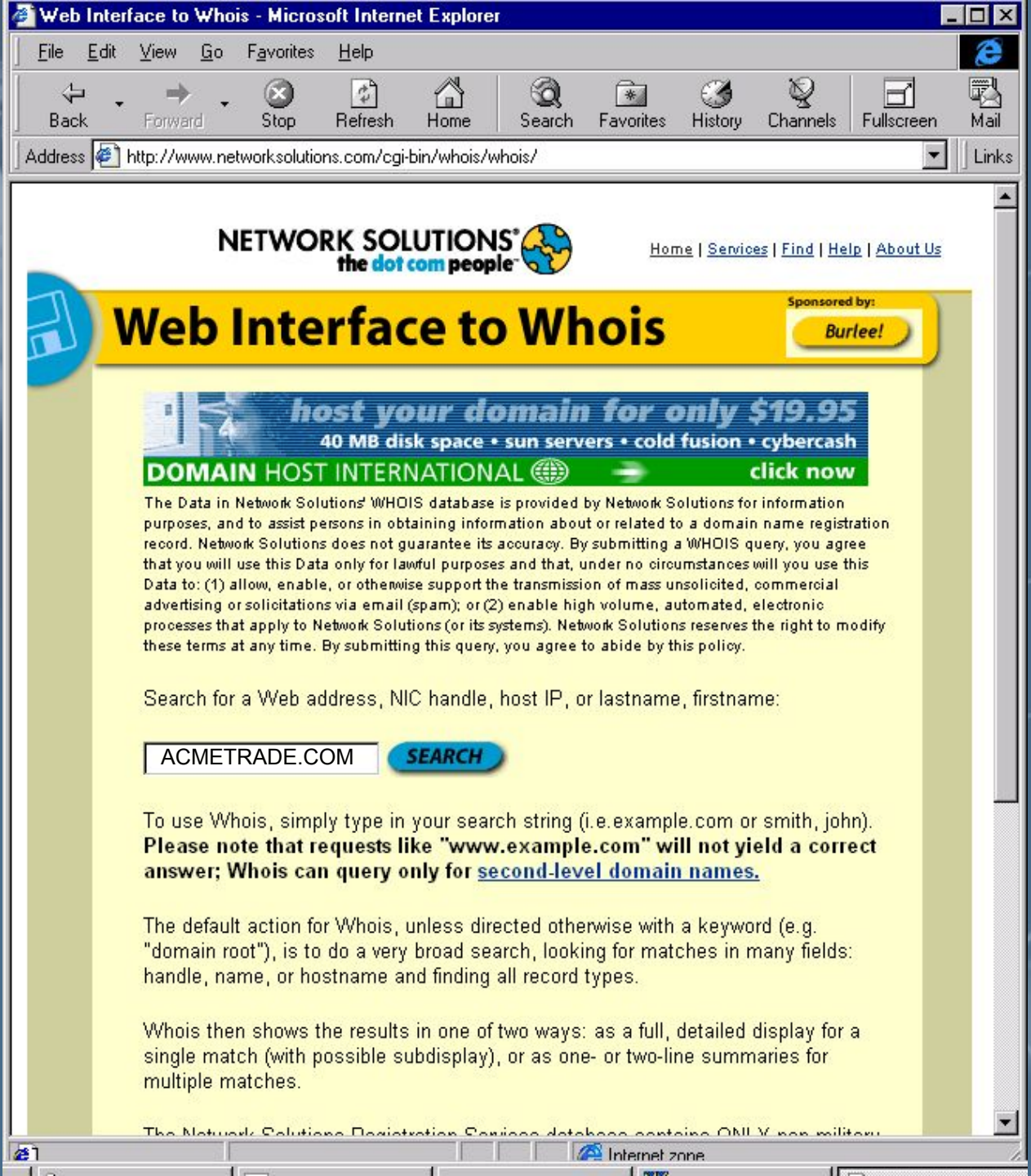
Повышение уровня привилегий или использование
узла в качестве платформы для исследования других узлов сети

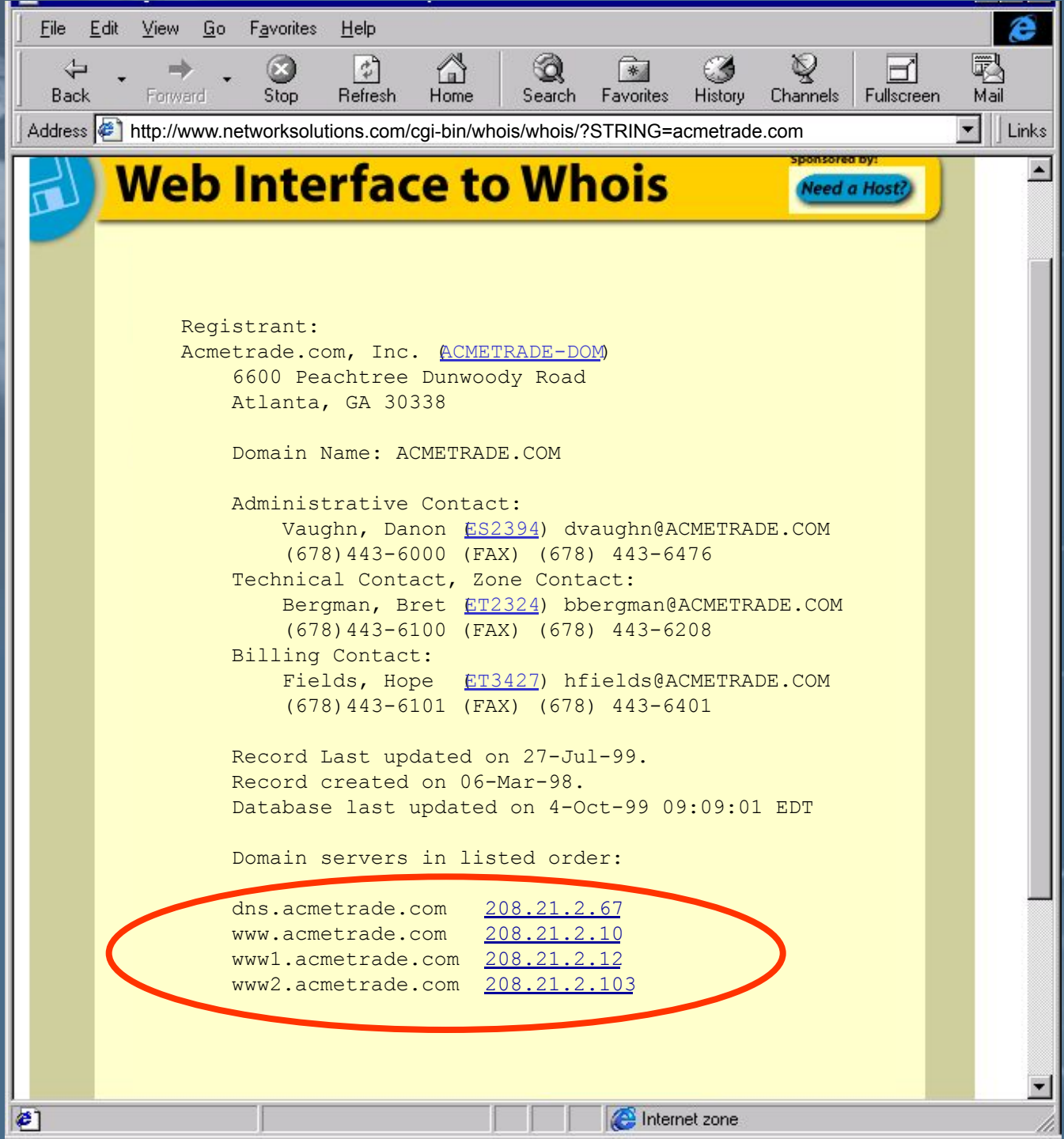
Получение полного контроля над одним из узлов
или несколькими

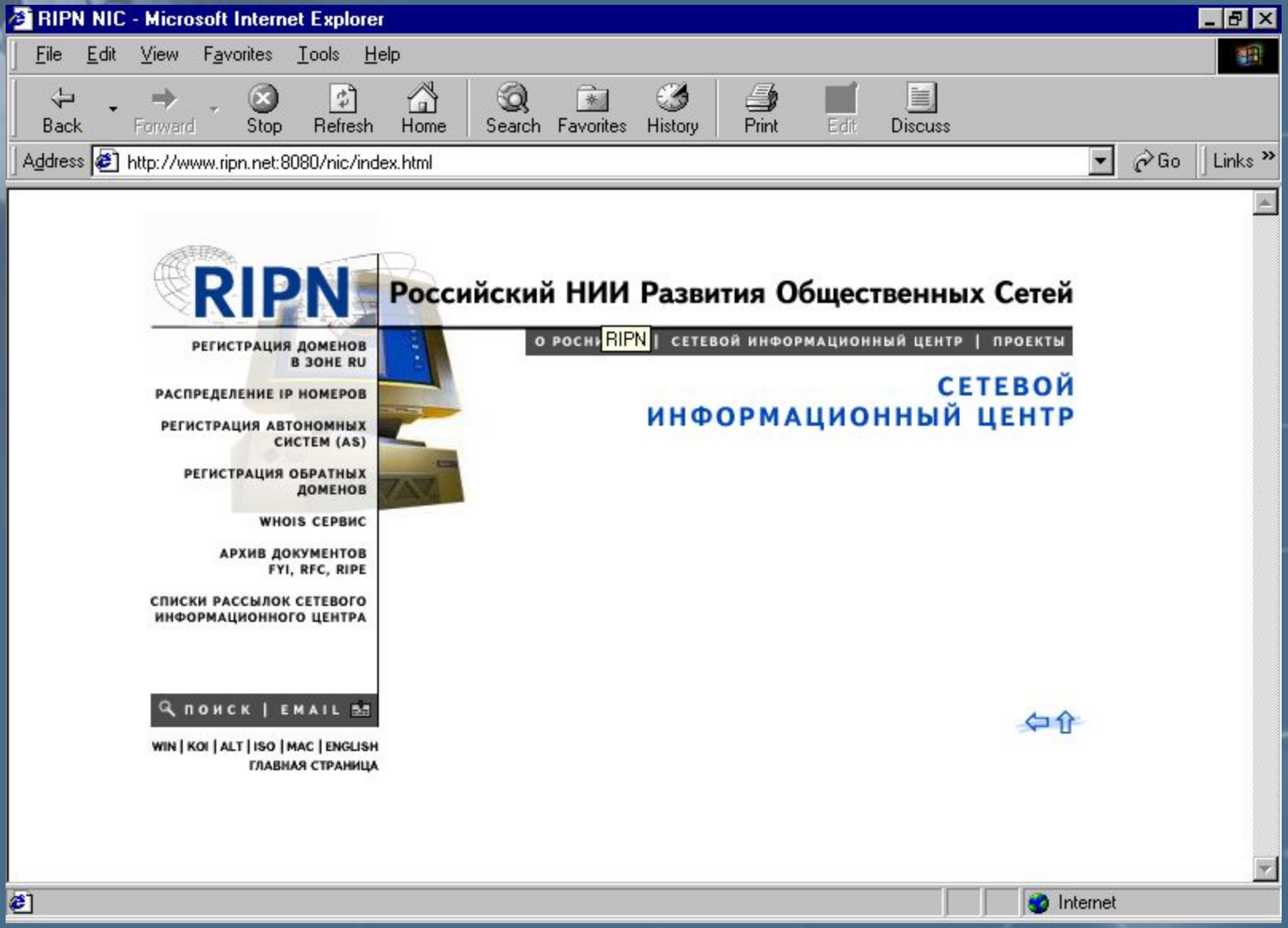
Этап сбора информации

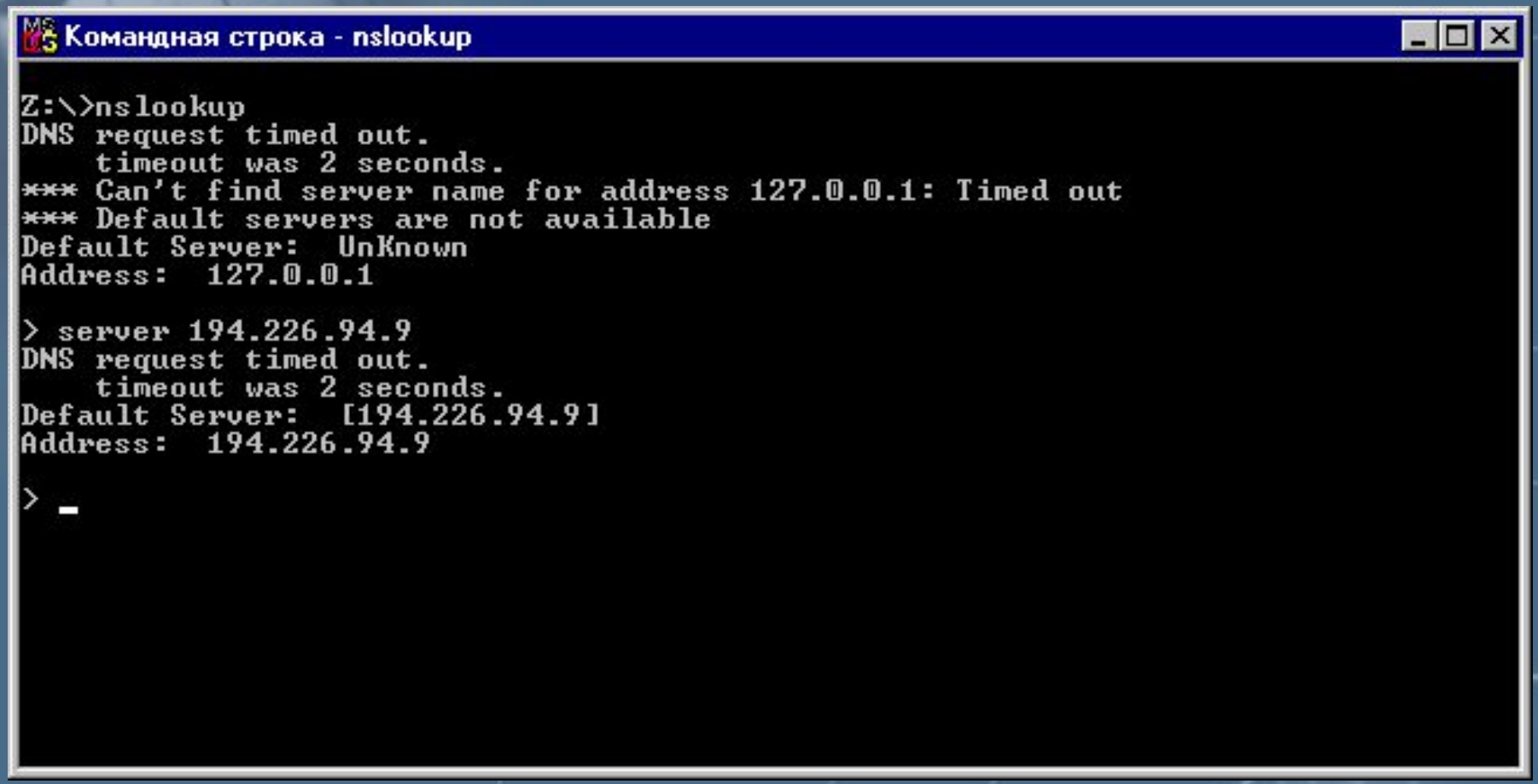


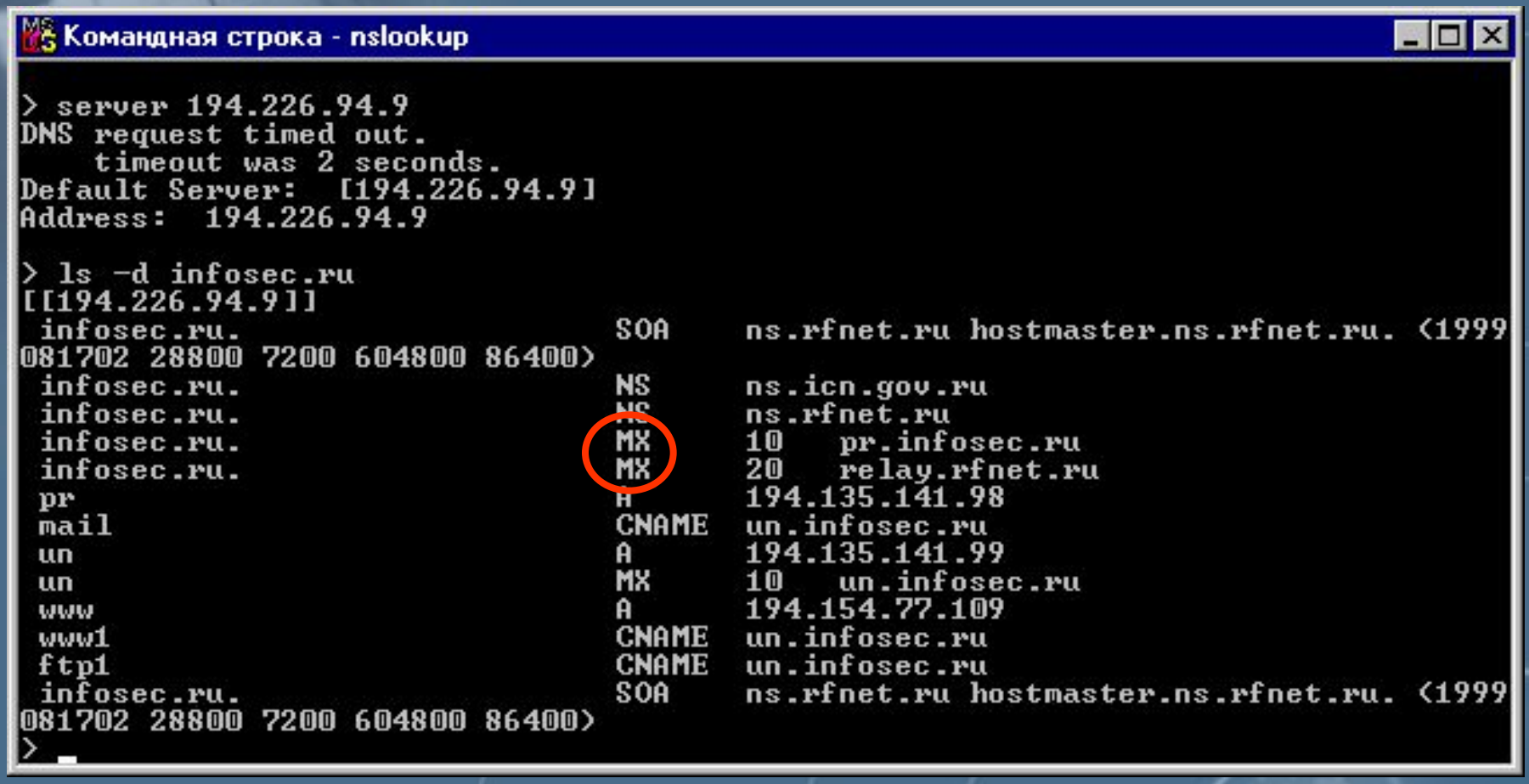

Network Solutions - Domain Name Registration Services from the dot com people - Microsoft Interne...
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/
