Service	TCP Ports	UDP Ports	Known Vulnerabilities	Tools to Identify	Command Example	Attack Type	Resource Link
SMB	445	445	MS17-010 (EternalBlue), SMBGhost (CVE-2020-0796) (hackviser.com)	`nmap`, `enum4linux`, `smbmap`, `Metasploit`	`nmap -p445 --script=smb-vuln-ms17-010 <target>`	Ransomware, Trojan (e.g., WannaCry)	aw-junaid/Hacking-Tools (SMB modules)
NetBIOS	137,139	137, 138	Null sessions, info leakage	`nmap`, `rpcclient`, `enum4linux`	`rpcclient -U "" <ip>`	Information Theft, Lateral Movement	aw-junaid/Hacking-Tools (NetBIOS tools)
LDAP	389	389	LDAP injection, anonymous binds	`ldapsearch`, `nmap`	`ldapsearch -x -h <server>`	Data Exfiltration	aw-junaid/Hacking-Tools (LDAP tools)
LDAP over TLS	636	–	Same plus SSL misconfig	`ldapsearch`, `openssl s_client`	`openssl s_client -connect <server>:636`	Data Interception	aw-junaid/Hacking-Tools (TLS tools)
Global catalog LDAP	3268	–	Similar to LDAP exploits	`ldapsearch -p3268`	`ldapsearch -x -p3268 -h <srv>`	Data Theft	aw-junaid/Hacking-Tools (LDAP tools)
Kerberos	88,464…	88,464 …	Pass-the-ticket, brute	`kerberoast`, `impacket`, `kinit`	`GetUserSPNs.py -request -dc-ip`	Credential Theft, Lateral Movement	aw-junaid/Hacking-Tools (Kerberos tools)
NFS	111,2049…	same	Export misconfig, root squashing bypass	`showmount`, `nmap`, `rpcinfo`	`showmount -e <target>`	Data Theft, Ransomware prep	aw-junaid/Hacking-Tools (NFS tools)
RPC	111,135,530	same	MSRPC overflow	`rpcclient`, `Metasploit`	`use exploit/windows/smb/ms08_067_netapi`	RCE, Ransomware	aw-junaid/Hacking-Tools (RPC tools)

			s, MS08-067				
DHCP	67,68…	same	DHCP spoofing	dhcpdump, nmap --script broadcast-dhcp-discover	dhcpdump -i eth0	MITM	aw-junaid/Hacking-Tools (DHCP tools)
FTP	21	21	Plaintext creds, bounce	nmap, hydra, ftp	hydra -l user -P passlist ftp://<target>	Trojan, Info theft	aw-junaid/Hacking-Tools (FTP tools)
SSH	22	22	Weak keys, brute	nmap, hydra, sshguard	hydra -l root -P passlist ssh://<target>	Botnet, Backdoor	aw-junaid/Hacking-Tools (SSH tools)
RDP	3389	3389	BlueKeep, weak creds	nmap --script rdp-vuln-cve*, rdp-sec-check	nmap -p3389 --script rdp-vuln-cve2019-0708 <target>	Ransomware (WannaCry family)	aw-junaid/Hacking-Tools (RDP tools)
MongoDB	27017…	–	No auth defaults	mongo, nmap	mongo <ip>:27017	Data Theft	aw-junaid/Hacking-Tools (Mongo tools)
SQL Server	1433	1434	SQL injection, brute	nmap, sqsh, sqlcmd; hydra	nmap --script ms-sql-brute -p1433 <target>	Data theft, RCE	aw-junaid/Hacking-Tools (SQL Tools)
MySQL	3306	–	Brute, default creds	nmap, mysql, hydra	nmap --script mysql-brute -p3306 <target>	Data theft	aw-junaid/Hacking-Tools (MySQL tools)
PostgreSQL	5432	–	Same as MySQL	nmap, psql, hydra	nmap --script pgsql-brute -p5432 <target>	Data theft	aw-junaid/Hacking-Tools (PostgreSQL tools)
Oracle	1521, 1630	–	SQL injection, weak creds	nmap, sqlplus, hydra	nmap --script oracle-brute -p1521 <tg>	Data theft	aw-junaid/Hacking-Tools (Oracle tools)
Elasticsearch	9200, 9300	–	CVE-2015/3337, open access	curl, nmap, elasticsearch-repo-script	curl http://<ip>:9200/_search?pretty	Data theft, Crypto/miner	aw-junaid/Hacking-Tools (ELK tools)
HTTP/ HTTPS	80/8080,443	same	XSS, SQLI, MITM	nmap, nikto, Burp, ZAP, ffuf	ffuf -u http://<tg>/FUZZ -w dict.txt	Trojan, Data theft	aw-junaid/Hacking-Tools (Web tools)