Guidelines for the individual laboratory project:

You are required to turn in a Microsoft Word Document and a Microsoft PowerPoint presentation (around 10-15 minutes of presentation since you need time to do the lab/demo) along with any software or links to software you used. In your lab word document be sure to include:

- Title
- Group Number and member Names blanks
- Date Assigned, Date Due, Last Edited blanks
- Lab Authored by
- Short Goal section
- Summary of what will be doing in the lab. Have an introductory paragraph that explains what the lab includes. This is an overview of what the students are about to do.
- List what equipment is necessary. When instructions are given to students about install or run something on your Linux machine, always use the words on your Linux xx Virtual Machine, or on your BackTrack physical machine, or on your Windows XP virtual Machine, etc. Provide near the beginning of the lab a section on what equipment is needed to complete this lab.
- Background and Theory Section
- Pages should be numbered and sub-sections used to break up lab
- All text that comes from someone else has to be referenced with [x] where x is the number of the reference in the references section of the lab. **You must give attribution to your sources.**
- All programs/exploits that we use in a lab have a web URL in the lab telling students where they may obtain the program. This is to make sure that a student can do the lab at home.
- If there are many parts to the lab, make sure you number the sections of the lab. Number the questions in the lab with the section number and a question number.
- **Include a section on defenses one can use against the exploits/vulnerabilities your laboratory examines.**
- Either leave enough space in the lab for the questions to be answered or provide an answer sheet in the back with the questions repeated where students can write their answers.
- Specific exercises with specific tasks to complete and method to determine students completed the tasks
- Include a section in the lab write up near the end “suggested additions and future enhancements”
- Provide an answer key sheet to the lab in the very last page (answers to all exercises)
- Power point presentation of background and lab intro/motivation
- Include in the power point presentation near the end “What you will do in the lab”

What to hand in to Fronter:

- Your lab/report to be submitted **prior** to your presentation
- Your lab solutions to be submitted **prior** to your presentation
- Your slides to be submitted **prior** to your presentation

An example lab template is on next side… presentation is up to you to create.
Note, when doing an attacker demo of a lab you have to select the highlights of it, things that work well in front of the audience. This lab is also rather long and simple.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

DT1013 Hacking and penetration testing
Lab XX: Windows Vista Security

Group Number: _____
Member Names: _____ _____

Date Assigned:
Date Due:
Last Edited:
Lab Authored By:

Please read the entire lab and any extra materials carefully before starting. Be sure to start early enough so that you will have time to complete the lab. Answer ALL questions in the Answer Sheet and be sure you turn in ALL materials listed in the Turn-in Checklist on or before the date due.

Goal:
The goal of this lab is to evaluate the security of Windows Vista using techniques and topics from previous labs in the course.

Summary:
You will learn to about Windows Vista's new security features and how to use/protect against password cracking, firewalls, rootkits, backdoors, viruses, and worms on the Windows Vista Business operating system.

Background:
Familiarity with tools like Cain, Nmap, Vmware and BackTrack. Theoretical understanding about malware, TCP/IP networking and password hashes.

Prelab:
Read the relevant white papers at:
http://www.symantec.com/business/theme.jsp?themeid=vista_research where the software company Symantec have done research and objective analysis of the security in Microsoft Windows Vista OS.

Lab Scenario:
For this lab, you will use VMware image with Windows Vista Business and BackTrack to perform various security evaluations as well as learn some advanced configurations using methods from previous labs applied to Windows Vista.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Section 1: Setup

1.1 - Networking

Boot up Windows Vista and login to the account “Adminstrator” with the password "password". The computer first needs to be set up on the network so that you can access needed files. This can be done through the following steps:

- Click the Start button with the Windows icon at the bottom left of the screen
- Click Network
- Click the yellow banner that appears to enable Network discovery
- Click Turn on network discovery and file sharing
- Click Continue when prompted by User Account Control (UAC)
- Click Yes
- Click the Network and Sharing Center button
- Click Manage network connections
- Right Click the Local Area Connection
- Select Properties
- Click Continue when prompted by UAC
- Select Properties for the Internet Protocol Version 4
- Set your IP address to one you were assigned in Lab 1
- Set your Subnet mask to 255.255.255.0
- Set the Default gateway to x.x.x.x
- Click OK and then Close

Section 2: User Account Control & Windows Defender

2.1 - User Account Control

Windows Vista comes with the User Account Control (UAC) enabled by default. UAC is a method of increasing the security of a computer by requiring users to run as standard users rather than as Administrators. Standard users have much less control over a computer and can therefore do much less damage than an Administrator account. When a user attempts to perform an action limited to Administrator accounts, or if a malicious program does, the user is prompted by the operating system with a window displaying what action is being attempted and two buttons to allow or disallow the action. If the action is allowed, then the account will temporarily be promoted to Administrator level.

