Edith Cowan University
CSI1101
Computer Security
Assignment 1

Contemporary Issue Report

Martin Ponce
Student 10371381

Tutor: Patryk Szewczyk

April 2, 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 software packaged with the operating system, such as the Internet browser and anti-virus application. Vulnerabilities have also been identified with user installed software. This report refers to such vulnerabilities with their respective Common Vulnerabilities and Exposures (CVE) Identifier (MITRE, 2015) where applicable and provides an explanation as to why these vulnerabilities are of concern.

Vulnerabilities have also been found in user practices, such as no password being set for the default operating system user account, storage of password manager master password in a plain-text file, and administrator user privileges for standard user accounts.

1.1 Assumptions

- The computer is connected to WAN (Internet) and LAN
- A firewall is implemented to protect the network
- User "green" is a standard employee account

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, n.d.-a).

In addition to no service packs, the operating system does not have any security updates installed. This leaves the operating system vulnerable to various known 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). This vulnerability would allow a user-assisted attacker to include malicious code on a CD-ROM or USB hard drive, and insertion of the CD-ROM or USB hard drive by the victim would result in the execution of the malicious code.

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). For example, a user-assisted attacker may send a victim a website link with an embedded malformed PNG image file, causing the computer to lock up when viewed by the victim.

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

2.1.2 Internet Explorer 7

Internet Explorer 7 (IE 7) is the default browser included with Microsoft Vista. IE 7 is considered an older browser and will no longer receive support or security updates after 12 January, 2016 (Capriotti, 2014). Furthermore, since no service packs or security updates have been applied to the operating system itself, no security patches have also been applied to this browser, rendering the browser vulnerable to various known attacks and exploits.

For example, CVE-2015-0067 describes a "remote memory corruption" vulnerability for Internet Explorer versions 6 through 9. A remote user-assisted attacker may exploit this vulnerability by sending the victim a link to view a "specially crafted" web page which can then execute malicious code (SecurityFocus, 2015).

Additionally, CVE-2013-3918 describes a vulnerability in an ActiveX Control Class which allows an attacker to remotely execute code on a victim's computer through a malicious website (Microsoft, 2013; Ozkan, 2013). Chen and Caselden (2013) assert that this particular vulnerability was exploited in a "watering hole" attack on a US based website. Visitors to the website were subject to a "drive-by download" attack, enabled by the vulnerability in order to propagate malware. Moran, Scott, Vashisht, and Haq (2013) have also found that the malware payload attacks the memory directly without writing to disk, and "generally cannot be detected by traditional anti-malware tools" (Wilson, 2013).

2.1.3 Windows Defender

Windows Defender is an anti-malware software included with Windows Vista. The lack of installed service packs or security updates for the operating system has left the included anti-malware software with a severely obsolete virus and malware signature list. The supplied VM image indicates that virus definitions for Windows Defender have not been updated since version 1.0.0.0 on 14 July, 2006.

In order for an anti-malware/virus application to protect a computer effectively, signatures for known viruses and malware must be updated frequently, so that the software is aware of current threats and can protect the system from them (Goodrich & Tamassia, 2011). In its current state, Windows Defender can only protect the system from threats that exist in the definitions list on or before the update.

In addition to the lack of virus definition updates, a virus test has been applied using the malware test files from www.eicar.org. Executable, plaintext and archive files which included signatures mimicking a virus/malware were allowed to be downloaded through Internet Explorer 7 without being stopped by Windows Defender.

The executable file was also able to be executed without any warnings from Windows Defender. An on-demand scan was then performed on the folder containing the test files, and no threats were found. This either indicates that little to no protection is provided by Windows Defender in its current state, or the eicar test files are not supported with this anti-malware application.

2.2 User Applications

2.2.1 Fake anti-virus

The VM image includes a desktop shortcut for "Symantec AV Scanner". The shortcut links to a html file located in the user's Documents folder which attempts to present itself as a legitimate anti-virus software. The "user interface" imitates an on-demand virus scan with a progress bar at 100% and declares "Scan complete! No threats Discovered!".

The fake anti-virus software may provide the user a false sense of security, making the user believe the computer is protected, when in fact it is not. The origin of the fake anti-virus is also of concern, as it is possible to have been installed as a result of a malware propagation. Removal of the desktop shortcut icon and related files is recommended to ensure that it does not provide the user a false sense of protection.

2.2.2 Firefox 8.0

Firefox 8.0, an alternative web browser to Internet Explorer is installed on the VM image. Several vulnerabilities have been identified with this particular version of the browser. For example, CVE-2014-1522 is a vulnerability which allows a remote attacker to execute arbitrary code or cause denial of service conditions if a victim loads a malicious web page (MITRE, 2014a).

