VISUACT$_{TM}$ Technical Paper

Network Analysis Technology for Microsoft Network Visibility

Version 1.0

SecurityFriday Co., Ltd.
Michiharu Arimoto <arimoto@securityfriday.com>

March 3, 2004

http://www.securityfriday.com/

- Contents -

<< Overview >>

This paper explains a network analysis technology for Microsoft network visibility.

This network analysis technology for Microsoft network visibility enables the monitoring of all access made to the file server over Microsoft networks, including who accessed the server, when the server was accessed and for what purpose. This technology was developed solely by SecurityFriday Co., Ltd., and currently no similar technology exists.

Microsoft networks allow remote access and use of computer resources (files and printers) over the network and comprise several services, such as name resolution service, computer browser service and resource sharing service. The communication protocols that support these services and functionalities are NetBIOS (Network Basic Input/Output System) over TCP/IP and SMB (Server Message Block) / CIFS (Common Internet File System).

This network analysis technology enables users to:

1) Capture and analyze the packets of several protocols related to Microsoft networks
2) Find related packets based on analysis
3) Develop action information according to analysis and output the information, including who did what action from which computer and to which server

Until now, it was impossible to see who did what on Microsoft networks. The SMB protocol is complicated because its specifications are continuously extended. Even if we focused on the analysis results of each packet of the SMB protocols, therefore, we could not determine who did what.

Utilizing our network analysis technology to monitor access to the file server and users' actions on Microsoft networks can enable anyone to visually understand who accessed the server, when the server was accessed and for what purpose. This technology offers a wide range of uses, such as network management, shared resource management and enterprise security. In particular, by enabling organizations to easily monitor all access and actions in order to find suspicious actions or deter unauthorized accesses over the Intranet, it can contribute to enhanced enterprise security.

1. Introduction

With the proliferation of the Intranet, there is a vast amount of digital information stored in the file server and shared within an organization, with Microsoft networks most commonly used for sharing files. The widespread use of Windows as a client operating system has also made it easy to share files and printers.

While installation and use of a Microsoft network are relatively easy, it is extremely difficult to monitor all access and action on a network. In other words, there are no realistic means of

managing access to the network and shared resources. With numerous incidents these days of information leaking from within an organization, the fact that the company cannot monitor all access and actions on its Intranet is a serious problem.

Our network analysis technology for Microsoft network visibility offers the means for anyone to follow the users' actions on Microsoft networks, and can be effective as an enterprise security measure as well as for network and shared resources management.

2. Features of our network analysis technology for Microsoft network visibility

Our network analysis technology for Microsoft network visibility offers advantageous features. Our technology can:

- Analyze Microsoft network packets and form a relationship between the analysis results of multiple related packets
- Develop action information of who did what from which computer to which server.
- Output action information as soon as an action occurs.

2.1. Analyzing Microsoft networks

Our analysis technology captures packets related to Microsoft networks for analysis. Then, it forms a relationship between the analysis results of multiple related packets. For more information, see the following chapters.

2.2. Developing action information

Even if you decode one Microsoft network packet, you cannot see who did what over Microsoft networks. Multiple related packets need to be analyzed to obtain more practical information about the operations network users have performed.

It is essential that such information be translated and shown in an easy-to-understand format to provide an intuitive view of who did what.

Our analysis technology develops users' action information based on correlated analysis results of related Microsoft network packets.

2.3. Output of action information

Developed action information can be output as soon as an action occurs toward a file server.

Action information can be:

- viewed as soon as an action occurs.
- used as input to a program featuring intuitively recognizable graphical representation of who did what, such as VISUACT Viewer.

- written to a history file to store action information, or used as input to a program capable of writing to a file such as VISUACT Recorder.

2.4. What is action information

Action information refers to information that shows what operation was performed from which computer to which computer, or from which account to which file or directory.

Action information consists of the following items:

A) Timestamp
B) Client IP Address
C) Client Name
D) Client OS
E) Server IP Address
F) Server Name
G) Server OS
H) User Account
I) Message *1
J) Share Name
K) Resource/Object Name *2

*1 The Message item contains information about what was performed from a client computer to a server, such as a file/folder operation, logon, and connection to a shared resource.

Example Message entries:

- An action to a file such as Read, Write, Delete, Rename, and Create
- An action to a directory, such as Delete, Rename, Create, and Search
- Logon/off a remote computer
- Connection/disconnection to a shared resource
- Other entries including obtaining information on or manipulating a remote computer

*2 The Resource/Object Name item contains the name of a target resource or object to which the above action was performed. The type of a resource/object name varies, depending on the type of the message. If a file operation is performed, this item will contain the file name. If a user logs on, it will contain his/her logon account name.

