Windows 11 Practice Round Step By Step

Read Me Information:
It is company policy to use only Windows 11 on this computer. Management has decided that the default web browser for all users on this computer should be the latest stable version of Google Chrome. Employees should also have access to the latest stable version of GIMP, Inkscape, and Tiled for company use. Any required software should not be installed using the Microsoft store.

Your company just hired a new employee. Make a new account for this employee named "esinclair".

Some users have just been placed into a new working group by management. Make a new group called "dragonfire" and add the following users to the "dragonfire" group: emunson, gareth, jeff, mwheeler, dhenderson, lsinclair, esinclair.

This is a standalone workstation machine and does not have any business critical services.

Users:

Authorized Administrators:
eleven (you): password: niNApr0je(t
mwheeler: password: p4Lac|In11
dhenderson: password: w@teRG/\t3
lsinclair: password: ne\/er3ND5try
nwheeler: password: inn3r5tRE|\|gth
sharrington: password: ahoy

Authorized Users (Alphabetized for Convenience):
alexei
argyle
bhargrove
bnewby
cpowell
dantonov
emunson
gareth
hwheeler
jbyers
jeff
jhopper
kwheeler
mbauman
mbrenner

mmayfield
ocallahan
rbuckley
sbingham
sowens
wbyers

1) Navigate to the Read Me and Take note of the following information:
    a) Users
        i) What Users are Admins?
        ii) What Users are on there?
        iii) Who has weak Passwords?
    b) Chrome is the default browser
    c) GIMP, Inkscape, and Tiled is the ONLY applications that can be on the computer
    d) Make a new user called “esinclair”
    e) Make a Group called “dragonfire” with the users noted by the read me.

2) Forensic Question #1: You intercepted a secret message meant for mmayfield and you need to decode it. The message is: 52756e6e696e6720557020546861742048696c6c
    a) Go to https://www.cachesleuth.com/multidecoder/
    b) Type in the ciphertext
    c) Press “Solve”
    d) Scroll down until you see “Hexadecimal” where the answer is “Running Up That Hill”

3) Forensic Question #2: What is the RIPEMD-160 hash of the file in your Pictures directory named nina.jpg?
    a) Go to the nina.jpg file in pictures
    b) Right click the file and press “Copy as Path”
    c) Navigate to Powershell
    d) Paste the Generated Path to Powershell for reference
    e) Type in “Get-FileHash -a RIPEMD160 C:\Users\eleven\Pictures\nina.jpg”
    f) A hash will load and that is your hash!

4) Delete Nina.jpg
    a) Go into Pictures from the file directory
    b) Delete nina.jpg

5) Windows Security and Firewall
    a) Search up “Windows Security” in the search bar
    b) Go to “Firewall & network protection” and click “Turn on”
    c) Turn on “Virus & Threat Protection” twice

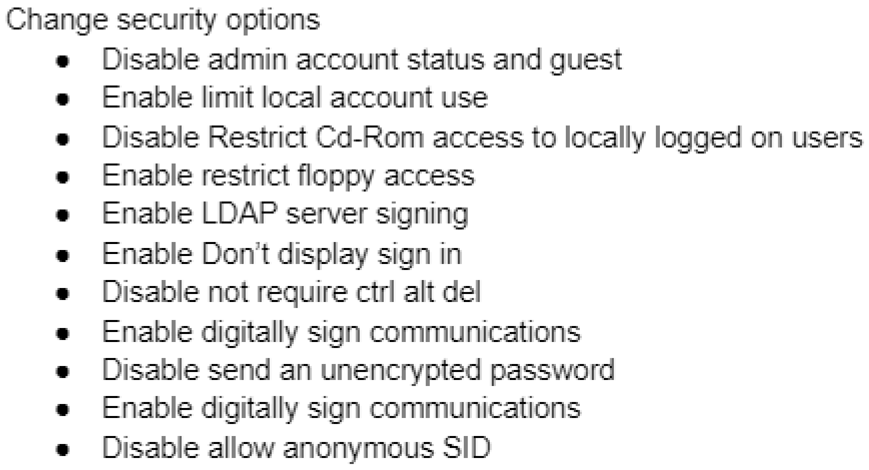
6) Windows Update
    a) Click the flash drive Icon at the bottom right of the screen
    b) Click “Eject USB Root Hub”
    c) Navigate to settings
    d) Scroll down and click “Update and Security”
    e) Click “Check for Updates” and install

7) Users!

