Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

SANS Windows Security Training

Almost every security checklist for Microsoft Internet Information Services (IIS) recommends that servers with the IIS web service installed on them should not be placed into Windows Domains. I have embraced this recommendation within the automated secure server builds that I have developed for a large dedicated hosting provider. However, the questions I am now being asked are "Why shouldn't I place my IIS Web Servers into a Windows Domain?" and "How do I add my IIS Web Server to a Windows Domain so that I maximise sec...

Copyright SANS Institute

Author Retains Full Rights

AD

IIS Web Servers and Windows Domains

Philip Blow

30th September 2001

Introduction

Almost every security checklist for Microsoft Internet Information Services (IIS) recommends that servers with the IIS web service installed on them should not be placed into Windows Domains. I have embraced this recommendation within the automated secure server builds that I have developed for a large dedicated hosting provider. However, the questions I am now being asked are "**Why shouldn't I place my IIS Web Servers into a Windows Domain?**" and "**How do I add my IIS Web Server to a Windows Domain so that I maximise security?**"

This paper will answer the above questions in relation to both the Windows Directory Services that are currently being utilised on the Internet – these being Windows NT 4.0 Domains and Windows 2000 Active Directory. This paper will suggest a network architecture and installation process that can be used when the inclusion of IIS web servers in a Windows Domain cannot be avoided.

Before the questions can be answered I will provide an overview of Windows Directory Services.

Overview of Windows Directory Services

This paper is concerned with the two recent implementations of Microsoft Windows Directory Services.

Both implementations of Directory Services provide a mechanism for network users to connect to multiple servers or services with a single network logon as well as allowing the administration and management of networked workstations and servers to be centralised.

Windows NT 4.0 Domains and the Windows 2000 Active Directory objects are the administrative units for the Directory Services provided by the operating systems they are implemented on.

Windows NT 4.0 Domains

Microsoft's definition of a Windows NT 4.0 Domain is a "logical grouping of network servers and other computers that share common security and user account information". A Windows NT 4.0 Domain does not imply a single physical location or any specific network architecture. A domain is only an administrative unit of the Windows NT 4.0 Directory Services.

Typically Windows NT 4.0 Domains contain each of the following components.

- Directory Database – This database stores all the security and user information for a domain. This database is often referred to as the Security Accounts Manager (SAM) database.
- Primary Domain Controller (PDC) – Primary Domain Controllers have the Windows NT 4.0 Server operating system installed on them and hold the master copy of the SAM database for a single domain. Any changes to the SAM database can only be performed on the PDC. There can only be one PDC per domain.
- Backup Domain Controller (BDC) – Backup Domain Controllers have the Windows NT 4.0 Server operating system installed on them and hold a copy of the domain's

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

SAM database. The BDCs also handle the majority of the requests for user authentication. The BDC's copy of the SAM database is periodically updated with the master database from the PDC. There must be at least one BDC in a domain.

- Member Servers – Member Servers have the Windows NT 4.0 Server operating system installed on them, but do not store copies of the SAM database. Member servers provide services, such as application services or file and printer sharing.
- Client Workstations – Client workstations have either Windows 9x or Windows NT 4.0 Workstation operating systems installed on them and are used by domain users to access shared services.

Windows NT 4.0 Domains allow security polices to be defined and implemented across any server or client in a domain. However, if different polices are required for different clients then the name of the client must be known and a separate policy must be defined for each named client.

Windows 2000 Active Directory

In Windows 2000 Server, Microsoft has introduced "Active Directory" to implement the Windows 2000 Directory Services. Active Directory is a distributed data store that contains information about network objects and their relationships. The relationships between the network objects are defined during the creation and evolution of an organisation's Active Directory.

The Active Directory data store is stored on a special type of Windows 2000 Server called a Domain Controller. A domain can have multiple Domain Controllers. Any Domain Controller can respond to a query on the Active Directory data store as the data store is replicated across all Domain Controllers in a domain.

An Active Directory data store contains object definitions that are used to represent physical or logical items on a network. The Active Directory contains object definitions for shared resources (i.e. servers or printers), user accounts, domains, security policies, applications and services.

All objects within an Active Directory can be placed into containers. The standard set of containers includes domains, trees, forests and organisational units. A description of each container and its relationship to other containers is detailed below.