CVE-2014-1532 describes a "heap memory corruption" vulnerability which would allow a remote attacker to either execute arbitrary code or cause denial of service conditions (MITRE, 2014b).

2.2.3 Adobe Reader 6.0.1

Adobe Reader 6.0.1 is installed in the VM image, allowing the user to view PDF files. Adobe Reader 6.0.1 is a legacy version of the application and has been identified with a number of vulnerabilities. For example, CVE-2011-2462 describes a vulnerability which allows a remote attacker to execute malicious code or cause a Denial of Service through memory corruption (Adobe, 2011).

Similarly, CVE-2009-3959 details a vulnerability where an attacker is able to execute arbitrary code by providing the victim with a malicious PDF file. When the PDF file is viewed, the code will be executed with the user's system privileges or cause the victim's application to crash (SecurityFocus, 2010; SecurityTracker, 2010).

2.2.4 OpenOffice.org 1.1.5

OpenOffice.org 1.1.5 is an open source productivity suite of applications comparable to Microsoft Office and is currently installed on the VM image. A number of vulnerabilities have been identified for version 1.1.5. For example, CVE-2006-2198 describes a vulnerability where an attacker can create a malicious document which

when opened by the victim, will execute arbitrary macro code using the victim's user privileges without prompting the victim. The macro will execute even if the application has been configured to disable macros (MITRE, 2006a).

CVE-2006-2199 describes another vulnerability where the attacker can create a malicious Java Applet in an OpenOffice.org document. When the document is loaded by the victim, the Java Applet will escape the Java runtime 'sandbox' and provide system wide access to the attacker with the victim's user privileges (MITRE, 2006b; SecurityTracker, 2006).

2.2.5 mIRC 6.0

mIRC 6.0 is an Internet Relay Chat (IRC) client which is installed on the VM image. CVE-2002-1456 describes a "buffer overflow" vulnerability which allows an attacker to remotely execute arbitrary code through a flaw in a scripting identifier (Martin, 2002; MITRE, 2003).

In addition to vulnerabilities in the software, IRC clients share similar risks of malware propagation as email. Attackers may send links through private messages or in chatrooms, using social engineering to convince a victim to open malicious web pages or files, or may even send files directly through IRC's file-sharing protocol. Therefore the risks involved in the use of IRC in a business environment must be considered before continuing its use.

2.3 User practices

2.3.1 Password protection

The VM image does not require a password while the operating system boots up, and automatically logs in to user "green". This would allow a local attacker to gain access to the system with user "green" privileges, simply by booting up the computer.

Additionally, the screen saver is not password locked. If the computer is left on while the victim is away from the computer, a local attacker would gain system wide access with user "green" privileges with ease.

2.3.2 Plaintext password

Keepass, an open-source password manager is installed in the VM image. While it is generally recommended to use a password manager, the storage of the master password in a plaintext file is not. The master password was found to be stored in a plaintext file inside the user "Documents" directory. If this folder were to be accessed by an attacker, the file could easily be read by an attacker and all encrypted passwords stored in the password manager would be compromised.

This report suggests that the practice of storing any passwords in plaintext files to stop. If passwords are to be stored within the computer itself, they should be placed inside an encrypted virtual disk device such as Truecrypt, or within the password manager itself.

2.3.3 User privileges

The default user account (automatically logged in at boot-up without requiring a password) "green" has administrator rights. It is assumed that this user is a standard employee and should not require administrator privileges to the system. If an attacker were to gain access to the computer through this user, it is possible the attacker would gain access with administrator rights to the system. Additionally, any malware propagated while under this user's control may potentially also receive administrator privileges.

User Account Control (UAC) has been disabled for this user. UAC is a Windows Vista function which assists in protecting the computer by helping to "prevent unauthorized changes to your computer". UAC will notify the user and request permission before any system changing actions are performed (Microsoft, n.d.-b). Generally, accounts with administrator privileges are authorized to approve such changes. While this option is disabled, changes made by malware could be made without knowledge of the user.

The elevated privileges of a normal user such as "green" coupled with the disabling of UAC may allow an attacker to gain administrator rights and make system changes without alerting the user.

3 Conclusion

In conclusion, a number of security issues have been identified in the operating system, installed applications and user practices during the analysis of Blue Ink's VM image. The current operating system, Windows Vista Business does not have any service packs or security updates installed. Known vulnerabilities for the current version of the operating system and bundled browser, Internet Explorer 7, have not been patched due to the lack of installed updates. The end of support date for the operating system and Internet browser must also be considered as no further security updates will be provided by the vendor from that date onward.

