****

**OPEN SOURCE TECHNOLOGIES**

**Class Assessment -3**

**Submitted by- Prabhat Pushp**

**Registration no: 11914390**

**Section: KE058**

**Roll no: 64**

**Submitted to: Navjot Kaur**

**Question Assigned (41):** Using desired Open Source Software list all the security updates missing in your Window OS and list all free system information about the hardware and software installed.

**Introduction**

The stability and security of any operating system, including Windows, must be maintained through security updates. These updates are intended to fix known security weaknesses and issues that could be used by hackers to compromise our machine. Installing these updates as soon as you can will help secure your device.

Microsoft frequently provides security updates for Windows to address these issues. Patches to repair bugs, plug security gaps, and enhance system performance may be included in these updates.

The use of strong passwords and maintaining the most recent versions of your antivirus and anti-malware software are two more steps you should take in addition to installing security updates to further safeguard your device.

* 1. **Objective of the project**

The goal of the effort to address the security updates that Windows lacks is to guarantee the stability and security of the operating system. The goal of this project is to locate and apply any security upgrades that are needed to fix known security flaws and other problems.

It also enhances Windows system security by applying all necessary security updates and patches. By doing this, you can lessen the risk of data breaches, unauthorised access to your system, and other security-related problems that may result from operating system flaws.

This project can also aid in enhancing system efficiency generally and lowering the possibility of system crashes by locating and implementing any missing security updates.

* 1. **Description of Project**

The project to address security updates that are missing in Windows involves identifying and installing necessary security updates and patches to improve the security and stability of the operating system. The first step in the project is to identify which security updates are missing from the system. This can be done by running a scan of the system using a Windows update tool or checking the update history in the Windows settings.

Once the missing security updates have been identified, the next step is to download and install them. This can be done manually by downloading the updates from the Microsoft website or through the automatic Windows update feature. In addition to installing missing security updates, the project may also involve updating the operating system to the latest version if necessary. Finally, it's important to verify that all necessary security updates have been successfully installed and that the system is running smoothly. This can involve performing a final system scan to ensure that there are no more missing updates and running tests to verify that the system is performing as expected.

Overall, the project to address security updates that are missing in Windows is an important step in ensuring the security and stability of the operating system. By regularly installing necessary updates and patches, users can help prevent security breaches and improve the overall performance of their system.

* 1. **Scope of the project**

The scope of the project to improve the security and stability of the operating system, the initiative to resolve security updates that are missing in Windows comprises locating and applying the essential security updates and patches.

The project's scope could include:

Finding the missing security updates: This project entails finding the system's missing security updates. This can be done by using a Windows update tool to scan the machine or by looking at the update history in the Windows settings.

After identifying the security updates that are still missing, the next step is to download and install them. The updates can be manually downloaded from the Microsoft website or downloaded automatically using the Windows update feature.

Operating system update: If necessary, the project may also comprise updating the operating system to the most recent version. By doing so, it will be possible to guarantee that the system is using the most recent software and security patches.

Checking the system: It's critical to ensure that the system is functioning properly and that all necessary security updates have been implemented. This may entail running tests to make sure the system is operating as intended and executing a final system scan to make sure there are no more missing updates.

In order to keep the system current and secure over time, it may also be included in the project's scope to develop a plan for continuous security updates and maintenance. The project may also involve educating users on security best practises for their Windows system, like using strong passwords and exercising caution when downloading files or opening email attachments.

The project's overall goal is to assist keep Windows operating system current and safe so that consumers have a dependable and secure platform for their computing needs.

1. **System Description**

A system description for addressing missing security updates in Windows would involve the tools, procedures, and requirements for identifying and installing necessary security updates and patches.

The following elements could be included in the system description:

Update tools: The system ought to include update tools for checking for uninstalled security upgrades. These resources can be obtained independently from the Microsoft website or as part of the Windows operating system.

Update procedures: The system should specify how to obtain and apply any necessary security upgrades. These steps should make sure that any required updates are correctly installed, whether they are done manually or automatically.

