Global Information Assurance Certification Paper

A Look at Novell Nterprise Linux Services (NNLS) from a Security Viewpoint

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b
Option 1

By: Chong Su Liang
August 2004

Table of Contents

Abstract

The main objective of this paper is to provide its readers with a basic understanding of the Novell Nterprise Linux Services (NNLS) product from a security viewpoint, and to explore how these services can be made more secured together with other deployment strategies as part of the defense in depth principle. A checklist is available specific to the service discussed that offers a range of non-exhaustive security pointers to the readers who will be deploying the NNLS.

What is Novell Nterprise Linux Services (NNLS)?

Novell Nterprise Linux Services (NNLS) is a set of enterprise services ported from Netware that allows organizations now to take advantage of the open-source benefits of Linux. New services that do not have Netware ancestry have also been included in the suite.

Nterprise Linux Services v1.0, Novell's first release on December 18, 2003, provides Linux servers with a the following services for the enterprise:

- Identity Services
- File Services
- Messaging Services
- Print Services
- Services Management
- Web Access to Services

Identity Management Services

Identity management solutions play a significant role in managing secure access to information and applications of diverse nature and technological origins in today's technological age.

The identity management services offered by NNLS leverage on eDirectory, Novell's market-leading LDAP technology, as well as DirXML, a technology that connects the eDirectory to multiple directories such as another eDirectory, NT Domains, or Active Directory.

eDirectory

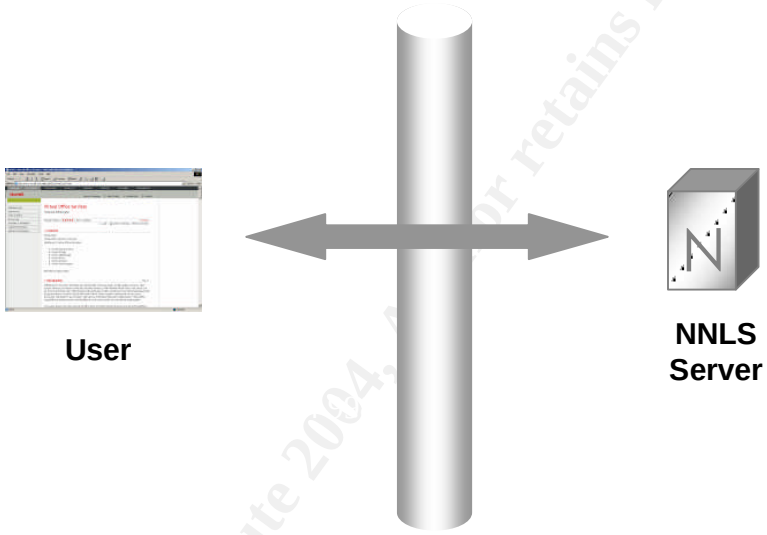
On its own, the Lightweight Directory Access Protocol (LDAP) allows users to search and access information in a directory structure. Because LDAP services include account management, authentication, authorization and identity management, LDAP is also well suited to form the basis of an authentication and network information system in an organization.

Since data stored in the directory is either an object or an object's attribute, permissions and rights can be configured right down to the attribute level. This

feature allows authentication (proving that the user is who he says he is) and authorization (controlling what the authenticated user is allowed to access based on his right and permissions) to be extremely granular in directories.

Access rights and permissions are security controls that are in line with the organization's security policy. Such information is more commonly read than written or updated, and this makes LDAP-compliant directories very suitable for the authorization process, as they possess very fast read operations.

The Novell eDirectory is the centerpiece of NNLS. It provides centralized LDAP-based authentication and authorization service on behalf of all other NNLS components, thus eliminating the need to implement access control mechanism within each service. With all user permission and rights centrally managed, the eDirectory acts as a secure LDAP-based authentication server to any request for information from the organization's directory.



Authentication through **eDirectory** running on NNLS Server

The eDirectory includes Public Key Cryptography Services (PKCS), which contains the Novell Certificate Server that provides Public Key Infrastructure (PKI) services, Novell International Cryptographic Infrastructure (NICI), and SAS-SSL server.[1] SAS (Novell's Secure Authentication Services) facilitate secure authentication via SSL and PKI.