UAC is often criticized for slowing down general computing with the many prompts for privilege elevation that can be generated. This is often a price for enhanced security, but users can disable UAC through User Accounts located in the Control Panel with the following steps. For now, though, leave UAC enabled.

- Click the Start button
- Click Control Panel
- Click User Accounts

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

- Click User Accounts
- Click Turn User Account Control on or off
- Click Continue when prompted by UAC
- Un-check the checkbox
- Click OK
- Click Restart Now

2.2 - Windows Defender

Windows Vista comes with a version of anti-spyware software called Windows Defender that is enabled by default. Windows Defender allows users to scan their computer for the detection and removal of malware while also providing real-time protection. Configuring Windows Defender and scanning your computer can be done through the control panel:

Click Security in the Control Panel
Click Windows Defender
Click Tools
Click Options

In this menu there are numerous options for configuring Windows Defender including scheduling automatic scans and updates, default actions, and real-time options. The default settings are adequate for now. You can scan your computer by clicking the Scan button at the top of the window. Clicking the arrow button next to the Scan button allows for choosing whether to perform a quick scan or a full scan.

2.3 - Trojan Simulator

Trojan Simulator (http://www.misec.net/trojansimulator/) is a free and harmless, demonstration trojan used to test security software. Copy Trojan Simulator from the [server] share and run Trojan Simulator by right-clicking the executable file, selecting Run as administrator, and clicking Allow when prompted by UAC. Now choose to install the Trojan Simulator.

Q2.1: Does Windows Defender detect the trojan? If so, how does it warn the user and what actions can be taken in response?

You can now choose to Uninstall the Trojan Simulator and Exit.

2.4 - Regtick

Regtick is a free program available for download (http://www.snapfiles.com/get/regtick.html) that is capable of performing a number of Windows system registry changes. There are a number of registry changes that this program can make by simply clicking a checkbox and then Apply or OK. Attempt to make various changes to your system as both a standard user and as an administrator and note how the program operates under each privilege and how

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Windows Defender and UAC monitor/control how the program runs. Because Regtick edits the registry, computer will probably need to be restarted in order for changes to take effect.

Q2.2: How does Windows Defender and UAC effect the operation of Regtick? How does privilege effect program operation?

Make sure to undo any changes made as some of these registry changes can have a profound effect on the Windows environment and then reboot the computer.

2.5 - Scoundrel Simulator

Scoundrel Simulator (http://www.geeksuperhero.com/scoundrelsim.shtml) is a free program designed to make malicious changes to your computer in a manner similar to viruses, trojans, spyware, worms, etc. Copy Scoundrel Simulator from the [server] share and run it normally (i.e. double-clicking the file and running it as a standard user rather than as an administrator). The program window contains five buttons and five checkboxes and each while make a change to the system. The checkbox will switch between checked and unchecked to indicate whether the change was successfully made. Try all five options and record the results.

Q2.3: What changes are made and which changes are not made? How does Windows Defender react?

Now close the program and re-run it, but this time run the program as an administrator by right-clicking the executable. Try all five options again and record the results.

Q2.4: What changes are made now and which changes are not? What causes the results to be different this time? How does Windows Defender react?

Q2.5: Does UAC and Windows Defender seem adequate to protect a system using these limited test programs? What else could be used to protect a Windows Vista computer?

2.6 - Spybot Search & Destroy

Copy Spybot Search & Destroy (http://www.safer-networking.org/en/index.html) from the [server] share and install it with the default settings minus the checkbox for downloading updates. Now run the Detection Update executable to update Sypbot. Run Spybot as Administrator and choose Next to skip creating a registry backup and searching for updates. Choose to Immunize the system and then click Next followed by Start using the program. Now open Scoundrel Simulator and try each button again.

