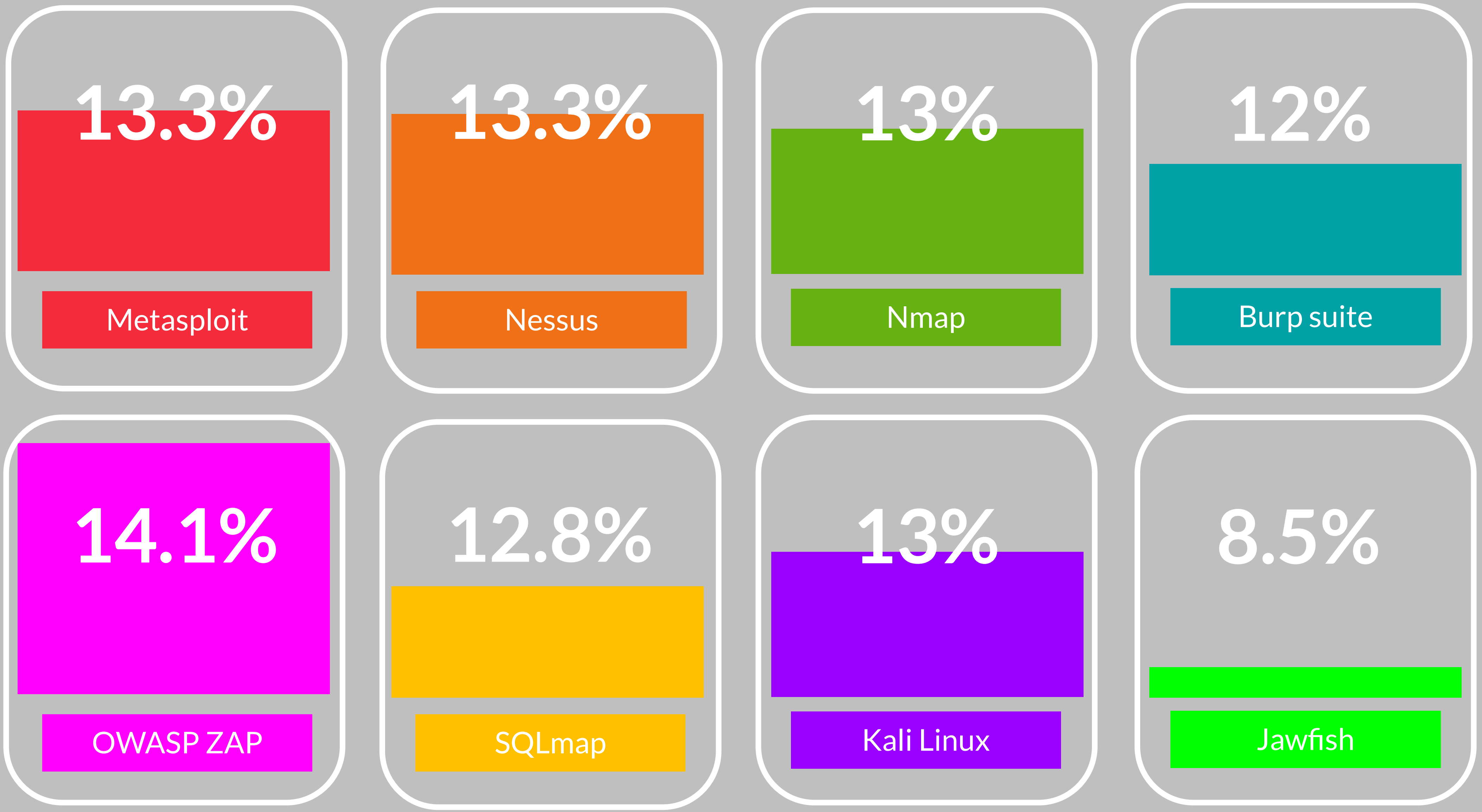
Group 3 Seminar 3: Unit 6 Evaluation exercise

