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
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Saundra Coward
Version Assignment: GSEC V.1.2e

Identify Intrusions with Microsoft Proxy Server, Web Proxy Service and WinSock Proxy Service log files

Abstract:
This is a guide on how to identify intrusions using Microsoft's Proxy Server log files. MS Proxy Server is an extensible firewall that provides passive defense against intrusions and functions as a gateway between an internal network and the Internet. This configuration allows clients to share a common connection point to the Internet.

Installing a MS Proxy Server between the Internet and an internal network provides packet-filtering services that will stop various types of protocols from entering the network. With the use of MS Proxy Server log files, system administrators can monitor and track all packets passing through the MS Proxy Server. There are several services that can run within the Proxy Server, and the two most common services are Web Proxy and WinSock Proxy. To manage the services open the Internet Service Manager within the Microsoft Internet Server folder. The General Tab within the Internet Service Manager window displays the Proxy services installed.

Services:
The Web Proxy service log contains connection-specific log information for proxy connections between the MS Proxy Server and its Web Proxy clients. The Web Proxy service provides support for HTTP, FTP, Gopher, and SSL communications (Hudson). The Web Proxy service works with any CERN-compliant Web browser, such as Internet Explorer or Netscape Navigator. The Web Proxy service log also stores the WWW Service information (Internet Information Server) as a subset of the information stored in the Web Proxy service log. To improve performance, turn off IIS logging within the WWW service (Ryvkin).

The WinSock Proxy service supports Microsoft Windows operating systems using Windows Sockets. The WinSock Proxy service log contains connection-specific log information for redirected Windows Socket-based connections. The Sockets interface was extended to support Windows-based clients running Microsoft implementations of TCP/IP. However, the

© SANS Institute 2000 - 2005 Author retains full rights.

service can support other protocols such as Internetwork Packet Exchange/Sequenced Packet Exchange (IPX/SPX). (Hudson)

Log File:
The MS Proxy Server log files can be configured in the IIS Management window within the logging tab. Each proxy service can log to separate log files. The file format can be either a comma-delimited text file, or an ODBC-compliant database. This document discusses text file logs only. When logging to a text file, log fields are separated by the use of a single comma (,). The default locations when logging to a text file are:

Web Proxy service:
C:\Winnt\System32\W3plogs\Filename.log

WinSock Proxy service:
C:\Winnt\System32\Wsplogs\Filename.log

Logging Format:
Both WinSock Proxy and Web Proxy log records contain the user name, client type, client protocol, and time and date stamp. However, there are two levels either Regular or Verbose. By Default the Regular level of logging is set, it supports a reduced number of information fields. The Verbose mode logs detailed information and requires more disk space. Table 1 describes each field for both levels of logging. (Eley)

Table 1. Log File Field Descriptions.

Logging Level: Verbose = V Regular = R	**Web Proxy service**	**WinSock Proxy service**
Client's Computer Name (V & R)	Network IP address for the source computer initiating a request.	Network IP address for the source computer initiating a request.
Client's User Name (V & R)	Windows NT logon account name for the current user on the source computer.	Windows NT logon account name for the current user on the source computer.
Client Agent (V)	None.	Name of the client application that is generating the Windows Socket process request.
Client Platform (V)	None.	0:3.95 Windows 95 (16-bit) 1:3.11 Win32 2:4.0 Windows 95 (32-bit) 3:3.51 Windows NT 3.51

© SANS Institute ins full rights.

Bytes Received (V)	Number of bytes Received from the remote computer.	None.
Bytes Sent (V)	Number of bytes sent to the remote computer.	None.
Protocol Name (V)	Protocol used for transfer: HTTP, FTP, or Gopher	Well-known port number for the socketed application.
Transport Protocol (V & R)	TCP	TCP, UDP, or IPX/SPX.
Operation (V)	Current HTTP method used: GET, PUT, POST, and HEAD.	Current socket API call: Connect, Accept, SendTo, RecvFrom, GetHostByName.
Object Name (V & R)	Shows the contents of the URL request.	None.
Object MIME (V)	Multi-purpose Internet Mail Extensions (MIME) type: application/x-msdownload, image/gif, image/jpeg, multipart/x-zip, or text/plain	None.
Object Source (V & R)	"Unknown" "Cache" "Rcache" Internet Source, object cached. "Vcache" Source is cache, object was verified. "NVCache" Source is cache, object could not be verified. "VFInet" Internet Source, object was verified and failed. "PragNoCacheInet" Source is Internet, Do not cache. "Inet" Internet Source object not cached.	None.
Result Code (V & R)	None.	Error Codes: <100 – Windows error 100 – HTTP status 200 – Successful connection 10060 – Connection timed out. 10065 – Host

© SANS Institute ins full rights.

6/19/01, 11:25:21, W3Proxy, PROXYSRVR, -, www.allsecure.net,
100.100.10.10, 3200, 475, 400, 460, http, TCP, GET,
http://www.allsecure.net/crime.gif, image/gif, Inet, 200
199.200.68.65, anonymous, Mozilla/2.0 (compatible; MSIE 5.0; Win32), N,
6/19/01, 12:21:21, MSFTPSCV, PRXYSRVR, -, 109, 16, 0, 0, 0, [14] USER,
anonymous, -,
200.200.20.20, anonymous, Mozilla/2.0 (compatible; MSIE 5.0; Win32), N,
6/19/01, 12:24:32, W3Proxy, PRXYSRVR, -, www.allsecure.net, 100.100.10.10,
4300, 465, 453, 465, http, TCP, GET, http://www.allsecure.net/prevention.gif,
image/gif, Inet, 200