Links
NETWORK SOLUTIONS
the dot com people
interNIC
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)
>

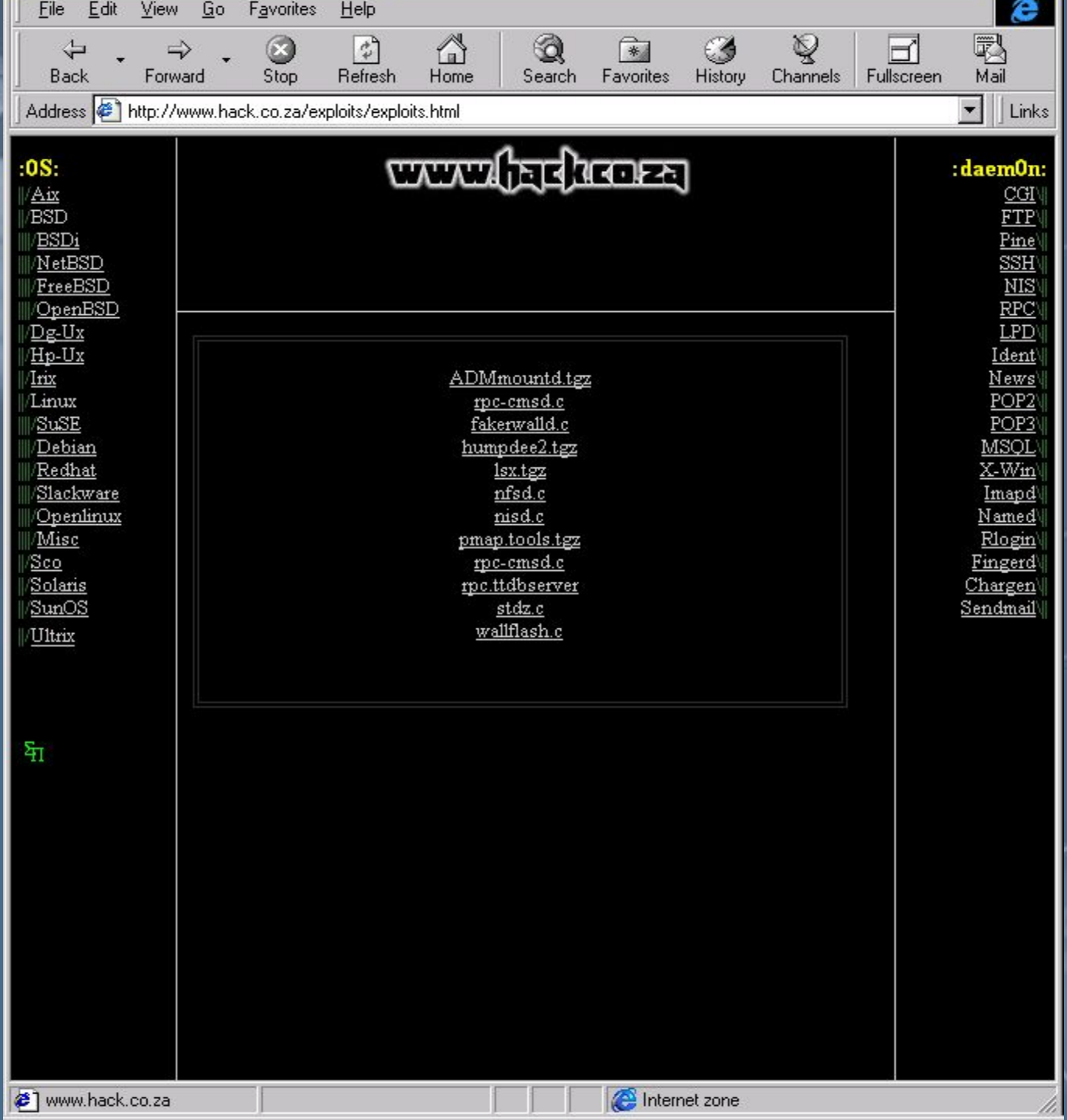
Shadow Scan.lnk

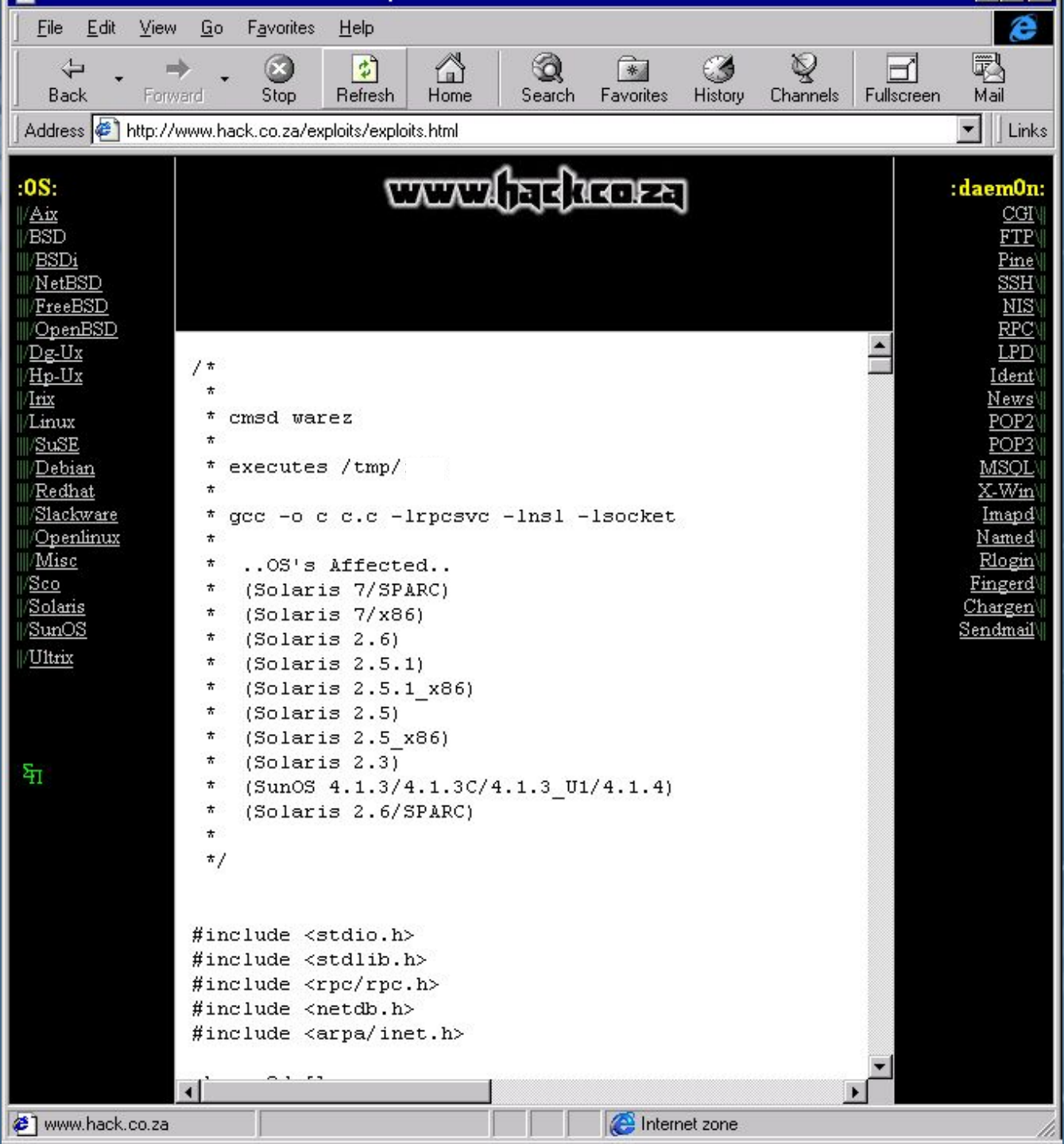
```
[hacker@linux131 hacker]$ nmap 200.0.0.143

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
:daemOn:
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
:OS:
/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

Этап получения доступа к узлу

```
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