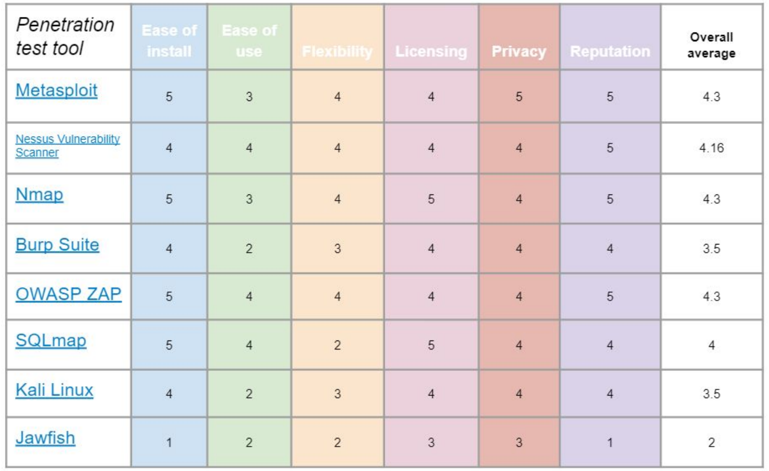
Jonathan, Ying & Haseeb

Friday 17th December 2021

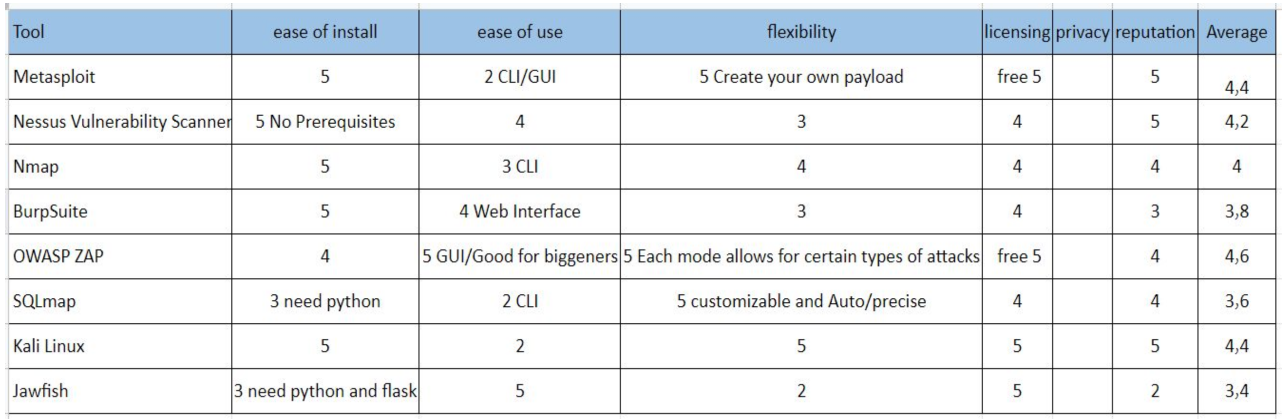
Overall evaluation



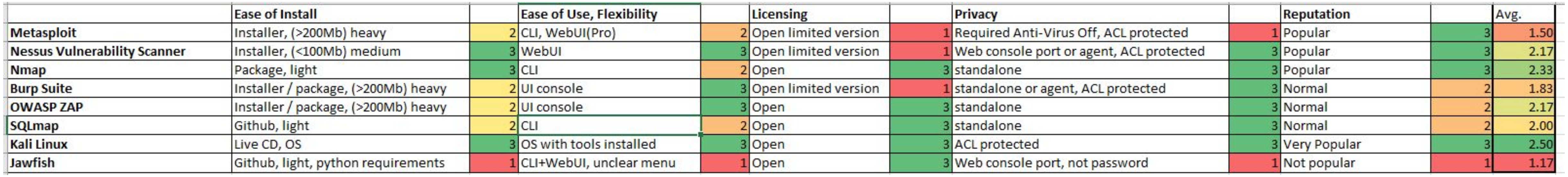
Group findings: How we got there…



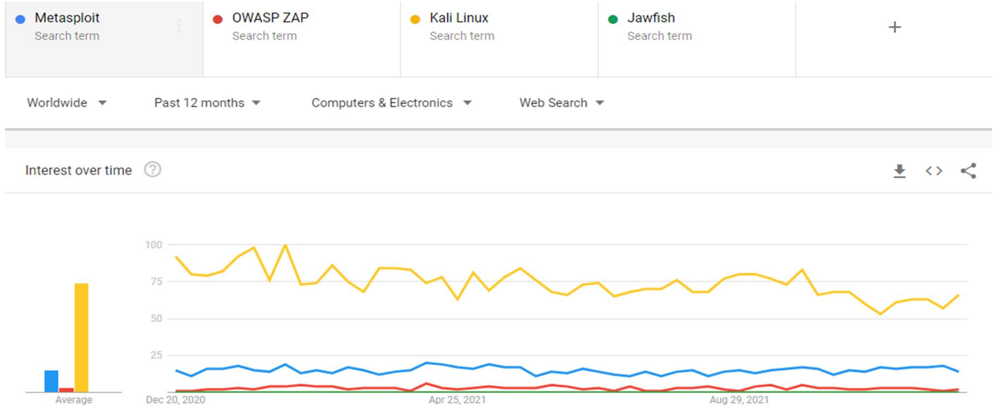
Penetration test tool	Ease of install	Ease of use	Flexibility	Licensing	Privacy	Reputation	Overall average
Metasploit	5	3	4	4	5	5	4.3
Nessus Vulnerability Scanner	4	4	4	4	4	5	4.16
Nmap	5	3	4	5	4	5	4.3
Burp Suite	4	2	3	4	4	4	3.5
OWASP ZAP	5	4	4	4	4	5	4.3
SQLmap	5	4	2	5	4	4	4
Kali Linux	4	2	3	4	4	4	3.5
Jawfish	1	2	2	3	3	1	2