3. Fundamentals for Microsoft network analysis

This section overviews the mechanism used for Microsoft network resource sharing.

Microsoft networks offer name resolution, computer browser, and file sharing services. When a user attempts to access a file on a file server, these services play their roles as follows:

To access a file on a file server, you need to connect to a shared folder on the server. There are several ways to connect to a shared folder on a server from a client:

- Click **My Network Places** and select a computer or a shared resource on the computer.
- Select **Map Network Drive** under **Tool** on Explorer and specify the path name of a shared resource in the dialog box that appears.
- Use the **NET USE** command at the command prompt.

Using one of these methods, a client tries to connect to a shared folder on a server. Establishing a connection depends on the authentication results. In a typical authenticating process, a client sends authentication information including a user name and password to a server. Then, the server sends back the authentication results to the client. If the authentication is successful, connection to the shared folder is established so that the client can gain access to a file/folder under the shared folder on the server.

3.1. Computer Browser Service

This is a service to provide the computer lists displayed in the My Network Places, Select Computer, and Select Domain dialog boxes. The browser service maintains a list of the domain/workgroup names and computer names to display when the My Network Places dialog box is opened.

The protocol used for communication to implement this service is NetBIOS over TCP/IP.

3.2. Name resolution service

This is a service that maps the names of Windows and SMB client computers to IP addresses. Using this service on an intranet using TCP/IP protocol, you can specify a computer name to connect to a server.

The protocols used for communication to implement this service are NetBIOS over TCP/IP and SMB.

3.3. File sharing service

This service allows a remote user to manipulate files in a given folder on a computer, by sharing it with other computers. Microsoft networks allow sharing printers and named pipes in addition to files and folders.

The protocol used for communication to offer this service is SMB (CIFS.)

3.4. Authentication

The authentication service checks if the user account connecting to a shared folder on a server has permission to access the folder. Strictly speaking, authentication takes place when an SMB session is initiated, before connecting to the shared folder.

Challenge and response authentication, including LM and NTLM authentications, are traditionally used, but the KERBEROS authentication service is commonly used in Active Directory domain environments for Windows 2000 or higher.

When LM or NTLM authentication is used, the SMB protocol is used to send/receive challenge and response data between a server and a client, while the KERBEROS or SMB protocol is used to send/receive keys and tickets when KERBEROS authentication is used.

4. Analyzing Microsoft networks

As described above, Microsoft networks rely on different services, communication protocols, and authentications that are intricately intertwined with each other. Numerous enhancements have also been made to the SMB protocol that is used for file sharing, resulting in increased complexity. In addition, all the specifications are not public, thus making it impossible until now to see who did what over Microsoft networks.

This section describes how our analysis technology visualizes who did what over a Microsoft network, based on the assumption that the lower-layer protocol for the Microsoft network is only TCP/IP.

4.1. Capturing Microsoft network packets

First, packets traveling between a client and a server need to be collected.

Using a packet capture driver, packets sent to a server can be collected at a computer other than the server. This driver allows your NIC to be switched into promiscuous mode to capture all collectable packets.

In today's networking environments, the port mirroring feature offered by switching hubs equipped with mirror ports, SPAN ports, or repeater hubs are commonly used.

4.2. Ports related to Microsoft networks

Microsoft network packets to be analyzed are captured at the following ports:

139: used mainly for the file sharing service using SMB/CIFS protocol

445: same as 139

137: used mainly for the name resolution service using NetBIOS over TCP/IP protocol

138: used mainly for the computer browser service using NetBIOS over TCP/IP protocol

88: used mainly for KERBEROS authentication

4.3. Analyzing Microsoft network packets

This section describes how collected packets are analyzed.

Upon receipt of a packet from a network, it is decoded in reference to its corresponding protocol format to extract and accumulate the data required to develop action information as described later.

Packets sent through the protocols used in Microsoft networks can be analyzed with some commercial and non-commercial packet analyzers, but none of them can fully decode all the packets since some of the protocol specifications have not been disclosed. There are not any packet analyzers that can support authentication packet formats that are frequently updated. At Security Friday, we have uniquely analyzed the authentication packet formats and our resulting technique is deployed to develop this analysis technology.

4.4. Forming a relationship with packet analysis results

Analyzing one SMB packet will not tell you who did what toward a file server, since the SMB protocol assigns ID numbers to a user, a connected resource, and a target object such as a file or a folder. In order to identify what each ID number represents, you need to trace back a series of related packets and reference their analysis results. It is essential to associate analysis results of the individual packets, especially SMB ones, to track who did what toward a file server.

