Accessible Security

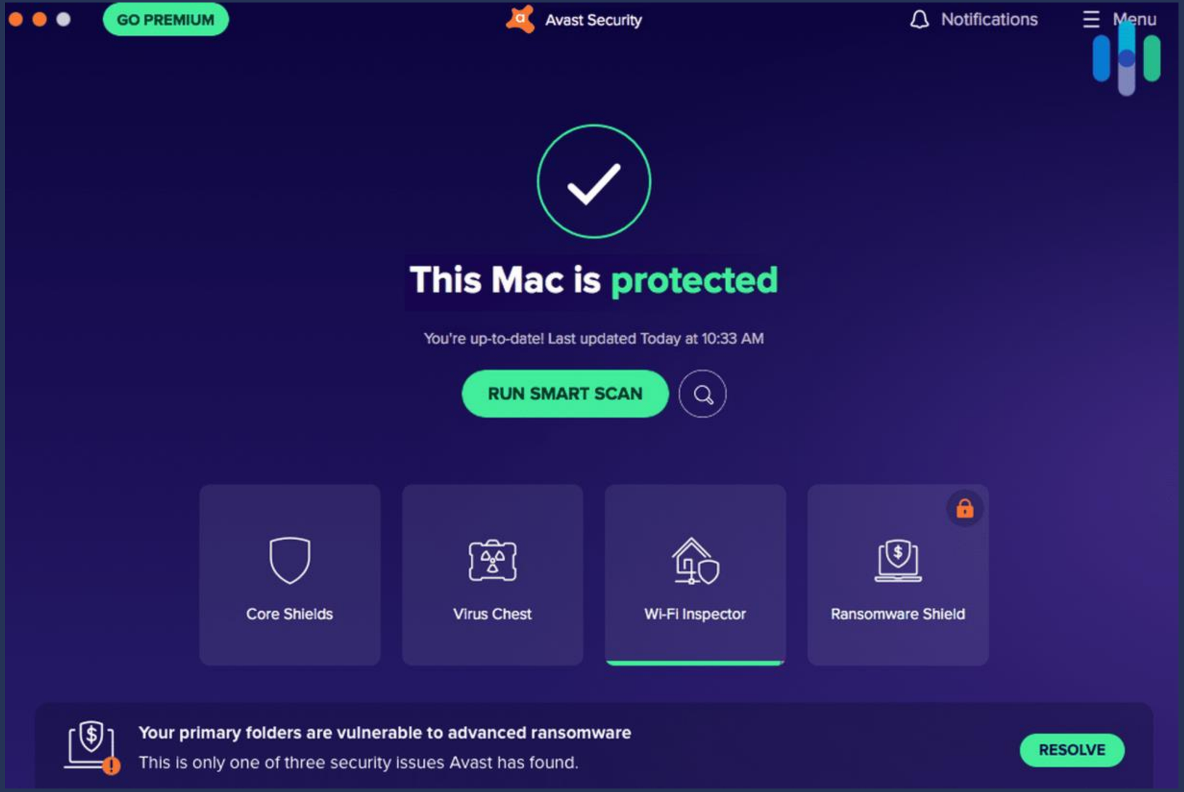
CS5472 Final Project Presentation

Trevor Hornsby

Introduction

- Problem – Popular security solutions are often oversimplified / vaguely informative
  - Limited visibility into what it’s doing to protect you
  - No knowledge of coverage gaps unless there’s a paid version
  - Few opportunities for users to learn about their specific security situation
- Solution – Created a Proof-of-Concept security product that fixes these issues using Python
  - Allows users to take control of their own security
  - Full visibility into your security
  - Ability for the user to learn more about their security issues