Testing and verification: To make sure that the updates have been successfully implemented, the system should have testing and verification methods.

Regular maintenance is necessary to keep the system current and secure throughout time. The system should outline the processes for regular maintenance. This can involve regular patches and upgrades, as well as instruction for users on the best ways to keep their Windows machine secure.

Reporting: In order to keep track of update history and make sure that all required security updates have been implemented, the system should be able to generate reports. Monitoring system performance and determining any problems or potential improvement areas are additional examples of reporting.

Overall, the system description for handling missing security updates in Windows should give a clear knowledge of the tools, processes, and requirements for preserving the security and stability of the operating system. By doing so, you can help make sure the system is always secure and up to date.

**2.1 Target system description**

The target system is not completely updated with the most recent security patches and fixes published by Microsoft if the target system description indicates that Windows security updates are missing.

As a result, Microsoft's patches for known security flaws may no longer protect the machine. In order to obtain unauthorised access to the system, steal data, or do other forms of harm, hackers and other bad actors can take advantage of these vulnerabilities.

**2.2 Assumptions and Dependencies (If applicable)**

**Assumptions:**

The target system is running a version of Windows that Microsoft continues to maintain.

The target machine has internet access, enabling it to download and set up the most recent security upgrades.

The target machine is set up to automatically download and install Microsoft updates.

**Dependencies:**

New security patches from Microsoft that are available

The target system has enough storage space for the updates to be downloaded and installed.

There are no technical difficulties or conflicts on the target system that would prohibit the installation of security updates.

The user has administrator rights on the target machine, allowing them to install security updates.

**2.3 Functional/Non-Functional Dependencies (if any)**

**Functional Requirements:**

Having access to the necessary Microsoft security updates.

The operating system's capacity to identify outdated security patches.

The capacity of the operating system to download and install the uninstalled security updates.

The capability of the operating system to examine the downloaded security updates for authenticity.

The capacity of the operating system to install security upgrades without adversely affecting the stability or performance of the system.

**Dependencies that do not function:**

The dependability and speed of the internet connection for downloading security updates.

Capacity of the system's storage for downloading and storing security updates.

The system's processing speed and memory capacity to install security updates without hindering other processes.

1. **Analysis Report**

Missing security updates in the Windows operating system can lead to a number of potential hazards and vulnerabilities, including:

Malware and viruses: By failing to apply security updates, your system becomes open to attacks from malware and viruses, which can corrupt your files, infect your machine, and steal important data.

