Enumeration/Footprinting – Enumeration, Tools and Commands

Service	Enumeration Checklist	Tools
FTP *{TCP 21}*	FTP_Version Auth Scanner (BForce – MSF ftp_login) Anonymous Access	MSF NMAP
SMB *{TCP 445}*	SMB Version User Enum Shares Enum Login Check Scanner (BForce – MSF smb_login) psexec.py *{Username@IP} {Command}*	MSF NMAP nmblookup smbclient smbmap rpcclient PsExec enum4linux
Webserver/HTTP *{TCP 80}*	HTTP_Version **|** HTTP_Header **|** HTTP_Put Dir_Scanner **|** Brute_dirs **|** dir_listing Robots file apache_userdir_enum File Scanner (MSF files_dir) Login Scanner (BForce – MSF http_login)	MSF
MySQL *{TCP 3306}*	Mysql_version Mysql_enum **|** Mysql_sql **|** mysql_schemadump mysql_file_enum **|** mysql_hashdump **|** mysql_writeable_dirs Login Scanner (BForce – MSF mysql_login) mysql -u *{user}* -p *{password}* -h *{Target}*	MSF
SSH *{TCP 22}*	ssh_version ssh_login (passwords BForce) **|** ssh_login_pubkey(keys login) ssh_enumusers	MSF
SMTP *{TCP 25}*	smtp_version smtp_enum VRFY/EXPN {user} (NetCat)	MSF netcat
RDP *{TCP 3389}*	rdp_scanner	MSF Hydra

- SMB Shares Access: `smbclient //{TARGET_IP}/{SHARE_NAME} -U {username}`
- SMB Anon/Null session: `smbclient -L {TARGET_IP} -N`
- RPC equivalent to above: `rpcclient -U "" -N {TARGET_IP}`