SEGURIDAD CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE
MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM
				


Curso Online
Ethical Hacking
Professional
Más Información Aquí

SEGURIDAD CERO

Fernando Conislla
Ethical Hacking Expert

- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor en SEGURIDAD CERO e instructor oficial Certiprof
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales CEH, CPTE, CSWAE, LCSPC

SEGURIDAD CERO

Santiago Muñoz
Ethical Hacking Expert

- Años de experiencia en ejercicios de Red Team para entidades gubernamentales, financiero, etc.
- Especializado en el hacking de aplicaciones web, Windows y Active Directory.
- Security researcher en Faraday
- Instructor en SEGURIDAD CERO de Ethical Hacking
- Certificaciones internacionales OSCP | CRTP | CTRE


SEGURIDAD
CERO

SEGURIDAD CERO

CLASE 1

LA METODOLOGÍA

LUNES 28 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM

NEGOCIOS

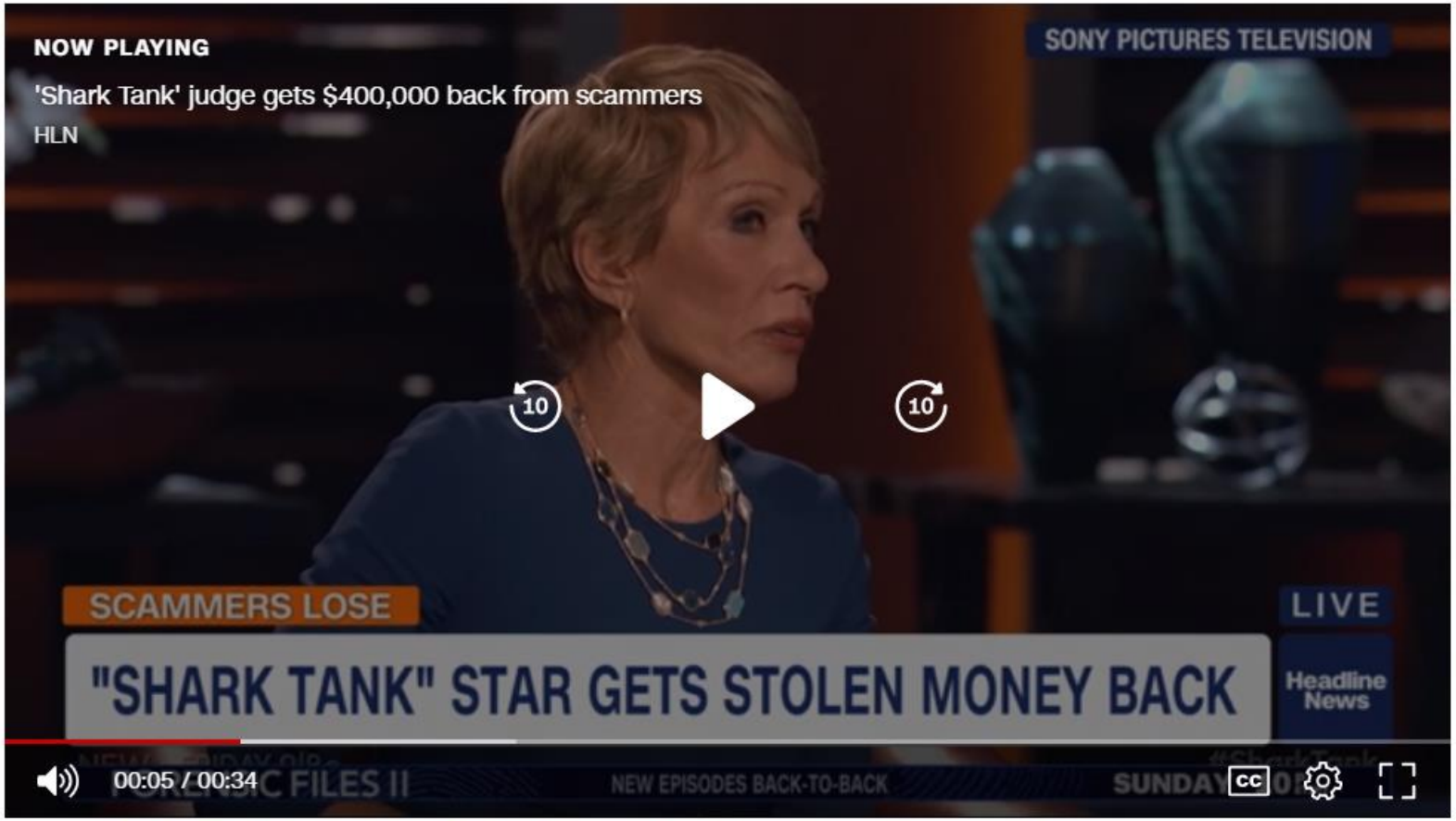
Hackers robaron US$10 millones en ataque al Banco de Chile

El caso sería el mayor ciberataque sufrido por un banco chileno, y se suma a otros contra instituciones financieras en la región y el mundo

'Shark Tank' judge Barbara Corcoran gets her $400,000 back from scammers

By Jordan Valinsky, CNN Business

Updated 1645 GMT (0045 HKT) March 3, 2020



TOP STORIES


New York judge rules Eric Trump must sit for deposition before...