Examples of Current Solutions

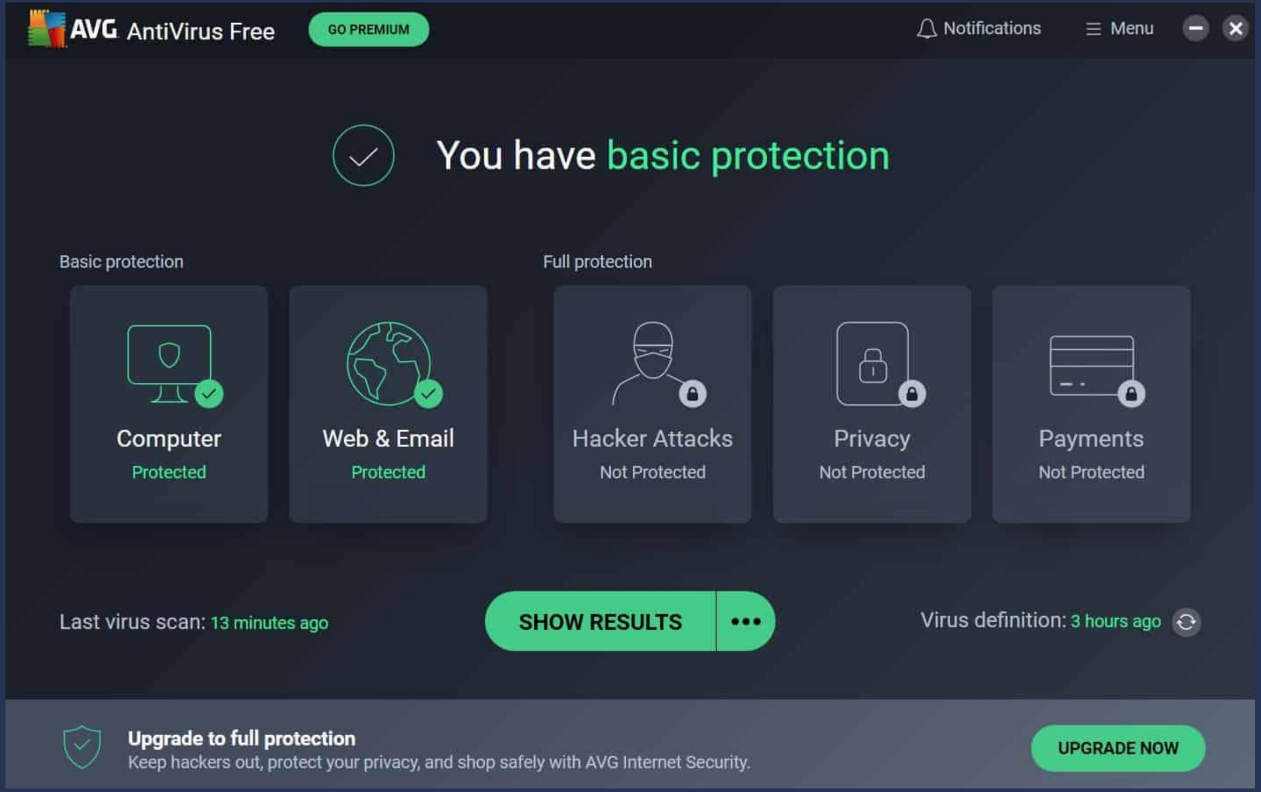


This Mac is protected

You're up-to-date! Last updated Today at 10:33 AM

Your primary folders are vulnerable to advanced ransomware

This is only one of three security issues Avast has found.



You have basic protection

Last virus scan: 13 minutes ago

Virus definition: 3 hours ago

Upgrade to full protection

Keep hackers out, protect your privacy, and shop safely with AVG Internet Security.

https://www.security.org/app/uploads/2020/12/Avast-Antivirus-Mac-is-Protected-Screenshot.png
https://www.security.org/app/uploads/2020/12/AVG_You-Have-Basic-Protection.jpg

Past Research

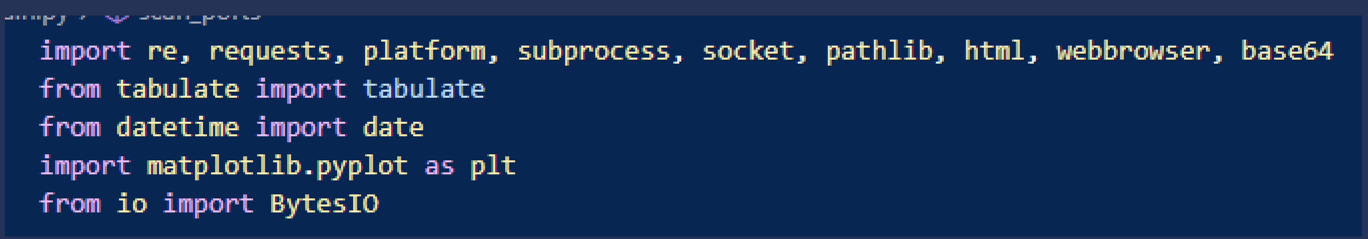
- Gamification [1]
  - Usability – levels can help users get comfortable using advanced features of a product
  - Trust – badges and achievements gives users a sense of accomplishment and interaction
  - Motivation – points can be used to motivate positive actions
- On Cybersecurity Education for Non-Technical Learners [2]
  - Everyone needs a baseline amount security education in order to keep themselves protected
  - Security concepts and education need to be accessible and understandable to everyone

