



# **Windows® and SuSE Linux EAL4+ Workload Comparison:**

**An Examination of Server Role Capabilities of  
EAL4+ Evaluated Software**

**February 2006**

---

**Analysis and conclusions reflect the best efforts and best public information available at the writing of this document and are subject to change should new data become available.**

**For more information, contact:**

**Dickerson Technologies, LLC.  
13601 Parreco Farm Court  
Germantown, MD 20874**

**Phone: 301.353.8448**

**Fax: 301.515.9688**

**Email: [info@dickersontech.com](mailto:info@dickersontech.com)**

**© Copyright 2005. Dickerson Technologies, LLC. All rights reserved. All trademarks are the property of their respective companies. This document may not be duplicated, reproduced or retransmitted, in whole or in part, without explicit permission from Dickerson Technologies, LLC.**

## Table of Contents

|          |  |           |
|----------|--|-----------|
| <b>1</b> | <b>EXECUTIVE SUMMARY</b>                 | <b>4</b>  |
| <b>2</b> | <b>SCOPE OF STUDY</b>                    | <b>5</b>  |
| 2.1      | Common Criteria Conformance Claims       | 5         |
| 2.2      | Evaluated Configurations                 | 6         |
| 2.3      | Roles in the Networked Enterprise        | 6         |
| <b>3</b> | <b>CLIENT AND SERVER ROLE COMPARISON</b> | <b>7</b>  |
| 3.1      | Methodology                              | 7         |
| 3.2      | Server Role Capabilities                 | 7         |
| 3.3      | Client Capabilities                      | 14        |
| 3.4      | General and Infrastructure Capabilities  | 18        |
| <b>4</b> | <b>CONCLUSION</b>                        | <b>20</b> |
|          | <b>REFERENCES</b>                        | <b>22</b> |

## **Acknowledgements**

Microsoft commissioned Dickerson Technology to explore practical differences between operating systems evaluated to the same evaluation assurance level, with the expectation that we would provide objective and vendor neutral analysis of the Common Criteria evaluated systems under study.

Dickerson Technology stands behinds the findings of this study and stands firm in the belief that any attempt to perform a similar comparison by another party would obtain similar results.

# 1 Executive Summary

This study examines two operating systems, both certified at Evaluation Assurance Level EAL4+ and meeting the same Common Access Protection Profile for operating systems, to determine differences in practical capabilities based upon the evaluated configurations.

In the lab, the systems were deployed following the security configuration guides to attempt to create and validate a directory server, certificate server, web server, file server, print server, and networking server using only the evaluated software. Similarly, systems were deployed following the security configuration guides to act as clients to the server roles.

We found a fairly significant difference in the evaluated server and client capabilities of Windows XP/2003 and the Novell SuSE SLES9 certified systems, with Microsoft having many useful server roles feasible that are not feasible using the SLES9 evaluated configuration.

With the evaluated Windows Server 2003 systems, we were able to deploy and validate all server roles, while the only role we were able to create with the Novell SLES9 systems was that of an FTP server. Our findings were similar for client capabilities, with the Windows XP systems having the necessary client components in the evaluated configuration, while the SuSE system lacked key client capabilities to leverage the server roles.

We additionally examined the evaluated software from a client user experience perspective and found key differences which are detailed in the body of the report. Finally, we examined both evaluated configurations for infrastructure differences and again found some key differences in capability.

Based upon the overall examination, this study has found that the software included in the Microsoft evaluated configurations provides the capabilities to build and utilize several common server roles, while the Novell SuSE evaluation seems to lack key necessary packages for those same common roles.

## 2 Scope of Study

The goal of this study is to look at two Common Criteria certified systems and examine them side-by-side to discover any practical advantages that one evaluated system has over the other.

The two operating systems examined in this study are, as identified in the Common Criteria Validated Products List on the Common Criteria Portal<sup>1</sup> are:

- SuSE Linux Enterprise Server Version 9 with certification-sles-ibm-eal4 package
- Windows 2003/XP

The study will look at the components of the evaluation in specific roles and examine evaluated capabilities from three perspectives: client capability, server capability and overall security capability in the network.

### 2.1 Common Criteria Conformance Claims

Both certified systems under examination have similar conformance claims, which are as follows:

- Controlled Access Protection Profile (CAPP), Version 1.d
- Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 2.2, January 2004, extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security Assurance Requirements, Version 2.2. EAL4 augmented with ALC-FLR.3

Novell's SuSE Linux Enterprise 9 achieved certification at assurance level EAL4+ in March of 2005 and Microsoft's Windows Server 2003 and Windows XP achieved certification at EAL4+ in December of 2005.