a) Search for the control panel
b) Click “User Accounts”
c) Click “User Accounts again”
d) Click “Manage another account”
e) Deleting Users
    i) Check the readme for all the allowed users on the system
    ii) Notice that “pmckinney” and “yismaslov” are not users on the system
    iii) Click on the unauthorized account and then click “Delete the account”
    iv) Do NOT keep the files for the user
    v) Do the same for the other unauthorized user
f) Changing Users from Admin -> Standard
    i) Check the readme for which users are administrators and which users are not
    ii) Notice that it says “jbyers” and “mbauman” should be a standard user but they are an administrator on the system
    iii) Click the account
    iv) Click “Change the account type”
    v) Click “Standard” and then go down and click “Change Account Type”
g) Users Missing Passwords
    i) Notice that “argyle” is missing a password
    ii) Click the user then click “Create a password”
    iii) Make a new COMPLEX password for the user
h) Users with Faulty Passwords (ONLY ADMINS)
    i) Notice within the readme that sharrington has a really bad password
    ii) Click the respective account and then click “Change the password”
    iii) Make a new COMPLEX password for the user
    iv) Do the same for the other account with a bad password

8) Local Security Policy!
    a) Search up “Local Security Policy”
    b) Open up the “Account Policies” Folder
    c) Open up the “Password Policy” Folder
    d) Set the Following Settings
        i) Enforce Password History: 5
        ii) Maximum Password Age: 30
        iii) Minimum Password Age: 10
        iv) Minimum Password Length: 12
        v) Password must meet Complexity Requirements: Enabled
        vi) Store Passwords using reversible encryption: Disabled
    e) Open up the “Account Lockout Policy” folder
        i) Set the “Account lockout threshold” to 5
        ii) Allow the “Suggested Value Changes” of the “Account lockout duration” and “Reset account lockout counter after” settings
    f) Open up the “Local Policies” Folder

g) Open up the “Audit Policy” Folder
i) Click each policy and click “Success” and “Failure” for all of them
h) Open up the “User Rights Agreement” Folder
i) Double click on the “Access this computer from the network”
ii) Press the “Everyone” tab and press remove
i) Open up the “Security Options” Folder
i)



Change security options

- Disable admin account status and guest
- Enable limit local account use
- Disable Restrict Cd-Rom access to locally logged on users
- Enable restrict floppy access
- Enable LDAP server signing
- Enable Don’t display sign in
- Disable not require ctrl alt del
- Enable digitally sign communications
- Disable send an unencrypted password
- Enable digitally sign communications
- Disable allow anonymous SID

ii) Use this Guide to help you know what to do

9) Programs
a) Search up “Control Panel”
b) Go into the “Programs” section
c) Go into the “Programs and Features” Section
i) Notice how there are several features that should be deleted
ii) Double click “Network Stumbler (REMOVE ONLY)” and uninstall it
iii) Double click “Npcap” and uninstall it
iv) Double click “PC Cleaner v9.7.0.3” and uninstall it
v) Double click “Wireshark 4.4.0 x64” and uninstall it
vi) Double click “Microsoft Edge” and uninstall it
d) Go to the desktop and right click “CCleaner” and delete it.

10) Updates
a) Go into google chrome
b) Search “Google Download”
c) Click the first link and then click “Download Chrome”
d) Open up “ChromeSetup.exe”
e) Click “Yes”
f) Let Google Download
g) When the update completes click “Close”
h) Update Programs
i) Notice that the readme says that “Employees should also have access to the latest stable version of GIMP, Inkscape, and Tiled for company use.”

ii) Search “GIMP download” on google

iii) Go to the 2nd link (the first one is fake)

iv) Go to the website and click “Download GIMP 2.10.38 directly” and install GIMP

v) Understand that you will lose points initially but you will get it back after it fully installs!

vi) Search “Tiled download” on google and download it (DO NOT PAY FOR ANYTHING click “No thanks, just take me to the downloads” when prompted for a payment)

11) Services

a) Search up “Services”

b) Disable the Following Services Print Spooler, FTP, Telephony, FileZilla, SNMP Trap, Telnet, DNS!

i) For this image disable the Microsoft FTP service

ii) Click on “Microsoft FTP Service”

iii) Click under Startup Type “Disabled”

iv) Click “Stop” under Service Status

12) Make a new User and Group!

a) Open Up “Computer Management”

b) Go into “Local Users and Groups”

c) Click the “Users” Group

d) Right click in the empty space and Press “New User”

e) Name It “esinclair” with the Full name still being “esinclair”

f) Click The “Groups” Folder

g) Right click in the empty space and Press “New Group…”

h) Name It “dragonfire”

i) Click “Add…”

j) Type out “emunson;gareth;jeff;mwheeler;dhenderson;lsinclair;esinclair”

k) Click “Ok”

i) Then Click “Create”

13) Disabling remote assistance

a) Search “Allow Remote Assistance invitations to be sent from this computer”

b) Unlock the checkbox under “Allow Remote Assistance connections to this computer”

14) Resetting the Computer System

a) Go back into Windows Update

b) Click “Restart Now”

c) Let the System Restart