As an inspiring cybersecurity professional, I sought to inform myself on some of the vulnerabilities I might have to combat in the future. The two most common among my research were remote code execution and privilege escalation attacks. I will explain these vulnerabilities and methods to combat against them.

"Remote code execution (RCE) is a type of security vulnerability that allows attackers to run arbitrary code on a remote machine, connecting to it over public or private networks. RCE is considered part of a broader group of vulnerabilities known as arbitrary code execution (ACE). RCE are possibly the most severe type of ACE, because they can be exploited even if an attacker has no prior access to the system or device. RCE vulnerabilities can have severe impacts on a system or application, including penetration where attackers can use RCE vulnerabilities as their first entry into a network or environment, then comes privilege escalation in many cases, because servers have internal vulnerabilities which can only be seen by those with inside access. RCE allows an attacker to discover and exploit these vulnerabilities, escalating privileges and gaining access to connected systems. There are various means to combat this form of attack and some of these are sanitize inputs to ensure the validity of the user, manage memory securely to prevent buffer attacks, inspect traffic to secure network traffic, and control access to prevent attacker access. ("Remote Code Execution (RCE) | Types, Examples & Mitigation | Imperva")".

"Generally, just like the cyber-attacks, privilege escalation exploits the system and process vulnerabilities in the networks, services, and applications. As such, it is possible to prevent them by deploying a combination of good security practices and tools. An organization should ideally deploy solutions that can scan, detect, and prevent a wide range of potential and existing security vulnerabilities and threats. In addition to deploying a real-time security solution, it is essential to regularly scan all the components of the IT infrastructure for vulnerabilities that could allow new threats to penetrate. Towards this, you can use an effective vulnerability scanner to find unpatched and insecure operating systems and applications, misconfigurations, weak passwords, and other flaws that attackers can exploit. It is also important to manage the privileged accounts and ensure that they are all secure, used according to the best practices, and not exposed. The security teams need to have an inventory of all the accounts, where they exist, and what they are used for. Practices to protect these privileged accounts include minimizing the number and scope of the privileged accounts, monitoring, and keeping a log of their activities, analyzing each privileged user or account to identify and address any risks, potential threats, sources, and attacker's intents, use major attack modes and prevention measures, follow the least privilege principle, and prevent admins from sharing accounts and credentials (Kingatua, 2020)."

Some external tools that businesses can use to combat these vulnerabilities are Heimdal, JumpCloud, Ping Identity, Foxpass, AWS Secret Manager, Exabeam, Cynet 360, Password Auditor, Password Manager Pro, Invicti, and Acunetix (Kingatua, 2020). Windows also provides some tools and configurations that the users can implement to fight these vulnerabilities within the system. These include Windows Defender SmartScreen, Credential Guard, Enterprise certification pinning, Device Guard, Microsoft Defender Antivirus, Memory protections, UEFI Secure Boot, Blocking of untrusted fonts, Early Launch Antimalware, and Device Health Attestation (Dansimp, 2023).

The two most executed security vulnerabilities are remote code execution and privilege escalation. The research conducted better informed me the severity of these vulnerabilities and methods/tools to utilize against them. This is knowledge that I can use later in my professional career to ensure that my employer is getting the most comprehensive cybersecurity strategy possible.

Work Cited

Dansimp. “Mitigate Threats by Using Windows 10 Security Features (Windows 10) - Windows Security.” *Learn.microsoft.com*, 8 Mar. 2023, learn.microsoft.com/en-us/windows/security/threat-protection/overview-of-threat-mitigations-in-windows-10.

Kingatua, Amos. “Privilege Escalation Attacks, Prevention Techniques and Tools.” *Geekflare*, 17 Nov. 2020, geekflare.com/privilege-escalation-attacks/. Accessed 17 Apr. 2023.

“Remote Code Execution (RCE) | Types, Examples & Mitigation | Imperva.” *Learning Center*, www.imperva.com/learn/application-security/remote-code-execution/. Accessed 17 Apr. 2023.