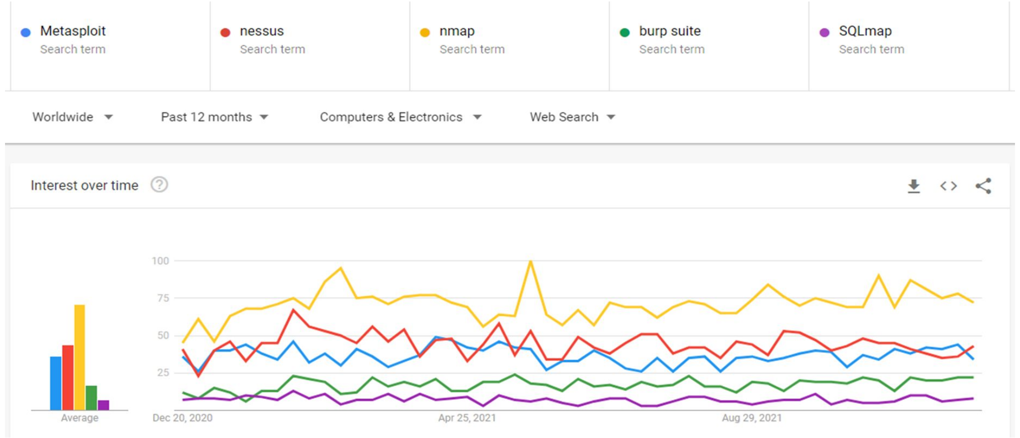


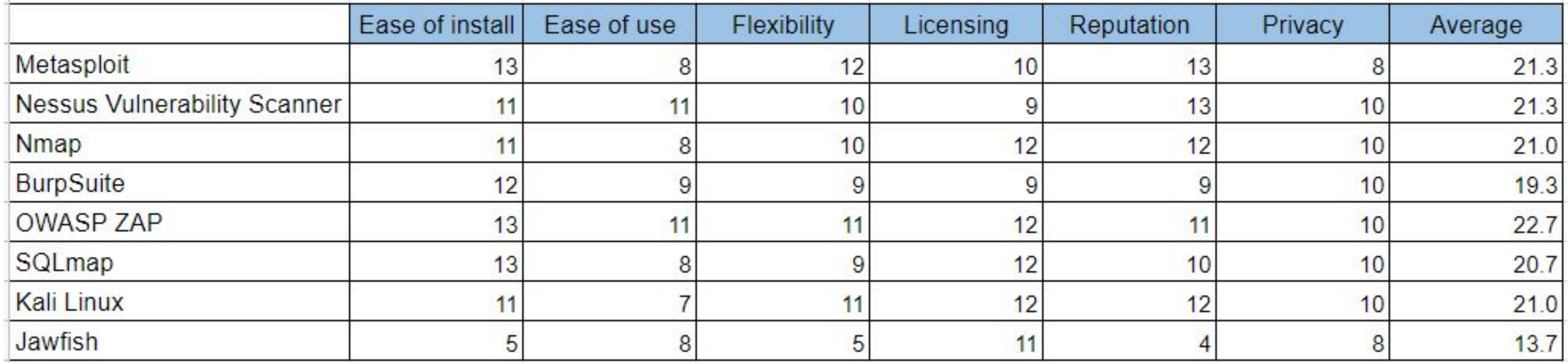
Tool	ease of install	ease of use	flexibility	licensing	privacy	reputation	Average
Metasploit	5	2 CLI/GUI	5 Create your own payload	free 5		5	4,4
Nessus Vulnerability Scanner	5 No Prerequisites	4	3	4		5	4,2
Nmap	5	3 CLI	4	4		4	4
BurpSuite	5	4 Web Interface	3	4		3	3,8
OWASP ZAP	4	5 GUI/Good for biggeners	5 Each mode allows for certain types of attacks	free 5		4	4,6
SQLmap	3 need python	2 CLI	5 customizable and Auto/precise	4		4	3,6
Kali Linux	5	2	5	5		5	4,4
Jawfish	3 need python and flask	5	2	5		2	3,4



