CS 5343 Secure Systems and Software Spring 2015

TOPIC: **Cyber patriot report for Windows and Ubuntu**

Team Members: **Chetna Khullar (voa808)**

Viswanath Nuggu (tef771)

Submitted to: **Dr. Gregory B. White**

Report on Windows Image Modifications

Scored Activities /Changes to the Image:

- **Forensics Question 1**
  Identified members of event log users as bratac, jquinn, ghammond

- **Forensics Question 2**
  Identified last login details of user 'djackson' by using the command "net user djackson"

- **System Protection has correctly configured**
  System protection is the feature that powers System Restore – Windows will automatically take snapshots of important system files and allow you to undo those changes. Hence, it is an important feature for security and implemented.

- **Removed unauthorized users**
  Users anubis, apophis , baal , ra are not in the authorized user list provided in the read me file. So these user accounts are removed.

- **Passwords for users hlandry and ckawalsky are included**
  The user hlandry, ckawalsky are set with a strong password for enhanced security so as to make their accounts more secure.

- **Insecure password changed for user scarter**
  The user scarter is set with a strong password for enhanced security so as to make password cracking difficult.

- **User cmitchell , jquinn is not an administrator**
  Users cmitchell , jquinn are not mentioned in the administrator list provided in the read me file, hence it is removed from the administrator list and are modified to standard users.

- **A secure minimum password length is required**
  The minimum password length policy is set so that the passwords are required to be of minimum length (more secure passwords) making them difficult to crack.

- **Windows automatically checks for updates**
  The windows 'Automatic check for updates' is enabled so that the system software is up to date and the patches for security vulnerabilities fix are always installed on the machine making the machine secure.

- **GIMP , Firefox has been updated**
  As per Readme file gimp, fire fox has to be updated so that we have the latest version installed which ensures that the system is always protected against latest updates.

- **Removed BitComet file sharing client**
  The BitComet is downloading manager and BitTorrent Peer-to-peer (P2P) file-sharing application. It is uninstalled because download of files and program is a security concern for the system because the downloaded files may contain malware affecting the system.

- **Removed Unreal IRC Daemon**

It is uninstalled as it is the internet relay chat software and is a security threat as the data can be easily shared on the IRC. Hence, it is removed so that the data and information is kept secure and safe.

- **Removed SmartPCFixer scareware**
  SmartPCFix is a scare ware program that displays false system diagnostic results and wants to push the user into purchase of license of a product. It is a security threat as it shows the false results and can mislead the organization management to purchase the license, hence it is uninstalled.

- **Firewall protection is enabled**
  A firewall refers to a network device which blocks certain kinds of network traffic, forming a barrier between a trusted and an un trusted network. Hence, it is a major check point for the security in windows 7. Hence, it is enabled.

- **Remote desktop sharing is turned off**
  The remote desktop sharing is a major security threat using which the cybercriminals use to execute code remotely. Hence, it is turned off.

- **The UAC secure desktop has been enabled**
  It is enabled as the user access control aims to improve the security of Microsoft Windows by limiting application software to standard user privileges until an administrator authorizes an increase or elevation. In this way, only applications trusted by the administrator may receive administrative or elevated privileges

- **Disable Telnet service**
  Telnet service is disabled because the Telnet is not encrypted, the password and all other data will be transmitted as clear text. The windows will listen on port 23 for incoming connections allowing users to login and allowing non-users to mess with the computer which would result in potential risk.

- **Disable FTP service**
  File sharing may result in sharing files between unauthorized users so it has been disabled.

- **Deleted unwanted music file for user "djackson"**
  As per read me file, no media files should be available for users so it is deleted.

