Windows Fundamentals and Hardening

35 Points

Due Date: Lesson 6

1 References

- "IADs Top 10 Information Assurance Mitigation Strategies"
  https://www.iad.gov/iad/library/ia-guidance/iads-top-10-information-assurance-mitigation-strategies.cfm
- "Hardening Windows 7"
  http://hardenwindows7forsecurity.com
- "Introduction to Windows Integrity Control"
  http://www.symantec.com/connect/articles/introduction-windows-integrity-control

2 Overview

This exercise will reinforce some of the concepts discussed in class and your book for securing Windows operating systems (OS). While this exercise covers skills common to many Windows OS, the focus will be Windows 7 and 10 operating systems, which have incorporated many significant security changes from previous Windows products. Note that many of skills may not be available in older Windows variants or may have a different user interface. As you go through the lab keep the following questions in mind:

- How do the Windows features differ from that of *Nix systems? How are they the same?
- Is it possible to accomplish many tasks the same way?
- How does the feature rich environment affect security?

This lab makes the assumption that you are going to secure a baseline image acquired from a trusted source. Thus, you can make a reasonable assertion that the image does not contain compromised programs, implants, rootkits, etc. Furthermore, as of the time of this lab, this Windows 7 image patches are up-to-date. The image, however, may have programs that have known vulnerabilities that are not patched and configurations that may not be at the most secure possible settings for our purposes.

3 Pre-exercise Questions

(Q1) What is the SAM database? Why is it important?
(Q2) What is LSASS? What is it used for?
(Q3) What is a LM hash? On what Windows systems was it implemented? Why did Microsoft continually put this into its products?
(Q4) What is Bitlocker? Give one benefit and one potential problem with using it.
(Q5) What is Microsoft Applocker used for? Give one benefit and one potential problem with using it.
(Q6) What are the two accounts created by default when Windows is installed?

4 Lab set-up

Login into the provided Windows 7 VM and log on to the `cs482` account (no password). There is also an OVA/OVF file available online from the course webpage ("Lab set-up").

5 Windows File Access Control

In Windows Explorer, go to the folder `C:\WindowsPE-Documents`. Right-click on `foo.txt`, choose Properties and choose the Security tab. Note the permissions on this file. The 'basic' permissions are shown on this page. Click the Advanced button to see where you can set finer-grained permissions, set auditing options for the file, and set the ownership of the file. [Compare this to using `chmod` and `chown` in Unix.] You should be able to double-click this file and open it in notepad.

Try to open the file `wisdomTeeth.txt`; you should get an access denied message. Open a command window (Start → All Programs → accessories → Command Prompt)

Go to the command line and use:

```
Cacls C:\WindowsPE-documents /G cs482:R /E
```

(Q7) What does this command attempt to do and what was the result of running this command?

This file is locked for editing based on the permissions granted to the CS482 account.

5.1 Elevating Priviledges

Windows 7 differs from previous versions of Windows in that elevated actions require prompt even if you are running as an administrator principal (i.e. a user profile that is in the group of administrators). From the command prompt, try using:

```
Runas /user:eecs cmd.exe
```

When you use 'runas', you will be asked for the `eecs` password. It is `scee` [Note: 'runas' is the Windows counterpart to the Unix/Linux `su` command. Running `runas /user:eecs cmd.exe` is somewhat like using `su` in UNIX; you get a new command window running in the context of `eecs`.]
Attempt:

```
Cacls C:\WindowsPE-documents\wisdomTeeth.txt /G cs482:R /E
```

(Q8) What was the result of running this command once?

Type `cmd` into the start menu and right click on the icon. Click on `Run as administrator` with the blue shield. You should see the user account control (UAC) prompt. Select `eecs`. You now have a command prompt running with elevate permission. You should now have the admin credentials to edit the privileges assigned to the file. Using `cacls` again, give read privileges to the cs482 account for the `wisdomTeeth.txt` file. Note: you can type `help cacls to get a list of command options`.

(Q9) What is the quote? BONUS why is the author of the quote famous?

6 Using the MMC

MMC is the Microsoft Management Console. It includes a number of 'snap-ins' for various system administration tasks. To start MMC, enter the mmc in the start prompt, right click on the icon and select "Run as administrator" with the blue shield.