With the common criteria conformance identical for two general purpose operating systems, then as long as both products achieve certification, comparison of assurance level and security target do not provide a useful distinction for decision makers. Therefore, this study will need to look deeper for practical differences that would be of interest to users and administrators.

---

<sup>1</sup> Validated Products List, Operating Systems:  
<http://www.commoncriteriaportal.org/public/expert/index.php?menu=7&orderindex=1&showcategories=256>

## 2.2 Evaluated Configurations

Each evaluated product requires that the vendor provide a detailed security configuration guide that enables IT administrators to deploy the product in the configuration that was examined and certified by the evaluating authorities. For example, if the evaluated configuration excluded a component, then the guide might advise that the component must be absent from a deployed system for the certification to be valid.

This detail puts a lot of control in the hands of vendors under evaluation. One vendor may define a very minimal evaluated configuration and be able to achieve certification quickly and relatively inexpensively. A different vendor could define a richer evaluated configuration and accept the extra cost in time and money, but ultimately provide more capabilities for users of the evaluated configuration.

This difference in evaluated configurations will be the primary comparative focus of this study. What exactly was evaluated to EAL4+ by each vendor, and can the evaluated components be used to build and deploy common roles for client and server computers in a network?

## 2.3 Roles in the Networked Enterprise

For each of the certified systems, this study will look at common roles that a server might fulfill in a networked environment, along with two other key factors: client capabilities for that role and infrastructure capabilities for that role.

For example, take the role of File Server. Can a file server be built using the evaluated configuration? Are there limitations on how it must be deployed and managed? Does the evaluated client have the necessary components to connect to and use the file server? Are there infrastructure capabilities to ensure that client to server interactions are secure and private in the network?

With these sorts of questions in mind, we examined several roles:

- Directory Server
- PKI Certificate Server
- Web Server
- File Server
- Print Server
- Networking Server

© Copyright 2005. Dickerson Technologies, LLC. All rights reserved.

## 3 Client and Server Role Comparison

### 3.1 Methodology

For each of the studied systems, we followed the respective security configuration guides and installed a server machine and client machine exactly as detailed. During this process, we took relevant notes concerning software packages, settings and capabilities that must be disabled or are not part of the evaluated configuration.

Next, starting from the base installation of the evaluated configurations, we attempted to configure server and client capabilities for each respective role using only the evaluated configuration. Where a necessary package is not present, we will note the implications. Since some server roles have optional capabilities, we will discuss them in the context of the evaluated configuration.

### 3.2 Server Role Capabilities

The primary focus for technical examination is the server capability in a given role. If particular server features or necessary capabilities are lacking to provide a service necessary to a role, then the secondary questions of client or network capabilities are moot.

| Server Role        | Windows 2003 / XP | SuSE SLES9 |
|--------------------|-------------------|------------|
| Directory Server   | ✓                 | X          |
| Certificate Server | ✓                 | X          |
| Web Server         | ✓                 | X          |
| File Server        | ✓                 | X          |
| Print Server       | ✓                 | ✓          |
| Networking Server  | ✓                 | X          |

**Table 1: Server role capabilities using Evaluated Software**

As summarized in Table 1, our technical examination found significant differences in the evaluated software capabilities of the two servers studied. Let us examine each role in detail to understand the findings.

### **3.2.1 Directory Server**

#### **Microsoft Windows Evaluated System**

In the Evaluation Technical Report for Windows [winetr05], directory capabilities are explicitly called out by the evaluation team. Under section 2.1, Product Type:

Other than an OS, Windows 2003/XP can also be categorized as the following types Information Assurance (IA) or IA enabled IT products: ...

Windows 2003/XP is a Directory Service product to support Security Infrastructure. The access control and replication of Windows Active Directory (AD) objects is part of the Windows 2003/XP TOE Security Function Interfaces (TSFI).

The Windows Server security configuration and administrator guides [w03sec05, w03adm05] provide guidance on installing and configuring Active Directory for proper use and which sub-components that must be disabled. Upon completion of our installation, and disabling of non-allowed services, we were able to verify that Window directory services were available.

Additionally, our findings indicate that all of the necessary components for establishing and managing a Windows Domain for use of user and group identity management, as well as group policy, are part of the evaluated software configuration.

