

Kali Linux Lab

Purpose & Features

Kali Linux is an open source Debian-based Linux distribution that is kept up-to-date by *Offensive Security*, a service organization that provides IT security training and network penetration services. Some features the distribution offers include; penetration testing, security research, computer forensics, and reverse engineering. Kali Linux can be installed on a hard drive, or booted from a live cd/usb stick. Kali Linux can also be installed on a virtual machine. Kali Linux is in 32-bit and 64 bit distributions based on the x86 architecture

Since the distribution is intended for penetration testing purposes, the distribution is designed so that:

- There is a single, root user
- Network services are disabled by default that will allow users to install other services while keeping the distribution secured
- It is a custom linux kernel
- It is used for the purpose of penetration testing. Using the distribution for other purposes such as development, web design, or gaming, will cause difficulty to users

Notable Tools

InviteFlood

This tool allows a user to flood an IP address over UDP/IP. Using a basic terminal command, a user specifies the interface to be used as well as the target IP and the number of packets to send to the target. The tool then overwhelms the target IP network with x amount of packets. This tool can be used for stress testing for a network.

Observations

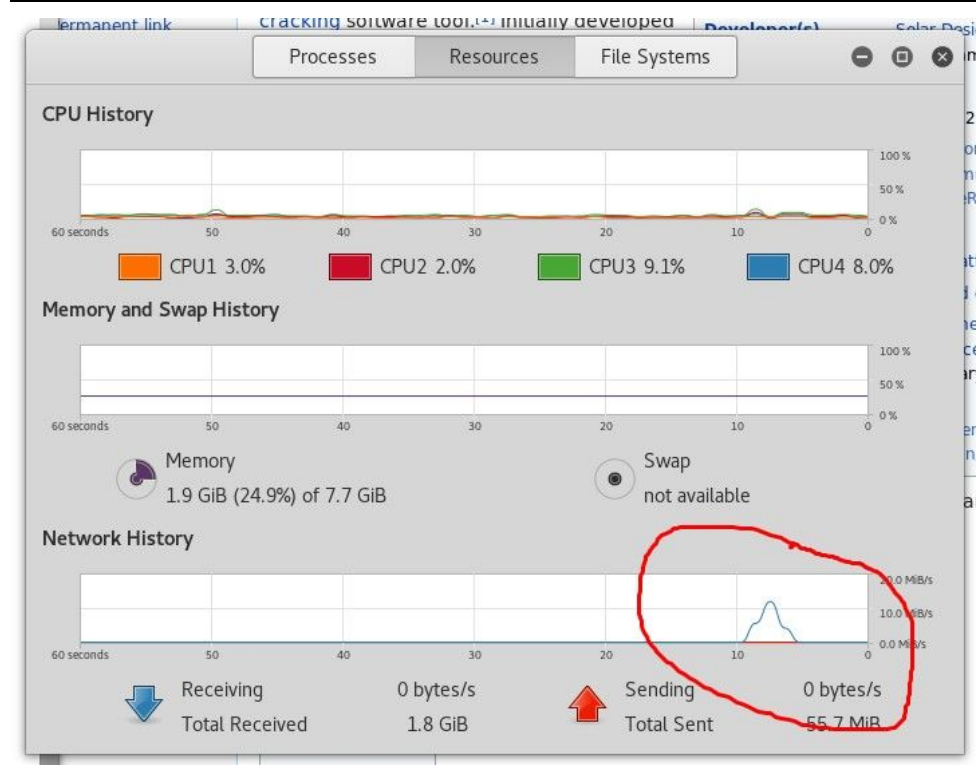
Sending a large number of packets (≥ 10000) shows the network usage for the target to spike. We also noticed that the target computer's internet speed becomes completely clogged up during the spike. In that sense, it could be used to target a specific network for a DOS attack. Not the most ideal tool, but it would work.

```
root@kali: /var/www/html
File Edit View Search Terminal Help
root@kali:/var/www/html# inviteflood eth0 5000 192.168.13.108 192.168.13.108 20000

inviteflood - Version 2.0
             June 09, 2006

source IPv4 addr:port = 192.168.13.146:9
dest   IPv4 addr:port = 192.168.13.108:5060
targeted UA           = 5000@192.168.13.108

Flooding destination with 20000 packets
sent: 20000
root@kali:/var/www/html#
```