In the MMC window, choose the File menu and Add/Remove Snap-in. Click `Add` to add these snap-ins to the local system: "Event Viewer", "Group Policy Object Editor", "Local users and group", "Services" and "Shared folders." Note that MMC gives you the option of applying the snap-in to the local system or another computer for remote administration. Choose local system for each of these snap-ins.

6.1 Group Policy Object Settings

Windows includes Group Policy Objects (GPO), which are collections of registry settings providing control of most every aspect of the operating system. In an Active Directory domain, GPOs are a powerful way to manage the security settings for users, groups, computers and other entities. The Local System GPO contains security settings that apply to the system if it is a stand-alone or if the setting is not specified by an AD GPO.
Go to the snap-in titled: `Local Computer Policy` (the group policy object editor) so we can make some changes to the Local System GPO. In the left-side window of the MMC Console, expand `Computer Configuration`, `Windows Settings` and `Security Settings`. Under `Account Policies` go to `Password Policy`. Note that password complexity is disabled and the minimum password length it 0. This is bad; a user can use a weak or even blank password. Enable password complexity, set the minimum length to 8 and the maximum age to 150 days.

(Q10) Take a screen shot of your changed settings. You many need to shrink the Policy column to get security settings to show in the main window.

Go to `Account Lockout Policy`. Note that a threshold of 0 means lockout is disabled. Set the threshold to 5 bad attempts, the duration to 30 minutes, and the reset account lockout counter to 30 minutes.

(Q11) Take a screen shot of your changed settings

Go to `Local Policies` and then `Audit Policy`. Note that no auditing is enabled. This is bad: a defensible system is monitored. Set these audit settings. Use the `explanation` tab to learn what each audit setting entails.

```
Audit account logon events - Success/Failure
Audit account management - Success/Failure
Audit directory service access - None
Audit logon events - Success/Failure
Audit object access - Failure
Audit policy change - Success/Failure
Audit privilege use - Failure
Audit process tracking - Failure
Audit system events - Success/Failure
```

These are typical settings. We do not necessarily want to log everything; the security event log would fill very quickly with routine events.

Now click on `User Rights Assignment`. This section allows you to allow or deny a variety of capabilities to users and groups. Double click on `Shut down the system`. If you wanted to prohibit your non-privileged users from shutting the system down, you could remove the Users group from this entry. NOTE: We might want to do this for a server. However, if a user has physical access he can still do a hard power-down, so it is not that useful as a security setting for a workstation.

Some user rights are considered "dangerous" because they can allow a user to escalate privileges or otherwise subvert security. These rights are: "act as part of the operating system", "create a token object", "debug programs", "load and unload device drivers", "modify an object label", "restore files and directories", "take ownership of files or other objects". These rights should be closely controlled and monitored.

(Q12) Who has the "debug programs" right on your system?

Note that while an overly lax local security policy can make your system vulnerable, many of these settings can really annoy users, cripple functionality or even prevent the computer from working at all. Security policy changes must be thoroughly tested to ensure you do not break something accidentally.

6.2 Local User And Group Management

Go to the `Local User And Groups` snap-in. View the properties for the `CS482` account. Note how you can disable and unlock accounts, force password changes, set group membership, control login behavior, etc. Privileges may be assigned to groups as well as to specific users. It is generally better to assign privileges to a group and then add the users requiring the privileges to that group, rather than assigning privileges directly to users. Adding or revoking a user's privileges is then as easy as changing his/her group memberships. This is an example of Role-based Access Control (RBAC). Windows provides several built-in groups for common 'roles'.

(Q13) Who are the members of the Network Configuration Operators group?

Rename the Administrator account to something creative (but safe for work), remember to change the description too. Create a new account called Administrator, give it a strong password and mark it as disabled. Ensure this new account is not a member of the Administrators group

(Q14) Why would we want to rename the Administrator account?

Create a new user account with your name. Try setting the password to something weak like "qwerty." Since you enabled the password complexity requirement earlier, this password should be rejected. Choose a stronger password that meets the complexity and minimum length requirements.

6.3 Windows Event Logs

Expand the `Event Viewer (local)` snap-in. Expand the `windows logs` item. This shows the basic windows event logs. Right-click on the Security log and choose properties. This allows you to edit the log location, log file size and the behavior if the log file becomes full. Set the log size to 50000KB and select `overwrite events as needed`. More extensive logging is important for a "well monitored" defensible system. There will be a brief error requiring you to set the log to a multiple of 64kb. Select OK and continue.