Design

- Simple, easy-to-use and easy-to-read security application. Give users insight and context into how they can improve their own security
- Used a raw points and a percentage / grade system to give the user a sense of their current standing
- Output has 3 sections
  - Overall information – total score, date run, security grade
  - Positive practices – what is the user doing right
  - Negative practices – what does the user need to fix
- Positive and Negative practices
  - Four Columns: Points impact, security type / category, detailed description, link to more information and instructions
  - Color coded for impact reinforcement

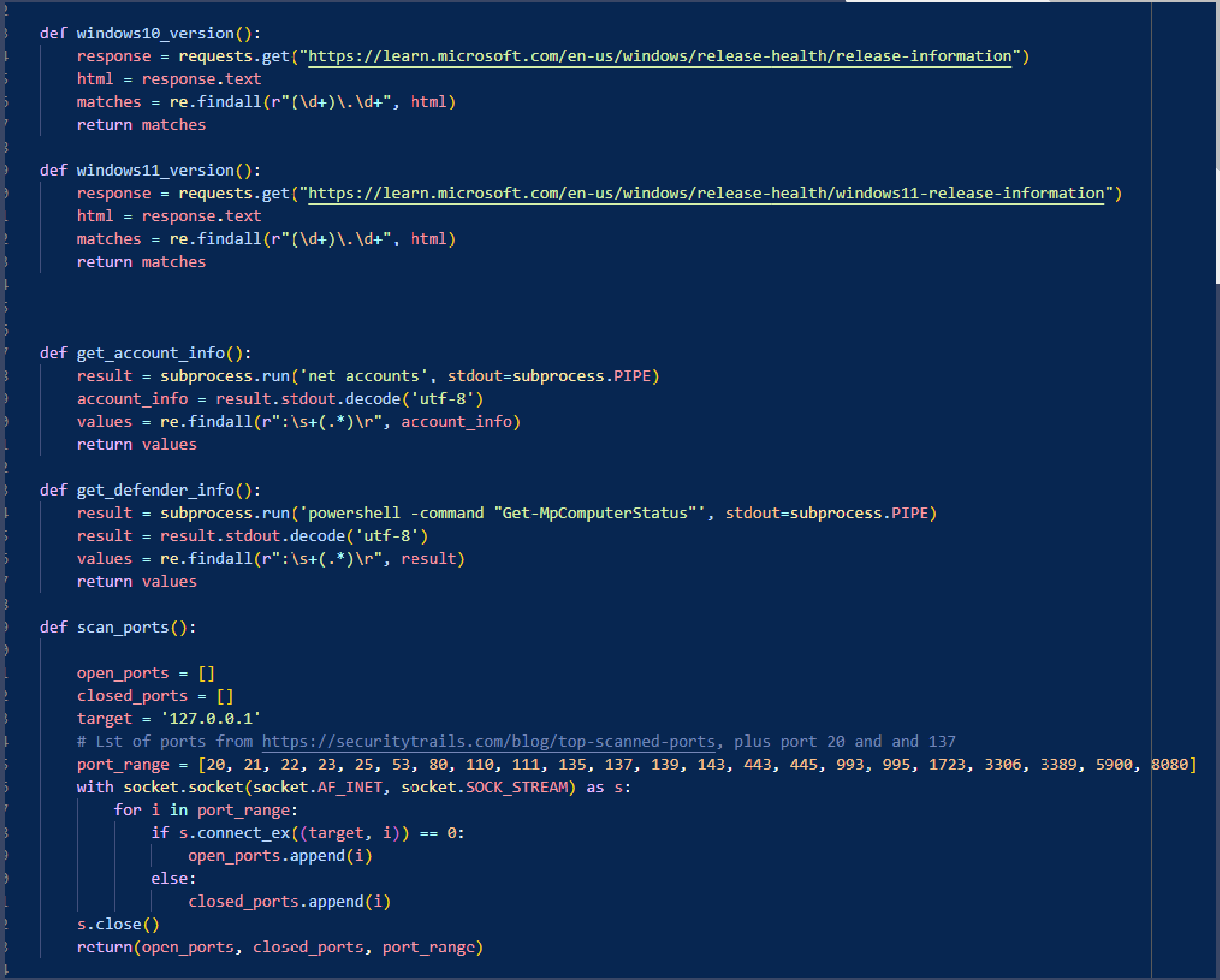
Implementation

- Python
- Three core functionalities
  - Collect data (HTTP Requests, Commands, Port Scanning)
  - Parse data, compare values to known best practices, change score, append output text and relevant URL
  - Generate, save, and open the report