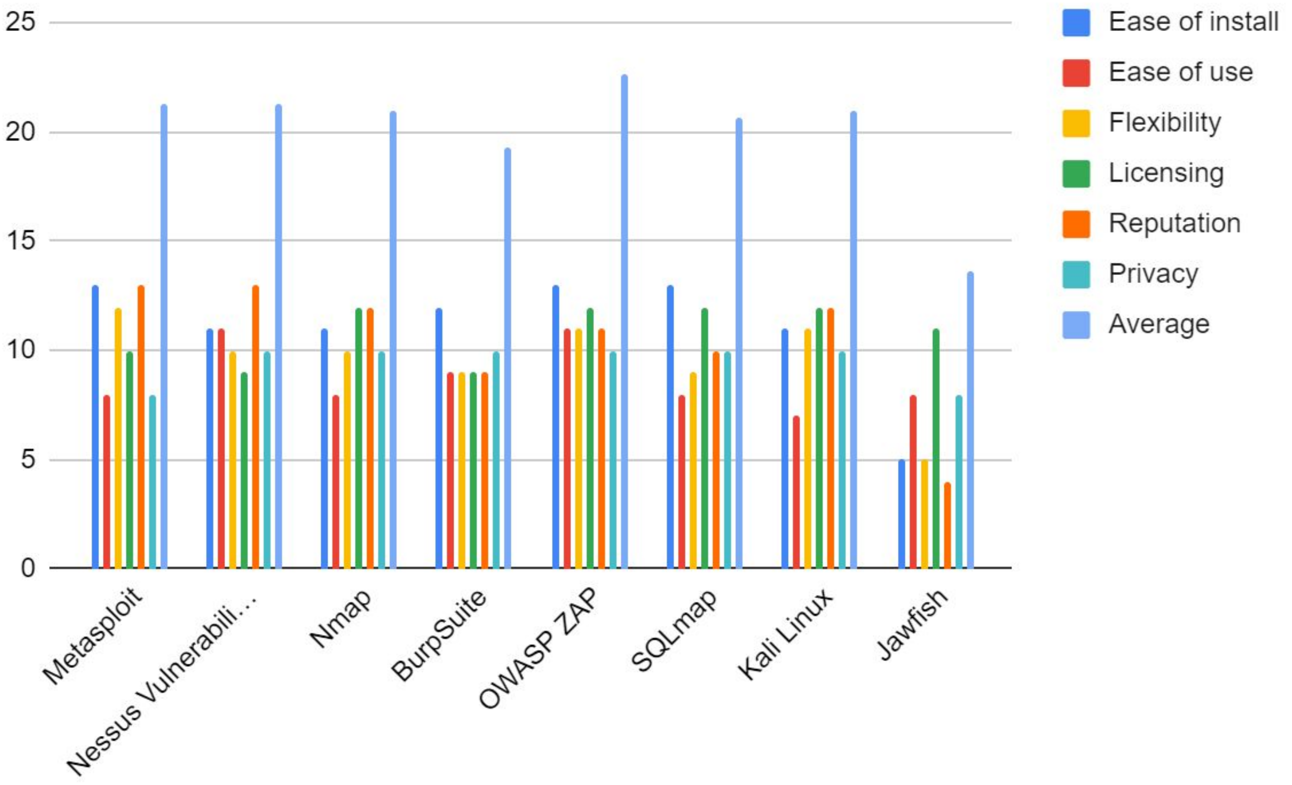
	Ease of Install		Ease of Use, Flexibility		Licensing		Privacy		Reputation		Avg.
Metasploit	Installer, (>200Mb) heavy	2	CLI, WebUI(Pro)	2	Open limited version	1	Required Anti-Virus Off, ACL protected	1	Popular	3	1.50
Nessus Vulnerability Scanner	Installer, (<100Mb) medium	3	WebUI	3	Open limited version	1	Web console port or agent, ACL protected	3	Popular	3	2.17
Nmap	Package, light	3	CLI	2	Open	3	standalone	3	Popular	3	2.33
Burp Suite	Installer / package, (>200Mb) heavy	2	UI console	3	Open limited version	1	standalone or agent, ACL protected	3	Normal	2	1.83
OWASP ZAP	Installer / package, (>200Mb) heavy	2	UI console	3	Open	3	standalone	3	Normal	2	2.17
SQLmap	Github, light	2	CLI	2	Open	3	standalone	3	Normal	2	2.00
Kali Linux	Live CD, OS	3	OS with tools installed	3	Open	3	ACL protected	3	Very Popular	3	2.50
Jawfish	Github, light, python requirements	1	CLI+WebUI, unclear menu	1	Open	3	Web console port, not password	1	Not popular	1	1.17

