File   Edit   View   Window   Help

Kali Tools
- Information Gathering
- Sniffing & Spoofing
- Vulnerability Analysis
- Exploitation
- Password Attacks
- Wireless Attacks
- Forensics
- Maintaining Access
- Hardware Hacking
- Web Applications
- Stress Testing
- Reverse Engineering
- Reporting

Welcome

T Y R I O N

Version 1.0

THE GO TO ALL|IN|ONE KALI LINUX TOOL REFERENCE APP

Left ✕

File   Edit   View   Window   Help

Kali Tools
- nbtscan-unixwiz
- Nmap
- ntop
- p0f
- Parsero
- Recon-ng
- SET
- smtp-user-enum
- snmp-check
- SPARTA
- sslcaudit
- SSLsplit
- sslstrip
- SSLyze
- THC-IPV6
- theHarvester
- TLSSLed
- twofi
- URLCrazy
- Wireshark
- WOL-E
- Xplico
- Sniffing & Spoofing
- Vulnerability Analysis
- Exploitation

Welcome   Wireshark ✕

Wireshark

Description:

Wireshark is the world's foremost network protocol analyzer. It lets you see what's happening on your network at a microscopic level. It is the de facto (and often de jure) standard across many industries and educational institutions. Wireshark development thrives thanks to the contributions of networking experts across the globe. It is the continuation of a project that started in 1998.

•Wireshark has a rich feature set which includes the following:

•Deep inspection of hundreds of protocols, with more being added all the time

Left ✕

---

cisco-torch ✕   CaseFile ✕   CDPSnarf ✕   Cookie Cadger ✕   DMitry ✕   DNSRecon ✕   fragrouter ✕   UrlCrazy ✕   TLSSLed ✕

Author: Raul Siles, Taddong SL

Usage:

```
tlssled
--------------------------------------------

 TLSSLed - (1.3) based on sslscan and openssl
             by Raul Siles (www.taddong.com)
--------------------------------------------

    openssl version: OpenSSL 1.0.1e 11 Feb 2013
    sslscan version 1.8.2
--------------------------------------------

    Date: 20140520-110731
--------------------------------------------


[!] Usage: /usr/bin/tlssled <hostname or IP_address> <port>
```

Examples:

```
root@kali:~# p0f -i eth0 -p -o /tmp/p0f.log
--- p0f 3.07b by Michal Zalewski <lcamtuf@coredump.cx> ---

[+] Closed 1 file descriptor.
[+] Loaded 320 signatures from 'p0f.fp'.
[+] Intercepting traffic on interface 'eth0'.
[+] Default packet filtering configured [+VLAN].
[+] Log file '/tmp/p0f.log' opened for writing.
[+] Entered main event loop.

.-[ 192.168.1.15/35834 -> 173.246.39.185/873 (syn) ]-
|
| client    = 192.168.1.15/35834
```

RUN ON TERMINAL :

```
nmap
```

Kali Tools

- ▼ Information Gathering
  - acccheck
  - ace-voip
  - Amap
  - Automater
  - bing-ip2hosts
  - braa
  - CaseFile
  - CDPSnarf
  - cisco-torch
  - Cookie Cadger
  - copy-router-config
  - DMitry
  - dnmap
  - dsenum
  - dnsmap
  - DNSRecon
  - dnstracer
  - dnswalk
  - DotDotPwn
  - enum4linux
  - enumIAX
  - Faraday
  - Fierce
  - Firewalk