#
```

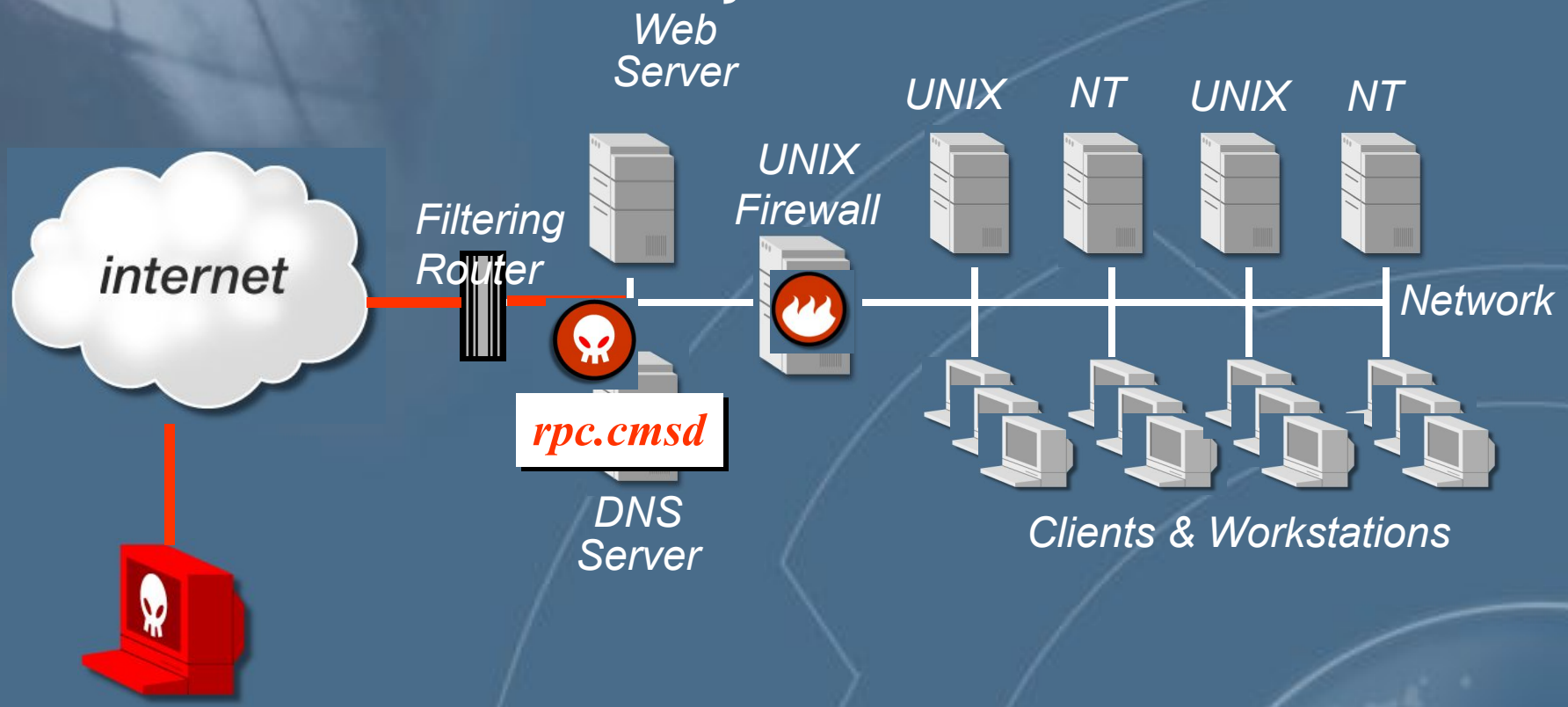
Использование узла в качестве платформы для исследования других узлов сети

```
# nslookup
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
#
```

Схема сети

(AcmeTrade's Network)



Уязвимости и атаки

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 уязвимостей по причинам возникновения

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

Классификация по уровню в информационной инфраструктуре

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

