GTFO Cheatsheet (30/09/2020) (2/2) (ingenieriainformatica.uniovi.es)

Executables to enable privilege scalation in Linux systems



GTFOBins is a collaborative project created by Emilio Pinna and Andrea Cardaci

Check the specifics of each executable in https://gtfobins.github.io/

<u>Limited SUID</u>



PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS	PROGRAM	POSSIBLE EXPLOITS
pg	Shell		<u>Shell</u>		Shell	<u>scp</u>	Shell	socat	Shell	<u>su</u>	<u>Sudo</u>		File upload	valgrind	Shell		File upload
	<u>File read</u> SUID		Reverse shell File upload	rsync	<u>SUID</u>		<u>File upload</u> File download		Reverse shell Bind shell		File read		File download SUID		<u>Sudo</u>	<u>whois</u>	File download
	<u>3010</u>		File download		<u>Sudo</u>		<u>Sudo</u>		File upload	<u>sysctl</u>	SUID	tftp	<u>3010</u>	<u>vi</u>	<u>Shell</u>	wish	Shell
	<u>Sudo</u>		File write		Shell				File download				<u>Sudo</u>		File write		Non-interactive
	Shell	python		ruby	Reverse shell		<u>Limited SUID</u>		Sudo		<u>Sudo</u>		Shell		File read		reverse shell
	Command		<u>Library load</u>		File upload	She	<u>Shell</u>	-	Limited SUID		<u>SUID</u>	time	SUID		<u>Sudo</u>		<u>Sudo</u>
	Reverse shell		<u>SUID</u>		File download	screen	screen File write			systemctl	<u>Sudo</u>	<u>unic</u>	<u>Sudo</u>	view	Shell	xargs	<u>Shell</u>
	<u>File upload</u> File download		Sudo		<u>File write</u> File read		<u>Sudo</u>		<u>File read</u> SUID		File read	timeout tmux	Shell		Reverse shell		<u>File read</u> <u>SUID</u>
	<u>SUID</u>		<u>Capabilities</u>		Library load	Shell Script File write Sudo Shell	Shell	<u>soelim</u>			SUID		SUID		Non-interactive		
				_					<u>Sudo</u>	<u>tac</u>					reverse shell Non-interactive bind		<u>Sudo</u>
	<u>Sudo</u>		<u>Shell</u>		<u>Sudo</u>		<u>File write</u>				<u>Sudo</u>		<u>Sudo</u>		shell		
	<u>Capabilities</u>	<u>rake</u>	<u>Sudo</u>		<u>Capabilities</u>		<u>Sudo</u>		File read				CI. II		File upload	xxd	<u>File write</u>
	Shell		<u>Limited SUID</u>		Shell		Shell		SUID		<u>File read</u> SUID		<u>Shell</u>		File download File write		<u>File read</u> SUID
<u>pic</u>	<u>Sudo</u>	readelf	<u>File read</u>	-	<u>File write</u>	Command			<u>Sudo</u>	<u>tail</u>	Sudo		<u>Sudo</u>		File read		Sudo
	<u>Limited SUID</u>		<u>SUID</u>	<u>run-mailcap</u>	<u>File read</u>	cod	File write sed File read		<u>Shell</u> File write		Shell		<u>Shell</u>		<u>Library load</u> SUID		File read
	<u>Shell</u>		<u>Sudo</u>		<u>Sudo</u>	<u>sed</u>	<u>SUID</u>		File read		File upload		<u>Sudo</u>		<u>Sudo</u>		<u>SUID</u>
pico	<u>File write</u>		<u>File write</u>		<u>Shell</u>		<u>Sudo</u>	<u>sqlite3</u>	<u>Sudo</u>	-	File download		<u>File read</u>		<u>Capabilities</u>	<u>XZ</u>	<u>Sudo</u>
	File read SUID	<u>red</u>	<u>File read</u>	run-parts	SUID		Shell	+	<u>Limited SUID</u>	<u>tar</u>	File write File read	<u>ul</u>	SUID		<u>Limited SUID</u>		
