Forensics Tools

p0f

P0f is a tool that can identify the operating system of a target host simply by examining captured packets even when the device in question is behind a packet firewall. P0f does not generate any additional network traffic, direct or indirect; no name lookups; no mysterious probes; no ARIN queries; nothing. In the hands of advanced users, P0f can detect firewall presence, NAT use, and existence of load balancers.

Type "**p0f – h"** in the terminal to see how to use it and you will get the following results.

```
root@kali: ~
File  Edit  View  Search  Terminal  Help
root@kali:~# p0f -h
```

```
/p0f: invalid option -- 'h'
Usage: p0f [ ...options... ] [ 'filter rule' ]

Network interface options:

  -i iface   - listen on the specified network interface
  -r file    - read offline pcap data from a given file
  -p         - put the listening interface in promiscuous mode
  -L         - list all available interfaces

Operating mode and output settings:

  -f file    - read fingerprint database from 'file' (p0f.fp)
  -o file    - write information to the specified log file
  -s name    - answer to API queries at a named unix socket
  -u user    - switch to the specified unprivileged account and chroot
  -d         - fork into background (requires -o or -s)
```

It will list even the available interfaces.

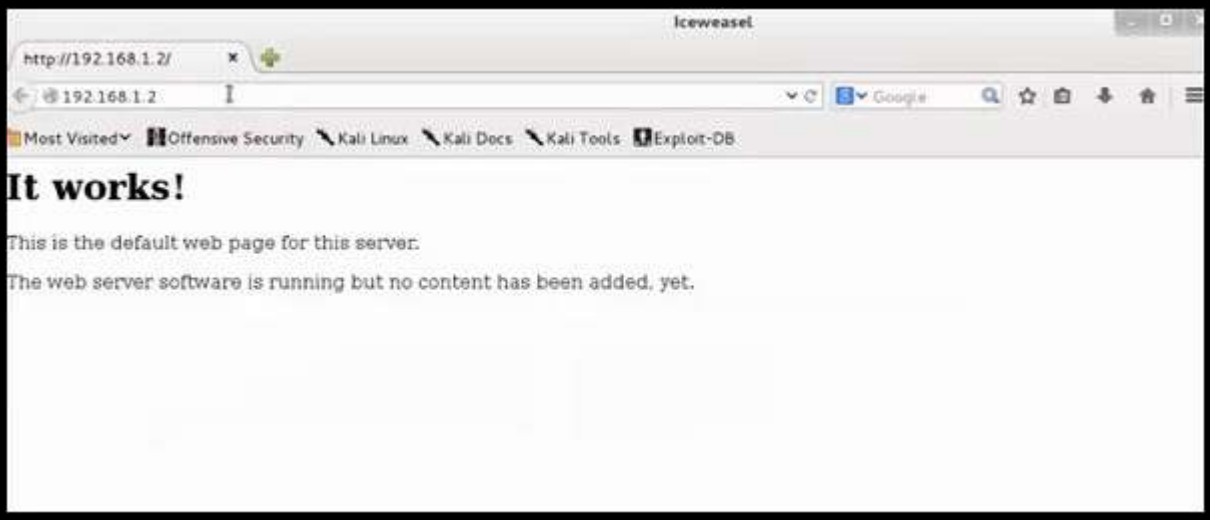
```
-- Available interfaces --

  0: Name        : eth0
     Description : -
     IP address  : 192.168.1.9

  1: Name        : nflog
     Description : Linux netfilter log (NFLOG) interface
     IP address  : (none)

  2: Name        : any
     Description : Pseudo-device that captures on all interfaces
     IP address  : (none)

  3: Name        : lo
     Description : -
     IP address  : 127.0.0.1
```

Then, type the following command: "**p0f –i eth0 –p -o filename**".

Where the parameter **"-i"** is the interface name as shown above. **"-p"** means it is in promiscuous mode. **"-o"** means the output will be saved in a file.

```
root@kali:~# p0f -i eth0 -p -o /root/Desktop/my.log
```

Open a webpage with the address 192.168.1.2



From the results, you can observe that the Webserver is using apache 2.x and the OS is Debian.

pdf-parser

pdf-parser is a tool that parses a PDF document to identify the fundamental elements used in the analyzed pdf file. It will not render a PDF document. It is not recommended for text book case for PDF parsers, however it gets the job done. Generally, this is used for pdf files that you suspect has a script embedded in it.

The command is –

```
pdf-parser  -o 10 filepath
```

where "-o" is the number of objects.

```
root@kali:~# pdf-parser  -o 10 /root/Desktop/[redacted].pdf
obj 10 0
 Type: /Action
 Referencing:

  <<
    /S /Launch
```

As you can see in the following screenshot, the pdf file opens a CMD command.

```
        /F (cmd.exe)
        /D '(c:\\\\windows\\\\system32)'
        /P (
        /Q '/C %HOMEDRIVE%&cd %HOMEPATH%&(if exist "Desktop\\\\template.pdf" (cd
 "Desktop"))&(if exist "My Documents\\\\template.pdf" (cd "My Documents"))&(if e
xist "Documents\\\\template.pdf" (cd "Documents"))&(if exist "Escritorio\\\\temp
late.pdf" (cd "Escritorio"))&(if exist "Mis Documentos\\\\template.pdf" (cd "Mis
 Documentos"))&(start template.pdf)\n\n\n\n\n\n\n\n\n\n\nTo view the encrypted con
tent please tick the "Do not show this message again" box and press Open.)'
      >>
  >>
```