Windows Checklist 2.0

Lakshay Kansal (HBI)

Here is a step-by-step guide to how I approach the Windows 10 images during competition. Windows Server is pretty much the same but there are some clear differences which I will mention at the end.

Forensics Questions

This is always the first thing you want to do. This is because if you decide to do basic securing of the computer first you accidentally delete the file necessary to solve the forensic questions, you would have to restart the image because forensics questions are worth a lot.

There isn’t really a way for me to make it easier to do forensics questions. It is basically just google.

For example, they might ask you to find the RIPEMD160 Hash of a file. In that case just search up something like “How to find RIPEMD160 Hash of file windows?” And one of the first links gives us the powershell command

```
Get-FileHash <file path> -Algorithm RIPEMD160 | Format-List
```

README

The README is **really really important**. It tells you what users are authorized, which ones are admins. Take a good look at the README and look at required applications as per “company” requirements and required services which might be there.

Some examples of required applications that have been seen in the README before are GIMP, Inkscape, and OpenCPN. An example of a possible required service is Remote Desktop Protocol or FTP.

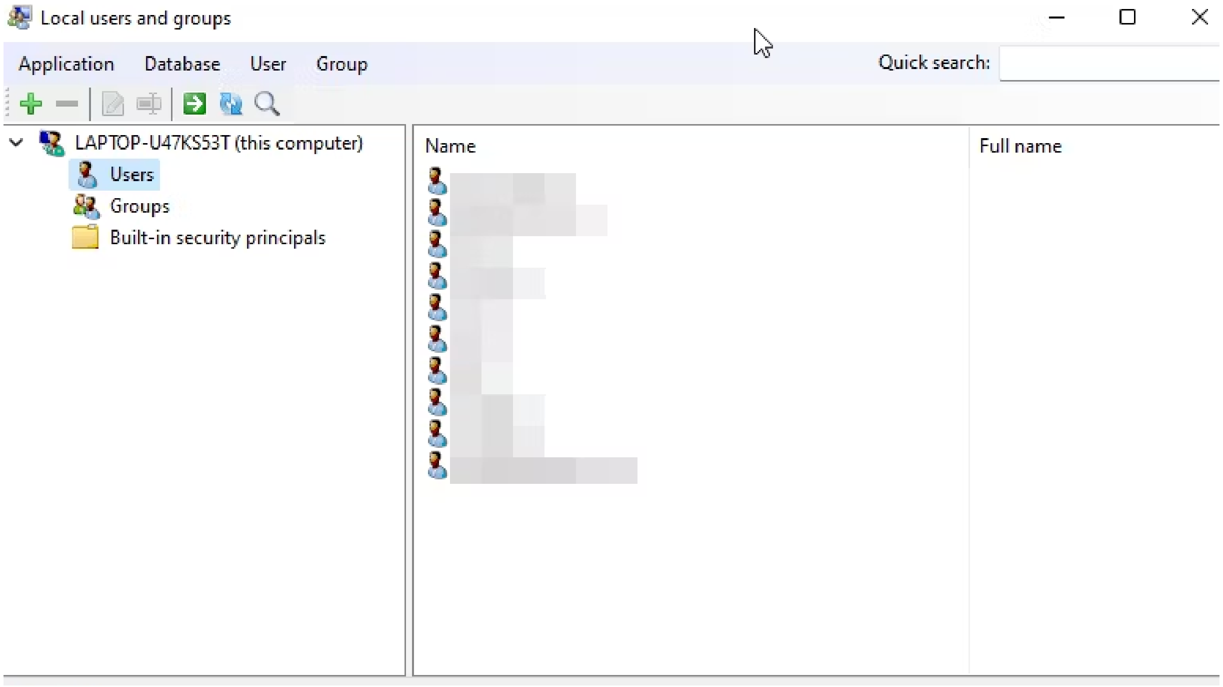
Users

Users are really important throughout all of the rounds. They are typically worth 15-30 points in every round.

There are many ways to add, delete, and modify users in Windows but the best way by far is probably lusrmgr.msc. Lusrmgr stands for local users and groups management console and it allows you to edit all of the groups and users in an organized way.

To access lusrmgr do:
Win + R -> type "lusrmgr.msc" -> run

You should arrive at a screen like this:



If you click on Users it gives you a list of every user that is currently on the computer. Ignore WDAGUtilityAccount, Guest, and Administrator for now (those are built-in Windows accounts)

Now go through the README and make sure that every user on the README is in lusrmgr and have their correct role (Admin or Standard User). If a user is not there, create an account for the user and if a user has Admin privileges but is not supposed to, remove them from the admin group. Same thing with users who are supposed to be admin's but are not.

Go through all the accounts present in lusrmgr and check if they are authorized as per the README. If they are not present in the README, then that is a finding and you should delete their account and their files.

Other things that you want to make sure of is making sure that every single user's account's password expires. If you double-click on the user there should be a checkbox for password expires.