	<u>Sudo</u>		<u>Sudo</u>		<u>Sudo</u>	service	Sudo		<u>Shell</u>		<u>Sudo</u>		<u>Sudo</u>		<u>Shell</u>	<u>yelp</u>	<u>File read</u>
	3440	-	<u>File read</u>		<u>Shell</u>		3000	<u>File upload</u>		Limited SUID		<u>File read</u>		Reverse shell	 <u>yum</u>	Sudo	
<u>pip</u>	<u>Shell</u>	restic rlogin	Conda		Reverse shell		<u>Shell</u>	<u>File download</u>		<u>Limited 301D</u>		<u>SUID</u>		Non-interactive reverse shell	<u>yum</u>	<u>Sudo</u>	
	Reverse shell		<u>Sudo</u>		Non-interactive		SUID	<u>ssh</u>	File read		Shell	unexpand			Non-interactive bind		Shell
					reverse shell Non-interactive bind	<u>setarch</u>	setarch setarch						<u>Sudo</u>		<u>shell</u>		
	<u>File upload</u>		File upload		<u>shell</u>	<u>Sudo</u>		<u>Sudo</u>	<u>taskset</u>	SUID				<u>File upload</u>	<u>zip</u> 	<u>Sudo</u>	
	File download File write		SUID	<u> </u>	<u>File upload</u> File download		Chall	start-stop- daemon	Shell	_	<u>Sudo</u>	uniq unshare	<u>File read</u> SUID	<u>vim</u>	File download		<u>Limited SUID</u>
	File read		<u>Sudo</u>	rview	File write	sftp File d Sudo File w File re	File upload		SUID		Shell		3010		<u>File write</u> File read		Shell
	Library load		51 1 1		File read		File download			tclsh	Non-interactive		<u>Sudo</u>		Library load		SUID
			<u>File upload</u>		Library load				<u>Sudo</u>		reverse shell SUID		Shell		SUID	zsoelim	<u> </u>
	<u>Sudo</u>		<u>Shell</u>		<u>SUID</u>		<u>Sudo</u>		<u>Shell</u>		Sudo		<u>SUID</u>	watch	<u>Sudo</u>		<u>Sudo</u>
pkexec	<u>Sudo</u>	rhyran	<u>File write</u>		<u>Sudo</u>		<u>File write</u>		SUID		Command		<u>Sudo</u>		<u>Capabilities</u>		<u>File read</u>
	Shell	rlwrap	<u>SUID</u>		<u>Capabilities</u>		SUID SUID		<u>Sudo</u>	tcpdump	<u>Sudo</u>		File read		<u>Limited SUID</u>		<u>SUID</u>
pry	<u>Sudo</u>		<u>Sudo</u>		<u>Limited SUID</u>		Sudo	<u>strace</u>	<u>Shell</u>				SUID		<u>Shell</u>		<u>Sudo</u>
	<u>Limited SUID</u>	<u>rpm</u>	<u>Shell</u> SUID		Shell Reverse shell		Shell stra File upload		SUID	-	<u>File write</u> SUID		<u>Sudo</u>		SUID Sudo		<u>Shell</u>
	Shall		2010		Non-interactive			Strace	<u>Sudo</u>	<u>tee</u>	<u>Sudo</u>				3440	zypper	<u>Sudo</u>
	<u>Shell</u>		<u>Sudo</u>		reverse shell	one ballows							<u>File read</u>		<u>Limited SUID</u>		
puppet	<u>File write</u>				Non-interactive bind shell	smbclient File download Sudo		<u>File read</u>			uuencode	<u>SUID</u>					
	<u>File read</u>		<u>Shell</u>		<u>File upload</u>		Sudo		<u>SUID</u>	telnet	<u>Shell</u>	-	<u>Sudo</u>	wget	<u>File upload</u>		
	<u>Sudo</u>	rpmquery	<u>SUID</u>	<u>rvim</u>	rvim File download File write				<u>Sudo</u>		Reverse shell Sudo				File download SUID		
	1		<u>Sudo</u>		File read				1	temet							
					<u>Library load</u>						<u>Limited SUID</u>				<u>Sudo</u>		
					<u>SUID</u> <u>Sudo</u>												
					<u>Capabilities</u>												
					1												