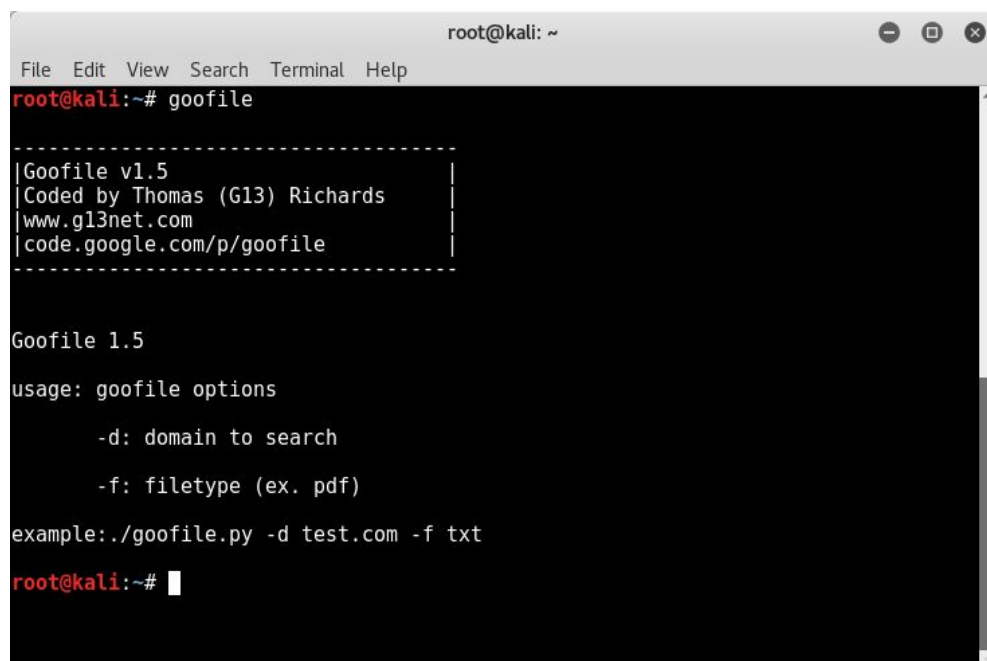
John The Ripper

This tool is a free password cracking software. It is one of the most popular password testing and breaking programs, as it combines a number of password crackers into one package, it auto-detects password hash types, and includes a customizable password cracker. It can be run against various encrypted password formats including several crypt password hash types most commonly found on various Unix Versions, and windows.

```
# cat pass.txt
user:AZl.zWwxIh15Q
# john -w:password.lst pass.txt
Loaded 1 password hash (Traditional DES [24/32 4K])
example          (user)
guesses: 1  time: 0:00:00:00 100% c/s: 752  trying: 12345 - pookie
```

Goofile

This tools allows a user to scan a domain site for certain file types. This can be helpful if a user is looking for a certain file within a domain. With the terminal, the user can save the results as a tx, which they can then use to do a mass download of files using *wget* in the terminal.



```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# goofile
-----
|Goofile v1.5
|Coded by Thomas (G13) Richards
|www.g13net.com
|code.google.com/p/goofile
|-----
Goofile 1.5
usage: goofile options
        -d: domain to search
        -f: filetype (ex. pdf)
example: ./goofile.py -d test.com -f txt
root@kali:~#
```

```
root@kali: ~/Desktop
File Edit View Search Terminal Help

root@kali:~/Desktop# goofile -d kali.org -f pdf

-----
|Goofile v1.5
|Coded by Thomas (G13) Richards
|www.g13net.com
|code.google.com/p/goofile
|-----

Searching in kali.org for pdf
=====

Files found:
=====

www.kali.org/dojo/bh2015/workshop-01.pdf
www.kali.org/dojo/ekol2/eko-workshop01.pdf
www.kali.org/dojo/ekol2/eko-workshop02.pdf
www.kali.org/dojo/bh2015/workshop-02.pdf
docs.kali.org/pdf/kali-book-fr.pdf
docs.kali.org/pdf/kali-book-es.pdf
docs.kali.org/pdf/kali-book-id.pdf
docs.kali.org/pdf/kali-book-de.pdf
docs.kali.org/pdf/kali-book-it.pdf
docs.kali.org/pdf/kali-book-ar.pdf
docs.kali.org/pdf/kali-book-ja.pdf
docs.kali.org/pdf/kali-book-nl.pdf
docs.kali.org/pdf/kali-book-ru.pdf
docs.kali.org/pdf/kali-book-en.pdf
docs.kali.org/pdf/kali-book-pt-br.pdf
docs.kali.org/pdf/kali-book-zh-hans.pdf
Issue.pdf
docs.kali.org/pdf/kali-book-sw.pdf
screen.pdf
docs.kali.org/pdf/articles/kali-linux-live-usb-install-en.pdf
```