#### **Novell SuSE Linux Evaluated System**

Our findings indicate that a directory server can not be implemented using the Novell SuSE Linux evaluated software. The security configuration guide [slesec05] is explicit in the "Add and Remove packages" section (3.3), listing out all REQUIRED and OPTIONAL packages that may be installed in the evaluated configuration. OpenLDAP is not in that list. Additionally, the security configuration guide [slesec05] is explicit in the installation section (2) , step 16 that "The OpenLDAP Server MUST be disabled."

The section further goes on to explain that "local" must be the selected user authentication method. Without the basic LDAP services as part of the evaluation, and without an alternative component, it is not possible to implement a directory server using the Novell SuSE Linux evaluated software.

### **3.2.2 Certificate Server**

#### **Microsoft Windows Evaluated System**

The Windows Server 2003 Certificate Server was evaluated with its own evaluation technical report against its own target of evaluation [mscetr05], available from the National Institute of Standards (NIST) National Information Assurance Partnership (NIAP) web site [mscni06]. In the Overview of TOE of the evaluation report, it describes

The TOE, Microsoft Windows Server 2003 Certificate Server, implements a Public Key Infrastructure (PKI) that issues and manages public key

certificates to facilitate the use of public key cryptography. To achieve this goal, the Microsoft Certificate Server implements the following core functional components:

- Policy-based generating and distributing Public Key (including X.509) Certificates to bind user public keys to other information after validating the accuracy of the information provided
  - Certificate Enrollment or Request based on
    - PKCS #7 (Cryptographic Message Syntax Standard),
    - PKCS #10 (Certification Request Syntax Standard),
    - RFC 2797 CMC (Certificate Management Messages over Cryptographic Message Syntax)
  - Certificate Renewal
  - Certificate Revocation
  - Certificate Retrieval
  - Request Pending Management
- Maintaining and distributing certificate status information for unexpired certificates
  - Certification and Certificate Revocation List (CRL) Management
- Certificate database backup and restore
- Security configuration and management of Microsoft Certificate Server

The Microsoft Certificate Server exceeds the CIMC Security Level 3 Protection Profile [10] requirements, which are appropriate where the risks and consequences of data disclosure and loss of data integrity are moderate. A CIMC meeting Security Level 3 includes mechanisms to protect against attacks by parties with physical access to the components and includes additional assurance requirements to ensure the CIMC is functioning securely.

We validated that we could utilize the Windows security configuration guide [winsec05] and the Microsoft Certificate Server security configuration guide [mscsec05] to deploy an issuing Certificate Authority (CA) using Active

Directory<sup>2</sup>. Note that we did not install the nCipher Hardware Security Module as required by the evaluated configuration, but assumed that it would work as documented in the evaluation report. A deploying customer would be required to purchase and use the FIPS (Federal Information Processing Standards) compliant module in order to run in the evaluated configuration.

### **Novell SuSE Linux Evaluated System**

Our findings indicate that a Certificate Server can not be implemented using the Novell SuSE Linux evaluated software, though some basic certificate capabilities are included with OpenSSL as part of the evaluated configuration:

- Cryptographic Key Generation
- Cryptographic Key Distribution, and
- Cryptographic operations

Based upon guidance in the SuSE security configuration guide [slesec05], administrators can create certificate requests and self-signed certificates using OpenSSL command line options. The examples included in the guide demonstrate using OpenSSL in conjunction with *stunnel* to create port connections.

While providing basic certificate capabilities, the Novell SuSE Linux evaluated software lacks a certificate directory capability and other necessary services to perform as a Certificate Server.

### **3.2.3 Web Server**

#### **Microsoft Windows Evaluated System**

In the Evaluation Technical Report for Windows [winetr05], web server capabilities are explicitly called out by the evaluation team. Under section 2.1, Product Type:

Other than an OS, Windows 2003/XP can also be categorized as the following types Information Assurance (IA) or IA enabled IT products: ...

Windows 2003 is a **Web Server** product by including the Internet Information Services (IIS) Version 6.0 (IIS6) component functionality which provides access control utilizing the underlying OS services for authentication.

The Windows Server administrator guide [w03adm05] provides guidance on installing and configuring Internet Information Services for proper use and which sub-components that must be disabled. Upon completion of our installation, and disabling of non-allowed services, we were able to verify that Window web services were available. Note that ASP and some standard authentication

---

<sup>2</sup> [mscsec05] indicates that the evaluated configuration requires the Certificate Server configuration to be an Issuing CA and use Active Directory. Offline CAs and stand-alone CAs were not part of the evaluated configuration.

methods are not supported under the evaluated configuration, so it is important to follow the guide.

A final interesting note is that the necessary cryptographic capabilities are included in the evaluated configuration to support SSL protected web content (https://) including, as previously discussed, an online Certificate Authority.