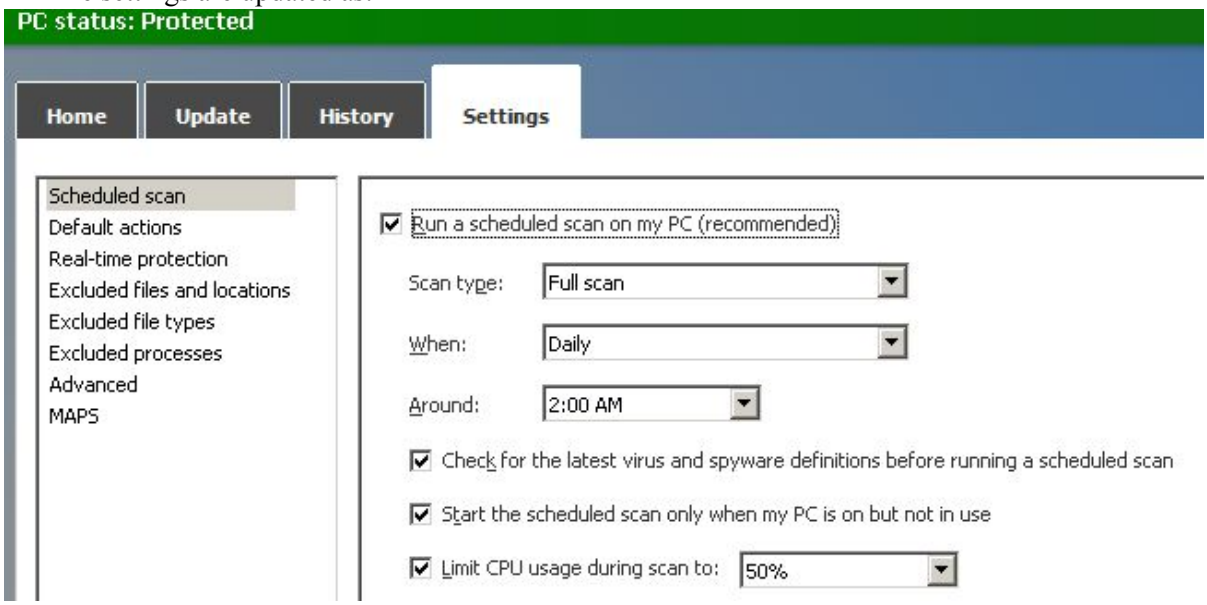
- **Screen Saver is secure**
  A secure screen saver locks our computer when the screen saver is on. Hence, it is enabled.

Un Scored changes to the Image

- **Installation of anti-virus**
  The window 7 is protected by installing windows essential antivirus. The system status is now protected.

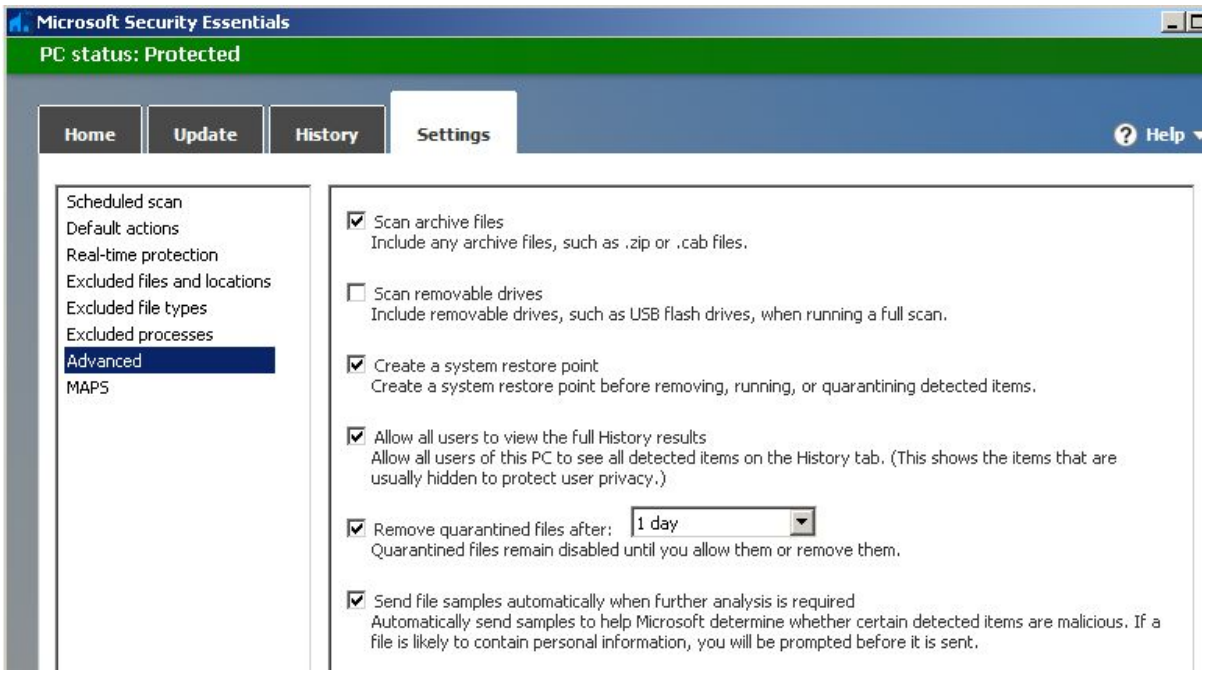
- **Settings of Microsoft Security Essentials**