- Domains – An Active Directory is made up of one or more domains. A domain is a container for organisational units, computers, printers, users and groups. The name of a domain must be defined within the Domain Name System (DNS). A domain also defines the boundary for the security and group polices.
- Trees – A tree is a set of domains that have a common root domain and hence a common root within the Domain Name System. For example, the domains *acme.com* and *marketing.acme.com* form a tree. Security or group policies can be inherited through the domain tree.
- Forests – An Active Directory forest contains more than one or more trees or root domains. For example, an Active Directory that contains the *acme.com* tree and *star.com* tree is considered to be a forest.
- Organisational Units (OU) – An Organisational Unit allows system administrators to logically store, organise and administer objects within a domain. An organisational unit can contain computers, printers, users, groups or other organisational units. Organisational Units can inherit or redefine security and group policies as required.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Active Directory allows security and group policies to be defined across domains and organisational units. Active Directory also allows for security and group policies to be inherited through domain trees and the organisational units defined within domains. The inheritance model provides the administrator with greater control over both the definition and application of security and group policies.

Why include IIS Web Servers in a Windows Domains

It is sometimes necessary to include IIS Web Servers in Windows Domains. Some of the most common reasons include:

- The administration and management of all web and application servers that make up a large site is easier within a domain. That is, a set of domain accounts can be used to administer both web and application servers.
- Some application services (for example, content publication or document indexing systems) may require that the web and application servers be placed in a domain to simplify authentication.

Why not to include IIS Web Servers in Windows Domains

Some of the issues with including IIS web servers in Windows Domains are described below along with some of the risks associated with each of the issues.

- A domain creates trust between servers and clients. You might ask, "Isn't that the whole point?" Yes it is the point of using domains, but once one of the web servers in the domain is compromised and user level access is achieved, any server in the domain can be compromised by using the relationship provided by domain accounts. It should be noted that using the same account name and password combination across multiple standalone servers will cause implicit trusts between the servers, which will cause the local accounts to act in the same way as a domain level account. See http://www.securityfocus.com/cgi-bin/infocus.pl?head=Windows%202000/NT:Securing&id=1353 for a more thorough description of the risks of using common account names and passwords.
- Installing web services on servers that are already part of a domain will cause the IUSR_*computername* account (used for anonymous web access) to be added to the Guests domain group. An example of what can be done when the IUSR_*computername* account in a domain is compromised can be found at http://packetstormsecurity.org/9906-exploits/iusr_bug.txt.
- Installing web services on a domain controller can allow domain accounts to be enumerated and their passwords cracked more easily if the web server is compromised. Installing a web server on a domain controller can also slow down the serving of content due to the additional processing required by domain authentication and management requests.
- Windows NT 4.0 is vulnerable to null session attacks if not secured correctly. Null sessions can allow the enumeration of the SAM database, which includes information about user names, passwords and group information. See http://www.securityfocus.com/cgi-bin/infocus.pl?head=Windows%202000/NT:Securing&id=1352 for more information
- The authentication and replication services implemented within the Windows Directory Services require the SMB (Server Message Block) and NetBIOS protocols. Both of these protocols are inherently insecure and are susceptible to SMB hijacking,

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

SMB downgrade and SMB encrypted handshake interception as well as password sniffing with programs such as L0phtCrack. These attacks can be mounted directly from the Internet if the web servers, firewalls or packet filters are not configured correctly. See http://www.sans.org/infosecFAQ/win/SMB.htm for more information on the vulnerabilities associated with the Server Message Block protocol. See http://www.atstake.com/research/lc3/index.html for more information on L0phtCrack version 3.

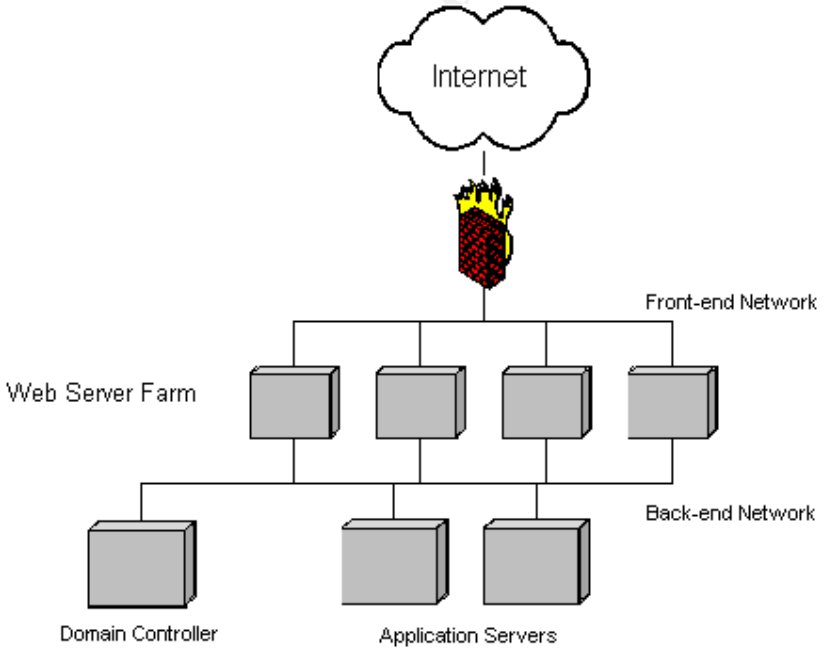
A Secure Windows Domain Architecture for IIS Web Servers

This section assumes that one or more web applications are to be made available over the Internet through two or more IIS Web Servers. The applications require that both the application servers and web servers be contained within the same Windows Domain.

