Windows Service	Purpose
Microsoft IIS *{TCP 80/443}*	Web Server Software
WebDAV *{TCP 80/443}*	HTTP extension to enable web servers to act as a file server
SMB/CIFS *{TCP 445}*	File sharing protocol for the sharing of files between computers on a LAN
RDP *{TCP 3389}*	GUI remote access protocol for remote authentication and interaction
WinRM *{TCP 5985/5986/443}*	Remote management protocol for remote access
NetBIOS *{TCP/UDP 137,138,139}*	
SNMP *{UDP 161/162}*	Monitoring and management protocol for networked devices, such as routers, switches, printers, servers, and more

Tool	Purpose	How to use
Searchsploit	Search ExploitDB	searchsploit "*service*" searchsploit "*service*" | grep -e "Metasploit"
metasploit-autopwn	Identify exploit modules for open ports found on MSF	DL from hahwul GitHub db_autopwn *{Args}*
davtest	Scan, authenticate and exploit a WebDAV server	davtest -url *{http://TARGET/DIR}* davtest -auth *{USERNAME:PWD}* -url …
cadaver	File manipulation (Upload, DL, MV, CP etc..) on WebDAV servers	cadaver *{http://TARGET/DIR}* put *{WebShell_Path}* – Once connected only
Nessus	Vuln Scanner	DL Nessus Essentials
Crackmapexec	Swiss Knife	BF : crackmapexec *{Protocol} {Target}* -u *{username}* -p *{password/filepass/-H for hash}* Command Exec: Like BF + -x "*{COMMAND}*"
evil-winrm.rb	WinRM Shell Spawner	evilwinrm.rb -u *{USERNAME}* -p *{PWD/Hash}* -i *{IP}*
nbtscan nmblookup	NetBIOS	
snmpwalk	SNMP	snmpwalk -v *{SNMP_Version}* -c *{COMMUNITY_STRING} {IP}* List: /usr/share/nmap/nselib/data/snmpcommunities.lst

WWW.DRAGKOB.COM