**Seminar 3- Notes**

**Metasploit**

* Ease of use
  + Metasploit has vast capabilities:
    - Discovery
    - Exploitation and payload delivery
    - Social Engineering and more
  + As a result there is much to be learnt about how to use the tool.
* Flexibility
  + As previously mentioned the tool has a host of different capabilities, it is a collection of tools within a tool.
* Licensing
  + There are two versions of Metasploit one is Open Sourced and the other is a commercial version of the product with support.
  + The Pro version provides a user interface where the community edition is a framework which is controlled via command line.
* Privacy
  + Metasploit can be very noisy and a penetration tester would need additional knowledge to cover their tracks.

**Nessus**

* Ease of use
  + Nessus provides an easy to use GUI which allows the user to add a new target host to the scan list. Additionally the interface provides a reporting section where you can evaluate the outcome of the scan on the system.
* Flexibility
  + Nessus is targeted at discovery of vulnerabilities and in some ways is similar to Nmap.
* Licensing
  + Nessus has various three tiers which grant access to additional features for each tier. The free version provides limited functionality and is purley a taste of what the purchased product would provide.
* Privacy
  + Nessus performs SYN which protect the scanner, a SYN scan sends a reset packet instead of an ACK which signals to the target host that there has been a connection error.

**Kali**

* Easy of use
  + This varies as the tool contains a variety of other tools, some are command line others have GUIs
* Flexibility
  + Kali has the majority of the well known tools in the industry, the distro was developed in an attempt to bundle these tools rather than needing to install 100’s of tools manually.
* Licensing
  + Impossible to rate here as there are 100’s of tools that range in their licensing terms and conditions. Most if not all of the tools are open sourced.
* Privacy
  + Privacy would vary on the penetration tester and their ability to clean up after they have performed scans.
* Reputation
  + Kali is the most widely used Linux Distro and is used by script kiddies and professionals a-like

**Nmap**

* Ease of Use
  + Nmap is a command line tool with a a GUI version called ZenMAP. However even within the GUI interface the tester needs an understanding of the commands used to drive NMAP
* Flexibility
  + Nmap is one of the most flexible tools in industry. It is natively designed to do network and service discovery however due to the NMAP scripting engine it can perform a variety of vulnerability scans and penetration tasks.
* Licensing
  + Nmap is fully open sourced and can be modified by anyone to achieve specific results.
* Privacy
  + Again this depends on the tester and their ability to use SYN scanning or other techniques to cover up their identity.
* Reputation
  + Nmap is the most widely used network discovery tool.