The following sections suggest a secure network architecture for including IIS Web Servers in a Windows Domain and a process for installing and configuring IIS Web Servers and their associated application servers for inclusion in a Windows Domain.

Network Architecture

The diagram below shows the suggested secure network architecture for use with Windows Domains. This architecture or minor variations to it should be suitable for web applications that utilise either IIS 4.0 or IIS 5.0 web services. The network architecture should only be used in conjunction with the installation and configuration procedure provided in the next section.



The features of the network architecture are:

- The front-end network connections are connected through a firewall or packet filter prior to being connected to the Internet.
- All web-facing servers must be connected to both the front-end and back-end networks.
- The back-end network directly connects to both the web facing servers and the back-end domain controllers and application servers.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- The domain controllers and application servers are never directly connected to the front-end network.

Installation and Configuration

The installation and configuration process following should only be used in conjunction with the network architecture described above.

- Install and rack all required hardware in a physically secure location.
- Initially install all web servers as standalone servers and only connect the web servers to the back-end network. This will ensure that all accounts created for use by the web servers are local accounts only and that the servers cannot be compromised during configuration.
- Install all application servers as standalone servers but do not install any of the required applications. The application servers should only be connected to the back-end network.
- Secure web and application severs using the applicable sections of at least one of the following security checklists.
    - The SANS Institute, Windows NT Security Step-by-step. (http://www.sans.org)
    - The SANS Institute, Windows 2000 Security Step-by-step. (http://www.sans.org)
    - National Security Agency, Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0. (http://nsa2.www.conxion.com/win2k/index.html)
    - Microsoft, Secure Internet Information Services 5 Checklist. (http://www.microsoft.com/technet/itsolutions/security/tools/iis5chk.asp)
    - Microsoft, Securing Internet Information Server 4.0 Checklist. (http://www.microsoft.com/technet/itsolutions/security/tools/iischk.asp)
    - Microsoft, Windows Domain Controller Checklist. (http://www.microsoft.com/technet/itsolutions/security/tools/dccklst.asp)
    - Microsoft, Windows NT 4.0 Member Server Configuration Checklist. (http://www.microsoft.com/technet/itsolutions/security/tools/mbrsrvcl.asp)
    - CERT® Coordination Center Windows NT Configuration Guidelines. (http://www.cert.org/tech_tips/win_configuration_guidelines.html)
- Install and secure the domain controllers using at least one of the checklists above.
- Add each of the web and application servers to the domain.
- Install and configure the web applications. Ensure that only the minimum set of accounts required for the web application to operate are added to domain groups.
- Secure all installed applications by following the application developer's instructions.
- Ensure that the most recent Microsoft service packs and hot fixes are applied to all servers. Also ensure that the most recent version of all application related patches are installed.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Ensure that the NTLMv2 authentication protocol is used across all servers in the Windows Domain.
- Ensure all local and domain administrator accounts have strong and unpredictable passwords. Also ensure that the passwords for all local accounts are unique, strong and unpredictable.
- Ensure that the NetLogon service on all servers in the domain is configured to require digital signing and encryption of all NetLogon Channel traffic.
- Ensure that anonymous access is restricted on all web and application servers.
- On Windows NT SMB over NetBIOS is required for domain authentication and file sharing. On Windows 2000 either SMB over TCP or SMB over NetBIOS can be used for domain authentication and file sharing. Ensure that all ports that provide SMB services are blocked by the packet filter or firewall so that they are not accessible from the Internet. The ports that should be blocked are TCP ports 135, 137, 139, 445 and UDP ports 137, 138, 445.

  Another method that could be used is to disable NetBIOS over TCP/IP on all servers and then install and bind the NetBEUI protocol to all back-end network interfaces. The NetBEUI protocol is non-routable and using NetBEUI will help to ensure that authentication traffic on the back-end network is not routed out of the back-end network.
- Ensure that IP forwarding is disabled on all servers that are connected between the Internet and the back-end network.
- Install and configure a lightweight (personal) firewall on all application servers and domain controllers.
- Configure the firewall/packet filter so that the only open protocols and ports are those required for application service delivery. Most commonly these would only be 80/TCP, 443/TCP, 53/TCP and 53/UDP. Packets directed to all other protocols and ports should be dropped.
- Connect the web servers to the front-end network but do not connect the firewall/packet filter to the Internet.
- Test the web site through the firewall/packet filter to ensure all web application services are provided as required prior to deployment.
- Perform an ethical hack of the web farm and evaluate the results. Ensure that all currently known vulnerabilities cannot be exploited.
- Perform a baseline audit of all servers in the web farm to assist in identifying any unexpected changes to the web farm's configuration.
- Connect the firewall/packet filter to the Internet.