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*

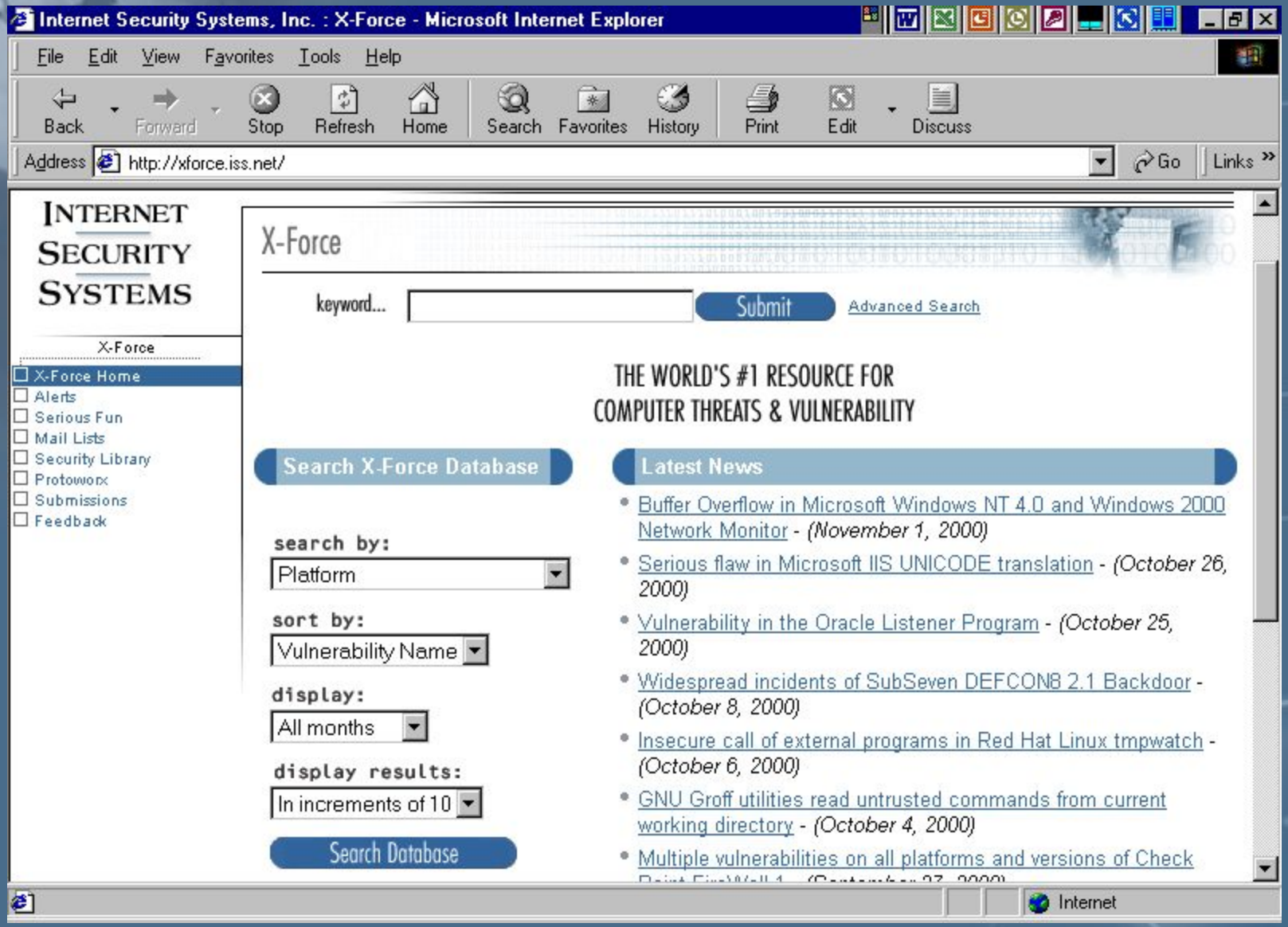
www.iss.net/xforce - *база данных компании ISS*

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

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

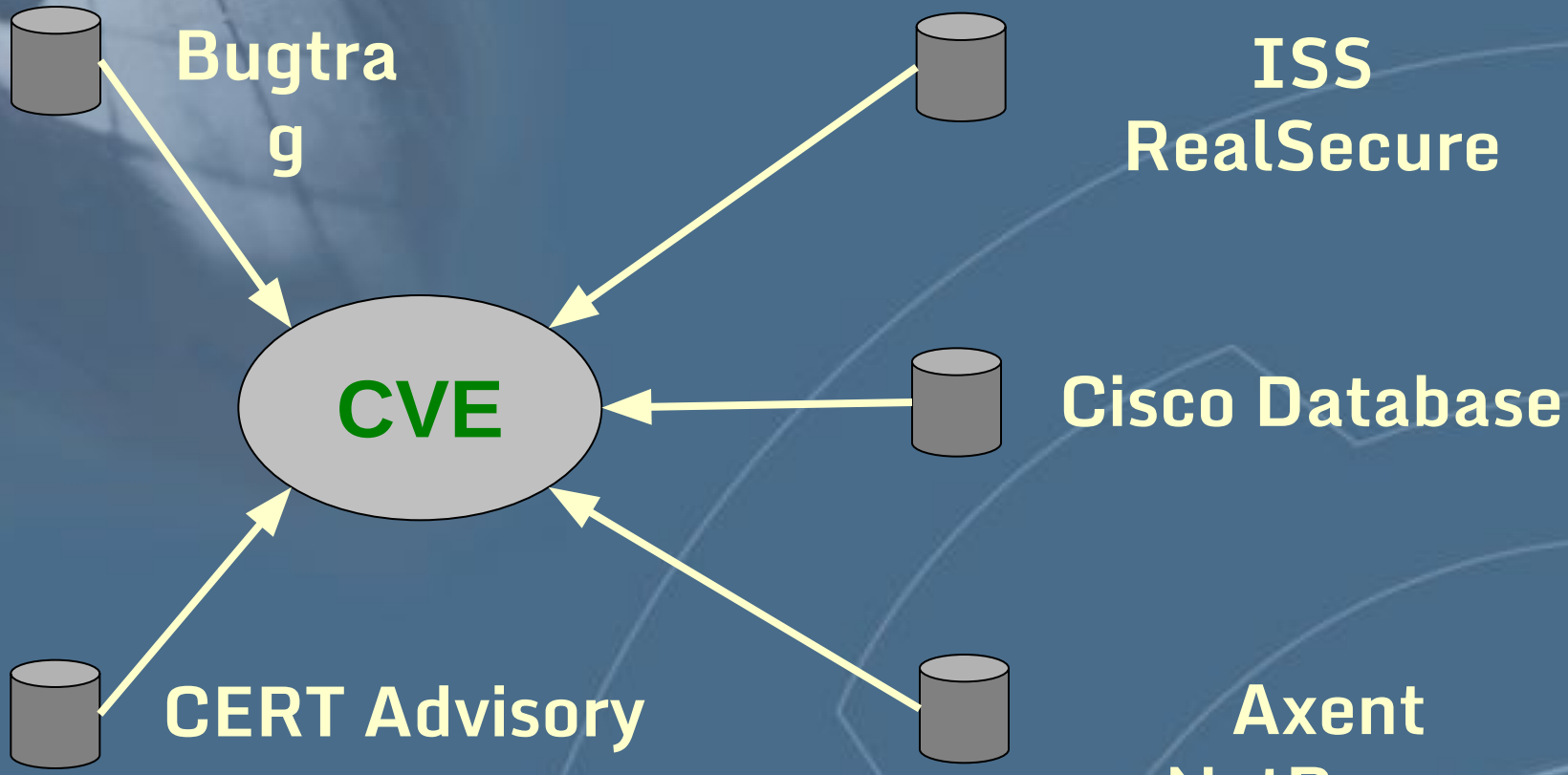
http://cve.mitre.org/cve

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

Классификация атак в IP- сетях

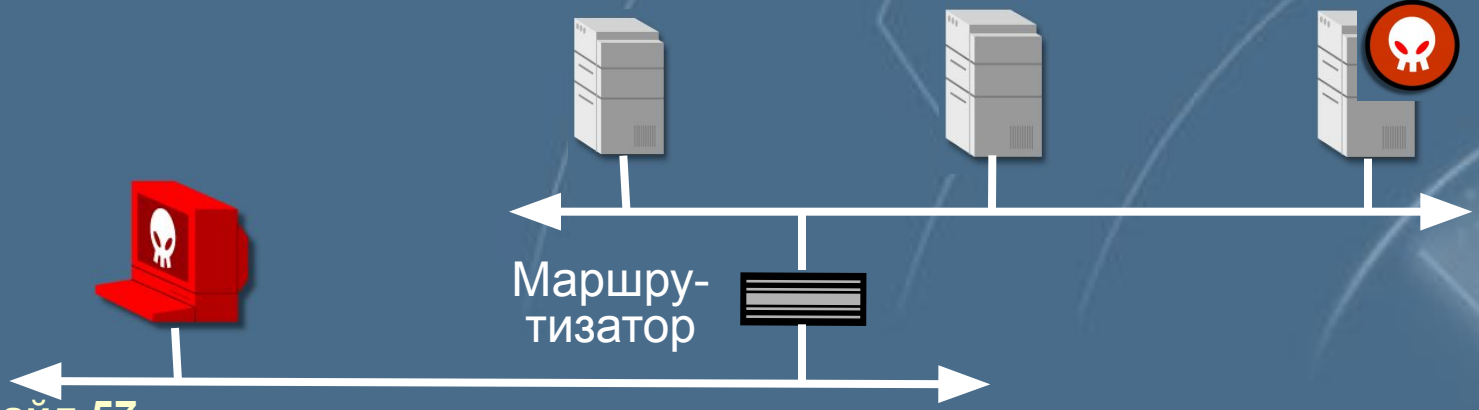
Классификация атак по целям

- *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*