Q2.6: How does Spybot respond to each attempted change?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Section 3: Windows Firewall

3.1 - Enabling Advanced Configuration

By default, Windows Vista comes with a firewall enabled that is nearly identical to the one in Windows XP. However, it is possible to enable and configure an "advanced" firewall that is capable of a much greater level of security including inbound and outbound traffic blocking. To enable the advanced firewall:

- Open the Command Prompt
- Enter "mmc.exe"
- With MMC open, go to File and then Add/Remove Snap-In
- In the Available Snap-ins list, select Windows Firewall With Advanced Security
- Click the Add button
- Click Finish and then OK

You can now access the firewalls more advanced settings including multiple firewall profiles, IPSec configuration, connection security rules, inbound/outbound rules, and rules monitoring. Connection security rules are easy to define through the Windows wizard interface and allow the user to isolate or restrict certain connections, set up server-to-server authentication rules, and create custom rules to meet the user's needs. The inbound/outbound rules are also wizard configurable and allow users to apply a rule to programs, ports, or services and make that rule apply to all programs or just one, block or allow all connections from a certain program, and configure source and destination IP addresses for both inbound and outbound traffic.

3.2 - Using the Advanced Firewall

Use your BackTrack machine to run an Nmap scan on your Vista computer and identify open ports.

< Screenshot #1 > **Take a screenshot of the Nmap output showing what ports are open.**

RealSecure Desktop Protector (RSDP) (formerly known as BlackICE™ Agent for Workstations) is for example a firewall for Windows that can be configured to block Nmap scans. The default Windows XP firewall does not have such capabilities, but the Windows Vista firewall does. To configure rules to block Nmap scans:

- Open MMC
- Click on Windows Firewall with Advanced Security
- On the middle window, scroll down to Inbound Rules
- Click New Rule on the right side of the window
- Choose Custom and click Next
- Choose All programs and click Next
- Choose ICMPv4 for Protocol type and click Next
- Click Next

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

- Choose Block the connection and click Next
- Click Next
- Name the rule "ICMP Blocker" and click Finish

Now do the same for Outbound Rules and then re-scan your Vista computer using Nmap on the BackTrack machine.

< Screenshot #2 > **Take a screenshot of the Nmap output showing what ports are open.**

Nmap should now no longer be able to scan the Windows computer except no extra firewall software was required. With the new advanced firewall, users can have much more control and security with a little bit of configuration. A large variety of rules can be defined for a variety of reasons and rules can be based on protocols, programs, ports, etc. making this firewall a huge improvement over the Windows XP firewall and much more comparable to Linux and third-party developers. Delete the firewall rules you have created.

Section 4: Password Cracking

4.1 - Ophcrack LiveCD

Password cracking is currently more challenging in Windows Vista than in Windows XP. This will most likely change over time, but currently two programs are needed to perform the cracking. The first program, Ophcrack (http://ophcrack.sourceforge.net/), is a popular Windows password cracker that operates through a boot CD to crack the passwords of an offline computer. The second program is Cain & Abel (http://www.oxid.it/cain.html), and it is also a Windows password cracker, but one that actively runs in Windows rather than offline. The basic process is to use Ophcrack to read the password hashes off of the hard drive, transfer them to another computer, and then crack the hashes to display the passwords.

First create a new, password protected account in Vista with a more complex password:

- Go to the Control Panel
- Click User Accounts
- Click Continue when prompted by User Account Control (UAC)
- Click Create a new account
- Enter an account name such as "GroupXX" with XX being your group number
- Change the account type from Standard user to Administrator
- Click Create Account
- Click the account you just created
- Click Create a password
- Enter a random password containing numbers, letters, etc.
- Click Create password
- Close the window by clicking the red "X" icon at the top right corner of the window

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Now, restart computer and boot the Ophcrack LiveCD ISO image from VMware. When the computer is booting press F2 to access the BIOS boot up selection and select boot from CD.

The computer should now boot from CD and load into Ophcrack. After a few minutes of loading files, etc. you will be loaded into Ophcrack's GUI with a window showing all of the user accounts on that machine and a warning that all LM hashes are empty. On a Windows XP machine, the passwords would all already be cracked and displayed, but Vista is currently more complicated. Select the Save As option and save the file "save.oph" to root. There are multiple ways to transfer the file to another computer, but I will describe using SFTP (SSH File Transfer Protocol, http://en.wikipedia.org/wiki/SSH_file_transfer_protocol) as I had the most success with it. Right-click the desktop and select xterm.
Note this is same protocol that is recommended to use at HDA for transferring files to your account at school, WinSCP:
http://du.se/Templates/InfoPage____3431.aspx?epslanguage=SV#datorkonto

Enter the following commands in the xterm window on the Vista computer:

ifconfig eth0 up
ifconfig eth0 <ip address of Vista chosen in Section 1>
sftp <ip address of Computer with SSH server>

When prompted type in "yes" and then the password. Once connected type:

put /root/save.oph
quit

You have now transferred the password hashes from the Vista machine to your SSH machine. You can exit Ophcrack by typing "poweroff" and make sure to remove the CD boot. The computer can now boot back to Vista and you can move on to cracking the hashes.

