

Kali Linux

Anteriormente conhecido como BackTrack Linux, é uma distribuição Linux de código aberto, baseada em Debian mantido pela Offensive Security. O Kali Linux é um sistema operacional especializado para realizar pentests, análises de vulnerabilidades e auditorias de segurança.



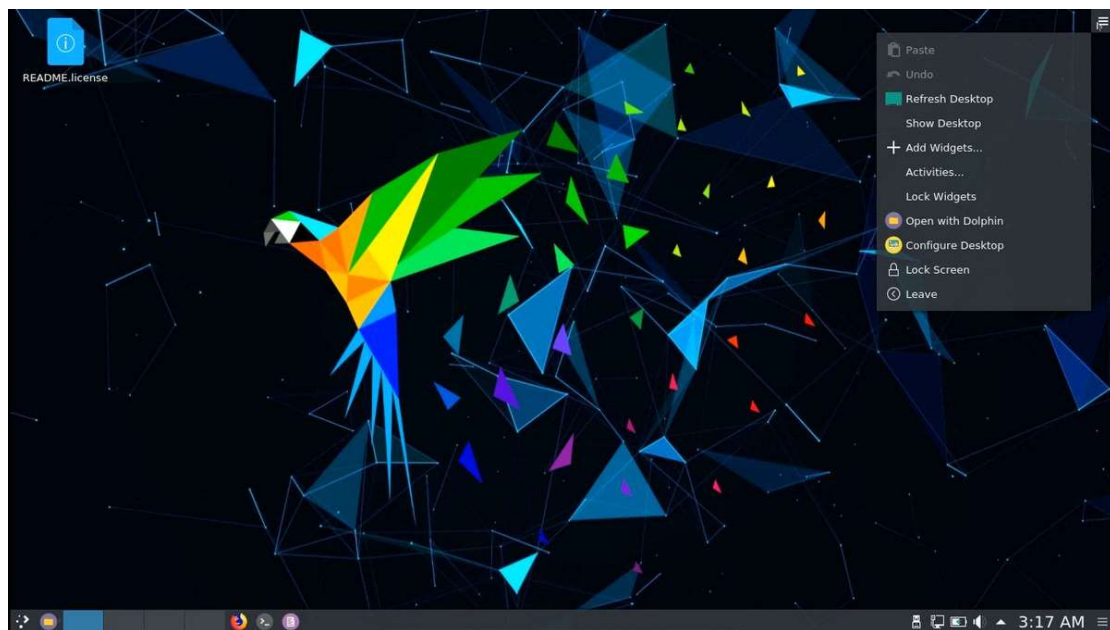
O Pentoo

É um Live CD com o foco na segurança da informação. Ela é baseada na distribuição Gentoo, e é caracterizada por possuir uma seleção bastante diversificada de ferramentas de segurança e testes de rede, desde escaneadores até exploradores de vulnerabilidades.



O Parrot OS

é uma distribuição Linux baseada no Debian com foco em segurança, privacidade e desenvolvimento. Ele também é usado por muitos especialistas em segurança cibernética.



O que é Nmap?