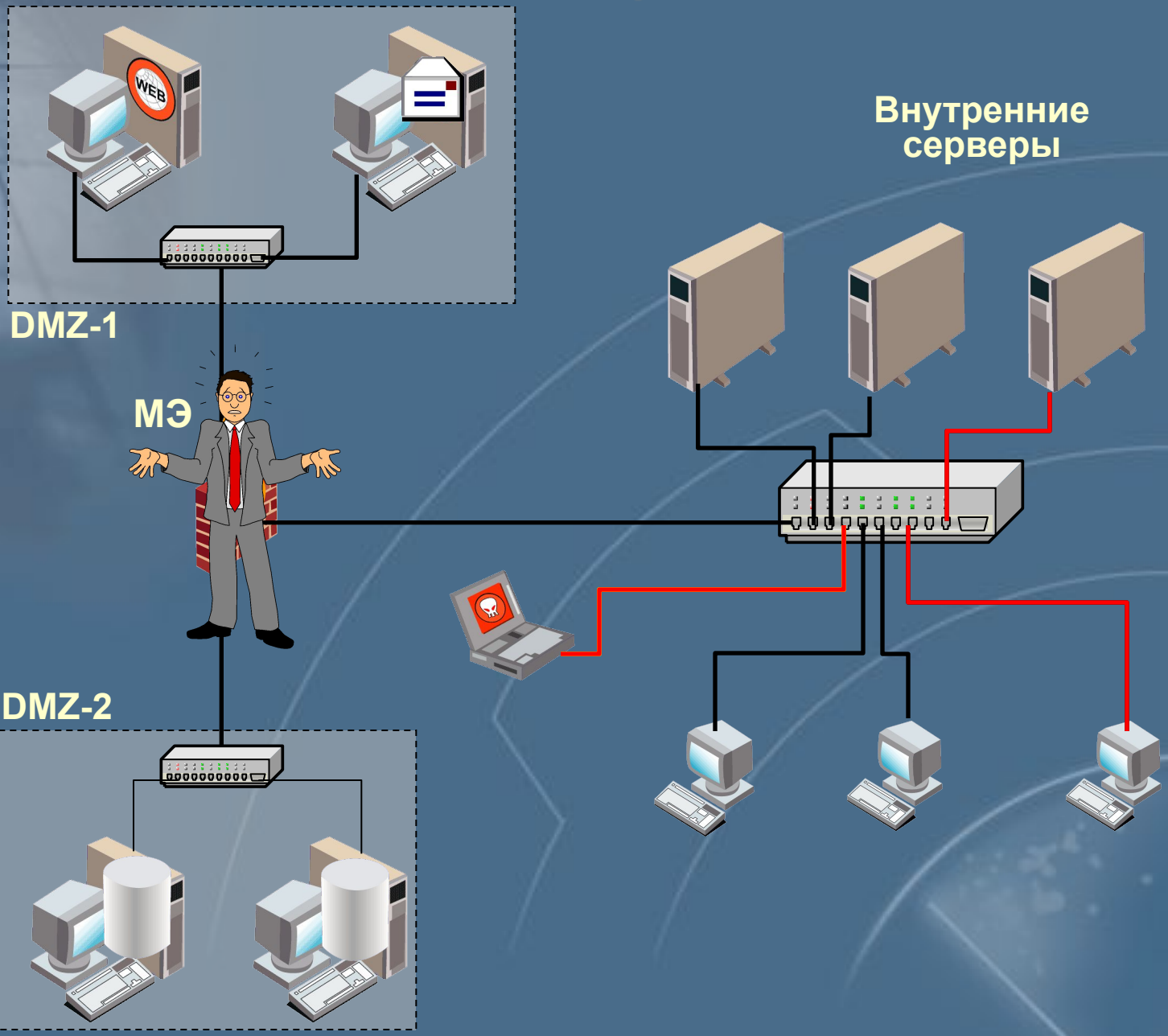
- *Атакующий и объект атаки находятся в разных сегментах*



Классификация атак по механизмам реализации

- *Пассивное прослушивание*

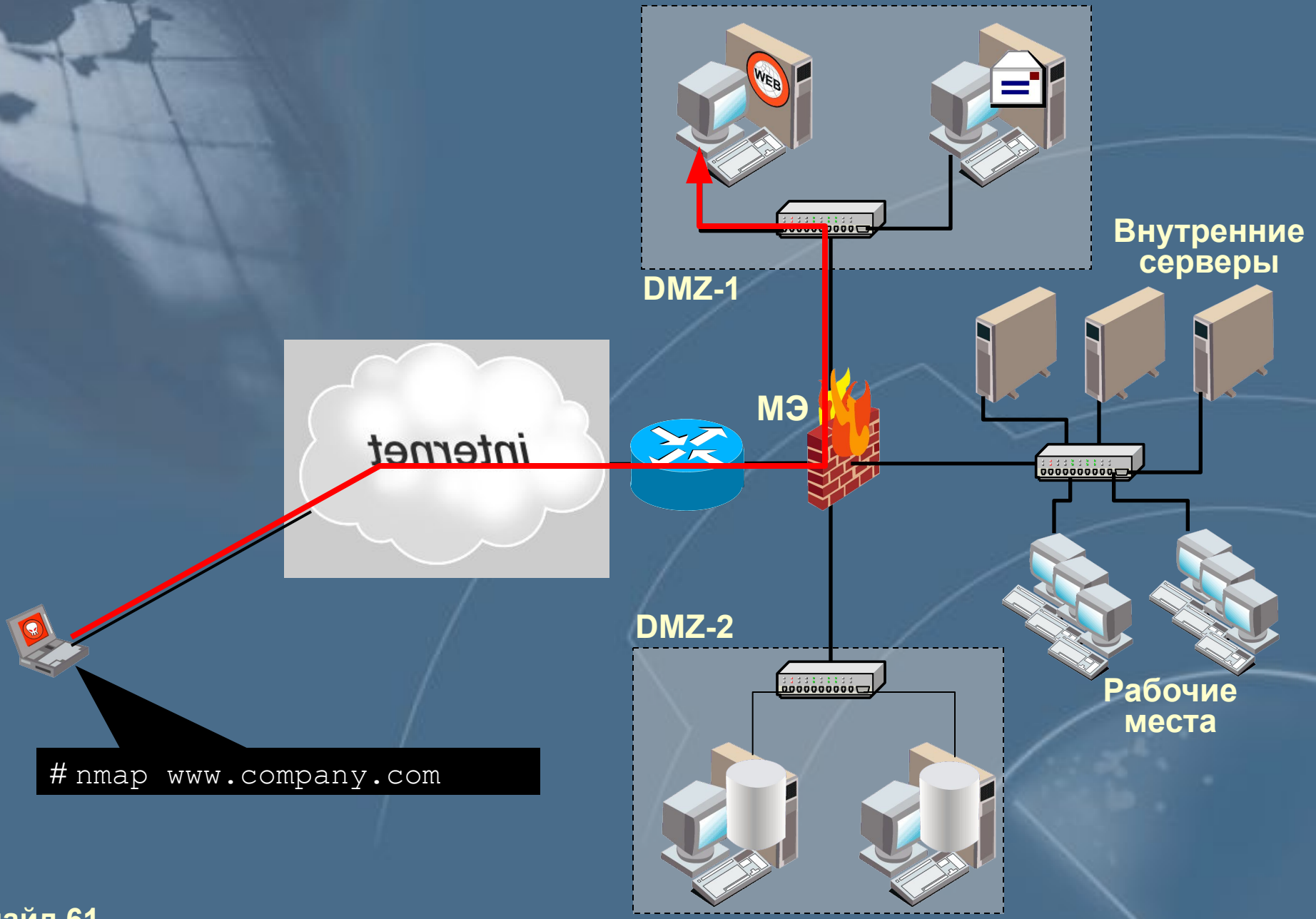
Пассивное прослушивание



Классификация атак по механизмам реализации

- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*

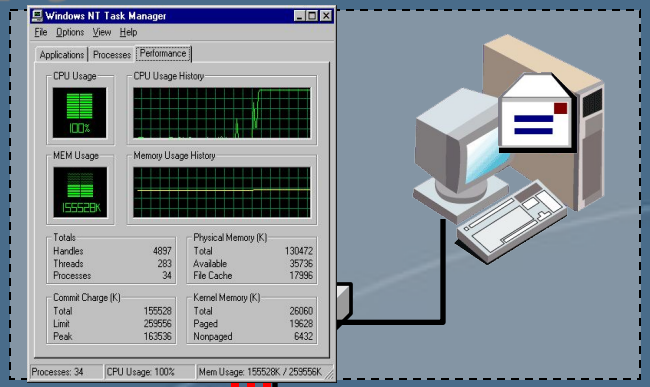
Подозрительная активность



Классификация атак по механизмам реализации

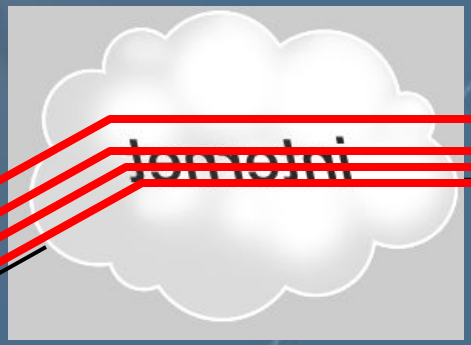
- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*