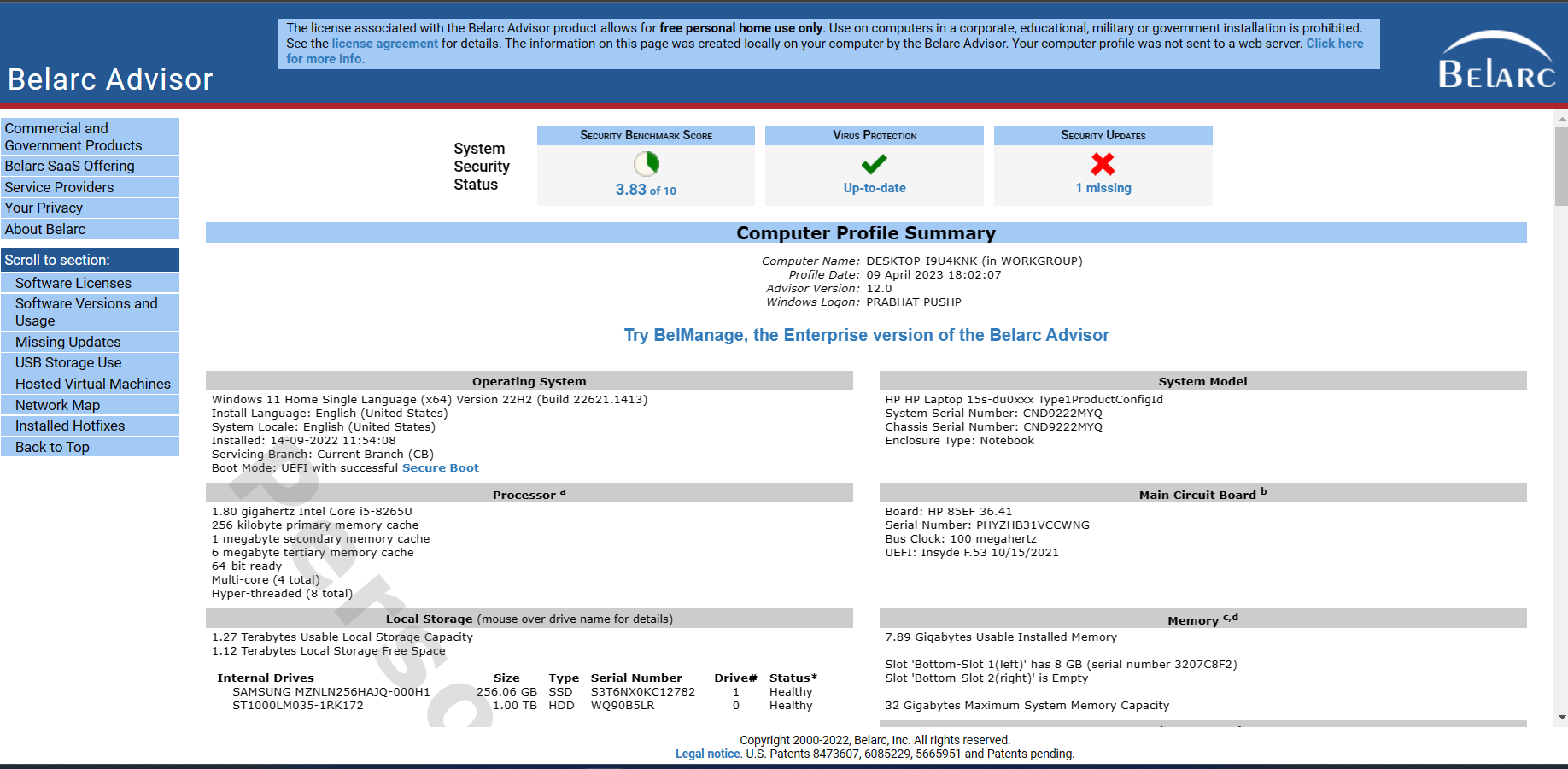
Data breaches: Older Windows systems have security flaws that hackers can use to access sensitive data, including login passwords, personal information, and bank account information, without authorization.

