CT437 – Student Project Guidelines, Topics and Marking Scheme Outline

In this project (worth 25%) you will explore one or more open-source ethical hacking / penetration testing / security tools used in industry. You can work, depending on your preferences, either alone or in a group of two or three. Generally, the number of topics you'll cover is linked to your group size, with one topic per student. For example, a team of 3 would work on 3 topics as a group, with 2 deliverables per topic, as follows:

1. A comprehensive PowerPoint presentation (> 20 slides) that includes a background section related to the specific tool, a tool description, a summary of your tool installation / deployment, and a critical reflection on both your findings (i.e. experimental results) and the relevance / importance of the tool.
   The presentation must also state which team member contributed what.
2. A 10 - 15 minutes project tool demo (pre-recorded with voice overlay).
   Please note that for your demo you must only attack your own infrastructure (e.g. Wifi hotspot or webserver). Docker container or virtual machines make great targets.
   Large deliverables (i.e. videos) that cannot be uploaded to Blackboard can be submitted via Dropbox or OneDrive link.

Most if not all of the suggested tools are part of the Kali-Linux distribution, which you should download and run in a virtual machine on your own computer. Also, please let me know if you'd like to work on a different topic (option #16 in the table). Note that some tools are more complex than others, so please let me know if you have any question about the scope and depth. While there are plenty of "training" videos on the web, I'd expect you to engage with and critically reflect on your chosen topic(s), i.e. showing a high level of understanding / domain expertise, both of which being reflected in your presentation and demo.
Note that in many ICT job interviews you are asked security-related questions, so being able to talk proficiently about your project with confidence would help you to pass that hurdle!

In order to get a bit of diversity, I'd like you to send me by email your top 10 choices based on the following list, as well as the names of your team members, by Wednesday March 10th 2021:

#	Title	Outline
1	Rogue APs using **EvilAp**	Focus on rogue access points in general and inner workings of EvilAp
2	**Tor** and anonymous pen testing	Focus on Dark Web and Tor architecture / Tor clients
3	The **Samurai Web Testing Framework**	Tool features and usage, hereby outlining / exercising a complete attack cycle (reconnaissance, mapping, discovery, exploitation)
4	Pentesting with the **Social Engineering Toolkit**	Focus on tool capabilities and underlying attack vectors
5	Port scanning with **nmap / Unicornscan**	Focus on port scanning concepts and nmap / Unicornscan features
6	Webserver scanning with **Nikto**	Focus on web server vulnerabilities and Nikto features
7	The **Metasploit Framework**	Summary of the Metasploit framework, showcasing selected modules

8	Browser Exploitation with **BeEF**	Focus on browser exploitation concepts; introduction BeEF
9	Vulnerability scanning with **OpenVas**	Vulnerability scanning and OpenVas features
10	Wifi Analysis / Wardriving using **Kismet Wireless**	Focus on WiFi, WiFi analysis/user activity monitoring, wardriving and Kismet
11	Password Cracking in Practice	Focus on modern password cracking concepts and tools, i.e. **John the Ripper**, **thc-hydra** and **RainbowCrack**
12	Exploiting SQL injection flaws with **sqlmap**	SQL injection attacks, and supporting tools e.g. sqlmap
13	Web Application Scanning with **Skipfish**	PPT and report on web scanning concepts and Skipfish tool
14	Network Intrusion Detection with **Snort**	Focus on network intrusion, detection techniques and Snort features / architecture
15	Security auditing with **Lynis**	Security auditing and Lynis features
16	Your suggestion	Please provide me with details.