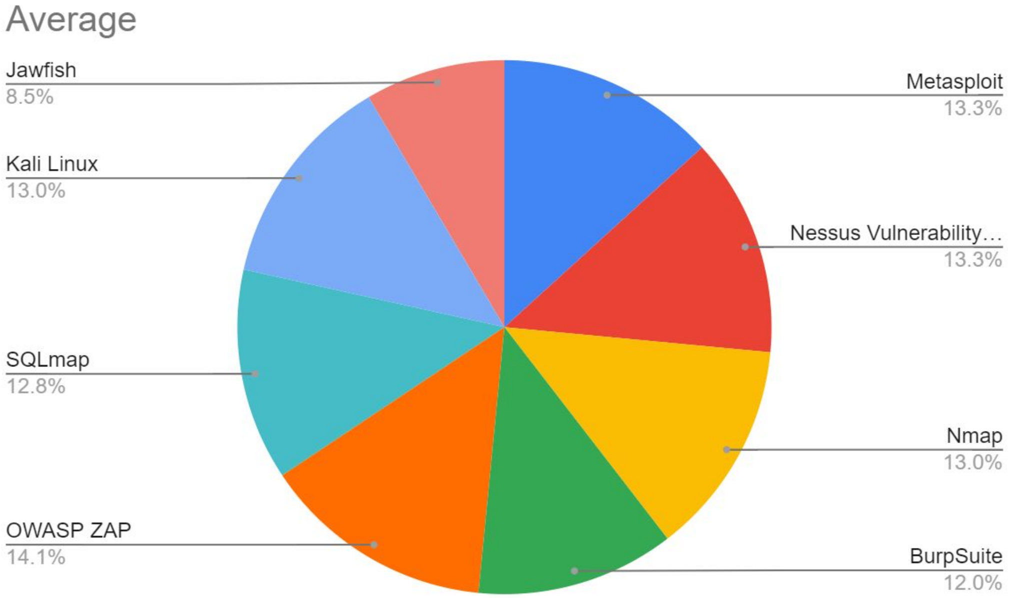






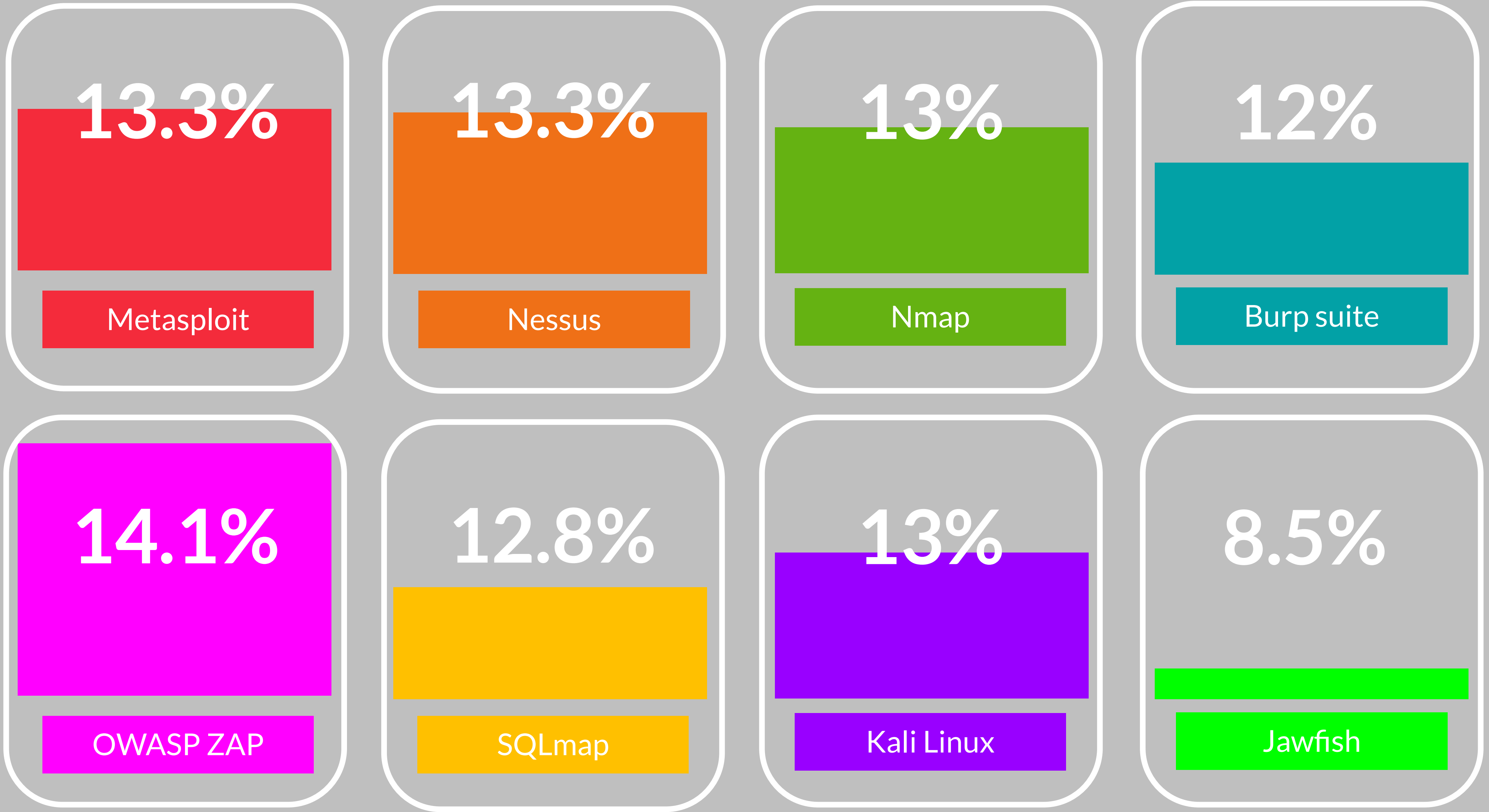
	Ease of install	Ease of use	Flexibility	Licensing	Reputation	Privacy	Average
Metasploit	13	8	12	10	13	8	21.3
Nessus Vulnerability Scanner	11	11	10	9	13	10	21.3
Nmap	11	8	10	12	12	10	21.0
BurpSuite	12	9	9	9	9	10	19.3
OWASP ZAP	13	11	11	12	11	10	22.7
SQLmap	13	8	9	12	10	10	20.7
Kali Linux	11	7	11	12	12	10	21.0
Jawfish	5	8	5	11	4	8	13.7