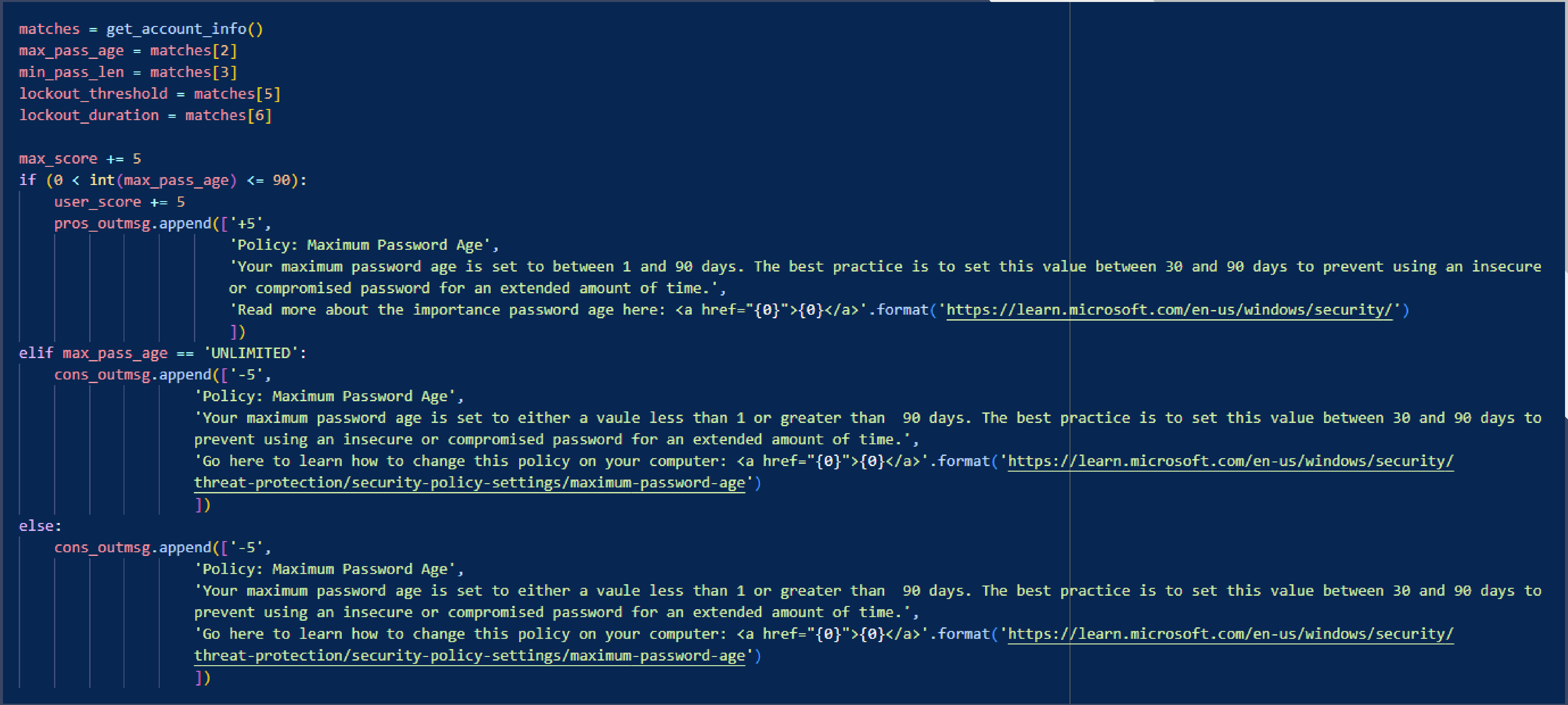
```
import re, requests, platform, subprocess, socket, pathlib, html, webbrowser, base64
from tabulate import tabulate
from datetime import date
import matplotlib.pyplot as plt
from io import BytesIO
```