### **Novell SuSE Linux Evaluated System**

Our findings indicate that a Web Server can not be implemented using the Novell SuSE Linux evaluated software. The security configuration guide [slesec05] is explicit in the “Add and Remove packages” section (3.3), listing out all REQUIRED and OPTIONAL packages that may be installed in the evaluated configuration. Most significantly, all of the Apache web server packages are missing from the list, as are several other modules for SSL and other web package integration.

Later, the guide also explicitly says, “Kernel modules other than those provided as part of the evaluated configuration MUST NOT be installed or loaded. You MUST NOT load the *tux* kernel module (the in-kernel web server is not supported).”

#### **3.2.4 File Server**

### **Microsoft Windows Evaluated System**

In the Evaluation Technical Report for Windows [winetr05], file server capabilities are addressed by the evaluation team at the beginning of the document:

Although the evaluation had no specific requirements addressing the function of the following services, all were evaluated to ensure they did not permit violations of the specific access control, information flow, or authentication policies of the TOE: ... File Replication, Directory Replication, ... Distributed File System service, Removable Storage Manager, and Virtual Disk Service.

The Windows Server security configuration and administrator guides [w03sec05, w03adm05] provide guidance on installing and configuring Windows Server for proper use and as a Server Message Block (SMB) file server (i.e. the “normal” Windows file server type). Upon completion of our installation, and disabling of non-allowed services, we were able to verify that file server capabilities were available.

Additionally, our findings indicate that all of the necessary components for establishing and managing Web Folders, served with Internet Information Services (IIS) Version 6.0 (IIS6).

The administrator guide gives direction on how to use the Encrypting File Service (EFS) in conjunction with either SMB file shares or Web Folders to provide further data protection and, in the case of Web Folders, protection in the network as well.

### **Novell SuSE Linux Evaluated System**

Our findings indicate that a standard file server can not be implemented using the Novell SuSE Linux evaluated software, as key necessary packages are not part of the evaluated configuration. The security configuration guide [slesec05] is explicit in the “Add and Remove packages” section (3.3), listing out all REQUIRED and OPTIONAL packages that may be installed in the evaluated configuration. None of the necessary Samba packagers are on that list, nor are the alternative NFS packages. Additionally, the security configuration guide [slesec05] is explicit in section 4.4, “Installation of additional software,” that:

The security requirements for additional software are:

- Kernel modules other than those provided as part of the evaluated configuration MUST NOT be installed or loaded. ... You MUST NOT activate *knfsd* or export NFS file systems.

One component that is included in the Novell SuSE Linux evaluated configuration is the File Transfer Protocol (FTP) daemon, *vsftpd*. FTP is not traditionally a file server protocol, but users could utilize it to remotely store and retrieve files using the included ftp client, *lukemftp*. The configuration guide does include a section on setting up FTP, “3.10 Setting up FTP,” that offers this guidance:

The evaluated configuration includes OPTIONALLY includes FTP services. Note that FTP does not provide support for encryption, so this is only RECOMMENDED for anonymous access to non-confidential files. If you do not specifically need FTP, it is RECOMMENDED that you disable the *vsftpd(8)* service.

### **3.2.5 Print Server**

#### **Microsoft Windows Evaluated System**

The Evaluation Technical Report for Windows [winetr05] indicates that printers and the ability to share them are part of the evaluated configuration.

The Windows Server security configuration and administrator guides [w03sec05, w03adm05] provide guidance on installing and configuring Windows Server for proper use and as a print server. Windows leverages file sharing capabilities for network availability of printers and the Print Spooler service is additionally part of the evaluated configuration.

Upon completion of our installation, and disabling of non-allowed services, we were able to verify that print server capabilities were available.

#### **Novell SuSE Linux Evaluated System**

Our findings indicate that a print server can be implemented using the *lprng* package, which is included in the Novell SuSE Linux evaluated software. This package includes the client and server components needed for a network print server implementation.

Note that CUPS, nor SAMBA, the package necessary for printing from Windows clients is not present, as the security configuration guide [slesec05] is explicit in

the “Add and Remove packages” section (3.3), listing out all REQUIRED and OPTIONAL packages that may be installed in the evaluated configuration.

### **3.2.6 Networking Server**

#### **Microsoft Windows Evaluated System**

The Evaluation Technical Report for Windows [winetr05] indicates that evaluated configuration includes the key networking protocols, security networking and network management protocols necessary to serve several types of networking server functions. It also recognizes evaluation as a network management product, a firewall product and a VPN product:

Other than an OS, Windows 2003/XP can also be categorized as the following types Information Assurance (IA) or IA enabled IT products: ...