In addition, bundled anti-malware software, Windows Defender, does not have up-to-date virus definitions, rendering the anti-malware software ineffective to current threats. Windows Defender was also tested with www.eicar.org pseudo-viruses, and failed to detect them.

A fake anti-virus resides on the computer. The origin of which is unknown, but potentially could have been installed by malware, luring the user with a false sense of protection. Furthermore, installed software such as Adobe Reader and OpenOffice have not been updated to their latest version. These legacy versions have been identified with vulnerabilities and leave the system vulnerable to attacks.

Access to IRC clients must also be re-considered. In addition to software vulnerabilities, IRC clients share similar risks of malware propagation as email. Attackers can easily share malicious links or files through IRC.

User practices have also been found not to follow security best practices. The computer boots into the operating system without asking for an account password, and logs into an administrator account by default. The screen-saver is also not protected by password. These practices leave the computer vulnerable to local attackers.

A plaintext file has been found to store a password manager master password. If

the computer were to be compromised by an attacker, the master password would be easily accessed, and therefore all passwords stored and encrypted by the password manager would also be compromised.

Finally, standard users are being provided with administrator privileges. If such an account were to be compromised, the attacker could potentially inherit the user's elevated access. The disabling of UAC could also lead to muted notifications if system changes were made by malware.

4 Glossary

- ActiveX Control: A small program which acts as an add-on or extension for Internet Explorer (Hoffman, 2013)
- Arbitrary code execution: To run commands that are not part of the vulnerable application code
- Auto-run: A feature of Microsoft Windows operating systems which automatically open files or execute actions when removable media has been mounted on the system
- Buffer Overflow: Occurs when a program attempts to utilise more data in its buffer than it can hold, or attempts to place data in an area of memory past its allocated buffer (Ferragamo, Weilin, Wichers, & Manico, 2014)
  - Corruption of data, denial of service conditions or arbitrary code may be executed if this occurs
- Denial of Service: An interruption in access, typically with malicious intent
  - For example, to flood a website server with requests in such a way that legitimate users of the website are unable to access the website
  - Or an attacker uses a program's vulnerability to crash the program and interrupt its use
- Drive-by download attack: Where an attacker injects malicious code into a vulnerable website so that it automatically and "silently" propagates malware as soon as a visitor views the website (George, 2014)
- Firewall: Software or hardware that protects a Local Area Network from unwanted network traffic, acts as a filter
- Heap memory corruption: Memory corruption caused by a buffer overflow in the heap data area and may be used to exchange pointers in memory from normal program code to attacker arbitrary code (*Heap overflow*, 2014; MITRE, 2014c)
- HTML: Hypertext Markup Language, a set of markup tags used to create a web page
- IRC: Internet Relay Chat, a network protocol that allows communication through text or chat

  - Also facilitates link and file-sharing

- Java: A programming language
- Java Applet: A small embedded application written in Java programming language
- LAN: Local Area Network, ie. Network within own walls
- Macro: Typically included in document creation software such as Microsoft Word, Excel etc. which allows users to create shortcuts for a series of repeated commands
  - Attackers may take advantage of this vulnerability and create malicious macros for a particular document application
- PDF: Portable Document Format
- Plaintext: A piece of communication in an unencrypted, readable format
- Sandbox: A security measure to partition the access of applications to the system
- SP0: Service Pack 0 (zero), no service pack updates installed for the base operating system
- User assisted attack: An attack where the user must take action before the attack can begin
  - An attacker may use social engineering to convince victim to take required action
- WAN: Wide Area Network, ie. the Internet
- Watering hole attack: An attack which targets a group, and originates from vulnerable websites which are known to be visited by members of the target group (Krebs, 2012; Mimoso, 2013)
  - The website/s are infected with malware, which then propagates to members of the target group visiting the website, and then spread it to other members of the target group

References

Adobe. (2011). *Adobe Security Advisories: APSA11-04 - Security Advisory for Adobe Reader and Acrobat.* Retrieved 2015-03-11, from http://www.adobe.com/support/security/advisories/apsa11-04.html

Capriotti, R. (2014). *Stay up-to-date with Internet Explorer - IEBlog - Site Home - MSDN Blogs.* Retrieved 2015-03-11, from http://blogs.msdn.com/b/ie/archive/2014/08/07/stay-up-to-date-with-internet-explorer.aspx

Chen, X., & Caselden, D. (2013). *New IE Zero-Day Found in Watering Hole Attack - Threat Research - FireEye Inc.* Retrieved 2015-03-11, from https://www.fireeye.com/blog/threat-research/2013/11/new-ie-zero-day-found-in-watering-hole-attack.html

Ferragamo, J., Weilin, Z., Wichers, D., & Manico, J. (2014). *Buffer Overflow - OWASP.* Retrieved 2015-04-01, from https://www.owasp.org/index.php/Buffer_Overflow

George, T. (2014). *The Internet's Big Threat: Drive-by Attacks — SecurityWeek.Com.* Retrieved 2015-04-02, from http://www.securityweek.com/internets-big-threat-drive-attacks

Goodrich, M. T., & Tamassia, R. (2011). *Introduction to computer security.* Boston: Pearson.

