Edith Cowan University
CSI1101
Computer Security
Assignment 1

Contemporary Issue Report

Martin Ponce
Student 10371381

Tutor: Patryk Szewczyk

March 7, 2015

Contents

1 Introduction

The Board of Directors at Blue Ink have recently become aware of the lack of computer security awareness and best practices amongst its employees. As a result, Blue Ink have requested that a sample Virtual Machine (VM) image of a typical computer within their organisation be analysed for security issues.

This report outlines the security issues identified during the analysis of Blue Ink's sample VM image. Vulnerabilities have been found with the operating system itself, and support software packaged with the operating system, such as the Internet browser and anti-virus application. Vulnerabilities have also been identified in outdated software whilst practices regarding the storage of passwords in plain-text files within user documents folders provide opportunities for unwanted access. The security issues identified in this report must be addressed in order to maintain the utmost security.

1.1 Assumptions

- A firewall is implemented within the network

2 Security analysis

2.1 Operating system

2.1.1 Windows Vista Business x86 SP0

The VM image provided includes Windows Vista Business 32 bit (x86) Service Pack 0 (SP0) as its operating system. Windows Vista is considered to be an older operating system with extended support due to end on 11 April, 2017 (Microsoft, 2014). Service Pack 0 indicates that no service packs have been installed. In addition, SP0 support has ended on 13 April, 2010. End of support means that the operating system will "no longer receive security updates that can help protect your PC from harmful viruses, spyware, and other malicious software that can steal your personal information" (Microsoft, 2015).

Analysis of the VM image has shown that no service packs or security updates from Microsoft have been installed, leaving the operating system vulnerable to various exploits or attacks. For example, CVE-2008-0951 describes an "Execute Code" vulnerability in the operating system's Auto-run function, which allows arbitrary code on removable media to be executed when inserting either a CD-ROM or USB device (SecurityFocus, 2008).

Additionally, CVE-2007-5133 describes a "Denial of Service Overflow" vulnerability in Microsoft Windows Explorer. Windows Explorer's inability to handle malformed PNG image files can be exploited, causing the CPU to waste cycles which results in an unresponsive system (SecurityFocus, 2007a).

Furthermore, CVE-2007-1658 describes a vulnerability in Windows Mail, an email application packaged with the operating system. The vulnerability allows an attacker to send an email containing a "maliciously crafted link" to execute local files (SecurityFocus, 2007b).

As seen in the examples above, withholding the installation of operating system service pack and/or security updates leave the system open to various attacks. In-

stalling regular operating system updates is a step towards a secure system, ensuring that the latest known vulnerabilities are patched, and is suggested to be performed as best practice. Blue Ink should also note the end of extended support date. In approximately two years from the time of writing this report, no further security updates to the operating system will be supplied by the vendor. This will be a point to consider if any sensitive information is planned to be stored on these systems after the "end of support" date.

2.1.2 Internet Explorer 7

2.1.3 Windows Defender

2.2 Applications

2.2.1 Anti-virus

2.2.2 Adobe Reader 6.0.1

2.2.3 OpenOffice 1.1.5

2.2.4 mIRC 6.0

2.3 User practices

3 Conclusion

4 Glossary

- Auto-run:
- Denial of Service:
- Firewall:
- SP0: Service Pack 0 (zero), no service pack updates installed for the base operating system
- Virtual Machine:
- x86: 32-bit operating system

References

Microsoft. (2014). *Windows lifecycle fact sheet - Windows Help.* Retrieved 2015-02-27, from http://windows.microsoft.com/en-au/windows/lifecycle

Microsoft. (2015). *Microsoft Support Lifecycle.* Retrieved 2015-02-27, from http://support.microsoft.com/lifecycle/search/default.aspx?alpha=Vista

SecurityFocus. (2007a). *Microsoft Windows Explorer PNG Image Local Denial Of Service Vulnerability.* Retrieved 2015-03-07, from http://www.securityfocus.com/bid/25816/info

SecurityFocus. (2007b). *Microsoft Windows Vista Windows Mail Local File Execution Vulnerability.* Retrieved 2015-03-07, from http://www.securityfocus.com/bid/23103/info

SecurityFocus. (2008). *Microsoft Windows NoDriveTypeAutoRun Automatic File Execution Vulnerability.* Retrieved 2015-03-07, from http://www.securityfocus.com/bid/28360/info