Windows 2003/XP is a **Network Management** product to support the Security Infrastructure of Windows 2003/XP networks. Windows 2003/XP Group Policy is part of the Windows 2003/XP TOE.

Windows 2003/XP is a **Firewall (Host-based)** product with the capability to filter network traffic based upon source and destination addresses/ports and protocol within a Windows 2003/XP network.

Windows 2003/XP is a **Virtual Private Network (VPN)** product providing an IPSec Service and its associated Transport Driver Interface (TDI) based network support within a Windows 2003/XP network.

In terms of basic services as a Network Server, the Windows Server security configuration and administrator guides [w03sec05, w03adm05] provide guidance on installing and configuring Windows Server to provide DHCP (dynamic host configuration protocol) and DNS (domain name service) in either a Workgroup<sup>3</sup> or Domain Controller<sup>4</sup> environment. The Windows evaluated configuration includes all of the necessary components to provide full Windows Domain Controller functionality.

Additionally, the Windows evaluated configuration includes advanced networking capabilities in the form of security protocols Kerberos and IPSec and the ability to manage and filter those protocols in the evaluated network environment.

#### **Novell SuSE Linux Evaluated System**

Our findings indicate that a basic networking server can not be implemented using the Novell SuSE Linux evaluated software, as key necessary packages are not part of the evaluated configuration. The security configuration guide

---

<sup>3</sup> It is important to understand the difference between a domain and a workgroup environment. The main difference between a domain and a workgroup is that workgroup environments use decentralized administration.

<sup>4</sup> **Domain controller (DC)** is a term used to describe the server that responds to security authentication requests within a Windows server network domain, a network management concept for Windows systems.

[slesec05] explicitly calls out that DHCP is not supported in the evaluated configuration, and that only static IP addresses are allowed. In the “Add and Remove packages” section (3.3), listing out all REQUIRED and OPTIONAL packages that may be installed in the evaluated configuration, the bind package is also present, so providing a domain name service (DNS) is not possible.

### **3.3 Client Capabilities**

In a distributed network, server functionality is only part of the picture, even taking the perspective of server roles. The next question to consider is if client capabilities exist to take advantage of the servers. In this case, we again want to consider just the evaluated software configurations, assuming that some customers would like to deploy systems in a manner compliant with the Common Criteria evaluated configuration. In that context, the study examines two client areas:

- User experience of the client, and
- Does the client have the software needed to interact with the server role. For example, if you can build a web server, does the client have a browser.

#### **3.3.1 Client User Experience**

##### **Microsoft Windows Evaluated System**

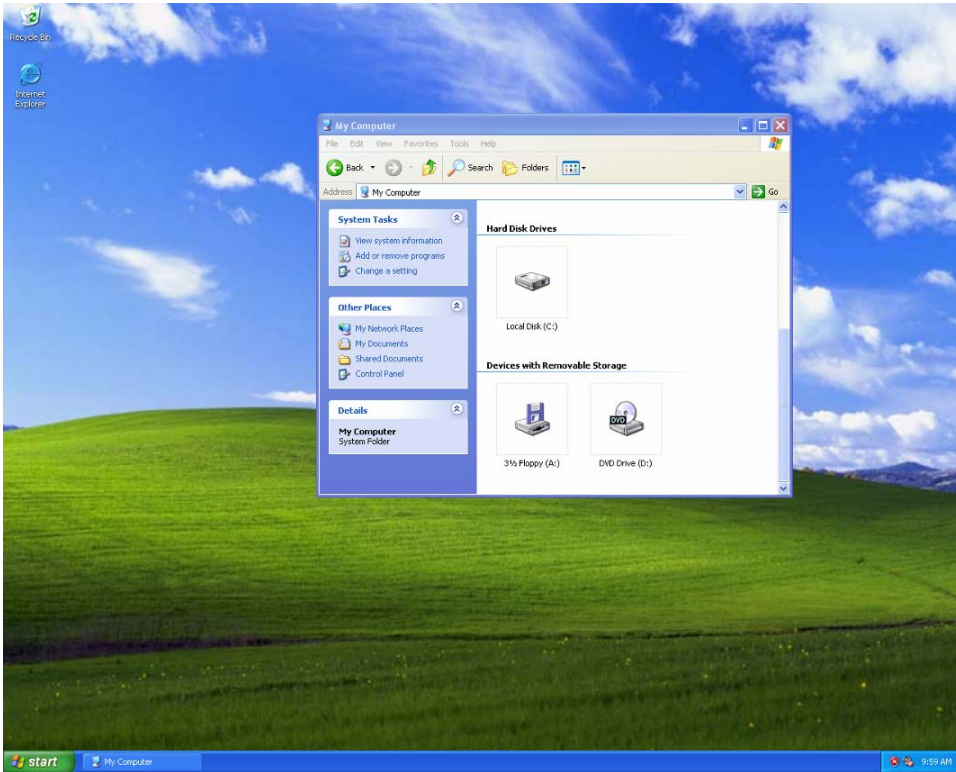
The Windows 2003/XP evaluation report [winetr05] describes the evaluated system as:

“Windows 2003/XP is an operating system that supports both workstation and server installations. The TOE includes five product variants of Windows 2003/XP: XP Embedded, XP Professional, Server 2003 Server, Server 2003 Enterprise Server, and Server 2003 Data Center. ...”

As a workstation, the software assessed as part of the EAL4+ process was Microsoft Windows XP Professional, SP 2. Figure 1 shows a screen shot of Windows XP that was installed in the evaluated configuration, as described in [wxpsec05], the Windows XP security configuration guide.

Immediately, one notices that the standard Windows graphical user interface is included as part of the evaluated configuration. Implicitly, this also means that multiple simultaneous applications are supported, along with copy-and-paste functionality, providing a nice ease of use.

The clients can be set up as in Workgroup networking mode or as Domain members, under which they could be subject to Group Policy. Also noted during installation is that the DHCP networking client code is included, making user connection to the network similar to what users expect on non-evaluated systems.



**Figure 1: Windows XP Service Pack 2 User Interface**

The installation process for an evaluated configuration was fairly straightforward, with specific guidance to (for example) prevent the automatic installation of unevaluated device drivers. After the basic installation, Security Configuration Templates were provided to configure domain-joined machines, but specific instructions were also provided to manually lock down clients. These actions included, for example:

- requiring passwords for accounts
- require authenticated access for file sharing (disabling “guest” access)
- disabling hibernation and the creation of dump files

The Windows Firewall is included in the evaluated configuration and [wxpsec05] provides a chapter describing recommended settings, such as blocking access for remote assistance. The Windows Firewall also utilizes IPSec filtering capabilities when IPSec is enabled.

Noteworthy inclusions to the evaluated configuration also include support for smart cards, IPSec services, IPv6 support, EFS, USB storage devices and hubs (if compatible with the evaluated Microsoft drivers), and the web browser.

### **Novell SuSE Linux Evaluated System**

The SuSE evaluation report [sleetr05] describes the evaluated system as:

© Copyright 2005. Dickerson Technologies, LLC. All rights reserved.

“... a general purpose, multi-user, multitasking Linux based operating system. It provides a platform for a variety of applications in the government and commercial environment. SLES is available on a broad range of computer systems, ranging from departmental servers to multi-processor enterprise servers. The SLES evaluation covers a potentially distributed, but closed network of IBM xSeries, pSeries, zSeries, iSeries and eServer 325 servers running the evaluated version of SLES.”

We should immediately acknowledge a key difference to the Windows evaluation in that Novell SuSE evaluation appears to be primarily targeted as a server evaluation and not specifically as a client workstation. However, it is also recognized that this is the sole choice for use of an EAL4+ evaluated Linux-based client and that as a general purpose, multi-user system, it could be used as client to SuSE Linux server machines.

The screenshot of an evaluated SuSE installation in Figure 2 highlights the most visible difference in the SuSE Linux system – the explicit exclusion of XFree86, Gnome, KDE and any other graphical user interface. Applications can certainly be launched in the background, but windowed functionality such as cut-and-paste or multiple visual applications are not possible.

```
linux:~ # dir
total 52
drwx----- 5 root root 4096 Oct 31 04:08 .
drwxr-xr-x 20 root root 4096 Oct 26 07:39 ..
-rw----- 1 root root 500 Oct 26 09:37 .bash_history
-rw-r--r-- 1 root root 1124 Feb 28 2000 .exrc
drwx----- 2 root root 4096 Oct 26 07:47 .gnupg
drwxr-xr-x 2 root root 4096 Oct 26 09:08 .kbd
-rw----- 1 root root 1024 Oct 26 09:11 .rnd
-rw----- 1 root root 3618 Oct 31 04:08 .viminfo
drwxr-xr-x 2 root root 4096 Jun 30 2004 bin
-rw-r--r-- 1 root root 1124 Oct 26 09:35 remove_through_3.3
-rw-r--r-- 1 root root 1046 Oct 26 09:50 remove_through_3.4
-rw-r--r-- 1 root root 2540 Oct 26 09:17 rpmlist
-rw-r--r-- 1 root root 1494 Oct 26 09:56 rpmlist_after_removes
linux:~ #
```