Data Collection



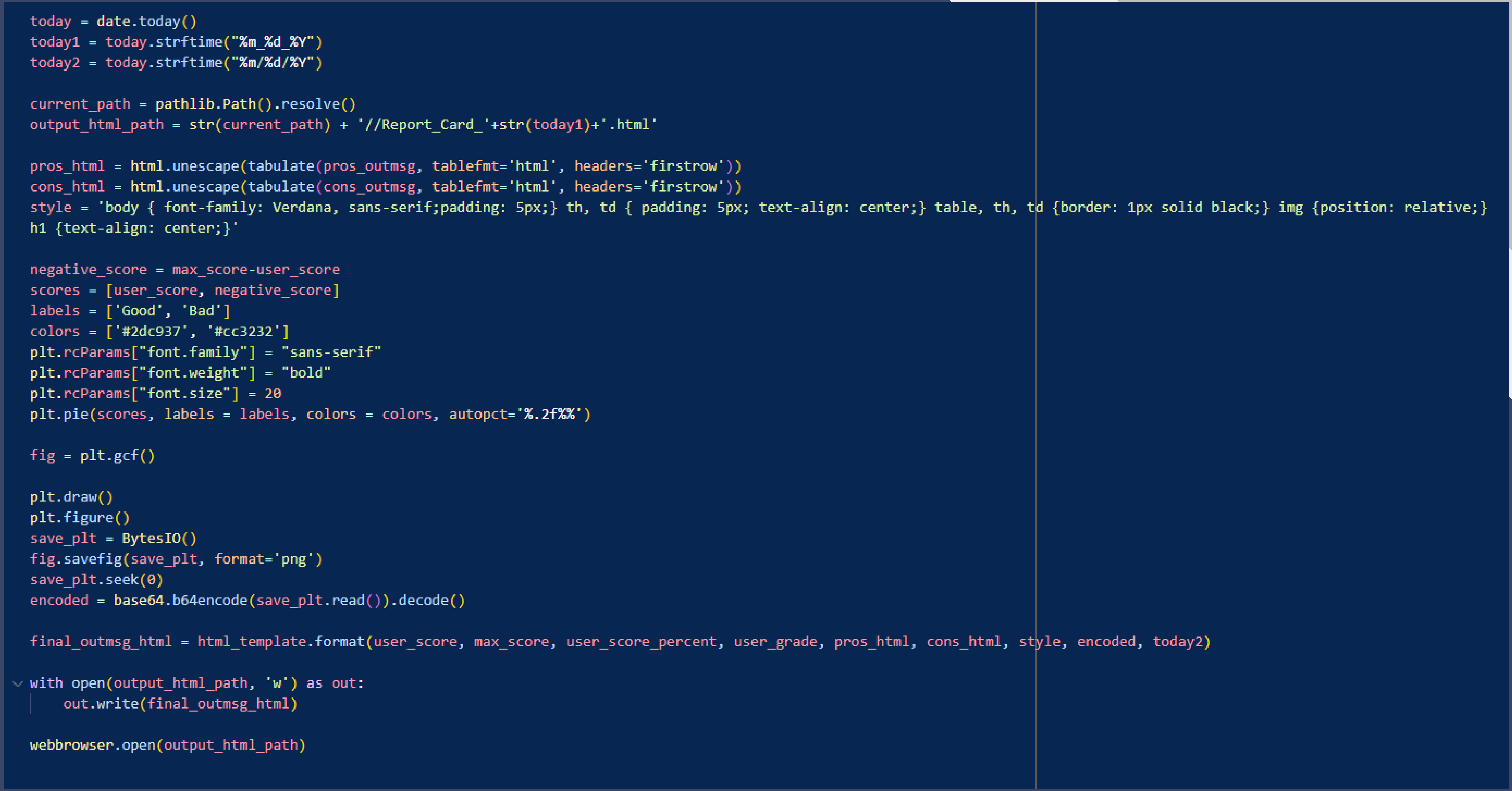
```python
def windows10_version():
    response = requests.get("https://learn.microsoft.com/en-us/windows/release-health/release-information")
    html = response.text
    matches = re.findall(r"(\d+)\.\d+", html)
    return matches

def windows11_version():
    response = requests.get("https://learn.microsoft.com/en-us/windows/release-health/windows11-release-information")
    html = response.text
    matches = re.findall(r"(\d+)\.\d+", html)
    return matches



def get_account_info():
    result = subprocess.run('net accounts', stdout=subprocess.PIPE)
    account_info = result.stdout.decode('utf-8')
    values = re.findall(r":\s+(.*)\r", account_info)
    return values

def get_defender_info():
    result = subprocess.run('powershell -command "Get-MpComputerStatus"', stdout=subprocess.PIPE)
    result = result.stdout.decode('utf-8')
    values = re.findall(r":\s+(.*)\r", result)
    return values

def scan_ports():

    open_ports = []
    closed_ports = []
    target = '127.0.0.1'
    # Lst of ports from https://securitytrails.com/blog/top-scanned-ports, plus port 20 and and 137
    port_range = [20, 21, 22, 23, 25, 53, 80, 110, 111, 135, 137, 139, 143, 443, 445, 993, 995, 1723, 3306, 3389, 5900, 8080]
    with socket.socket(socket.AF_INET, socket.SOCK_STREAM) as s:
        for i in port_range:
            if s.connect_ex((target, i)) == 0:
                open_ports.append(i)
            else:
                closed_ports.append(i)
    s.close()
    return(open_ports, closed_ports, port_range)
```