4.4.1. Forming a relationship with SMB packet analysis results

As far as we know, there are seventy or more commands coded for the multifunctional SMB protocol and some of the commands have subcommands.

The following characteristics of the SMB protocol should be considered for analysis.

- For most of the commands, a request/response pair is defined.
- ID numbers contained in the SMB header identify a user and resources.
- To perform an identical operation to manipulate an object such as a file, different combinations of commands may be used.

4.4.2. SMB file access process flow

SMB allows access to files in the following steps:

A) Negotiation

A server and a client negotiate to determine what version should be used for communication.

B) SMB session establishment

A SMB session is established. At this stage, user authentication is performed. If authentication is successful, an ID (UID) is assigned to the user.

Selection of the authentication to be used depends on several factors including authentication schemes supported by clients and servers, security settings, and what client application was used.

If a traditional challenge-response authentication is used, the user account name used to logon to a server will be found by decoding packets used at this phase. For KERBEROS authentication, however, a user account name will not be ascertained.

C) Connecting to shares

A connection to a shared resource designated by a client is initiated. If the connection is established, an ID (TID) will be assigned to the connected resource.

D) Object manipulations including READ, WRITE, DELETE, RENAME, CREATE

To perform one identical operation to manipulate an object such as a file, different combinations of commands may be used.

When an object is typically opened or created, however, an ID (FID) is assigned to the object and this FID is used to designate the object to which subsequent commands such as read and write are issued. An FID is not contained in the SMB header. Different SMB commands put an FID in different locations (offset) within a packet. Some SMB commands do not use an FID. They specify the exact name of an affected object.

E) Disconnecting a shared resource

Connected shares are disconnected. The share to be connected is specified with its ID (TID).

F) Disconnecting an SMB session

The established session is disconnected. The user is specified with its ID (UID) assigned when the connection was established.

4.4.3. Forming a relationship with NetBIOS over TCP/IP packet analysis results

Packets sent through SMB, a protocol designed to allow networked computers to share files, do not provide enough information about each computer.

Analyzing packets sent through the NetBIOS over TCP protocol lets you know local logon account names, computer names, and types of operating systems. Our analysis technology correlates this data with analysis results of SMB packets, using an IP address.

4.4.4. Forming a relationship with KERBEROS packet analysis results

If KEBERROS authentication is used when establishing an SMB session, the name of a

network logon account will not be determined by simply analyzing SMB packets.

A network logon account name is specified in KERBEROS packets that request a domain controller (Kerberos key distribution center or KDC) to issue a ticket-granting ticket (TGT). Therefore, the packets used when a TGT is issued need to be decoded and referred to.

By associating analysis results of packets containing a request for a TGT, an issued TGT, and a service ticket to access a file server, our analysis technology can locate the network logon account name used for KERBEROS authentication.

5. Conclusion

The development of our network analysis technology for Microsoft network visibility enables anyone to monitor all access and actions on Microsoft networks.

This technology was utilized by SecurityFriday in order to develop the products, VISUACT tm and VISUACT tm TRANSLATOR. These products can be used to deter unauthorized access within an organization and record all evidence of network intrusion. They are also equipped with a function to write action information to text format log file, or send it with Syslog or our uniquely formatted UDP packets to the network. This output function can be used in conjunction with IDS (Intrusion Detection System), IDP (Intrusion Detection and Prevention) and log management tools to prevent unauthorized access within the Intranet as well as improve network management.

[References]

- Karl Auerbach, " PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: CONCEPTS AND METHODS", RFC 1001, March 1987.
- Karl Auerbach, " PROTOCOL STANDARD FOR A NetBIOS SERVICE ON A TCP/UDP TRANSPORT: DETAILED SPECIFICATIONS", RFC 1002, March 1987.
- P. Leach, D. Naik, "Common Internet Files System Protocol (CIFS/1.0) Internet Draft", December 19, 1997.
- Hidenobu Seki, "Cracking NTLMv2 Authentication" , February 8, 2002.
  URL: http://www.blackhat.com/presentations/win-usa-02/urity-winsec02.ppt
- Samba. URL: http://www.samba.org/
- Luke Kenneth Casson Leighton, "DCE/RPC OVER SMB: SAMBA AND WINDOWS NT DOMAIN INTERNALS", MacMillan Technology , December 1999.
- J. Kohl, C. Neuman, "The Kerberos Network Authentication Service (V5)", RFC 1510, September 1993.
- Microsoft Corporation, "Windows 2000 Kerberos Authentication White Paper", July 9, 1999.