< Screenshot #3 > **Take a screenshot of the contents of the save.oph file in your root directory on the SSH server.**

4.2 - Cain & Abel

Transfer the "save.oph" file to the Vista machine via whatever method is most convenient (i.e. USB drive), though this could be done on any Windows machine. Copy Cain & Abel from the [server] share and install it by running the executable file. Once installed, run Cain with administrator privileges by right-clicking the shortcut and choosing Run as administrator and then Allow. In Cain, select the Cracker tab and choose the first option on the left pain, LM & NTLM Hashes. Now click the blue plus icon and choose to Import Hashes from a text file. Click the browse button, indicated by "..." and select the "save.oph" file (you will have to type in the name since it is filtering out all but .txt files) and click Open followed by Next.

You should now see all of the accounts on the Vista computer and you can perform a number of attacks to crack the password. The Dictionary Attack is reasonably fast, but may not always

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

succeed while the Brute-Force attack will eventually succeed, but it may take hours, days, weeks, months, or even years.

To run the Dictionary Attack, right-click the account, go to the Dictionary Attack context menu, and choose NTLM Hashes. Click the Add button and add the word list file found in C:\Program Files\Cain\Wordlists, then click Start. To run a Brute-Force Attack, right-click the account, go to the Brute-Force Attack context menu, and choose NTLM Hashes. You can edit the settings to effect how long the attack will run. Using a bigger predefined character set or password length will have a greater chance of success, but will take longer to run and vice versa. Attempt to crack the password for the default Administrator account with the simple password "password" using either attack method.

Q4.1: Were you able to crack the password for Administrator account? What attack did you use and how long did it take?

Now try to crack the more complex password using the Dictionary Attack (the Brute-Force Attack probably won't work unless you are very lucky or have a lot of free time).

Q4.2: Was the Dictionary Attack able to crack the more complex password? Why?

4.3 - Plain-Text.info

A much more effective means of cracking passwords is using rainbow tables. Cain is capable of using rainbow tables, but they must first be downloaded to the local machine. An alternative is to use the rainbow tables at http://www.plain-text.info/add/. Copy and paste the account line with the more complex password from the "save.oph" file into the box, select ntlm as the algorithm, enter in the security code provided, and click Send. You will be redirected to a list of hashes where yours has been entered into the queue for cracking. You can find your hash by checking the NT Hash shown in Cain versus the list of hashes and algorithms on Plain-Text's list. Check back later and the correct value should be shown on the table and the password has been successfully cracked.

Q4.3: Where you able to crack the more complex password using Plain-Text.info?

< Screenshot #4 > Take a screenshot of the hash highlighted on Plain-Text.info.

Note: Plain-Text.info may queue your hash for quite some time before cracking it. If this is the case, just screenshot your queued hash and move on.

Rainbow tables are by far the most effective method of cracking, while dictionary and brute-force attacks are somewhat limited. Cracking passwords in Vista is somewhat involved and requires more work than in Windows XP, but it is definitely possible and the only defense against it is to monitor who uses your computer and make sure your passwords are strong by using a variety of numbers, upper case and lower case letters, and characters. The longer your password and the more variety, the harder it will be to crack.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE
Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Section 5: Rootkits & Backdoors

5.1 - F-Secure BlackLight Rootkit Eliminator

F-Secure has developed a free rootkit detector for Vista called the BlackLight Rootkit Elminator (http://www.softpedia.com/get/Antivirus/F-Secure-BlackLight-Rootkit-Detection.shtml). Copy the executable from the [server] share and run it with Administrative privileges. The program will access you, accepts the terms of use or something so click Accept. Simply click Scan to scan your computer for rootkits. Once the scan is complete, you can view running processes or click Next and any rootkits found will be cleaned. Rootkits do not appear to be a prominent threat at this time, but that will surely change as new code and techniques are developed.

Note: DFK Threat Simulator is a rootkit simulator program, but does not currently work with Windows Vista. This may be fixed sometime in the future.

