Tool	Purpose	Strengths	Limitations
Nmap	Nmap is used to find live host in the network and to perform port scanning , ping sweep, OS Detection and version detection	You can perform any networking related task for a target or set of targets	SYN scans can be particularly aggressive and cause problems on remote systems.
Metasploit	It is a kali Linux pentesting tool. It helps us to find, exploit and validate Vulnerabilities. It provides the infrastructure, content, and tools to perform penetration tests and extensive security auditing	1. Open source 2. Easy to deploy user specific payloads	1. Can crash system if not used wisely 2. Lesser GUI Based Support
Wireshark	It is a free open source packet analyzer.t is used for network troubleshooting, analysis, software and communications protocol development,Wireshark intercepts traffic and converts that binary traffic into human-readable format. This makes it easy to identify what traffic is crossing your network, how much of it, how frequently, how much latency there is between certain hops, and so forth.	1. Captures all kind of traffic in the network 2. Deep Packet Inspection 3. Various Filters are there which make the analysis more easy and convenient	1. Can't modify or manipulate things/data on the network
Burpsuite	Burp Suite is one of the best web application penetration testing tools. It is widely used in security field. It is a product of portswigger. Burp Collaborator technology allows Burp to detect server-side vulnerabilities that are completely invisible in the application external behavior, and even to report vulnerabilities that are triggered asynchronously after scanning has completed.	1. Various Payloads are there which make testing more easy 2. Wider Scope is there for Pen Testing	1. It take more time to carry out few operations 2. Paid Version is quite costly

HashCat	It is a password recovery tool which supports five unique modes of attack for over 200 highly-optimized hashing algorithms. It currently support CPUs, GPUs, and other hardware accelerators on Linux, Windows and has facilities to help enable distributed password cracking.	1.Can exploit WPA2 vulnerabilities 2.Can be highly useful to digital forensic analysts and used for positive	1. Requires more RAM and computing power
Nessus	Nessus is one of the many vulnerability scanners used during vulnerability assessments and penetration testing engagements, including malicious attacks. This article will focus on this vulnerability scanner, discussing the fundamentals that one needs to have before getting started with the tool, the different scanning capabilities that it provides, what it takes to run the tool and how results appear once scans are complete.	1. Easy to List out blackhole in the organizations infrastructure 2. Easy and flexible reporting which we can customize in our way.	1. Integration with other tools is difficult 2. Sometimes scan takes a lot of time to complete
Hydra	Hydra is a brute forcing tool mostly used in field of pentesting .It is able attack multiple network protocols such as ssh,ftp,etc It is quite easy to use that you can use users list as text file (a parameter) and also password as a text file (a parameter) and hydra will brute force with username and password supplied to it .An example is " hydra -L username.txt -P password.txt 192.168.2.1 ssh"	1.Easy to Perform Brute Force Attack	1. Can be easily detected by IDS
DirBuster	It is a Java Application (Multi -Threaded) which is useful to bruteforce the directories anf files on web application. It Attempts to discover the hidden page/directorie and directories with a web application, thus giving another attack vector (For example. Finding an unlinked to admin page).	1.Multi Threading functionality 2.	1. Noisy tool , will generate a lot of logs

PowerShell	• PowerShell offers a multitude of offensive advantages, including full .NET access, application whitelisting, direct access to the Win32 API, the ability to assemble malicious binaries in memory, and a default installation on Windows	**PowerShell Empire** is a post-exploitation framework for computers and servers running Microsoft Windows, Windows Server operating systems, or both	its convenient interface will ease the task of manipulating the OS after the attacker gained access.