Evaluating Data



```
matches = get_account_info()
max_pass_age = matches[2]
min_pass_len = matches[3]
lockout_threshold = matches[5]
lockout_duration = matches[6]

max_score += 5
if (0 < int(max_pass_age) <= 90):
    user_score += 5
    pros_outmsg.append(['+5',
                        'Policy: Maximum Password Age',
                        'Your maximum password age is set to between 1 and 90 days. The best practice is to set this value between 30 and 90 days to prevent using an insecure
                        or compromised password for an extended amount of time.',
                        'Read more about the importance password age here: <a href="{0}">{0}</a>'.format('https://learn.microsoft.com/en-us/windows/security/')
                        ])
elif max_pass_age == 'UNLIMITED':
    cons_outmsg.append(['-5',
                    'Policy: Maximum Password Age',
                    'Your maximum password age is set to either a vaule less than 1 or greater than  90 days. The best practice is to set this value between 30 and 90 days to
                    prevent using an insecure or compromised password for an extended amount of time.',
                    'Go here to learn how to change this policy on your computer: <a href="{0}">{0}</a>'.format('https://learn.microsoft.com/en-us/windows/security/
                    threat-protection/security-policy-settings/maximum-password-age')
                    ])
else:
    cons_outmsg.append(['-5',
                    'Policy: Maximum Password Age',
                    'Your maximum password age is set to either a vaule less than 1 or greater than  90 days. The best practice is to set this value between 30 and 90 days to
                    prevent using an insecure or compromised password for an extended amount of time.',
                    'Go here to learn how to change this policy on your computer: <a href="{0}">{0}</a>'.format('https://learn.microsoft.com/en-us/windows/security/
                    threat-protection/security-policy-settings/maximum-password-age')
                    ])
```