Section 6: Worms & Viruses

6.1 - AnnaKournikova Worm

Copy the file AnnaKournikova.jpg.vbs.txt from the [server] share or http://packetstormsecurity.org/viral-db/. Rename the file to AnnaKournikova.jpg.vbs and run the file as a standard user.

Q6.1: What effect does the AnnaKournikova worm have on the Windows Vista operating system? How does Windows Defender respond?

Right-click on the taskbar and select the Task Manager. Find the process "wscript.exe" (it should be the one consuming 90% or greater of your CPU) and terminate it.

This example should serve to show that worms are a danger to Windows Vista just as previous Windows operating systems and that UAC and Windows Defender alone are not enough to properly protect a system. Users should always ensure that an updated antivirus program and possibly another anti-spyware program are installed on their computers. Grisoft's AVG anti-virus (http://free.grisoft.com/) and Safer Networking's SpyBot Search & Destroy are both free program available online. Follow the procedure from http://www.ciac.org/ciac/bulletins/l-046.shtml to remove the worm from your computer before proceeding.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Turn-In Checklist:

[1] Answer Sheets

[2] Screenshots (4)

[3] Any corrections or additions to the lab

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

DT1013 Hacking and penetration testing
Lab XX: Windows Vista Security

Group Number: _____
Member Names: _____ _____

Date Assigned:
Date Due:
Last Edited:

Section 2: User Account Control & Windows Defender

Q2.1: Does Windows Defender detect the trojan? If so, how does it warn the user and what actions can be taken in response?

Q2.2: How does Windows Defender and UAC effect the operation of Regtick? How does privilege effect program operation?

Q2.3: What changes are made and which changes are not made? How does Windows Defender react?

Q2.4: What changes are made now and which changes are not? What causes the results to be different this time? How does Windows Defender react?

Q2.5: Does UAC and/or Windows Defender seem adequate to protect a system using these limited test programs? What else could be used to protect a Windows Vista computer?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

Q2.6: How does Spybot respond to each attempted change?

Section 3: Windows Firewall

< Screenshot #1 > Take a screenshot of the Nmap output showing what ports are open.

< Screenshot #2 > Take a screenshot of the Nmap output showing what ports are open.

Section 4: Password Cracking

< Screenshot #3 > Take a screenshot of the contents of the save.oph file in your root directory on the RedHat WS 4.0 machine.

Q4.1: Were you able to crack the password for ECE 4112? What attack did you use and how long did it take?

Q4.2: Was the Dictionary Attack able to crack the more complex password?

Q4.3: Where you able to crack the more complex password?

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

< Screenshot #4 > **Take a screenshot of the cracked hash highlighted on Plain-Text.info.**

Section 6: Worms & Viruses

Q6.1: What effect does the AnnaKournikova worm have on the Windows Vista operating system? How does Windows Defender respond?

Q6.2: What did the scan find in regards to the AnnaKournikova worm and what does this say about Windows Defender?

General Questions

Was this a relevant and appropriate lab and what about length etc?
What corrections and/or improvements do you suggest for this lab?
Please be very specific and if you add new material give the exact wording and instructions you would give to future students in the new lab handout.
You may cross out and edit the text of the lab on previous pages to make minor corrections/suggestions. General suggestions like add tool xyz to do more capable scanning will not be awarded extras points even if the statement is totally true. Specific text that could be cut and pasted into this lab, completed exercises, and completed solutions may be awarded additional credit. Thus if tool xyz adds a capability or additional or better learning experience for future students here is what you need to do.
You should add that tool to the lab by writing new detailed lab instructions on where to get the tool, how to install it, how to run it, what exactly to do with it in our lab, example outputs, etc. You must prove with what you turn in that you actually did the lab improvement yourself.

Screen shots and output hardcopy are a good way to demonstrate that you actually completed your suggested enhancements.

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/

References

[1] Auditing Windows Vista Passwords With Ophcrack And Cain <http://irongeek.com/i.php?page=videos/cracking-windows-vista-passwords-with-ophcrack-and-cain>

[2] The Windows Vista Firewall <http://www.support4vista.com/tutorial/windows-firewall.htm>

[3] Test Files <http://www.voiceofthepublic.com/test_tools/testfiles.html>

Correct answers to the lab

Q2.1:

Q2.2:

… :

To be done!

Högskolan Dalarna
Röda vägen 3
781 88 BORLÄNGE

Telefon: 023-77 80 00
Telefax: 023-77 80 50
URL: http://www.du.se/