After the site is connected to the Internet the following periodic maintenance tasks should be performed.

- Ensure all relevant operating system and application related security updates are applied to all servers as soon as possible after the update is released.
- Make sure that the number and use of domain accounts is tightly controlled.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- Perform regular audits of all accesses to the web site via domain accounts to ensure that the accounts are being used for their intended purpose.
- Monitor all firewall and server logs for any unauthorised access and take appropriate action if required.
- Perform an ethical hack of the web farm and evaluate the results. Ensure that all previously tested vulnerabilities cannot be exploited. Especially test for new vulnerabilities since the last ethical hack.

Conclusions

There are an ever increasing number of vulnerabilities and exploits being discovered for both Microsoft Windows and IIS. When IIS web servers are used as the Internet connect point for a web application all known and unknown vulnerabilities are exposed to malicious users on the Internet.

The inclusion of IIS web servers in a Windows Domain extends the exposure to vulnerabilities beyond the scope of individual web servers to include the web application and any associated data. The exposure is primarily due to the trust relationships provided within Windows Domains and the services required to support the domain environment.

If IIS web servers are to be included in a Windows Domain, a secure network architecture should be defined and implemented; a set of installation and configuration steps must be derived from known best practice and used to build all servers in the domain; and all associated risks and exposures must be identified, assessed, documented, monitored and periodically re-evaluated to ensure that the integrity of the web farm is maintained.

References

Brown, Brian. "WINDOWS NT SERVER v4.0, NT Domains." Networking Windows NT Server. URL: http://www.cit.ac.nz/smac/winnt/pt3_4.htm (8 Sep 2001)

Brown, Brian. "Active Directory: Part 1." Networking Windows 2000 Server. URL: http://www.cit.ac.nz/smac/win2000/pt5_1.htm (8 Sep 2001)

Kling, Judi. "Exploring Windows NT / So many Active Directory domain models, so little time..." September 2000. URL: http://www.elementkjournals.com/ewn/0009/ewn0091.htm (7 Sep 2001)

Marvin, Daniel. "The NT Local Administrator and Shared Passwords." 2 Apr 2001. URL: http://www.securityfocus.com/cgi-bin/infocus.pl?head=Windows%202000/NT:Securing&id=1353 (5 Sep 2001)

Microsoft Corporation. "Active Directory Architecture White Paper." 12 Oct 1999. URL: http://www.microsoft.com/windows2000/techinfo/howitworks/activedirectory/adarch.asp (1 Sep 2001)

Microsoft Corporation. "Domain Planning Guide (Downloadable Document)." Microsoft Windows NT Server Concepts and Planning Guide – Chapter 1. 13 Jul 2001. URL: http://www.microsoft.com/ntserver/techresources/deployment/NTserver/DomainPlanGuide.asp (1 Sep 2001)

Mullen, Timothy M. "RestrictAnonymous: Enumeration and the Null User". 12 Feb 2001. URL: http://www.securityfocus.com/cgi-bin/infocus.pl?head=Windows%202000/NT:Securing&id=1352 (10 Sep 2001)

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Network ICE Corporation. "Port Knowledgebase." URL: http://networkice.com/advice/exploits/ports/ (9 Sep 2001)

Northcutt, Stephen, et al. Windows NT Security Step-by-Step – Version 3.03. The SANS Institute, Feb 2001.

Shawgo, Jeff, et al. Windows 2000 Security Step-by-Step – Version 1.0c. The SANS Institute, 20 May 2001.

Shores, Elizabeth. "Security Concerns with Microsoft Networking or SMB". 27 May 2001. URL: http://www.sans.org/infosecFAQ/win/SMB.htm (6 Sep 2001)

Sutton, Steve. "Windows NT/2000 Security – a Perspective". URL: http://www.trustedsystems.com/nt_security.htm (3 Sep 2001)

Unknown Author. "Internet User Bug Security Hole". 10 Jun 1999. URL: http://packetstormsecurity.org/9906-exploits/iusr_bug.txt (10 Sep 2001)

Walker, William E, et al. Guide to the Secure Configuration and Administration of Microsoft Internet Information Services 5.0 – Version 1.2. Network Applications Team of the Systems and Network Attack Center, 20 Aug 2001.

© SANS Institute 2001, Author retains full rights

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced