Enumeration

NetBIOS & SMB (Port 139/445)

- Metasploit
  - auxiliary/scanner/smb/smb_enumusers_domain
  - auxiliary/scanner/smb/smb_enum_gpp
  - auxiliary/scanner/smb/smb_enumshares
  - auxiliary/scanner/smb/smb_enumusers
  - auxiliary/scanner/smb/smb_lookupsid
- nmblookup
- SMBMap
- smbclient
- crackmapexec
- polenum
- Nmap
  - smb-enum null sessions
  - smb-enum sessions
  - smb-enum groups
  - smb-enum-users
  - smb-enum admins
  - smb-enum shares
  - smb-enum policies
- Samrdump
- nbtscan
- enum4linux

LDAP (Port 389/636)

- jxplorer
- Nmap
  - ldap-brute
  - ldap-rootdse
  - ldap-search
- Softerra LDAP Administrator
- ldapsearch
- LDAPDomainDump
- windapsearch

RPC (Port 135)

- rpcinfo

SMTP (Port 25)

- Metasploit: auxiliary/scanner/smtp/smtp_enum
- Nmap: nmap --script smtp-enum-users
- iSMTP
- smtp-enum-vrfy
- NetScanTools
- smtp-enum-rcpt

SNMP (Port 161/162)

- Metasploit
  - auxiliary/scanner/snmp/snmp_enum
  - auxiliary/scanner/snmp/snmp_enumshares
  - auxiliary/scanner/snmp/snmp_enumusers
- SNMP Scanner
- OpUtils
- snmp-check
- snmpbulkwalk
- snmpwalk

RDP (Port 3389)

- Nmap
  - rdp-enum-encryption
  - rdp-ntlm-info
  - rdp-vuln-ms12-020
- ncrack
- Crowbar

FTP (Port 21)

- Metasploit
  - auxiliary/scanner/ftp/anonymous
  - auxiliary/scanner/ftp/ftp_login
- ftp-vulnerability-scan
- ftp-default

HTTP/HTTPS (80,443)

- feroxbuster
- Burpsuite
- Nmap Scripts
- Nikto
- Whatweb
- sslscan
- httpx
- OWASP Zap
- cewl
- wafw00f
- katana
- curl
- gobuster
- ffuf
- sslyze

MySQL (Port 3306)

- Nmap
  - mysql-audit
  - mysql-brute
  - mysql-databases
  - mysql-dump-hashes
  - mysql-empty-password
  - mysql-enum
  - mysql-info
  - mysql-query
  - mysql-users
  - mysql-variables
- Metasploit
  - auxiliary/scanner/mysql/mysql_version
  - auxiliary/scanner/mysql/mysql_authbypass_hashdump
  - auxiliary/scanner/mysql/mysql_hashdump
  - auxiliary/admin/mysql/mysql_enum
  - auxiliary/scanner/mysql/mysql_schemadump
- mysql commands

MSSQL (Port 1433)

- Metasploit
  - admin/mssql/mssql_enum
  - admin/mssql/mssql_enum_domain_accounts
  - admin/mssql/mssql_enum_sql_logins
- Nmap
  - nmap --script
  - ms-sql-info
  - ms-sql-empty-password
  - ms-sql-xp-cmdshell
  - ms-sql-config
  - ms-sql-ntlm-info
  - ms-sql-tables
  - ms-sql-hasdbaccess
  - ms-sql-dac
  - ms-sql-dump-hashes
- PowerUpSQL

Postgres (5432)

- Metasploit
  - auxiliary/scanner/postgres/postgres_login
  - auxiliary/admin/postgres/postgres_readfile
  - auxiliary/admin/postgres/postgres_sql
  - auxiliary/scanner/postgres/postgres_version
  - auxiliary/scanner/postgres/postgres_hashdump
  - auxiliary/scanner/postgres/postgres_schemadump
- psql

Oracle (1521)

- Nmap
  - oracle-brute-stealth
  - oracle-brute
  - oracle-enum-users
  - oracle-sid-brute
  - oracle-tns-version
- Metasploit
  - auxiliary/scanner/oracle/spy_sid
  - auxiliary/admin/oracle/oraenum
- oracle-version
- oracle-default
- oracle-sid

NFS (Port 2049)

- Metasploit: auxiliary/scanner/nfs/nfsmount
- showmount
- Nmap
  - nfs-ls
  - nfs-showmount
  - nfs-statfs

DNS (Port 53)

- dnsenum
- dnsdict6
- dnsrecon
- dig

www.hackingarticles.in