Choose the `Security log` and find an entry for **Event ID 4720**.

(Q15) What was the message for this event? What happened to the system to cause this event to be logged?

6.4 Shared Folders

Go to the `Shared Folders` snap-in. Note that this allows you to view and manage all the shared folders on the system. It also allows you to view (and disconnect) sessions and to see which shared files are open. A poorly configured share can be a huge vulnerability on a Windows system. Click `Shares`; you should see that the `C:\WindowsPE-Documents` folder is shared. Right-click on this folder entry and choose properties. Go to the `Share Permissions` tab. This will show you the permissions for the shared folder.

(Q16) What is the share name for `C:\WindowsPE-Documents`? What are the share's permissions?

The most restrictive of the file or share permissions apply when a user access a file via a share. For example, user may have read permissions to the share but he/she still cannot read the `wisdomTeeth.txt` file since the file's access control list prohibits it. However, giving Everyone Full Control is a bad thing. [This was the default permission applied to a new share in earlier versions of Windows!] Everyone means anyone who can touch this computer on the network. Even though they cannot access the files in the shared folder, they could still do malicious things like create multi-gigabyte garbage files in the folder.

Remove the entry for Everyone. Add an entry for `Authenticated Users` with read-only permission to the share (HINT: use the "check name" feature to populate the box). This is a much more reasonable way to share out documents in a broad but controlled way.

(Q17) Provide a screenshot of the new access control list.

(Q18) What does a $ at the end of a share name mean?

6.5 Services

Go to the `Services` snap-in. Choose the `Standard` view tab at the bottom of the window. This snap-in allows you to control and view the status of the services running on the system. [Compare this to rc.conf in UNIX.] Find the `UPnP Device host`. Double click it to get the properties. You should see that this service is started.

(Q19) What is UPnP Device host? Why would we want to disable it?

Note that you can start, stop and restart services and set the startup type. Stop the UPnP service and set its startup type to disabled. Click the `Log On` tab; this allows you to set the context in which a service will run. [This is similar to `suid` in Linux. A service running as the Local System account is like a service running suid root in UNIX; avoid if possible.]
Click the `Recovery` tab; this allows you to specify what should happen if the service fails. [Attackers often cause services to fail in the process of finding vulnerabilities and exploiting them.]
At this time, start `Application Identification` and ensure that it is set to automatically start. This will be necessary for the next task in the lab.

6.6 BONUS Putting it together: Least priviledge (5 PTS)

6.6.1 AppLocker

AppLocker is a feature introduced in Windows 7 that can deny users from executing programs or scripts. Furthermore it has the ability to configure auditing policies on an application basis as well.

In this scenario we are going to enforce the principle of least privilege by restricting `cs482`'s access to Wireshark and all standard users from the ability to elevate permissions to administrator.

Wireshark blockage

- From the `Local Computer Policy` (the group policy object editor), expand `Computer Configuration`, `Windows Settings`, `Security Settings` and go to `Application Control Policies`, click on `AppLocker`.
- Click on `Configure rule enforcement` and enable `Executable rules` "Configured"; click on `Ok`.
- When you arrive back at the "Overview section" click on `Executable Rules`.
- Right-click and select `Create New Rule`
- Select click on `Permissions` tab then, under action, select click on `Deny`, add `cs482` (HINT: Use "check name" here), click on `Ok`, click on `next`
- Choose `Path` and click next. Then select `Browse Folders..` and browse to Wireshark is located. The string should end with an asterisk, i.e.

  ```
  %PROGRAMFILES%\Wireshark\*
  ```

- Click `Next` twice (do not allow an exception or change the name) and then create the rule.

NOTE: You may be prompted to create default rules, please do so. Log out and log back in.
(Q20) Attempt to access Wireshark and take a screen shot of the pop-up.

Account restriction We can use all the controls from this section to prevent standard users from attempt to elevate their permissions. There are two primary mechanisms by which users can go from standard to administrator: using "run as" and through the "User Account Control (UAC)" prompt. To restrict the "run as" command:

1. Disable `Secondary login service` under `Services`

   (Q21) Provide a screen shoot of trying to issue the runas command from `cs482` to open a command prompt as `eecs`.

2. Disable runas via group policy:

   - Go to `Computer Configuration` → `Windows Settings` → `Security Settings` → `Software Restriction Policies` → `Additional Rules`
   - Select `New Path Rule`.
   - Navigate to the path to `runas.exe`, located in `C:\Windows\System32`, and make sure the policy is set to disallowed.