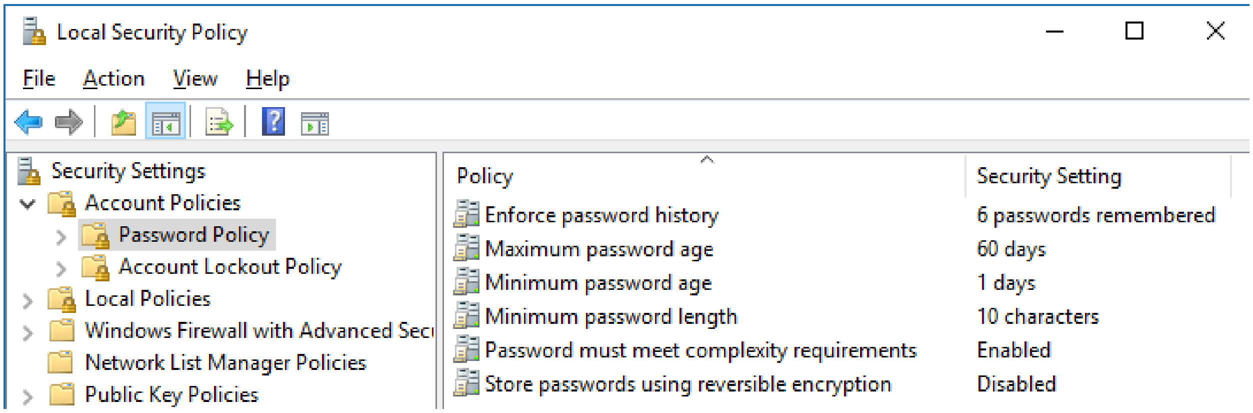
Also look at the admin passwords given in the README, if any of the passwords look insecure or weak to you, change their passwords to a more secure password like "Cyb3rP@tr!0t@123"

Disable and rename the built-in Guest and Administrator accounts that I mentioned earlier. Renaming the account makes it harder for attackers to breach the computer and disabling the account further prevents that from occurring.

Always double check the users or have someone else on the team check the users as well because you might miss something. The Ubuntu person on my team missed an unauthorized user last year in the State round and almost missed an unauthorized user this previous round if we didn't have another teammate check the users.

Account Policies

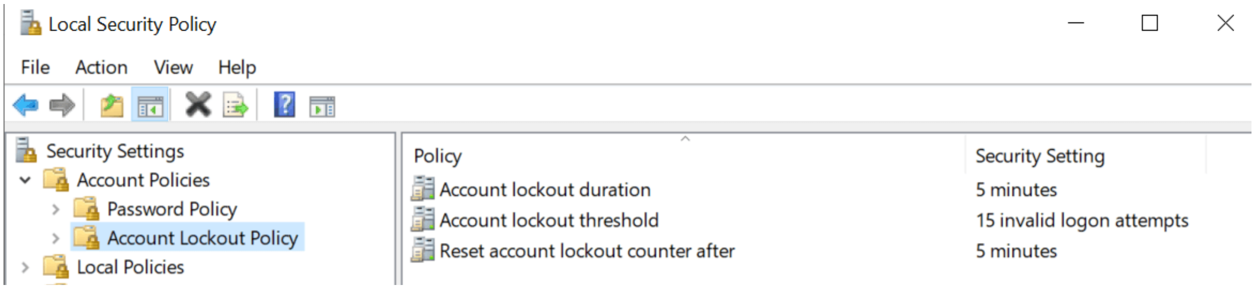
Once all of the users are configured I usually configure the account policies next.
You can probably make a script to do this but it is not too hard to do it manually.



Policy	Security Setting
Enforce password history	6 passwords remembered
Maximum password age	60 days
Minimum password age	1 days
Minimum password length	10 characters
Password must meet complexity requirements	Enabled
Store passwords using reversible encryption	Disabled

Win + R -> type “secpol.msc” -> Account Policies -> Password Policy

- Enforce Password History = 5
- Maximum Password Age = 90
- Minimum Password Age = 30
- Minimum Password Length = 8-10
- Must Meet Complexity Requirements = enabled
- Store Password Using Reversible Encryption for All Users = disabled



Policy	Security Setting
Account lockout duration	5 minutes
Account lockout threshold	15 invalid logon attempts
Reset account lockout counter after	5 minutes

Win + R -> type “secpol.msc” -> Account Policies -> Account Lockout Policy

- Account Lockout Duration = 30 min
- Account Lockout Threshold = 5
- Reset Account Lockout Counter After = 30 min

Usually at least one of these protocols gains points but in later rounds it might not.

<u>Firefox</u>

Firefox is always there on the images and there is almost always at least one point related with Firefox so I felt like I should make this a separate section.

Always update Firefox. Click on the dropdown menu, click help, then click about. Keep on updating Firefox because it is usually not done updating after the first update. If you are having trouble updating Firefox it might be because of school wifi. In that case tell Mrs. Norris and she will try to help.

