

TOOLS REQUIRED FOR PENTESTING

Reconnaissance and Information Gathering:

- Nmap
- theHarvester
- Recon-ng
- Shodan
- Maltego

Scanning and Enumeration:

- Nessus
- OpenVAS
- Nikto
- Dirb/Dirbuster
- Burp Suite

Vulnerability Assessment:

- OpenVAS
- Nexpose
- Nessus
- QualysGuard

Exploitation and Post-Exploitation:

- Metasploit Framework
- Cobalt Strike
- Empire
- PowerShell Empire
- BeEF

Web Application Testing:

- Burp Suite
- OWASP ZAP
- Acunetix
- SQLMap
- Skipfish

Password Cracking:

- John the Ripper
- Hashcat
- Hydra

Wireless Network Testing:

- Aircrack-ng
- Kismet
- Reaver
- WiFite

Varshini Ramesh