Em sua essência, o Nmap é uma ferramenta de varredura de rede que usa pacotes IP para identificar todos os dispositivos conectados a uma rede e fornecer informações sobre os serviços e sistemas operacionais que eles estão executando.

```

root@kali:~/home/spect# nmap -sV scanme.nmap.org -oX /home/spect/scanResults.xml
Starting Nmap 7.80 ( https://nmap.org ) at 2021-01-18 23:25 +01
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.21s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 987 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    filtered smtp
80/tcp    open  http
135/tcp    filtered msrpc
139/tcp    filtered netbios-ssn
445/tcp    filtered microsoft-ds
593/tcp    filtered http-rpc-epmap
1068/tcp   filtered instl_bootc
4444/tcp   filtered krb524
5800/tcp   filtered vnc-http
5900/tcp   filtered vnc
9929/tcp   open  nping-echo
31337/tcp  open  tcpwrapped
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel; Ubuntu 2.13 (Ubuntu Linux; protocol 2.0)

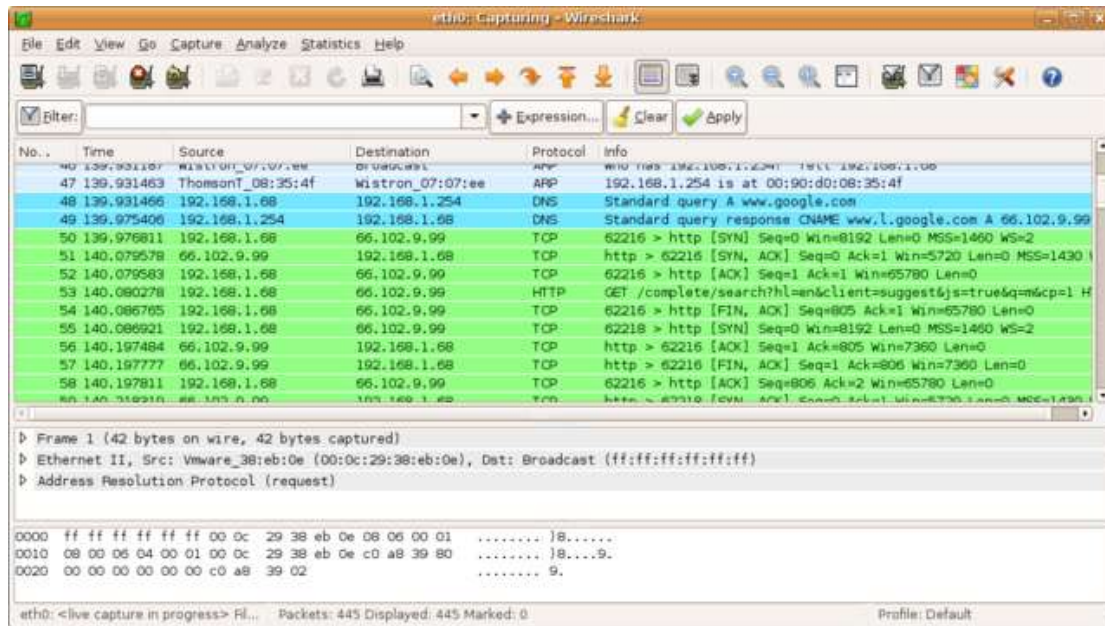
Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 39.35 seconds

```



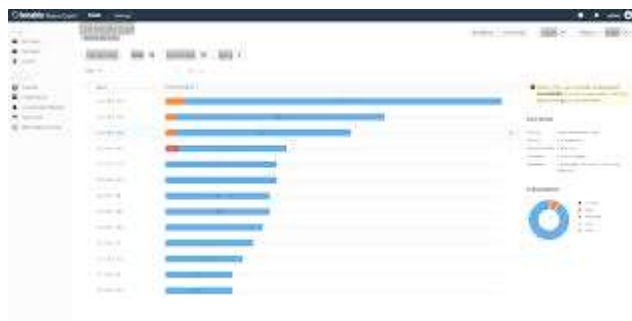
Wireshark

é um programa que analisa o tráfego de rede, e o organiza por protocolos. As funcionalidades do Wireshark são parecidas com o tcpdump mas com uma interface gráfica, com mais informação e com a possibilidade da utilização de filtros.



O Nessus

pode executar verificações de vulnerabilidades de serviços de rede e também fazer login nos servidores para descobrir eventuais patches ausentes.



A Hydra

permite realizar procedimentos de ataque de força bruta contra serviços de autenticação online, tendo suporte a dezenas de protocolos, como por exemplo os FTP's, HTTP, Banco de dados, SHH, entre outros.

Fern Wifi Cracker

É uma ferramenta que tem como objetivo quebrar a segurança de redes sem fio do tipo WPS, WEP e WPA, executando ataques de força bruta e com dicionários.