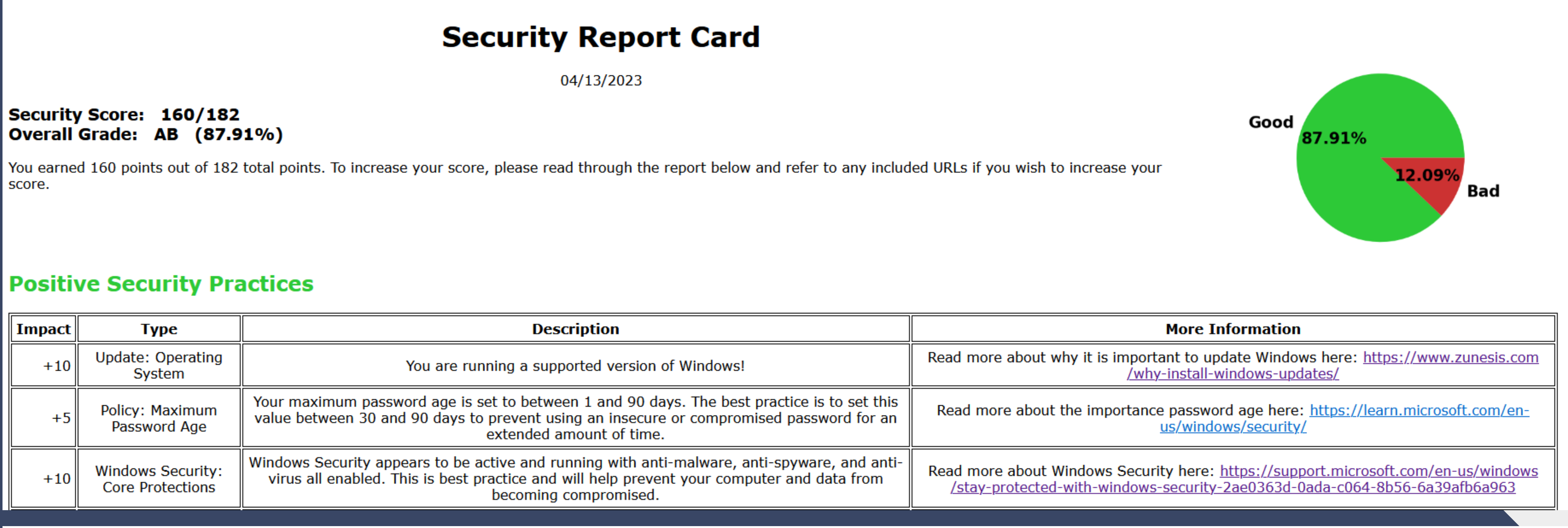
Report Generation



```
today = date.today()
today1 = today.strftime("%m_%d_%Y")
today2 = today.strftime("%m/%d/%Y")

current_path = pathlib.Path().resolve()
output_html_path = str(current_path) + '//Report_Card_'+str(today1)+'.html'

pros_html = html.unescape(tabulate(pros_outmsg, tablefmt='html', headers='firstrow'))
cons_html = html.unescape(tabulate(cons_outmsg, tablefmt='html', headers='firstrow'))
style = 'body { font-family: Verdana, sans-serif;padding: 5px;} th, td { padding: 5px; text-align: center;} table, th, td {border: 1px solid black;} img {position: relative;}
h1 {text-align: center;}'

negative_score = max_score-user_score
scores = [user_score, negative_score]
labels = ['Good', 'Bad']
colors = ['#2dc937', '#cc3232']
plt.rcParams["font.family"] = "sans-serif"
plt.rcParams["font.weight"] = "bold"
plt.rcParams["font.size"] = 20
plt.pie(scores, labels = labels, colors = colors, autopct='%.2f%%')

fig = plt.gcf()

plt.draw()
plt.figure()
save_plt = BytesIO()
fig.savefig(save_plt, format='png')
save_plt.seek(0)
encoded = base64.b64encode(save_plt.read()).decode()

final_outmsg_html = html_template.format(user_score, max_score, user_score_percent, user_grade, pros_html, cons_html, style, encoded, today2)

with open(output_html_path, 'w') as out:
    out.write(final_outmsg_html)

webbrowser.open(output_html_path)
```

Evaluation

- Successfully completed the three core functionalities
  - Data is collected efficiently
  - Known best practices are hard-coded into the comparisons
  - HTML report opens automatically
- Scoring is provided in three ways
  - Easy for user to comprehend their current situation and where / how they can improve
  - User points / total points
  - Letter grade and percentage of points earned
  - Color-coded pie chart showing how big the security gaps really are



Security Report Card

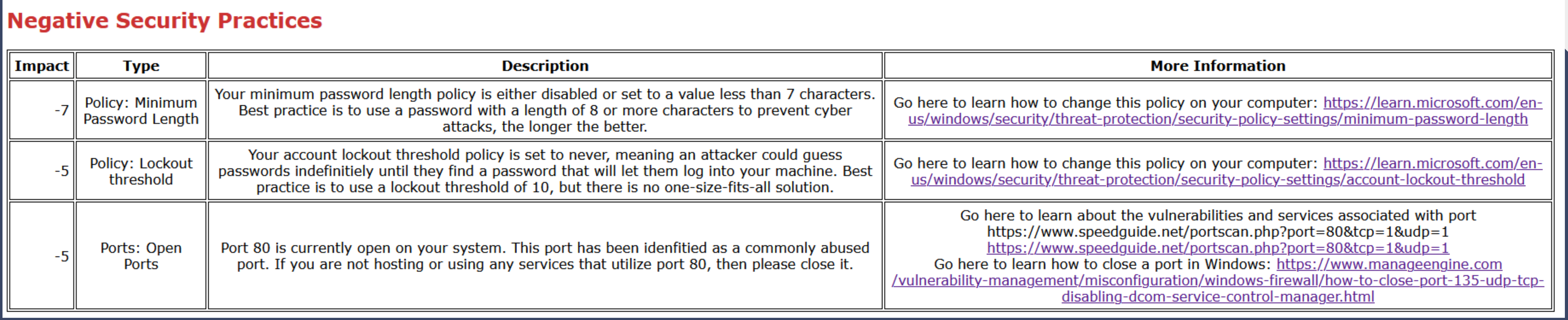
04/13/2023

Security Score: 160/182
Overall Grade: AB (87.91%)

