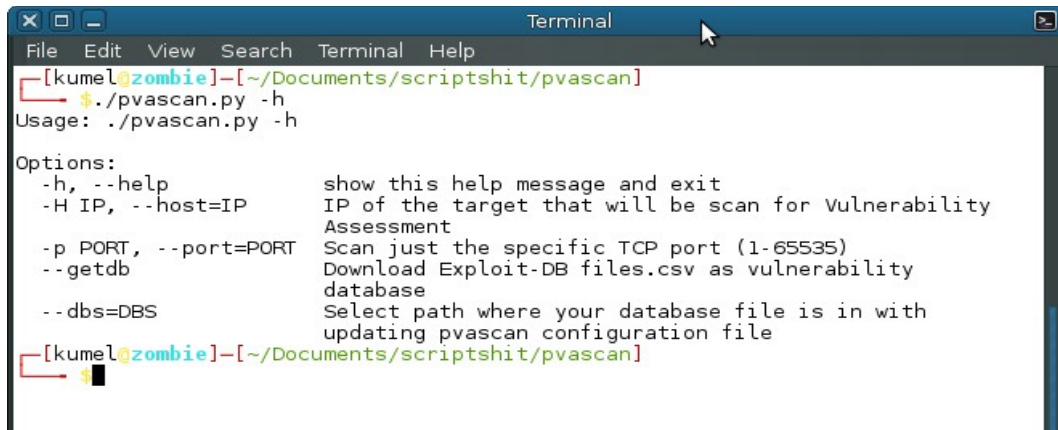


# Cara Penggunaan Program

## 1) Menu Bantuan

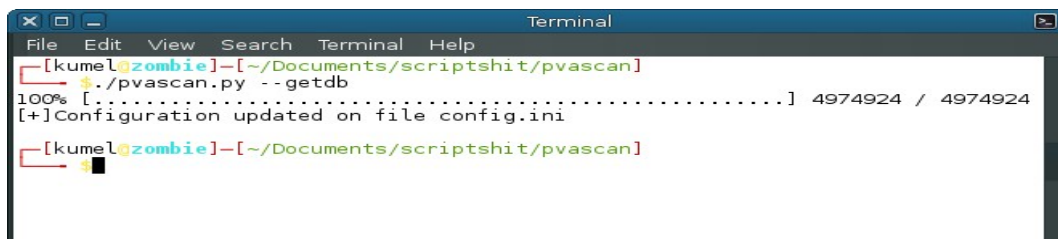


```
[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$ ./pvascan.py -h
Usage: ./pvascan.py -h

Options:
  -h, --help            show this help message and exit
  -H IP, --host=IP      IP of the target that will be scan for Vulnerability
                        Assessment
  -p PORT, --port=PORT  Scan just the specific TCP port (1-65535)
  --getdb                Download Exploit-DB files.csv as vulnerability
                        database
  --dbs=DBS              Select path where your database file is in with
                        updating pvascan configuration file

[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$
```

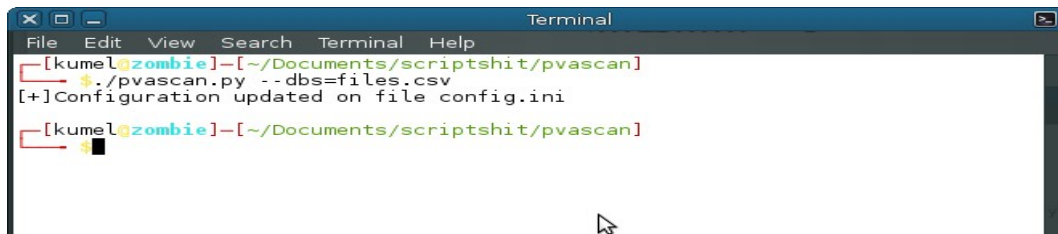
## 2) Download Database



```
[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$ ./pvascan.py --getdb
100% [.....] 4974924 / 4974924
[+]Configuration updated on file config.ini

[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$
```

## 3) Pilih Database



```
[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$ ./pvascan.py --dbs=files.csv
[+]Configuration updated on file config.ini

[kumel@zombie]--[~/Documents/scriptshit/pvascan]
└─$
```

#### 4) Vulnerability Scanner

```
Terminal
File Edit View Search Terminal Help
[kumel@zombie]-[~/Documents/scriptshit/pvascan]
$ sudo ./pvascan.py -H 192.168.56.101
From Linux 4.1.8-parrot-amd64
On Wed Nov 25 10:24:14 2015
Scanning for host 192.168.56.101
OS detection accuracy 95%
Vendor : Microsoft, Windows 2000
Discovered host ports [ 4 ]
[+]PORT 445 [microsoft-ds] Microsoft Windows XP microsoft-ds
[+]PORT 139 [netbios-ssn]
[+]PORT 21 [ftp] WAR-FTPD 1.65
| VULNERABLE DETECTED!
|- Description :
|   1 WAR-FTPD 1.65 (MKD/CD Requests) Denial of Service Vuln
|   | For more information please visit url below
|   | _ https://www.exploit-db.com/exploits/9496/
|   2 War-FTPD 1.65 Password Overflow
|   | For more information please visit url below
|   | _ https://www.exploit-db.com/exploits/16706/
|   3 War-FTPD 1.65 Username Overflow
|   | For more information please visit url below
|   | _ https://www.exploit-db.com/exploits/16724/
|- 3 exploits found,
|_ Please contact the application's vendor to patch the vulnerable
[+]PORT 135 [msrpc]
```