GTFO Cheatsheet (30/09/2020) (1/2) (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/

PROGRAM	POSSIBLE EXPLOITS
apt-get	Shell Sudo
apt	Shell Sudo
aria2c	Command SUID Sudo
arp	File read SUID Sudo
ash	Shell File write SUID Sudo
awk	Shell Non-interactive reverse shell Non-interactive bind shell File write File read Sudo Limited SUID
base32	File read SUID Sudo
base64	File read SUID Sudo
bash	Shell Reverse shell File upload File download File write File read Library load SUID Sudo
bpftrace	Sudo
bundler	Shell Sudo
busctl	Shell Sudo
busybox	Shell File upload File write File read SUID Sudo
byebug	Shell Sudo Limited SUID
cancel	File upload
cat	File read SUID Sudo
chmod	SUID Sudo
chown	SUID Sudo
chroot	SUID Sudo
cobc	Shell Sudo
cp	File write File read SUID Sudo
cpan	Shell Reverse shell File upload File download Sudo
cpulimit	Shell Sudo
crash	Shell Command Sudo
crontab	Command Sudo
csh	Shell File write SUID Sudo
curl	File upload File download File read SUID Sudo
cut	File read SUID Sudo
dash	Shell File write SUID Sudo
date	File read SUID Sudo
dd	File write File read SUID Sudo
dialog	File read SUID Sudo
diff	File read SUID Sudo
dmesg	Shell File read Sudo
dmsetup	SUID Sudo
dnf	Sudo
docker	Shell File write File read SUID Sudo
dpkg	Shell Sudo
easy_install	Shell Reverse shell File upload File download File write File read Library load Sudo
eb	Shell Sudo
ed	Shell File write File read Sudo Limited SUID
emacs	Shell File write File read SUID Sudo
env	Shell SUID Sudo
eqn	File read SUID Sudo
expand	File read SUID Sudo
expect	Shell SUID Sudo
facter	Shell Sudo
file	File read SUID Sudo
find	Shell SUID Sudo
finger	File upload File download
flock	Shell SUID Sudo
fmt	File read SUID Sudo
fold	File read SUID Sudo
ftp	Shell File upload File download Sudo
gawk	Shell Non-interactive reverse shell Non-interactive bind shell File write File read Sudo Limited SUID
gcc	Shell File read Sudo
gdb	Shell Reverse shell File upload File download File write File read Library load SUID Sudo Capabilities
gem	Shell Sudo
genisoimage	File read SUID Sudo
gimp	Shell Reverse shell File upload File download File write File read Library load SUID Sudo
git	Shell Sudo Limited SUID
grep	File read SUID Sudo
gtester	Shell SUID Sudo
hd	File read SUID Sudo
head	File read SUID Sudo
hexdump	File read SUID Sudo
highlight	File read SUID Sudo
iconv	File write File read SUID Sudo
iftop	Shell Sudo Limited SUID
ionice	Shell SUID Sudo
ip	File read SUID Sudo
irb	Shell Reverse shell File upload File download File write File read Library load Sudo
jjs	Shell Reverse shell File download File write File read SUID Sudo
journalctl	Shell Sudo
jq	File read SUID Sudo
jrunscript	Shell Reverse shell File download File write File read SUID Sudo
ksh	Shell Reverse shell File upload File download File write File read SUID Sudo
ksshell	File read SUID Sudo
ld.so	Shell SUID Sudo
ldconfig	Sudo Limited SUID
less	Shell File write File read SUID Sudo
logsave	Shell SUID Sudo
look	File read SUID Sudo
ltrace	Shell Sudo
lua	Shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read Sudo Limited SUID
lwp-download	File download SUID Sudo
lwp-request	File read SUID Sudo
mail	Shell Sudo
make	Shell File write SUID Sudo
man	Shell File read Sudo
mawk	Shell File write File read Sudo Limited SUID
more	Shell File read SUID Sudo
mount	Sudo
mtr	File read Sudo
mv	SUID Sudo
mysql	Shell Library load Sudo Limited SUID
nano	Shell File write File read SUID Sudo
nawk	Shell Non-interactive reverse shell Non-interactive bind shell File write File read Sudo Limited SUID
nc	Reverse shell Bind shell File upload File download Sudo Limited SUID
nice	Shell SUID Sudo
nl	File read SUID Sudo
nmap	Shell Non-interactive reverse shell Non-interactive bind shell File upload File download File write File read Sudo Limited SUID
node	Shell Reverse shell Bind shell SUID Sudo Capabilities
nohup	Shell Command SUID Sudo
nroff	Shell Sudo
nsenter	Shell Sudo
od	File read SUID Sudo
openssl	Reverse shell File upload File download File write File read Library load SUID Sudo
pdb	Shell Sudo
perl	Shell Reverse shell SUID Sudo Capabilities