The Novell Certificate Server allows an organization to create, issue and manage certificates on its own without having to go through an external Certificate Authority (CA). This has significant cost savings in terms of obtaining key pairs and managing public key certificates. However, key management tasks like issuing, key recovery, updating and key revocation can be daunting if the organization is very large. Organizations should weight the pros and cons of managing their own certificate server before deciding to do so.

[1] Novell, Para 1.
http://www.novell.com/documentation/edir87/index.html?page=/documentation/edir87/edir87/data/a7elxug.html#a7gpwfg

The eDirectory natively supports the directory standard LDAPv3 and provides support for TLS/SSL services based on the OpenSSL source code.[2]

The IETF corrected some defects in the SSL mechanism and published a standard called RFC 2246 which describes TLS ("Transport Layer Security"), which is simply a cleaned up and standardized version of SSL.[3]

TLS/SSL provides the following security features:

1. **Confidentiality**. Supports symmetric key cryptosystems such as RC4 (128-bit key by RSA) and 3DES (Triple Data Encryption Standard). Encryption of information ensures that the necessary level of secrecy has been enforced and unauthorized disclosure prevented during the transmission process.

2. **Integrity**. Supports hash functions such as MD5 (Message Digest 5) and SHA (Secure Hash Algorithm). The resulting hash values provide assurance that the information received is accurate, reliable and has not been modified by unauthorized means.

3. **Authentication**. RSA is being used for key exchange and digital signatures in SSL, while TLS added support for Diffie-Hellman key exchange. Strong authentication is made possible by allowing two parties exchange a secret key securely even in the presence of an attacker or over a non-secure network.

4. **Non-repudiation**. The employment of digital signatures ensures non-repudiation between different parties making a transaction.

A normal LDAPv3 connection is susceptible to DNS poisoning or other attempts to impersonate as the real LDAP server, where the integrity of directory information received by the client becomes questionable.

Clients should be connected to the LDAP server over TLS/SSL to address this issue. This connection method, commonly known as secure LDAP, ensures that clients with the LDAP server's certificate and the certifying authority (CA) are communicating with the authentic server. Secure LDAP also encrypts sensitive data such as passwords during an LDAP-based connection, to prevent sniffing attacks and ensure the confidentiality of data being transmitted.

When a user logs in anonymously and subsequently requests for privileged data, all traffic will switch from clear text to encrypted data via TLS that supports such on-demand encryption over an LDAPv3 connection.

Although TLS/SSL can be employed to provide a secure encrypted tunnel between the users and NNLS server, security is often found lacking where data gets decrypted on both ends. Attackers have found that it is much easier to target at the

---

[2] Novell Inc, Para 3.
http://www.novell.com/documentation/edir873/edir873/data/fbadjaeh.html
[3] Ridd, Chris, Para 1.
http://search.cpan.org/~gbarr/perl-ldap/lib/Net/LDAP/Security.pod#How_does_LDAP_and_TLS_work

data decrypting ends instead of trying to sniff the packets during transmission, since so much data nowadays are encrypted via SSL. Thus one should not have the misconception that just by having SSL alone will solve all security issues. Understanding what SSL can protect and what it cannot protect from is important to securely protect the organization's network and resources. Efforts should be made to secure the client machines from viruses, worms and Trojans, and to harden the server from other attacks. Moreover, one should also take note of the fact that attacks transmitted over TLS/SSL cannot be detected by network-based IDS, thus other forms of detective measures must be taken to provide proper alerts and warnings to the administrator.

A security checklist to remember when implementing eDirectory:

- The eDirectory login security is not provided in the default installation. Administrators can configure the appropriate security measures supported by eDirectory, such as enforcing strong login passwords, imposing login restrictions by location and time, or limiting the number of concurrent logins sessions.
- The *User Admin* account by default has complete control over the entire directory, so be careful not to assign this account to any administrator of lesser rights.
- Any public user accessing the directory services by default has the right to browse through any object in the tree, although access to the attributes is not permitted. Administrators may want to limit a public user's default read access since it is not a good idea to reveal too much information to the public, as an attacker is able to make use of these information to help him gain unauthorized access.
- Implement a time synchronization service across the servers' network. Time synchronization is provided by Linux OS in NNLS, and is important for accurate logging so that different events can be properly time-correlated when necessary, especially in the event of a suspected attack.
- Configure iMonitor to be accessible only from trusted locations, as far as possible. The iMonitor is a web-based management utility that provides important information about the directory for the administrator who is accessing from any remote location. Enforce that all remote access to iMonitor must be through a VPN connection. Limit the type of access allowed through iMonitor to further protect from Denial of Service (DoS) attacks.[4]
- Monitor the eDirectory to ensure that it is running. The LDAP server will first be loaded before running, and then it will start listening for requests. Checking that the server runs properly is important because it could be either under a D0S attack or the configuration objects are misconfigured or corrupted, when it is loaded but not running. The DoS attack could be caused by a valid user's extensive search request that holds up all the server's resources.
- Limit the size of a search. This can help reduce the possibility of a DoS attack described in the previous point.