- *Бесполезное расходование вычислительных ресурсов (перегрузка)*

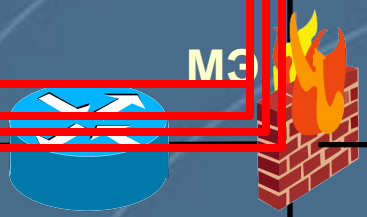
Перегрузка

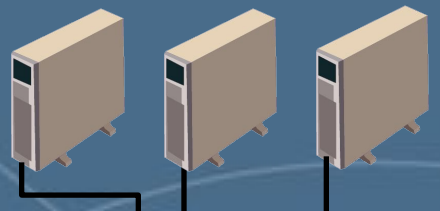


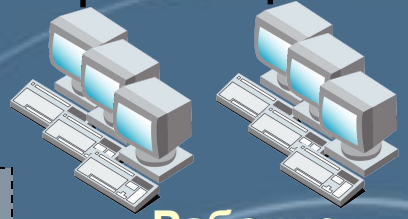
DMZ-1

Внутренние серверы



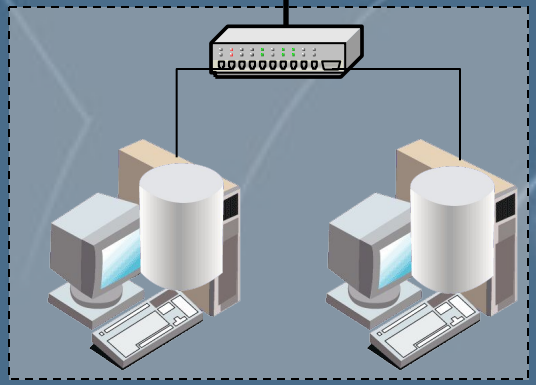






Рабочие места

DMZ-2

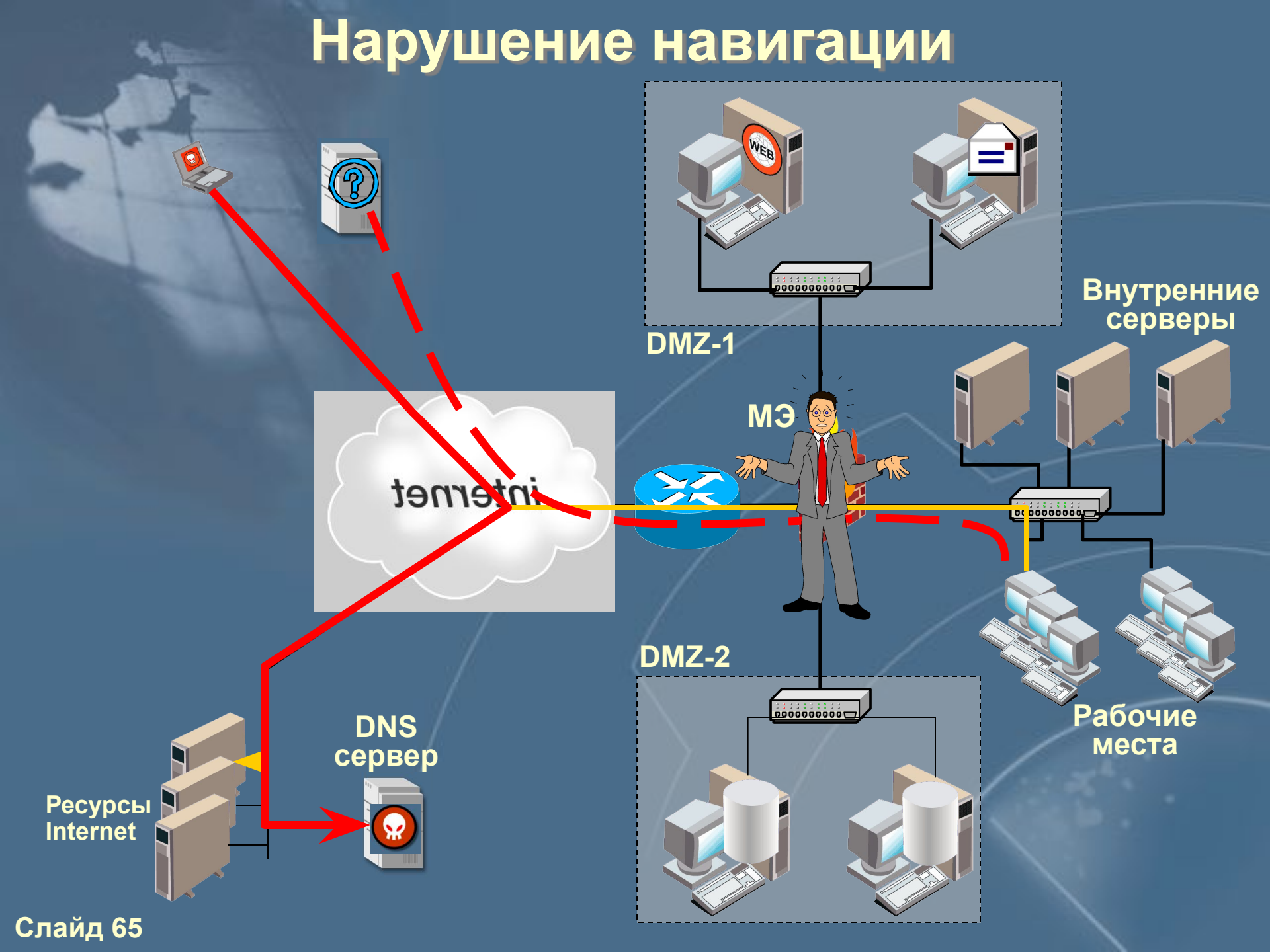


```
# ./neptun www.company.com
```

Классификация атак по механизмам реализации

- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*
- *Бесполезное расходование вычислительных ресурсов (перегрузка)*
