Task 3

1. Viruses and Malware
Malware and viruses are capable of destroying files, leaking personal data, and interrupting operational functions of a system. Against such threats, Windows has used Windows Defender for real-time protection, while MacOS uses Gatekeeper and XProtect. In Linux, antivirus software can be installed like ClamAV. Hence, built-in OS features and external tools both play an important role in preventing malware infection.

2. Software Vulnerability Exploitation
Software vulnerabilities provide avenues through which attackers may gain unauthorized access and run arbitrary malicious code. Windows and MacOS fix this through regular updates via Windows Update and the App Store respectively. Most Linux distributions are also regularly updated through package managers. OS and independent third-party vulnerability management and updates are crucial in the maintenance of security.

3. Phishing and Social Engineering
It can also be used to steal identities and bring financial losses by convincing users to disclose personal information. Windows does have email filtering and SmartScreen, and MacOS does have anti-phishing in Safari. Linux users should remain very careful and make use of email filters. Built-in OS features and third-party tools also help minimize the chances of a phishing attack.

4. Drive-by Downloads
This would be a danger that will automatically install malware in just mere visits to compromised websites. For Windows users, this could be prevented because it blocks suspicious downloads. MacOS accomplishes this through warning users via Safari. Linux users may disable automatic download by using script-blocking utilities. OS features and browser extensions alike are very much important and crucial for protection against this threat.

5. Zero-Day Exploits
Zero-day exploits are those that attack unknown vulnerabilities. Because of this, malicious code may be easily executed before a patch is made available. Windows deploys advanced threat protection tools, while MacOS uses System Integrity Protection. Linux users should ensure operating systems are current and utilize various security tools like Apparmor. Native security mechanisms in combination with external control toools play an important role in mitigation against these threats.

6. USB/Removable Media Attacks
Also, it causes unauthorized access by malwarei nfected USB devices. For Windows users, one can disable autorun features and scan USBs with Defender. MacOS automatically checks USB drives for malware, while on Linux, one can disable auto-mounting. The OS has given specific options for USB security reinforcement; also ,enhancing the protection can be done with the help of external antivirus tools.

7. Password Cracking

Poor passwords can easily give rise to unauthorized access and breaches. Windows enforces password policies and provides BitLocker for encryption. MacOS enables FileVault to promote strong passwords. Linux users can impose complexity requirements on passwords by using PAM. The inbuilt password management features and the external password managers do assist in strengthening this feature.