[4] Novell Inc, Para 1, Point 2.
http://www.novell.com/documentation/edir873/edir873/data/a7gq3a8.html

- Change or remove informative banners that the server will display to users who have logged in. Withholding the product name and version number can help make an attack's reconnaissance work more difficult.

One may be interested to know how Novell eDirectory compares to another popular directory product, Microsoft Active Directory in terms of security.

Both eDirectory and Active Directory support a range of authentication options, such as simple passwords, (including SHA-1 and MD5 password hashing), PKI, biometrics, smart cards, tokens, etc.[5] Both are able to support multi-factor authentication using a user's password (what he knows), tokens or smart cards (what he has), and biometrics (who he is).

Novell eDirectory, however, offers support for graded authentication. This means that a user's access right can vary by the method of authentication or the combination of several methods. Thus an employee can have access to only company confidential files with his normal password, while with a token and the password he can now have access to more sensitive data. This feature makes it possible for an organization to limit a user's access level to protected resources right down to the task that he is performing at any time.

The eDriectory is able to carry out backup of its data while it is online and active, making it possible for the directory service to be available at all times. Moreover, it has the hot continuous backup capability to record all directory data changes almost real-time, meaning data backup of up to the last second's data.

Active Directory follows the same backup-and-restore methodology Microsoft used with Windows NT.[6] At scheduled backup times, the Active Directory needs to be shut down so that a copy of the directory database at that time instance can be made. This affects the availability of the directory service. A restore will only bring the directory back to the point when the last scheduled backup was made.

Of course, the availability of the directory service may not pose as a serious issue to some organizations due to the nature of their businesses. But this should be an important feature to take into account when deciding between different directory products.

DirXML

Novell DirXML works by offering XML-based data transformation engines and connectors for integration across multiple directories to simplify time-consuming administrative tasks. DirXML allows a data to be keyed in only once into eDirectory, a master directory, and this data will be transformed into each specific format and replicated across the different directories that an organization may be having.

[5] Novell Inc, Page 20, Para 6.
http://www.novell.com/collateral/4621396/4621396.pdf
[6] Novell Inc, Page 15, Para 1.
http://www.novell.com/collateral/4621396/4621396.pdf

Single Sign-On across directories is achieved when the identity management services are completely implemented and various directories integrated using DirXML. Passwords are generated once in a directory and they get replicated across to the other directories. However, retrieval of passwords and compromising any of these directories would mean access to all the applications and systems in the organization. Hence proper securing of the directories is crucial to a secured identity management solution.

Since DirXML has been designed to integrate tightly with the eDirectory, the DirXML connectors help to reduce the risk of fault line attacks. In general, interfaces between various systems and subsystems in multi-vendor environments fit well but not perfectly due to varying standards used. Thus a skilled attacker could well be able to exploit weaknesses in these gaps and gain unauthorized access to the directory data. The tighter the integration between systems, the lesser would be the chance of such attacks occurring.

The eDirectory and DirXML also help tighten access control management to keep data confidential. When an employee leaves the organization, the Novell identity management solution is able to disable his associated user accounts and change his associated role passwords for in all the different applications using their individual directory systems - all from a single master directory. Without this integrated feature, organizations may run the risk of having unchanged passwords or active accounts that should be disabled, even months after the employee has left.

This access control feature also minimizes the window of time between when a security control is applied and when the service is used, known as the Time of Check/Time of Use (TOC/TOU). In this case, will be the time when the account is being disabled and the time when the ex-employee can continue to gain access with his soon-to-be disabled account. Without tight integration among difference directories in a multi-platform organization, this window could be considerably long enough to be susceptible to what can be considered as a form of TOC/TOU attack. Updates to the master directory server will trigger almost real-time synchronizations across directories on other platforms that would not be possible without DirXML.