  The settings are updated as:



- **Real time protection is set to ON**
  This alerts the user whenever the malicious or potentially unwanted software attempts to install itself or run on the computer. Hence, it helps to make the system more secure.

- **Advanced Settings**
  They are set so that there is a scheduled scan on the system.



- **Enable System Back Up**
  The system back up is taken so that in event when the system is effected by a virus, it can be restored. Hence, the backup is one of the most important things that should be done for system protection and security.

- **Turn On bit locker**
  BitLocker can help block hackers from accessing the system files or from accessing the drive by physically removing it from the PC and installing it in a different one. The user can still sign in to Windows and use the files as he normally would.
  This could not be implemented in the VM.

- **Deleted unwanted video files**
  The unwanted video files are deleted as they should not be in the system according to the readme file.

- **Uninstalled Windows media player**

- **Removed Games**
  Games were not required for functioning of AFA so they were removed from machine.

- **Deleted unwanted images**

Report on Ubuntu Image Modifications

Scored Activities /Changes to the Image:

- **Forensics Question 1**
  Extracted the shared file and it contains message as “27-7-15-32-12-30”.

- **Forensics Question 2**
  The cipher is decrypted.

- **Firewall Configuration**
  Firewall has been configured by using gufw and rejected all incoming connections by default. The corresponding ports are opened to allow incoming http, https, SSH, SMB connections.

- **Restricting unauthorized users**
  As per readme file, the unauthorized users baal, apophis, nirrti have been removed.

- **Modified unauthorized administrators to authorized users**
  As per readme file, the users- cmitchell, vmdran are modified from unauthorized administrators to authorized users.

- **Root Password Modified**
  The given password for is weak, which can be cracked easily and can lead to system hacking easily. Hence, the password is modified to a more secure password.

- **Disabled Guest Account**
  Guest account is a paswordless account which allows users to get access to Ubuntu machine, which makes system insecure. So it has been disabled.

- **Enabled automatic Updates**
  The automatic updates are enabled for securing the system to ensure improved security and reliability.

- **Updated Firefox, Samba, and bash**
  The latest versions of software's provide more security features so latest versions of Firefox, Samba, and bash is installed on the machine.

- **Removed Maria DB**
  Maria DB is disabled as it is not required for functioning of AFA.

- **Removed Prohibited Software**
  Kismet is a wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring mode. Kismet also supports plug-in which allow sniffing other media such as DECT. So presence of this software will make machine less secure so it is removed.

- **Root Login Disabled**
  Enabling root login allows direct logging in as root through ssh, and cracker can attempt to brute force the root password and potentially get access to the system if he finds out the root password.. The disabling of root login ensures system security from such attacks, hence it is disabled.

- **Removed unwanted media**
  As per Readme file there should be no media files available so the media files are deleted available for user "tealc".
- **Disabled FTP**
  File sharing results in sharing files between unauthorized users so it is disabled.

Un Scored changes to the Image:

- **Enabled automatic backup**
  This is enabled for automatic backup which helps to restore files and data in case of critical system failures.

- **Removed Games**
  Games were not required for functioning of AFA so they were removed from machine.

- **Installed Antivirus**
  The antivirus is installed to secure system from malware attacks.

- **Deleted unwanted images**
  The unwanted images are deleted available in pictures folder.