- *Нарушение навигации (ложный маршрут)*

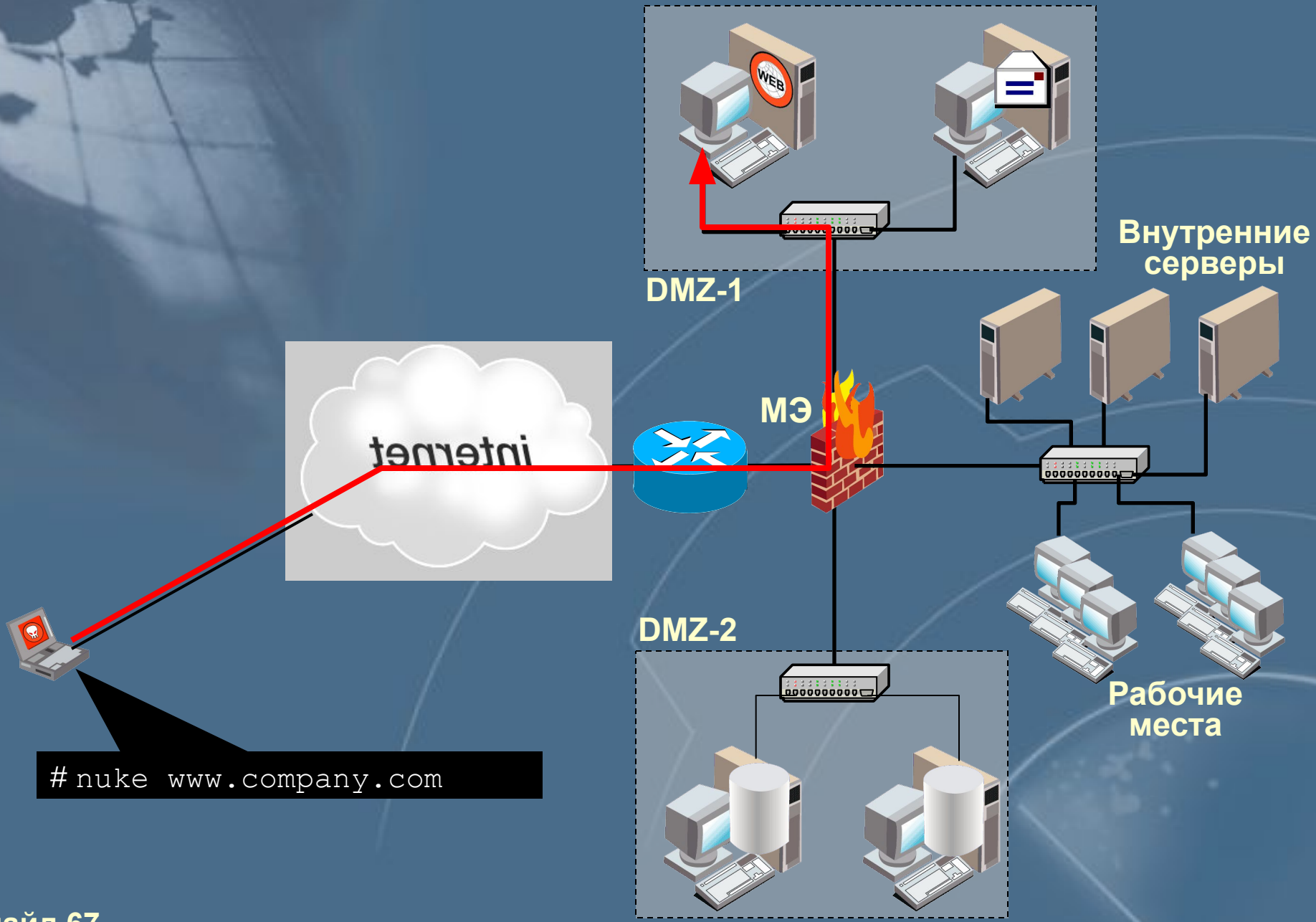
Нарушение навигации



Классификация атак по механизмам реализации

- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*
- *Бесполезное расходование вычислительных ресурсов (перегрузка)*
- *Нарушение навигации (ложный маршрут)*
- *Провоцирование отказа объекта (компонента)*

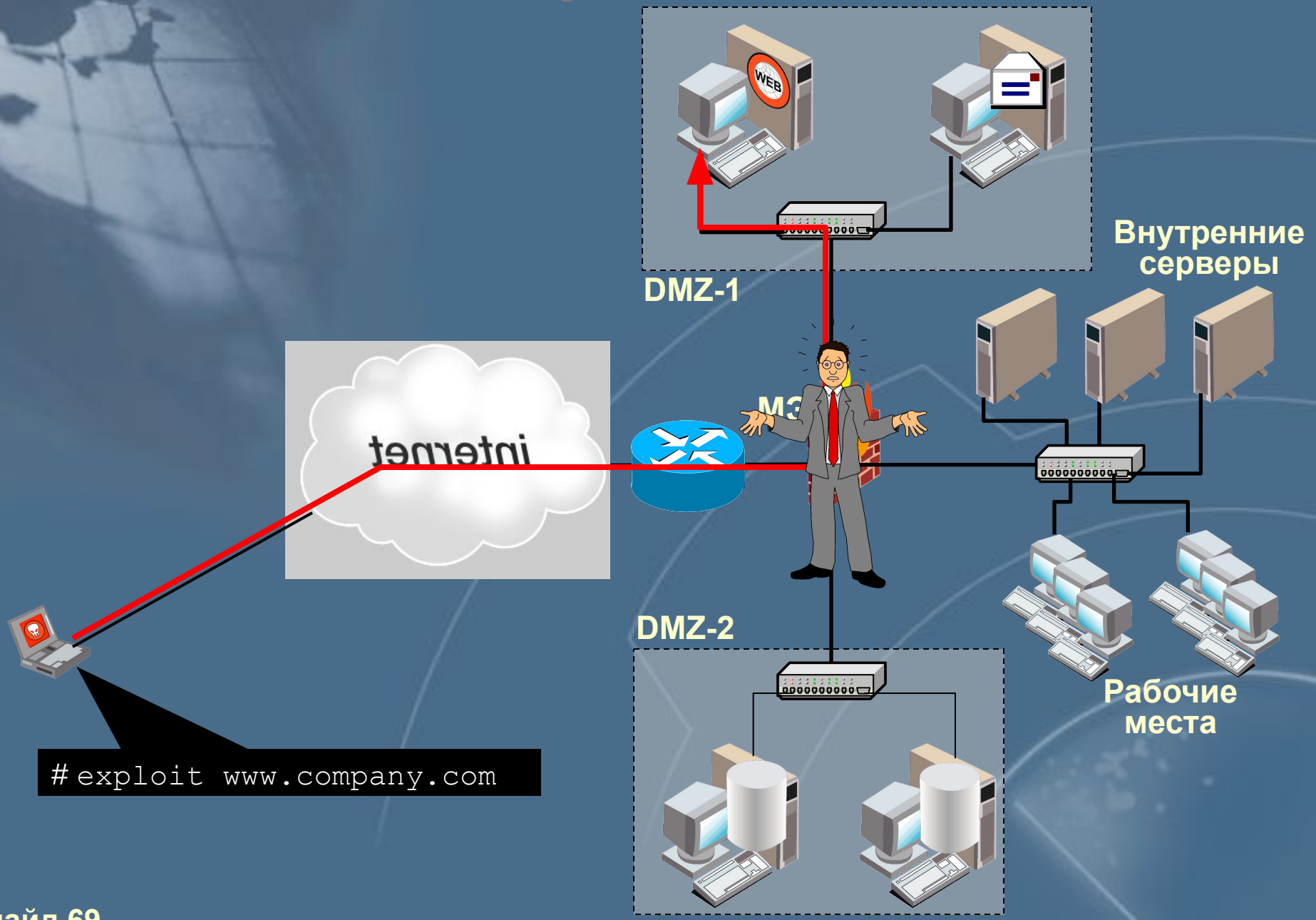
Провоцирование отказа



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*

Запуск кода


WEB
DMZ-1
Внутренние серверы
Internet
DMZ-2
Рабочие места
exploit www.company.com

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*

SANS Institute resources

Статистика по уязвимостям и атакам

Версия 2.504 Май 2, 2002

Источник: SANS

Часто используемые уязвимости

1. Установленные «по умолчанию» ОС и приложения
2. Слабые пароли (системная политика)
3. Отсутствие механизма резервирования системы
4. Работающие, но не используемые сетевые службы
5. Отсутствие защиты от IP-спуфинга на пакетных фильтрах
6. Отсутствие процедуры аудита
7. Уязвимости CGI-программ