A security checklist to remember when implementing DirXML:

- Because implementing DirXML may involve other directory products such as Active Directory, NT Domain or even another non-master eDirectory, efforts must be taken to secure these directory products first before linking them up to the eDirectory as the master directory server. Compromising these systems will also affect the security of the eDirectory server in NNLS.
- Because it is common to implement Single Sign-On through DirXML's password synchronization feature, it is important to enforce strong passwords chosen by the users. It is a challenging task to educate and facilitate the users' efforts to provide strong passwords without having to write them on post-it pads beside their computers.

File Services

The file services offered allow enterprises to provide web- and network-based file storage to their network users.

The file services components in NNLS include the following:

Novell iFolder

The Novell iFolder is a personal file management service that synchronizes data automatically between the client and server, while providing data protection and backup.

There are several components in iFolder: the iFolder server and iFolder client – available either as a client program or as a Java applet accessible through a browser. First, the user will authenticate to the iFolder server via the LDAP server, after which he will have access to the iFolder data from his client machine. The iFolder ensures that the user will always have the latest version of his data. During data transfer sessions, users accessing the iFolder service online will be able to encrypt their files via SSL as long as the server has been configured accordingly.

The unique feature that iFolder offers is its ability to synchronize files without having to transmit the whole chunk of data all the time. The iFolder seeks to recognize only the delta changes in files and synchronizes these delta changes across the network, which is faster and less bandwidth-intensive. This feature however, is subjected to how the different third-party applications write to their data. For instance, Microsoft Word rewrites the complete file regardless of how minor the change. Thus iFolder will recognize it as a 100% new content and synchronize the whole file.[7]

The client version uses a more secured file encryption mechanism through 128-bit Blowfish algorithm. Users need to activate this feature by supplying a pass phrase. The file encryption feature should not be an option that users need to turn on explicitly, and a pity that it has been turned off by default. Sending files in clear text is highly susceptible to network sniffing attacks.

Another security concern common to all web-based file management systems is that users will need to download the files to the local drives before they can edit their files. This subjects the confidentiality of the files to how secure the client machine is. The client machine used by the users could be in a public place, or a common terminal shared by multiple users. The letdown in iFolder is that data cannot stay encrypted in the client's local disk, so administrators may need to use a third-party file encryption program to protect company confidential data especially on laptops that can get stolen easily.

[7] Novell Inc, Para 3
http://www.novell.com/documentation/ifolder21/admin/data/agmq9e8.html

A security checklist to take note when implementing iFolder:

- Ensure that users conform to the security policy of the organization, such as enforcing the need to encrypt company data files during transmission. This can be configured under Global Client Policies in iFolder.
- Enforce that guest users must use clear text when storing iFolder data on the iFolder server. This is to ensure no exploit or illegal content are stored on the server by the guest user whose intent is not clear.
- Enforce that the client version of iFolder should be installed unless there is a good reason for web access. This minimizes the chance of the users accessing the company confidential data from a public terminal such as Internet kiosks.
- Install a third party file encryption software on laptops, and make it mandatory for laptop users to encrypt company confidential data on the local disk. This can help to provide some form of protection from unauthorized users in the event that the laptops get stolen or accessed illegally. Although this may not be foolproof against skilled professional attackers, it serves well to ward off the most common class of attackers who lack good computer hacking skills and only prey at easy targets. Scott Baldwin's GSEC paper entitled "A Consumer Guide for Personal File and Disk Encryption Programs" provides a good overview of the importance of encrypting confidential data, and recommends DdCrypt and DriveCrypt programs.

Samba on NNLS

Samba on NNLS provides Windows (CIFS and HTTP-WebDAV) access to files stored on the NNLS server.[8] Users can access their files on the NNLS server using any CIFS/SMB client (such as Windows Explorer) or through the Web Folders feature in Windows Explorer and the Internet Explorer browser.

NNLS compiled Samba to enable LDAP authentication by default. These options have the purpose to authenticate users against the LDAP-based eDirectory. Samba is now able to ride on eDirectory's authentication service instead of having to implement and maintain a separate set of access control list, which is essential if an external authentication service is unavailable.