W3plogs in Regular Mode:

200.200.20.20, anonymous, 6/19/01, 11:18:22, 1, PRXYSRVR,
www.allsecure.net, -, 3495, 428, 400, 460, 0, GET,
http://www.allsecure.net/secrets.gif, -,
200.200.20.20, anonymous, N, 6/19/01, 11:21:22, 1, PRXYSRVR,
www.allsecure.net, -, 3500, 438, 450, 470, 0, GET,
http://www.allsecure.net/evidence.gif, -,
200.200.20.20, anonymous, N, 6/19/01, 11:25:21, 1, PROXYSRVR,
www.allsecure.net, -, 3200, 400, 460, 475, 0, GET,
http://www.allsecure.net/crime.gif, -,
199.200.68.65, anonymous, N, 6/19/01, 12:21:21, 1, PRXYSRVR, -, 109, 16, 0,
0, 0, [14] USER, anonymous, -,
200.200.20.20, anonymous, N, 6/19/01, 12:24:32, 1, PRXYSRVR,
www.allsecure.net, -, 4300, 465, 453, 465, 0, GET,
http://www.allsecure.net/prevention.gif, -,

Example WinSock Proxy Log File:

The WinSock Proxy log file below represents the following activity: On June 19, 2001 at 9:35 to 9:47 a.m. three different users: Wright, Smith and Jones accessed the Webpage not2secure.com via TCP on port 80. The Proxy server with the system name of PRXYSRVR responded to the requests on port 3249. In the log file, Field 1 of each log entry record represents the IP address of the source machine. Compare the detailed information in the Verbose log file with that of the Regular log file.

Wsplogs in Verbose Mode:

192.168.10.100, WRIGHT, -, N, 6/19/01, 9:35:15, WSProxy, PRXYSRVR, -,
not2secure.com, 100.100.10.10, 3249, 477, 80, TCP, Connect, 0
192.168.10.128, SMITH, -, Y, 6/19/01, 9:36:16, WSProxy, PRXYSRVR, -,
not2secure.com, 100.100.10.10, 3249, 477, 80, TCP, Connect, 0
192.168.10.128, SMITH, -, Y, 6/19/01, 9:38:25, WSProxy, PRXYSRVR, -,

© SANS Institute 2000 - 2005 Author retains full rights.

not2secure.com, 100.100.10.10, 3249, 477, 80, TCP, RecvFrom, 0
200.200.20.20, JONES, -, Y, 6/19/01, 9:47:30, WSProxy, PRXYSRVR, -,
not2secure.com, 100.100.10.10, 3249, 477, 80, TCP, Connect, 0

Wsplogs in Regular Mode:

192.168.10.100, WRIGHT, -, N, 6/19/01, 9:35:15, 2, -, -, not2secure.com, -, 3449, 658, 80, -, -, 0
192.168.10.128, SMITH, -, N, 6/19/01, 9:36:16, 2, -, -, not2secure.com, -, 3449, 658, 80, -, -, 0
192.168.10.128, SMITH, -, N, 6/19/01, 9:37:25, 2, -, -, not2secure.com, -, 3449, 658, 80, -, -, 0
200.200.20.20, JONES, -, N, 6/19/01, 9:37:30, 2, -, -, not2secure.com, -, 3449, 658, 80, -, -, 0

Analysis:
When an unusual event occurs, the first step is to identify the IP address in question followed by analysis for more detailed information about the source IP address. RFC1700 is an excellent reference to get a detailed list of ports and the assigned protocol parameters for the Internet protocol suite. The following are basic tools used to gather information about the source address: NSLOOKUP, Ping, Traceroute and a Whois database search. See Scambray Joel, et al Hacking Exposed 2nd Ed for more examples of tools used to gather information.

The next step is for the system administrator to isolate the log files to prevent them from being tampered with since they may need to be used later for forensic evidence. Make a copy of the log files and control access to the files until they are turned over to the investigator (Poulsen).

Summary:
To keep track of what's happening between the internal network and the Internet, the MS Proxy Server allows logging for both WinSock Proxy and Web Proxy Services.
Periodically, the system administrator should monitor the Proxy logs to establish a baseline with "normal" events. Overtime, with practice they will be able to quickly identify unusual activity. If unusual activity appears in either of the log files, further analysis of the event should be performed to determine if an intrusion has occurred. Protective measures should be taken immediately to reduce the risk of attack.

© SANS Institute 2000 - 2005 Author retains full rights.

References:

Eley, Brad. **MS Proxy Server** Installation and Administration Guide: MS Proxy Server Logs. Botkins Local School (BLS) Tech Center, 01 Dec. 1998. 19 Jun. 2001 <http://www.botkins.woco-k12.org/techcenter/faq/mspdocs/10_msp.htm>.

Hudson, Kurt. An Introduction to MS Proxy Server. Windows IT Library, 2000. 10 Jun. 2001 <http://www.windowsitlibrary.com/Content/265/1.html>.

Poulsen, Kevin, et al. Hack Proofing your Network: Internet Tradecraft. Syngress Publishing, Inc., 2000.

Reynolds, J., et al. Request For Coments (RFC) 1700: Assigned Numbers. 1994. 21 Jun. 2001. <http://www.attrition.org/~modify/texts/rfc/rfc1700.txt>

Ryvkin, Kostya, et al. MCSE: Implementing and Supporting MPS 2.0. Prentice Hall, 1999.

Scambray, Joel, et al. Hacking Exposed: 2nd Ed. Osborne, McGray-Hill, 2001.

© SANS Institute 2000 - 2005 Author retains full rights.