Firefox security is also important to keep important data safe.
Menu -> Settings -> Privacy & Security

- Send websites a “Do Not Track” signal: Always
- Block dangerous and deceptive content: Check
- Block dangerous downloads: Check
- Warn you about unwanted and uncommon software: Check
- Enable HTTPS-Only Mode in all windows
- Enhanced Tracking Protection: Strict
- Block pop-up windows: Check

Here is an advanced config file for firefox created by people to make firefox secure if you want to try that out.
https://github.com/pyllyukko/user.js

Security for Chrome

- https://www.digitaltrends.com/computing/5-easy-ways-to-increase-security-in-google-chrome/
- Just go through Chrome settings and look at what looks like it would make the computer more secure.

Applications

Delete Unwanted Applications:
There are many ways to delete unwanted applications on Windows with the most common and straightforward way being the Windows application manager. To access that you right click on the windows logo and select apps and features. The only qualm I have about this is that sometimes it is unable to detect some bad applications and when uninstalling some applications there are trace files left which aren't good.

So instead I recommend downloading either the IoBit uninstaller or BCUninstaller.
IoBit: https://www.iobit.com/en/advanceduninstaller.php
BCUninstaller: https://www.bcuninstaller.com/
(If you have another application uninstaller that you like that is fine)

The problem with IoBit is that it is kind of like adware so there might be a few popups and ads for other IoBit applications. Just decline all of them since you only want the uninstaller. Use these to uninstall any application that is either not on the README or doesn't seem important. Like Java is not on the readme but it is pretty important for many computer features so don't uninstall that. If something like Wireshark or Nmap is there without being present as an authorized application in the README, delete it and all of its trace files.

Update All Applications:
Update every application mentioned in the README. Some applications have an update button in the application while others require you to download the latest version from the web to update it.

Windows Updates

Around 2-3 hours into the competition I suggest that you begin windows updates. Because of the school wifi, it takes a really long time to update and if you start at like 5 hours you might not finish updating by the time the timer runs out.

Also make sure to enable auto-updates for Windows. That is sometimes worth points.

Local Policies

This is probably the most boring section to do, but it is important to do because it is always points. It really is just going to every single local policy and editing it to its most secure setting.

Win + R -> type "secpol.msc" -> Local Policies

Here is a list of recommended Local Policy settings:
https://docs.google.com/spreadsheets/d/1JlMF0mSBHi7H4M2HStt66UeJZU5q3sohUiatcaet7U8/edit?usp=sharing
I would suggest learning to script in Batch or Powershell and creating a script to do these. It is much better and faster.

If you are on a time crunch, here are the local policies that usually give points so you can try them first:

- Do not display last username: Enabled
- Limit local account use of blank passwords to console logon only: Enabled
- Do not require CTRL + ALT + DEL: Disabled
- Send Unencrypted Passwords to Third-Party SMB Servers: Disabled
- Prevent users from installing printer drivers: Enabled
- Digitally sign communications (always): Enabled
- Allow automatic administrative logon: Enabled

Audit Policy

Audit Policy is hit or miss but it is always good to turn on auditing so you can detect problems.

Win + R -> type “secpol.msc” -> Local Policies -> Audit Policy

Just set everything to success and failure.

Defensive Countermeasures

Here are some defensive countermeasures that are a given

- Turn on Windows Defender
- Turn on Firewall
  - You can configure inbound and outbound rules but they are rarely points and are very complicated
- Turn off Autoplay
  - Type AutoPlay in the search bar and disable from there.
  - Win + R -> gpedit.msc -> Computer Configuration -> Administrative Templates -> Windows Components -> AutoPlay Policies -> Turn off AutoPlay -> Enabled (All Drives)

- Disable Remote Desktop (unless README says otherwise)
- Configure Windows SmartScreen

Windows Features

There are some bad Windows features that leave backdoors open.
Control Panel -> Programs -> Turn Windows Features on or off
Disable all of the following:

- Telnet
- SNMP
- RIP Listener
- Client for NFS
- IIS
- World Wide Web Services
- FTP, TFTP
- Disable SMBv1
    - Uncheck SMB 1.0/CIFS File Sharing Support

Service Auditing

There are a lot of services and a lot of them allow hackers to find a way to infiltrate the computer. Here is a list of services that should be disabled unless otherwise mentioned in the README.

Bad Services:

- UPnP Device Host
- RDP: Based on README
- Telnet
- SNMP Trap
- Remote Registry

Good Services:

- Windows Event Collector
- DHCP (Regulates Internet Connection)

If you see a sketchy service or think a service is bad, just google it and see if it has any security issues or things like that and if you get a penalty for disabling it just enable it again.

Malware

Malware is probably the biggest gray area. It is probably the hardest set of points to get as well.

Here are some links to tools to help find malware.
http://www.reconstructer.org/code.html
https://processhacker.sourceforge.io
https://live.sysinternals.com/
In Sysinternals:

- Autoruns.exe helps find bad services
- Procmon
- Process Explorer
- RootkitRevealer

You can also use MalwareBytes but proceed with caution because running MalwareBytes may mess with the scoring system.

https://www.lifars.com/2020/10/are-open-ports-a-security-risk/
Look for bad open ports but be careful because they may be required.

Windows Server

Here are some key vulnerabilities that are typically found in Windows Server but not Windows 10.

- Remove WebCompanion
- Disable file sharing for the C drive

That's it. Pretty much everything else is the same.