**Exploring kali linux tools**

Kali Linux is a Debian-derived Linux distribution that is maintained by Offensive Security. It was developed by Mati Aharoni and Devon Kearns. Kali Linux is a specially designed OS for network analysts and penetration testers, or in simple words, it is for those who work under the umbrella of cybersecurity and analysis.
Linux tools that could save a lot of your time and effort.

## Nmap

Nmap is an open-source network scanner that is used to recon/scan networks. It is used to discover hosts, ports, and services along with their versions over a network. It sends packets to the host and then analyses the responses in order to produce the desired results. It is one of the most popular reconnaissance tools.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.67.75.162
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:26 IST
Nmap scan report for 172.67.75.162
Host is up (0.053s latency).
Not shown: 996 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Cloudflare http proxy
443/tcp  open  ssl/https     cloudflare
8080/tcp open  http          Cloudflare http proxy
8443/tcp open  ssl/https-alt cloudflare

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.97 seconds
```

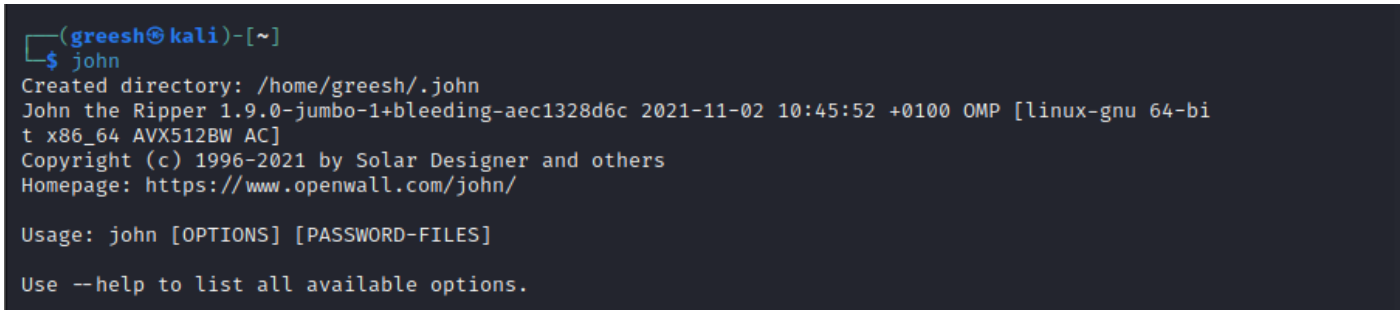
```
┌──(kali㉿kali)-[~]
└─$ nmap -A 172.67.75.162
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:27 IST
Nmap scan report for 172.67.75.162
Host is up (0.072s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        (generic dns response: NOTIMP)
80/tcp   open  http          Cloudflare http proxy
|_http-server-header: cloudflare
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
443/tcp  open  ssl/https     cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
8080/tcp open  http          Cloudflare http proxy
|_http-title: Site doesn't have a title (text/plain; charset=UTF-8).
|_http-server-header: cloudflare
8443/tcp open  ssl/https-alt cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
|_http-server-header: cloudflare
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port53-TCP:V=7.94%I=7%D=10/9%Time=6523DC96%P=x86_64-pc-linux-gnu%r(DNSV
SF:ersionBindReqTCP,E,"\0\x0c\0\x06\x81\x84\0\0\0\0\0\0\0\0");

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 34.69 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap -p 443 172.67.75.162
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-09 16:29 IST
Nmap scan report for 172.67.75.162
Host is up (0.041s latency).

PORT    STATE SERVICE
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

## John the Ripper:

John the Ripper is a tool designed to help systems administrators to find weak (easy to guess or crack through brute force) passwords, and even automatically mail users warning them about it, if it is desired.

Besides several crypt (3) password hash types most commonly found on various Unix flavors, supported out of the box are Kerberos AFS and Windows NT/2000/XP/2003 LM hashes, plus several more with contributed patches.




**NIKTO**

Nikto is a popular open-source web server scanner that checks web servers for multiple items, including:

- The presence of multiple index files
- HTTP server options
- Installed web servers and software
- Potentially dangerous files/programs
- Outdated versions of over 1250 servers
- Version specific problems on over 270 servers
- Other security configuration problems

Nikto performs both generic and server type-specific checks. It also captures any cookies received.

Nikto is a powerful tool for finding vulnerabilities in web servers, but it is important to note that it is not a stealthy tool. This means that it will likely be detected by an intrusion detection system (IDS).

Nikto is included by default in Kali Linux, so you can start using it right away. To scan a web server for vulnerabilities, simply open a terminal and type the following command:

nikto -h https://en.wikipedia.org/wiki/Web_server

This will start a scan of the web server and display the results in the terminal. You can also save the results to a file by using the -o option. For example, to save the results to a file called scan.txt, you would use the following command:

nikto -h https://en.wikipedia.org/wiki/Web_server -o scan.txt

Nikto has a number of options that you can use to customize the scan. For more information, please see the Nikto documentation.

Here are some examples of how to use Nikto:

- To scan a single web server for vulnerabilities:

nikto -h https://en.wikipedia.org/wiki/Web_server

- To scan multiple web servers for vulnerabilities:

nikto -h https://en.wikipedia.org/wiki/Web_server -h
https://en.wikipedia.org/wiki/Web_server ...

- To scan a web server for vulnerabilities using a specific plugin:

nikto -h https://en.wikipedia.org/wiki/Web_server -p [plugin name]

- To save the results of a scan to a file:

nikto -h https://en.wikipedia.org/wiki/Web_server -o [filename]

Nikto is a powerful tool for finding vulnerabilities in web servers. However, it is important to note that it is not a replacement for manual penetration testing.