**Figure 2: SuSE Linux Enterprise Server 9 User Interface**

Another key difference was found in networking, where the installation guidance in [slesec05] explicitly disallows the use of DHCP and requires a static IP

address to be used. The iptables firewall package is likewise disallowed and required to be removed from an evaluated configuration, as are other commonly used applications such as the Internet browser (which would have required a graphical user interface in order to function.) In a similar vein, USB devices are not allowed and IPv6, IPSec and smart cards are not supported.

### 3.3.2 Client Role Capabilities

Very briefly, this section will review the client side availability of functions capable of utilizing the server roles analyzed earlier. Assuming a server role is implemented using the evaluated server software, does the client have the capability of utilizing the server? The summary of results are shown in Table 2 and a brief discussion of each client system follows.

| Client Capability                     | Windows 2003 / XP | SuSE SLES9 |
|---------------------------------------|-------------------|------------|
| Client for Directory Server           | ✓                 | ✓          |
| Client for Certificate Server         | ✓                 | X          |
| Client for Web Server                 | ✓                 | X          |
| Client for File Server                | ✓                 | X          |
| Client for Print Server               | ✓                 | ✓          |
| Client for Network Server (DHCP, DNS) | ✓                 | X          |

#### **Microsoft Windows Evaluated System**

The evaluated configuration for Windows XP includes the necessary components to function as a domain-joined workstation, authenticating to a server utilizing Active Directory for users, groups and policies.

Similarly, the evaluated configuration allows domain-joined workstations, Windows XP workstations to request, retrieve and utilize certificates from a Windows directory as specified via policy.

The evaluate Window XP workstation includes functions to access networked file and print servers, and as previously described, has the necessary client functionality evaluated to get an IP address using DHCP and utilize DNS lookup from an evaluated Network Server.

Finally, we the evaluated Internet Explorer browser is available to access the Web Server.

In our technical testing, each of these functions was validated using system deployed in the evaluated configurations.

### **Novell SuSE Linux Evaluated System**

The evaluated configuration for Novell SuSE Linux Enterprise Server 9 does include some client-side components for the server roles, even when the server role software was not included. The openldap2-client and lprng packages both include necessary client-side software for directory and printing respectively.

Other than those two, the client side software for the other roles is not part of the evaluated configuration.

## **3.4 General and Infrastructure Capabilities**

There are several general and infrastructure capabilities that are not strictly related to the client/server roles studied, but can provide additional optional value. This section will highlight these capabilities and discuss their expression on each system.

### **3.4.1 Host Firewall**

The versions of Windows Server 2003 and Windows XP in the evaluated configurations include a host firewall application with the ability to do stateful packet inspection for IPv4 and IPv6 network traffic.

The SuSE Linux firewall package, iptables, is not allowed in the evaluated configuration.

### **3.4.2 Kerberos and IPSec**

The Kerberos and IPSec capabilities for both Windows Server 2003 and Windows XP, as well as the ability to manage IPSec policies with Group Policy are part of the evaluated configuration. Authentication and encryption policies can be used in conjunction with the client-server capabilities discussed previously to provide more secure and private interaction of protocols.

Neither Kerberos nor IPSec are supported in the Novell SuSE evaluated configuration.

### **3.4.3 Configuration Templates**

Both the Novell and the Microsoft evaluated systems come with configuration templates to help ease the deployment of systems in the evaluated

configurations. The Novell SuSE system provides scripts that serve this function and the Microsoft solution provides templates that can be applied locally to machines or imported into a central policy.

#### ***3.4.4 Encrypting File System***

The versions of Windows Server 2003 and Windows XP in the evaluated configurations include Encrypting File System (EFS) capabilities, allowing users to selectively store data in an encrypted folder.

An encrypted file system capability is not included as part of the Novell evaluated configuration.

## 4 Conclusion

This study attempted to go beyond the label of Evaluation Assurance Level and examine the evaluated configurations of two EAL4+ evaluated systems to determine practical capabilities.

Our technical findings indicate a fairly significant difference in the evaluated server and client capabilities of Windows XP/2003 and the Novell SuSE SLES9 certified systems, with Microsoft having many useful server roles feasible which are not feasible using the SLES9 evaluated configuration.