The added advantages of Samba on NNLS are as follows:

- Samba users are created in eDirectory using Linux User Management (LUM) tools included with NNLS.
- Home directories are automatically created and appropriate file access rights are automatically assigned the first time a LUM user logs in to the NNLS server from a shell prompt.
- Access to Samba services requires that users authenticate using secure LDAP to the eDirectory database specified during NNLS installation.[9]

[8] Novell Inc, Section 4, Para 1.
http://www.novell.com/documentation/nnls/implgde/data/anm8ha4.html
[9] Novell Inc, Section 2, Para 1.
http://www.novell.com/documentation/nnls/implgde/data/anf5dhi.html

With eDirectory now acting as the authentication layer to any users attempting to access files through Samba, the Samba service is made more secure, as compared to its non-NNLS counterpart. A default installation of Samba without NNLS will accept connections from any host, and contains several other insecure default configurations. Samba being packaged in the NNLS suite offers better out-of-the-box security for organizations that would want to use LDAP as an authentication and network information system. Administrators, however, should never assume that any out-of-the-box installation needs no additional security configuration and hardening.

A security checklist to take note when implementing Samba in NNLS:

- Do not provide guest shares and disallow anonymous requests. Define valid user for each share and always demand passwords. An example is to disable IPC$ connections in Samba. An IPC$ share is the only share that is always available anonymously.
- Hide files that are unreadable to users. The automatic sharing of user's home directory in Samba's default settings is not a good security practice.
- Configure the firewall to block all incoming and outgoing SMB/CIFS packets, unless these packets come from a secure tunnel such as VPN.
- Configure Windows clients to use at least NTLMv2 authentication. NTLMv1 authentication traffic can be sniffed with tools like L0phCrack to reveal the user's clear text password.

Novell NetStorage

Novell NetStorage is installed as part of Virtual Office and provides network and Web access to various file services, including iFolder and Samba services.[10] It is a software solution that acts as a bridge between a company's protected network and the Internet, allowing users to access files securely via SSL from any Internet location, without the need to install any program on the client machine.

For security reasons, the persistent cookies setting should always be turned off in NetStorage. Having this setting turned on allows the NetStorage's web session to continue even after the first user closes the current browser without logging off. The next user of the client computer will be able to access the first user's resources through NetStorage. This has serious security implications on the confidentiality of the organization's data.

Like iFolder, the web-based Netstorage should be carefully deployed where confidential data is involved. Web-based access poses a serious security threat and subjects a data's confidentiality to how secure the client machines are, after the data gets downloaded and decrypted on the client's local drive. Administrators should conduct regular security updates and audits on these client machines especially laptops to enhance client-side security.

[10] Novell Inc, Para 1
http://www.novell.com/documentation/nnls/implgde/data/anm8ha4.html

A security checklist to take note when implementing NetStorage:

- Make sure that the persistent cookie setting in NetStorage has been turned off, though it is already turned off by default.
- NetStorage runs on the apache web server, so take note of the default settings and security configurations that are necessary to secure the web server. Apache's official website, http://httpd.apache.org/ is a good starting point.

Messaging Services

NNLS provides a web-based email service through NetMail, as well as GroupWise collaboration client only available on Windows client machines.

NetMail

Novell NetMail is an e-mail and calendaring system based on Internet-standard messaging and security protocols. The advantage is that NetMail is also tightly integrated with Novell eDirectory by storing all user and server configuration information centrally on the directory.

For encryption protocols, NetMail supports SSL and Secure Multi-purpose Internet Mail Extension (S/MIME). NetMail also has this feature that enables email and calendaring services to be distributed across multiple servers, thus protecting an organization against disruptions and attacks, ensuring the availability of the email service.

Like most mail servers with features that tackle the lack of SMTP (Simple Mail Transfer Protocol) authentication flaw particularly for remote mail clients, NetMail's SMTP Agent provides two options to secure SMTP connections to prevent itself being used as a relaying system for SPAMs:

1. SMTP Authentication. This option if enabled will force all email clients to authenticate through the ESMTP (Enhanced Simple Mail Transport Protocol) before the SMTP Agent relays their messages to remote recipients. As its name suggests, ESMTP enhances SMTP security by providing authentication to SMTP. Clients like Outlook Express and Netscape Communicator support ESMTP authentication.