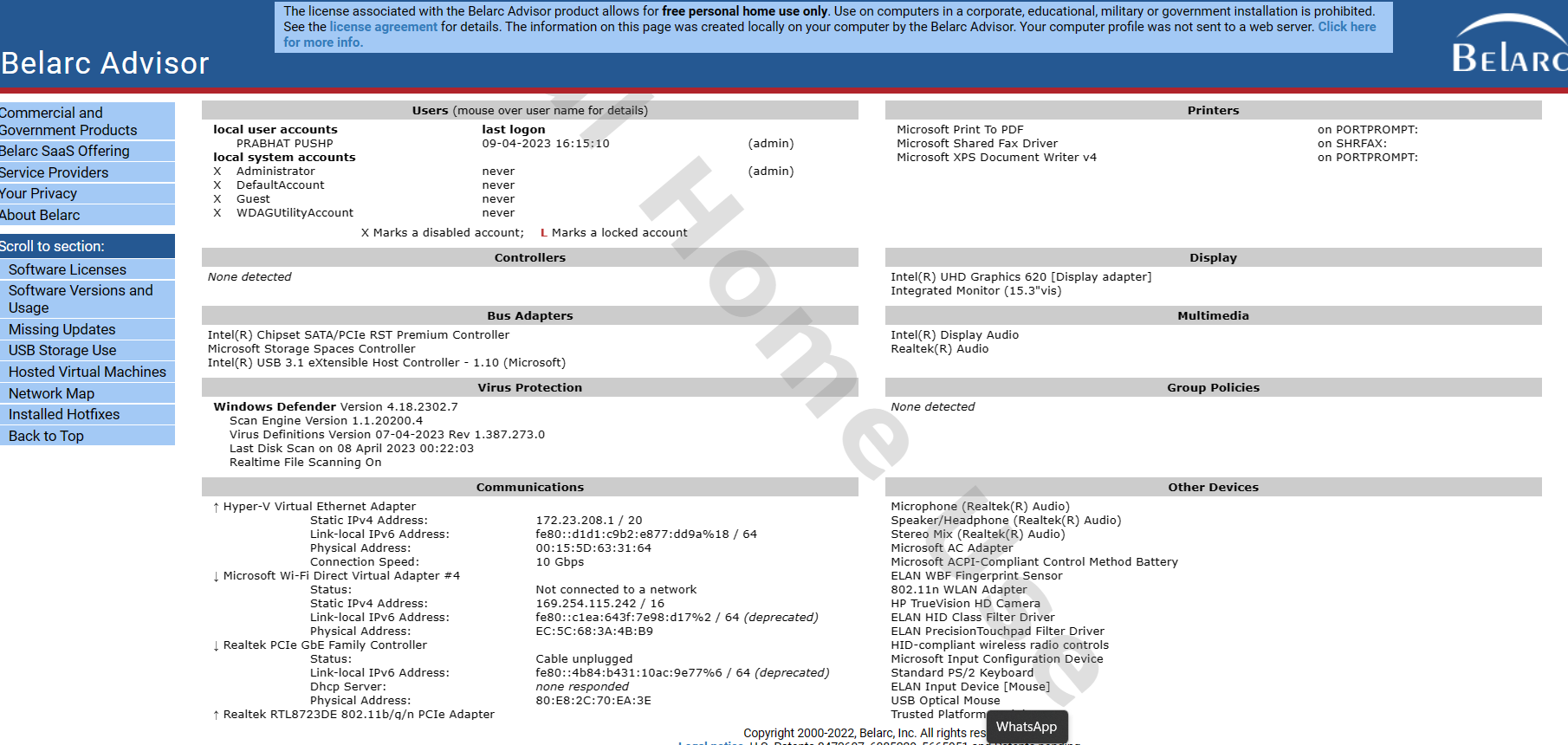
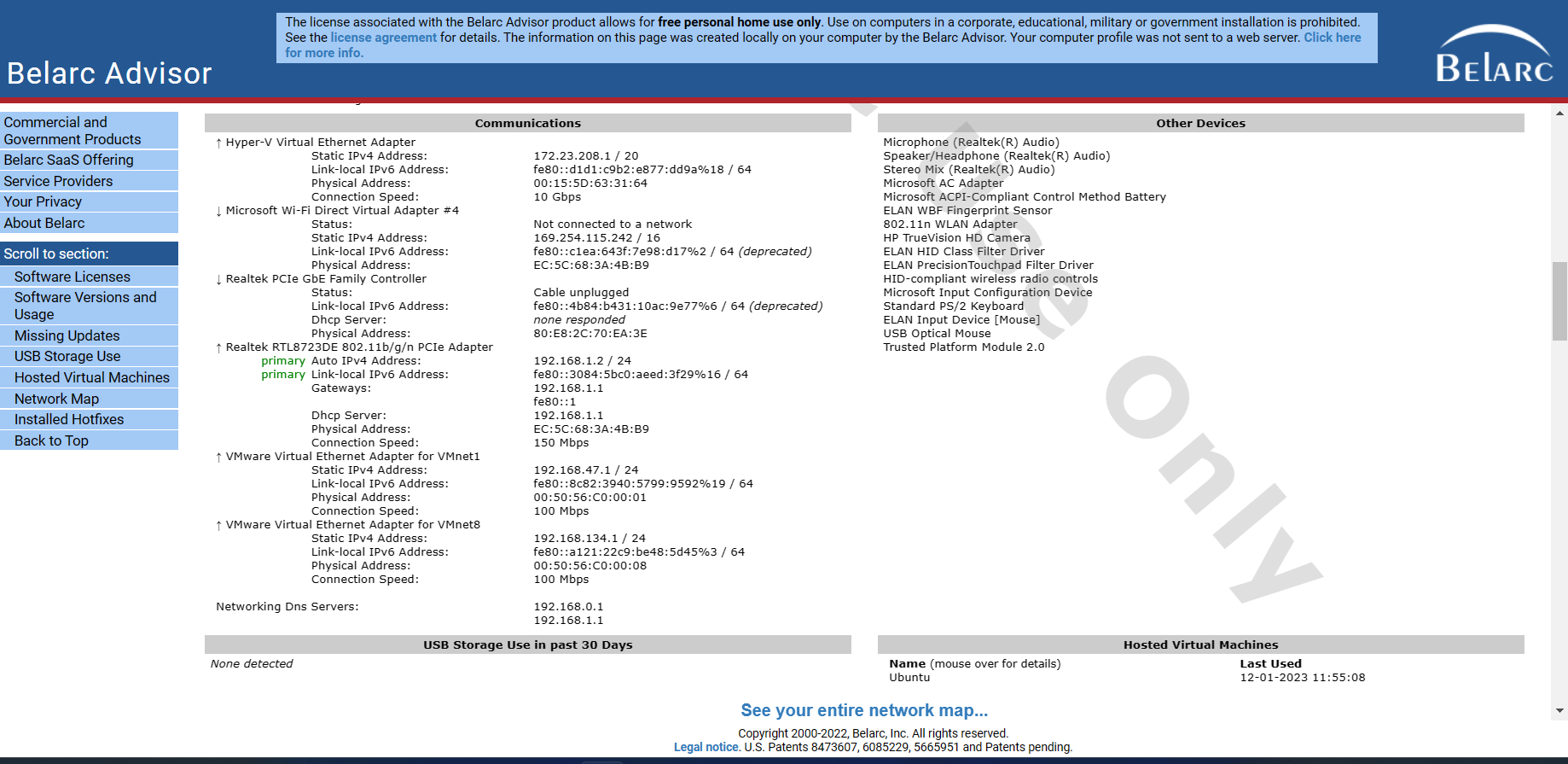
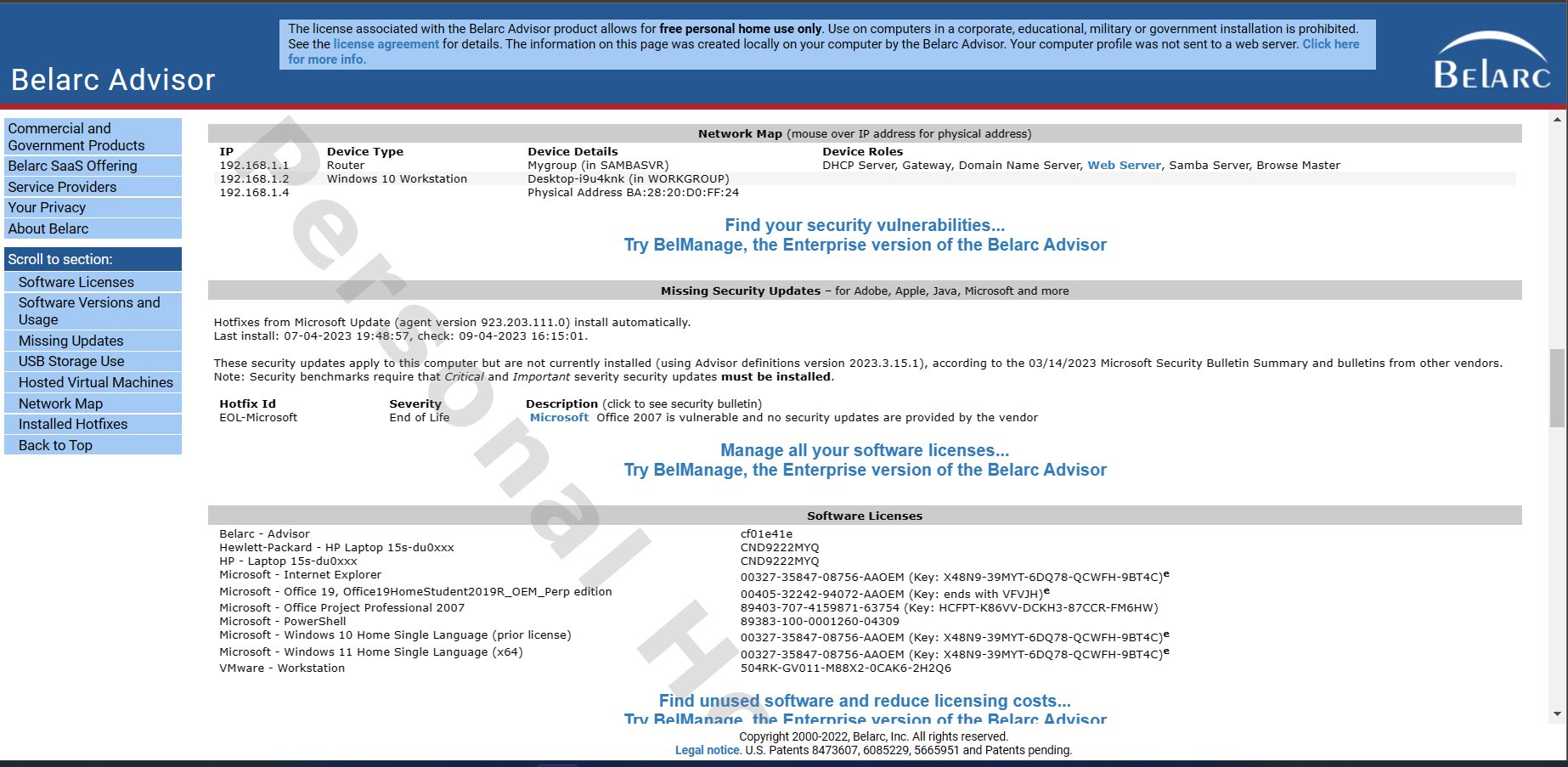
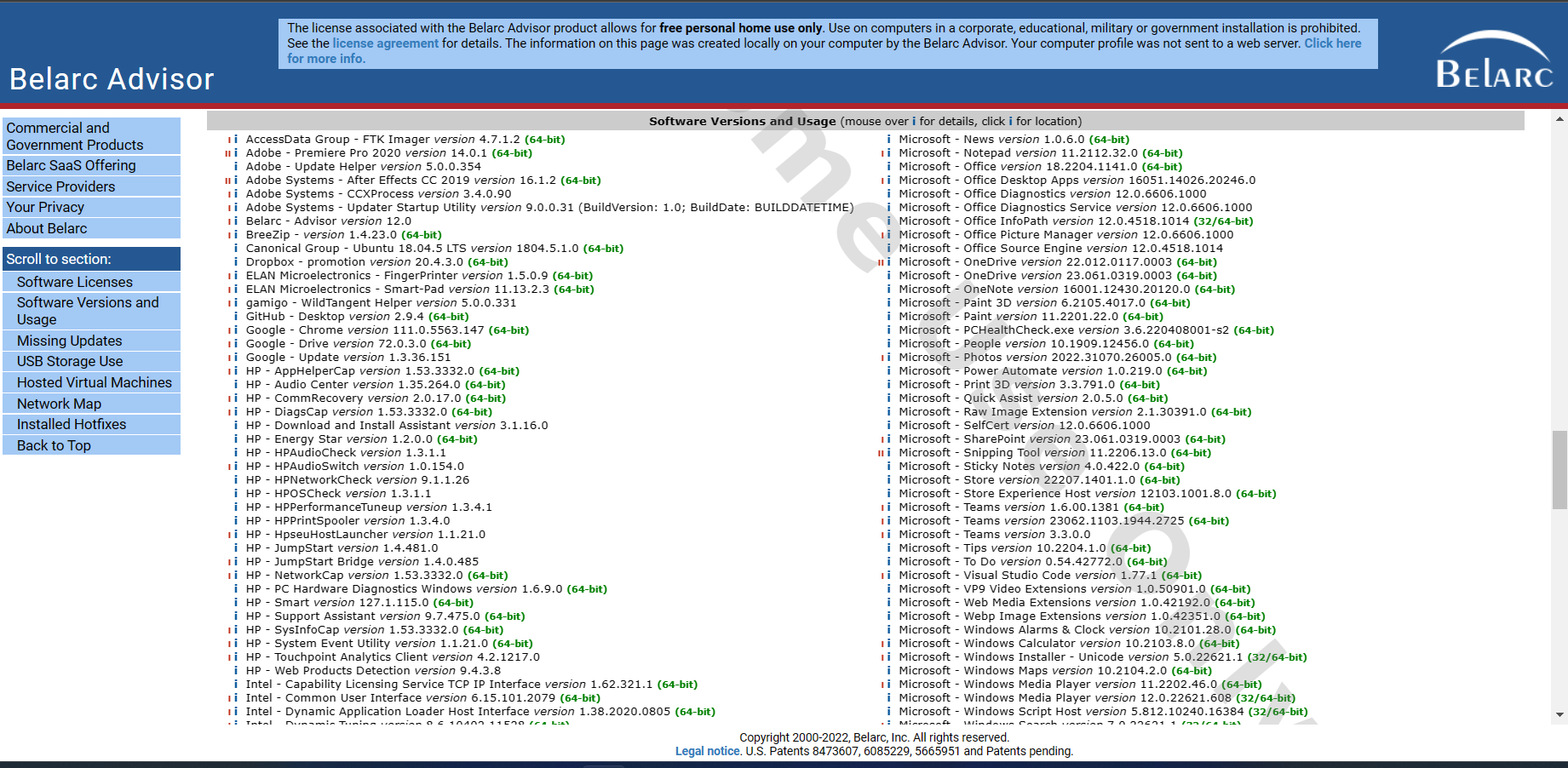
Performance issues: Security updates frequently include performance improvements and bug fixes that can boost the overall performance and stability of your computer. Installing these updates could prevent issues with system instability and decreased system performance.

Violations of regulatory requirements: To preserve compliance, many organisations and industries have regulations that demand the installation of security upgrades. If these updates are not installed, there may be fines or penalties for not complying with legal or regulatory requirements.

Regular Windows OS updates with the most recent security patches and fixes offered by Microsoft are essential to reducing these threats. Additionally, updating antivirus software might help shield your computer from malware and virus attacks.

* 1. **System snapshots and full analysis report**



1. **Reference/ Bibliography**

An in-depth system examination of the Windows operating system is provided to consumers through the software utility known as Belarc Advisor. It offers details on different characteristics of the system, such as hardware configuration, installed software, security patches, and other system specifics. In terms of security information, Belarc Advisor specifically offers:

a list of the security updates and patches that have been installed, along with a note about which updates are either missing or need to be installed.

a list of the installed firewall and antivirus programs, together with information about their versions and current states.

a review of user account settings, including the strength of the password and the implementation of two-factor authentication.

Information on the network configuration of the system, including network adapters, IP addresses, and open ports.

a brief description of the system's potential vulnerabilities and general security condition.

1. **GitHub Link**

**https://github.com/Prabhatpushp9**