Notes on Website Penetration Tests/Ethical Hacking, specifically addressing what I further researched outside of the provided Capstone:

> Website penetration tests, they're used to identify vulnerabilities in web applications and their underlying infrastructure. Ethical hacking, mostly involves using the same techniques and tools as malicious hackers to identify vulnerabilities in a system and improve its security

Port Scanners:

- Port scanners, these are used to identify open ports and services on a target system

- Some relevant tools are NmapG, Zenmap, and SuperScan.

Vulnerability Scanners:

- Vulnerability scanners, these are used to identify known vulnerabilities in a target system

- Some relevant tools are Nessus, OpenVAS, and Qualys

Web Application Scanners:

- Web applications, these scanners are used to identify vulnerabilities in web applications.

- Some relevant tools are Burp Suite, OWASP ZAP, and Acunetix.

Password Cracking Tools:

- Password cracking tools, these are used to recover lost or forgotten passwords.

- Some relevant tools are John the Ripper, Hashcat, and Cain and Abel.

Exploitation Frameworks:

- Exploitation frameworks, these are used to automate the exploitation of identified vulnerabilities.

- Some relevant examples are Metasploit, Empire, and Cobalt Strike.

Network Sniffers and Protocol Analyzers:

- Network sniffers and protocol analyzers, mostly used to capture and analyze network traffic.

- Some relevant tools are Wireshark, tcpdump, and Fiddler.

These are some of the top software tools used by website penetration testers and ethical hackers to identify vulnerabilities in systems and improve their security. By learning about and mastering these tools, professionals in the field of cybersecurity can better secure their organization's network and assets.