2. SMTP-after-POP. This option requires users to authenticate with the mail server via their POP3 or IMAP client before sending remote messages. This works for most Internet e-mail clients because e-mail clients always check for e-mail (log in) just before sending messages.[11]

[11] Novell Inc, Section 3, Para 1.
http://www.novell.com/documentation/netmail35/netmail35/data/amzmmc4.html

A better approach is to use the first method since it ensures that authentication is always performed.

There are several SPAM-blocking features in NetMail. First, with its AntiSpam Agent administrators are able to build a blackout list of undesirable email domains and addresses that have known to be sources of SPAMs received in the past.

Next, anti-SPAM options can be configured in NetMail's SMTP Agent to become the logical filter point for all incoming email messages against SPAMs. These options includes refusing connections from any email host with a black-listed IP address, providing reverse DNS look-ups such that connections from unmatched sources will be dropped, and real-time checks with the Real-time Black Hole List (RBL) to deny connections with any confirmed spammers and open relays.

Lastly, there is the Bounced Message Control feature found on the NMAP Agent's options page. This feature sets a threshold for the number of bounced messages NMAP can process within a set number of seconds[12], thus preventing NetMail from wasting system resources during an excess inflow of bounced messages. This situation will occur when spammers falsify the sender's address to be under NetMail's domain, and their SPAMs get bounced back to the NetMail server if the recipient accounts are unable to receive them. This may result in a form of Denial of Srevice (DoS) attack to the NetMail server.

From the features discussed, NetMail has been developed to be a relatively secured mail server with common email vulnerabilities in mind. Mail servers often fall prey to SPAMs that choke up the organization's bandwidth and mail storage space. NetNail offers basic email filtering features that help reduce these undesirable situations. Nevertheless, like all other software, vulnerabilities of NetMail are being discovered and patches released subsequently. Patches should be religiously tested and installed whenever new exploits are made known publicly.

A security checklist to take note when implementing NetMail:

- Configure TLS/SSL to secure Internet mail connections.
- Use either SMTP authentication instead of SMTP-after-POP option in NetMail to authenticate all SMTP connections.
- Configure the various anti-SPAM options in NetMail to filter away unwanted emails.
- Go through the options under the SMTP Agent's UBE Relaying page in NetMail to prevent others from using your NetMail server to relay SPAMs.
- Install Anti-Virus software on NetMail to provide anti-virus protection. Products like McAfee NetShield, Computer Associates InoculateIT, and Symantec CarrierScan are able to integrate with NetMail through anti-virus agents. The anti-virus protection should be properly configured and customized to better scan all incoming mails for viruses before letting them come in.

[12] Novell Inc, Section 4, Para 1
http://www.novell.com/documentation/netmail35/netmail35/data/amzmmc7.html

GroupWise Collaboration Client

The GroupWise collaboration client is part of Novell's GroupWise mail solution originally on Netware. The current client version is only available for Windows workstations.

The GroupWise client is very much like any other mail client available on the market such as Outlook and Netscape Communicator. What is worth mentioning in terms of security feature would probably be its ability to send secure messages via S/MINE.

A third-party security provider module (available on most Windows workstations as long as a reasonably updated Internet Explorer has been installed) is required to provide encryption for secure messaging to work in the collaboration client. GroupWise is compatible with the S/MINE v2/3 specification. The secure messaging process involves digitally signing an item by hashing it into a message digest using SHA-1. The message digest is then distributed with the item being sent out.

A security checklist to take note when implementing GroupWise client:

- Turn on LDAP authentication to enforce password protection on GroupWise clients. If the client machine has already logged in to Novell eDirectory as the same identity, no password prompt will appear again. This is an obvious advantage of employing NNLS services that can achieve single sign-on to some extent. However, if the workstation is shared among different users, then the security is subjected to well the users has understood and followed the company's security policy, to log out of the workstation after use.
- Depending on the company's security policy, there may be the need to securely encrypt email messages that are company confidential. While the NetMail web-based client version can be enforced to encrypt messages over an SSL connection, the GroupWise client requires more manual configuration and consciousness on the users' part to send secured mails out.
- Although the anti-virus protection on the NetMail server has already done its first round of virus scanning on all emails, some viruses can still get through by disguising ingeniously in attachments that appear harmless. Thus there must be anti-virus protection on the email client, with the real-time email scanning option turned on. This is part of the defense in depth strategy that should be adapted in any organization.