With the evaluated Windows Server 2003 systems, we were able to deploy and validate a directory server, certificate server, web server, file server, print server, and networking server. With the Windows XP SP2 systems in the evaluated configuration, we were able to act as a client to each of the server roles successfully.

In contrast, we found that the evaluated configuration for Novell SuSE Linux Enterprise Server 9 excluded key packages necessary to deploy the common server roles. No directory (LDAP) was included in the evaluated configuration, limiting both directory and certificate server capabilities. No web server software (APACHE) was included, limiting the ability to deploy a web server. Print server is the one area that we could get to function, using the lprng package included in the evaluated configuration. Finally, DHCP and DNS were excluded from the evaluated configuration, limiting the ability to build a SuSE networking server. Similarly, the client packages necessary to leverage these server roles was generally not available in the evaluated configuration, except for the lprng and openldap2-client packages.

We additionally examined the evaluated software from a client user experience perspective and found key differences, with the Windows evaluated software providing the “normal” multiple Window experience, an Internet browser, ability to automatically acquire a network address and the ability to user Smart Cards. In contrast, the evaluated SuSE configuration requires use of a single command-line interface, static IP address and lacks support for Smart Cards.

Finally, we examined both evaluated configurations for infrastructure differences and found that the Windows evaluation had included some key security capabilities not present in the Linux system including host firewalls, IPsec, an encrypting file system and IPv6 support.

Based upon the overall examination, this study has found that for operating systems having equivalent assurance level certifications (EAL4+) and satisfying the same Common Access Protection Profile under the Common Criteria for Information Technology Security Evaluation are not necessarily created equal. The vendor selection of the evaluated configuration is critical and will make a

huge difference in the types of server and client roles that can be deployed while following the security configuration guidelines as approved by the certifying authorities.

## References

Common Criteria for Information Technology Security Evaluation, *Part 3: Security Assurance Requirements*, August 1999

[http://niap.nist.gov/cc-scheme/cc\\_docs/cc\\_v21\\_part3.pdf](http://niap.nist.gov/cc-scheme/cc_docs/cc_v21_part3.pdf)

[ccpepl06] Common Criteria Portal List of Evaluated Products. Operating Systems, January 2006

<http://www.commoncriteriaportal.org/public/consumer/index.php?menu=4&orderindex=1&showcatagories=256>

[mscsec05] Science Applications International Corporation  
Common Criteria Testing Laboratory, *Windows Server 2003 Certificate Server Security Configuration Guide*, September 2005

[mscetr05] Science Applications International Corporation  
Common Criteria Testing Laboratory, Evaluation Technical Report for Microsoft Windows Server 2003 Certificate Server - Part 1 (Non-Proprietary), 15 November 2005

[Mscnia06] Validated Product Entry for Microsoft Windows Server 2003 Certificate Server at the National Institute of Standards (NIST) National Information Assurance Partnership (NIAP) web site. January 2006  
[http://niap.nist.gov/cc-scheme/st/ST\\_VID4024.html](http://niap.nist.gov/cc-scheme/st/ST_VID4024.html)

[sleetr05] Bundesamt für Sicherheit in der Informationstechnik, *Certification Report BSI-DSZ-CC-0256-2005 for SuSE Linux Enterprise Server 9 with certification-sles-ibm-eal4-package from Novell SUSE Linux AG*, March 2005

[slesec05] Weidner K., atsec GmbH, *Common Criteria EAL4+ Evaluated Configuration Guide for SUSE LINUX Enterprise Server on IBM Hardware*, January 17, 2005

[winetr05] Science Applications International Corporation  
Common Criteria Testing Laboratory, *Evaluation Technical Report For the Windows 2003/XP Product Part 1 (Non-Proprietary) Version 3.0*, October 19, 2005

[w03adm05] Science Applications International Corporation  
Common Criteria Testing Laboratory, *Windows Server 2003 Evaluated Configuration Administrator's Guide Version 1.0*, September 21, 2005

[w03sec05] Science Applications International Corporation

Common Criteria Testing Laboratory, *Windows Server 2003 Security Configuration Guide*, August 11, 2005

[wxpsec05] Science Applications International Corporation  
Common Criteria Testing Laboratory, *Windows XP Professional Security Configuration Guide, Version 1.0*, September 22, 2005

[Winnia06] Validated Product Entry for Microsoft Windows Server 2003 and Microsoft XP at the National Institute of Standards (NIST) National Information Assurance Partnership (NIAP) web site. January 2006  
[http://niap.nist.gov/cc-scheme/st/ST\\_VID4025.html](http://niap.nist.gov/cc-scheme/st/ST_VID4025.html)