Heap overflow. (2014). Retrieved 2015-04-01, from http://en.wikipedia.org/wiki/Heap_overflow

Hoffman, C. (2013). *What ActiveX Controls Are and Why They're Dangerous.* Retrieved 2015-04-01, from http://www.howtogeek.com/162282/what-activex-controls-are-and-why-theyre-dangerous/

Krebs, B. (2012). *Espionage Hackers Target 'Watering Hole' Sites — Krebs on Security.* Retrieved 2015-04-01, from http://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/#more-16707

Martin, J. (2002). *NEOHAPSIS - Peace of Mind Through Integrity and Insight.* Retrieved 2015-03-11, from http://archives.neohapsis.com/archives/vulnwatch/2002-q3/0092.html

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

Microsoft. (n.d.-b). *What is User Account Control? - Windows Help.* Retrieved 2015-03-14, from http://windows.microsoft.com/en-au/windows/what-is-user-account-control#1TC=windows-vista

Microsoft. (2013). *Microsoft Security Bulletin MS13-090 - Critical.* Retrieved 2015-03-11, from https://technet.microsoft.com/library/security/ms13-090?f=255&MSPPError=-2147217396

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

Mimoso, M. (2013). *Why Watering Hole Attacks Work — Threatpost — The first stop for security news.* Retrieved 2015-04-01, from https://threatpost.com/why-watering-hole-attacks-work-032013/77647

MITRE. (2003). *CVE - CVE-2002-1456.* Retrieved 2015-03-11, from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2002-1456

MITRE. (2006a). *CVE - CVE-2006-2198.* Retrieved 2015-03-11, from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2198

MITRE. (2006b). *CVE - CVE-2006-2199.* Retrieved 2015-03-11, from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-2199

MITRE. (2014a). *CVE - CVE-2014-1522.* Retrieved 2015-03-18, from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1522

MITRE. (2014b). *CVE - CVE-2014-1532.* Retrieved 2015-03-18, from http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-1532

MITRE. (2014c). *CWE - CWE-122: Heap-based Buffer Overflow (2.8).* Retrieved 2015-04-01, from https://cwe.mitre.org/data/definitions/122.html

MITRE. (2015). *CVE - Common Vulnerabilities and Exposures (CVE).* Retrieved 2015-03-18, from https://cve.mitre.org/

Moran, N., Scott, M., Vashisht, S. O., & Haq, T. (2013). *Operation Ephemeral Hydra: IE Zero-Day Linked to DeputyDog Uses Diskless Method — Threat Research — FireEye Inc.* Retrieved 2015-03-11, from https://www.fireeye.com/blog/threat-research/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

Ozkan, S. (2013). *CVE-2013-3918 : The InformationCardSigninHelper Class ActiveX control in icardie.dll in Microsoft Windows XP SP2 and SP3, Windows Server.* Retrieved 2015-03-11, from http://www.cvedetails.com/cve/CVE-2013-3918/

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

SecurityFocus. (2010). *Adobe Reader and Acrobat U3D Support Remote Code Execution Vulnerability.* Retrieved 2015-03-11, from http://www.securityfocus.com/bid/37756/info

SecurityFocus. (2015). *Microsoft Internet Explorer CVE-2015-0067 Remote Memory Corruption Vulnerability.* Retrieved 2015-03-11, from http://www.securityfocus.com/bid/72423/info

SecurityTracker. (2006). *OpenOffice.org Bugs Let Java Scripts Escape the Sandbox, Macro Code Be Executed, or Arbitrary Code Be Executed on the Target System - SecurityTracker.* Retrieved 2015-03-11, from http://securitytracker.com/id?1016414

SecurityTracker. (2010). *Adobe Acrobat and Adobe Reader Flaws Lets Remote Users Execute Arbitrary Code and Deny Service - SecurityTracker.* Retrieved 2015-03-11, from http://www.securitytracker.com/id?1023446

Wilson, T. (2013). *New IE Vulnerability Found In The Wild; Sophisticated Web Exploit Follows.* Retrieved 2015-03-11, from http://www.darkreading.com/new-ie-vulnerability-found-in-the-wild-sophisticated-web-exploit-follows/d/d-id/1140858?