Print Services

iPrint

Novell iPrint is a special breed of its kind. First, to provide iPrint service, the administrator needs to configure the IPP-compatible (Internet Printing Protocol RFC 2910) printers to be iPrint-aware. Next the printers are deployed for service via a web interface in the form of printer icons along with their drivers. If a custom graphical map of the organization is available, the printer icons can even be matched

to their physical locations on the map – all in the form of web pages available to the users.

iPrint uses eDirectory as the central printing authentication server to ensure that only authorized users can access the printers. Users are required to authenticate with their LDAP's usernames and passwords. Print data from the client to server can be encrypted via SSL on port 443.

Allowing print jobs to be sent via the Internet medium exposes an organization's network through yet another potential exploited channel. Printing over the Internet should be cautiously weighted against its associated security risks. VPN connections and proxy servers are some of the ways to secure printing over Internet.

It is not totally unimaginable for attackers to gain unauthorized access to network printers and store their exploit codes / files on the printers' ROM. Network printers nowadays are shipped with a considerably good amount of ROM memory, and they respond well to anyone who is well-versed in printing protocols to handle requests to store information locally. The printing service is therefore an area important enough to pay more attention to in terms of security.

iPrint offers user-friendliness and convenience to users, at the same time, enforcing that proper authentication be made for every print request, whether directly or indirectly through the LDAP server.

A security checklist to take note when implementing iPrint:

- The directory where all printer drivers that are centrally located on iPrint should be properly secured to prevent unauthorized access. It would be disastrous if the drivers get trojanized on the server and installed on the client workstations. Install a host-based IDS to ensure the integrity of these files.
- Use proxy servers together with a firewall to keep internal addresses private while exposing only the proxy servers' addresses to external users. In this way, even if Internet printing is enabled, users outside of the internal network can only send print jobs through the proxy servers.
- Configure the printer persistence setting with iPrint Map Designer. This option applies to the scenario when there is a need to remove the installed printer from the client machine, such as a vendor's laptop that needs to print out documents to an iPrint printer in the company, after it reboots. Keeping the printer's driver and settings in the client that does not belong to the network is definitely not a good security practice.
- Enable print auditing feature in every printer deployed under the iPrint service. This setting allows the administrator to generate audit reports that show print jobs information, and determine if there has been any unauthorized print jobs carried out.

Services Management

NNLS provides several management consoles for its services. Almost all the management applications except the eGuide are available only to the administrators.

Novell eGuide is a web application that allows its users to search through directory information such as employee and company data, via a web browser. eGuide can even search multiple LDAP data sources in organizations that have multiple directories.

With such powerful searching capabilities, access to eGuide must be restricted only to authorized personnel. Allowing any employee or user to have just read access to eGuide could pose serious threats to the organization, as malicious users can conduct reconnaissance work and map out important information about the organization and its network.

Almost all the management consoles are available in web-interface. This web-based architecture allows access points to be platform independent, but also exposes the consoles to the threats and attacks faced by all web-based applications. NNLS uses the apache web server to host all web pages and applications. Thus the web server and network perimeter must be properly secured and closely monitored.

Web Access to Services

NNLS allows its users to access all the services they are authorized to on a single web portal, known as Virtual Office. The Virtual Office enables users to access the different services from a single access point on the web page after login. The design of the various services to work seamlessly with the eDirectory makes the Virtual Office portal very well integrated and secured from the access control point of view.

Like the services management feature, Virtual Office runs on the web platform through apache. All common web vulnerabilities and exploits should be examined in securing the web-based services.

An advantage that the web applications in NNLS have over others is their directory-driven authentication method. Most web applications will make use of the same RDBMS (Relational Database Management System) that holds the application data, to store the usernames and passwords too. Database-driven authentication mechanism, besides having slower access speed, is also vulnerable to SQL injections, if the input data from the users are not properly validated.

Conclusion

Novell Nterprise Linux Services do offer an attractive alternative to enterprises. It was developed with a lot of convenience to its users in mind, with reasonable security considerations taken. However, some of the services it provides may be just good-to-have's. Thus any organization that wants to deploy NNLS should examine each service and its security implications discussed in this paper before deciding

whether the service should be made available to its users. The principle of shutting down unneeded services must always be applied to reduce the risks that an organization faces.

