**Module 2 Technologies & Tools**

**2.2 Security Tools**

**Protocol Analysers**

* AKA Packet Sniffers
* Gathering packet level information on network
* Eg. Wireshark, TCPDump

**Network Scanners/Mappers**

* Knowing what’s on your network
* Network enumeration
* Eg. Solarwinds, Nmap, Zenmap, Fing (IOS & Android)

**Vulnerability Scanners**

* Software utility that scans range of IP addresses & tests for presence of known vulnerabilities in software configuration & accessible services
* Relies upon database of known vulnerabilities
* Examples

1. Nessus (Tenable)
2. OpenVAS (Linux)
3. Nexpose Community Edition – scan web apps, databases & virtual environments
4. Qualys FreeScan – checks for hidden malware & SSL issues among other network vulnerability

**OWASP ZAP (Zed Application Proxy)**

* Discovers security vulnerabilities in web apps

**Exploitation Frameworks**

* Platforms used for penetration testing & risk assessments
* Frameworks contains set of exploits for known vulnerabilities
* Eg. Metasploit, Canvas & Core Impact
* Browser Exploitation Framework (BeEF) – pen testing tool for exploiting web vulnerabilities

**Kali Linux**

* Debian-derived Linux distribution, designed for digital forensics & penetration testing
* Preinstalled with numerous penetration testing programs
* Can be run from hard disk, live CD or live USB
* Supported platform of Metasploit Project’s Metasploit Framework, a tool for developing & executing security exploits
* Eg. Social Engineering Toolkit (SET), Metasploit

**Wireless Scanners**

* Gather information about Wi-Fi networks
* Detect access points (rogue/valid)
* Break encryption keys
* Eg. Aerodump, Kismet/KisMAC, Netstumbler, Vistumber, insider

**Configuration Compliance**

* Microsoft Baseline Security Analyser (MBSA) – software vulnerability scanner to analyse targeted Microsoft systems, to detect whether software security patches/baseline configuration settings are missing
* Centre for Internet Security (CIS)
* Nessus (Vulnerability scanning)

**Banner Grabbing**

* Technique to identify OS, apps & services on system
* Narrows vulnerability searches
* Netcat

1. Free download for Windows & Linux
2. Read & write TCP & UDP network connections
3. Run from command line

**Password Crackers**

* Used to disclose passwords & access password strength
* Online password-cracking tools enable you to type in hash & get password in plain text
* Eg. Brutus, Cain & Able, John the Ripper, THC Hydra

**Honeypots/Honeynets**

* Use

1. Systems/networks exposed to capture malicious activity
2. Gather information evidence
3. Study attack strategies

* Separated from business networks

**Steganography**

* Means “hidden writing” – hiding messages, often in other media so unintended recipients not aware of any messages
* Approaches

1. Least significant bit insertion
2. Masking & filtering
3. Algorithms & transformations

* Common steganography tools include – OpenPuff, Camouflage, Steghide, rSteg

**Data Sanitisation Tools**

* Sanitisation – process of removing contents from device/media
* Eg. DBAN, BCWipe, Cryptographic Erase (CE)

**Command Line Tools**

* man
* ping
* netstat
* tracert
* nslookup/dig
* arp
* ipconfig/ip/ifconfig
* tcpdump
* nmap
* netcat
* SysInternals Suite (contains troubleshooting tools