3. Block runas.exe via AppLocker

(Q22) Provide another screen shoot of trying to issue the runas command from `cs482` to open a command prompt as `eecs`. How is it different?

To restrict UAC, go to `Computer Configuration` → `Windows Settings` → `Security Settings` → `Local Policies` → `Security Options` and change the option of `User Account Control: Behavior of the elevation prompt for standard users` to "automatically deny..."

(Q23) Take a screen shot of an attempt to run the cmd prompt as an administrator by right clicking "run as administrator."

7 BONUS CLI Windows Administration (5 PTS)

The Windows command line offers a number of tools to manage the system. These tools are often more efficient to use than the GUI tools we have seen above. Also, if the GUI is not available these commands can allow you to get the system operating again. If you are going to do Windows administration or security you should also be familiar with `netstat`, `sc`, `schtasks`, `tasklist` and `taskkill`, and the 'net' commands.

Windows versions since XP also offer Windows Management Instrumentation Command-line (WMIC, pronounced "wee-mick"). We will look at a few tasks that WMIC can accomplish. Mastery of WMIC is required for a black belt in command line kung-fu. (see http://blog.commandlinekungfu.com/) [Note that the MMC snap-ins you used above and many other GUI tools use WMI calls to do their jobs. WMIC lets you get under the hood and do things your way.]

7.1 Process management

- Go to the command line.
- Enter: `wmic process call create calc.exe` The calculator application should start.
- Now enter: `wmic process list brief`. HINT: You may find it useful to use the Windows equivalent of `grep` called `findstr`. You can "pipe" the output similiar to Linux as well, i.e. `xxxx xxxx | findstr cmd.exe`
- Find the process id `<pid>` for calc.exe and enter: `wmic process <pid> delete` to kill the process. Observe that the calculator closes.

View user accounts . Now enter: `wmic useraccount list full`. This gives details on all the local user accounts. Note that each has a unique SID (security identifier) value. This is the actual value Windows uses to identify users, groups and computers. [Compare to uid and gid values in UNIX.] For example, file access control lists (ACL) use SIDs, not account names. Deleting an account and then creating a new account with the same name will not give the new account ownership of the old accountâs files, file permissions, etc. since the new account will have a different SID from the old account.

(Q24) What is the SID for the 'stewie' account?

Note that the Relative SID (RSID), the number after the last dash in the SID, is always the same for the default Administrator account. Thus, renaming this account provides a bit of security by obscurity, but a knowledgeable adversary can still find it by its RSID.

7.2 Integrity Controls

Starting with Vista, Microsoft provided Windows with yet another layer of granularity. There are mandatory access controls that can prevent lower integrity subjects from accessing higher integrity objects, even if the discretionary ACL allows access to that subject/principal. Huh? This control was put into place to reduce the attack surface of user and depth to defenses. With integrity controls a user can browse the web in low integrity mode while having separate files in a higher integrity state. If (and when) the user's browser is compromised, the attacker (in the context as the compromised process) would not be able to access the higher integrity object. An attacker would first have to find a way to elevate from the lower integrity process. Thus in a complex system where there is a higher probability of compromise with certain applications, an administrator can configure them to be not as trustworthy as more critical objects. It makes a great deal of sense to run processes typically associated with attack vectors at lower integrity levels.

(Q25) What is the command to set the "integrity level" of `foo.txt` to low?

8 Summary

This lab only begins to scratch the surface of securing Windows systems. There are numerous other topics to investigate such as how to ensure that all programs "opt-in" to security measures like DEP and ASLR, how configure the Windows firewall, anti-malware programs like a EMET or Malwarebytes, and how to administer Windows in an enterprise environment through Active Directory.

9 Submission requirements

9.1 Partner Submission

Provide one written lab report, answering each question properly labelled with the number and original question, per partner team. Be sure to include the time spent on the lab and document any external resources used.

9.2 Individual Submission

Each member needs to submit a detailed lab reflection. This includes

- approximately one half page that talks about the various themes in the Windows 7 design, access control models, and how it relates to the security principles discussed in lesson 2-4.
- any challenging points or thoughts on what you found interesting during the lab
- time spent you personally spent and how much effort you put forth
- time your partner spent, and how much effort they put forth
- be sure document any external resources used.