Penetration test tool	**Advantages**	**Disadvantages**
Metasploit Popularity: ●●●●○	GUI environment, Easy install, Community edition is free Pro edition, Open source, Wide range of applications Listeners, Reliable, Use any language and platform Cleaner exits, CLI, Create your own payload	Can be challenging to learn to use but there are training course and an exam certification can be taken Knowledge of Ruby, GUI has limitations and CLI driven Can crash if not used safely, Antivirus can affect the use, installer/ package >200mb heavy. Techniques needed before using tools.
Nessus Vulnerability Scanner ●●●●○	Compares scans to known standards High success rate in accuracy, Free and paid version, Speed Training available, No prerequisites, installer/ package <100mb medium. Continuous scanning for your network and up to date.	Pro version is a yearly fee Cannot use with a Host based Intrusion Prevention System Training costs
Nmap ●●●●○	Open source, Many features for networking, Easy setup GUI and CLI, light	Give clear directions of scans will be time consuming Some platforms not all features Exporting information is not always that presentable Takes learning
Burp Suite ●●●○○	Can perform many scans, web interface Offers variability Cheaper price options	Takes time to learn, Time consuming GUI could be improved, installer/ package >200mb heavy Limited update compared to ZAP
OWASP ZAP ●●●○○	Beginners as well as more advanced users, GUI Open source, Automated and manual testing, Cross platform	Report output, installer/ package >200mb heavy
SQLmap ●●●○○	Database, Cost, Automates, Customizable, CLI, light, easy to use	GUI, Need python
Kali Linux ●●●●○	Languages supported, Customise, Cost, Powerful separate OS	Speed, Knowledge is required for use, Live CD, OS
Jawfish ●○○○○	Light, simplistic	Could not access the site, Had to search Github, Need python and flask, basic options, difficult to learn - lack of resources

Overall evaluation



Concluding remarks

1. Team expertise

2. Budget

3. Time management

4. Accuracy

5. Infrastructure

6. Features