You earned 160 points out of 182 total points. To increase your score, please read through the report below and refer to any included URLs if you wish to increase your score.

Positive Security Practices

Impact	Type	Description	More Information
+10	Update: Operating System	You are running a supported version of Windows!	Read more about why it is important to update Windows here: https://www.zunesis.com/why-install-windows-updates/
+5	Policy: Maximum Password Age	Your maximum password age is set to between 1 and 90 days. The best practice is to set this value between 30 and 90 days to prevent using an insecure or compromised password for an extended amount of time.	Read more about the importance password age here: https://learn.microsoft.com/en-us/windows/security/
+10	Windows Security: Core Protections	Windows Security appears to be active and running with anti-malware, anti-spyware, and anti-virus all enabled. This is best practice and will help prevent your computer and data from becoming compromised.	Read more about Windows Security here: https://support.microsoft.com/en-us/windows/stay-protected-with-windows-security-2ae0363d-0ada-c064-8b56-6a39afb6a963



Negative Security Practices

Impact	Type	Description	More Information
-7	Policy: Minimum Password Length	Your minimum password length policy is either disabled or set to a value less than 7 characters. Best practice is to use a password with a length of 8 or more characters to prevent cyber attacks, the longer the better.	Go here to learn how to change this policy on your computer: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/minimum-password-length
-5	Policy: Lockout threshold	Your account lockout threshold policy is set to never, meaning an attacker could guess passwords indefinitiely until they find a password that will let them log into your machine. Best practice is to use a lockout threshold of 10, but there is no one-size-fits-all solution.	Go here to learn how to change this policy on your computer: https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/account-lockout-threshold
-5	Ports: Open Ports	Port 80 is currently open on your system. This port has been idenfitied as a commonly abused port. If you are not hosting or using any services that utilize port 80, then please close it.	Go here to learn about the vulnerabilities and services associated with port https://www.speedguide.net/portscan.php?port=80&tcp=1&udp=1 https://www.speedguide.net/portscan.php?port=80&tcp=1&udp=1 Go here to learn how to close a port in Windows: https://www.manageengine.com/vulnerability-management/misconfiguration/windows-firewall/how-to-close-port-135-udp-tcp-disabling-dcom-service-control-manager.html

Future Work

- Automate security patching
  - Use GPO / commands to close ports, change policies, update windows, etc.
- Add more security categories to query and evaluate
- Create a more aesthetically pleasing HTML report design
- Improve scoring to be more dynamic and case-by-case
- Tune scoring to have well-defined weights
- Integrate with automation
- Allow user to configure what they want to have scanned

Takeaways

- From reading the paper on security education [2], making security education tools accessible and easy to use will be a growing problem as ransomware and other advanced threats continue to emerge and develop
- Difficult to balance technical features and usability features
  - Designing something that both looks user friendly and functions well at a technical level takes a large amount of effort
- Microsoft does not automatically implement their own best practices for password policies

Conclusion

- Main Contributions:
  - Created a user-controlled security appliance
    - Give users visibility into their own security
    - Allow users to educate themselves about security
  - Successfully implemented gamification concepts
    - Risk and impact are easy for anyone to interpret and understand
    - Encourages positive security practices
- GitHub: https://github.com/tjhornsb/CS5472_Final_Project

Questions

Citations

[1] D. Basten, “Gamification,” IEEE software, vol. 34, no. 5, pp. 76–81, 2017, doi: 10.1109/MS.2017.3571581. https://ieeexplore.ieee.org/document/8048643

[2] M. McNulty and H. Kettani, "On Cybersecurity Education for Non-technical Learners," 2020 3rd International Conference on Information and Computer Technologies (ICICT), San Jose, CA, USA, 2020, pp. 413-416, doi: 10.1109/ICICT50521.2020.00072. https://ieeexplore.ieee.org/document/9092220