Every deployment scenario is unique that is dependent on the company's security policy, hence certain points in the security checklist may not apply although all should be noted by the administrator. The defense in depth principle is a powerful strategy that protects an organization's network and valuable resources, and should always be applied when designing the company's security infrastructure.

List of References

1. Ridd, Chris. “Net::LDAP::Security - Security issues with LDAP connections”. URL: http://search.cpan.org/~gbarr/perl-ldap/lib/Net/LDAP/Security.pod (11 June 2004).

2. Mahajan, Vikas. “Directory, Database, or Both?” URL: http://developer.novell.com/edirectory/dirvsdb.html (17 July 2004)

3. Garfinkel, Simson; Spafford, Gene; Schwartz, Alan. Practical Unix & Internet Security, Third Edition. Reading: O’Reilly & Associates, Inc, February 2003. 447-449, 496.

4. Novell, Inc. “Novell eDriectory vs. Microsoft Active Directory.” 2004. URL: http://www.novell.com/collateral/4621396/4621396.pdf (23 June 2004)

5. Novell, Inc. “Novell Nterprise Linux Services Overview, Planning, and Implementation Guide”. URL: http://www.novell.com/documentation/nnls/index.html?page=/documentation/lg/nnls/implgde/data/front.html (1 June 2004)

6. Novell, Inc. “Novell eDirectory 8.7.3 Administration Guide.” URL: http://www.novell.com/documentation/edir873/index.html?page=/documentation/edir873/edir873/data/a2iii88.html#bktitle (23 June 2004)

7. Novell, Inc. “Novell iFolder 2.1 Installation and Administration Guide.” URL: http://www.novell.com/documentation/ifolder21/index.html?page=/documentation/ifolder21/admin/data/a2iii88.html#bktitle (1 June 2004)

8. Vugt, Sander van. 26 February 2003. “File Sharing in Novell Nterprise Linux Services 1.0.” URL: http://www.novell.com/coolsolutions/nnlsmag/features/a_file_sharing_nls.html (1 June 2004)

9. Tridgell, Andrew; Terpstra, John. Samba 26 May 2003. “Chapter 14. Securing Samba”. URL: http://sg.samba.org/samba/docs/man/Samba-HOWTO-Collection/securing-samba.html (1 July 2004)

10. Novell, Inc. December 2003. “Novell Nterprise Linux Services 1.0 - NetStorage Administration Guide.” URL: http://www.novell.com/documentation/nnls/pdfdoc/netstor/netstor.pdf (10 June 2004)

11. Novell, Inc. “Novell NetMail 3.5 Administration Guide.” URL: http://www.novell.com/documentation/netmail35/index.html?page=/documentation/netmail35/netmail35/data/front.html#bktitle (1 July 2004)

12. Ou, George. “Fixing the SPAM problem once and for all White paper”. Revision 1.1. 12 August 2003. URL: http://www.lanarchitect.net/Articles/SPAM/FixingSPAM/ (17 July 2004)

13. Novell, Inc. “GroupWise 6.5 Windows Client User Guide.” URL: http://www.novell.com/documentation/gw65/index.html?page=/documentation/gw65/gw65_userwin/data/ab32nt1.html#bktitle (22 July 2004)

14. Novell, Inc. 19 December 2003. “Novell Nterprise Linux Services - Novell iPrint Administration Guide” URL: http://www.novell.com/documentation/nnls/pdfdoc/iprint/iprint.pdf (10 July 2004)

15. ExtremeTech. “Printing Made Simple with iPrint”. URL: http://www.extremetech.com/article2/0,1558,1157507,00.asp (10 July 2004)

16. Berkeley Lab. “iFolder and iPrint Services Make it Easy to Update, Print Files from Almost Any PC Almost Anywhere Using a Web Browser.” September 2003. URL: http://www.lbl.gov/ITSD/CIS/compnews/2003/September/04-iFolder.html (10 July 2004)

17. Internet RFC/STD/FYI/BCP Archives. “RFC 2910 - Internet Printing Protocol/1.1”. URL: http://www.faqs.org/rfcs/rfc2910.html (10 July 2004)