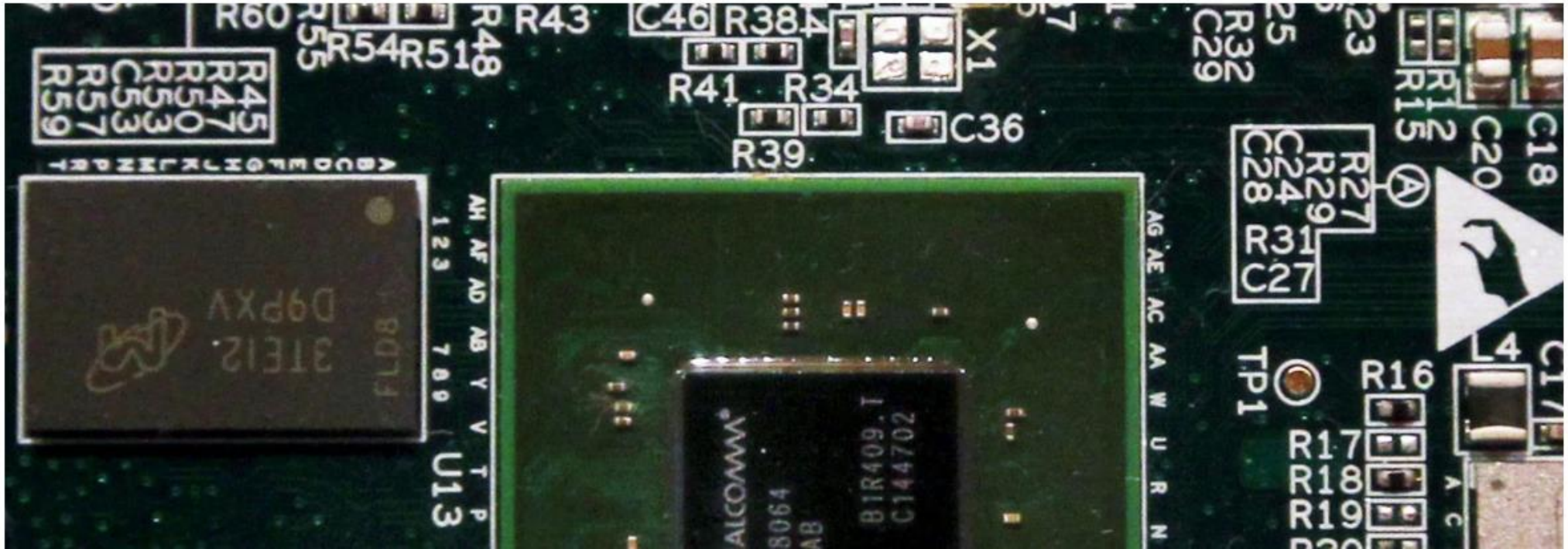

Fact check: Trump baselessly claims Democratic politicians wrote Ruth...

Recommended by Outbrain

DAN GOODIN, ARS TECHNIC A SEGURIDAD 08.10.2020 03:09 PM

Más de mil millones de dispositivos Android están en rie de datos

Qualcomm ha publicado una solución para las fallas en su chip Snapdragon, que los atacantes podrían aprovechar para mon que el teléfono no responda.



The New York Times

Two Major Saudi Oil Installations Hit by Drone Strike, and U.S. Blames Iran

A Saudi Aramco plant in Abqaiq, Saudi Arabia, was attacked early Saturday, one of two sites hit. Hamad I Mohammed/Reuters

EDITORS' PICK | 20,861 views | Feb 19, 2020, 04:37am EST

Hackers Made Tesla Cars Autonomously Accelerate Up To 85 In A 35 Zone

Davey Winder Senior Contributor ⓘ

Cybersecurity

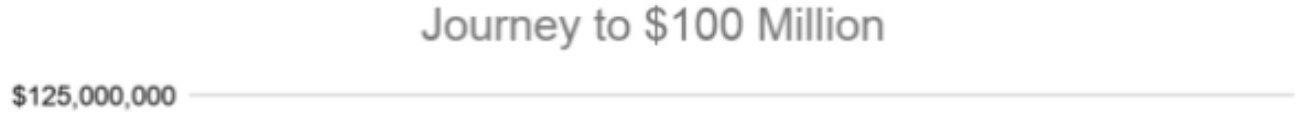
I report and analyse breaking cybersecurity and privacy stories

Featured news

Industry News
May 28, 2020

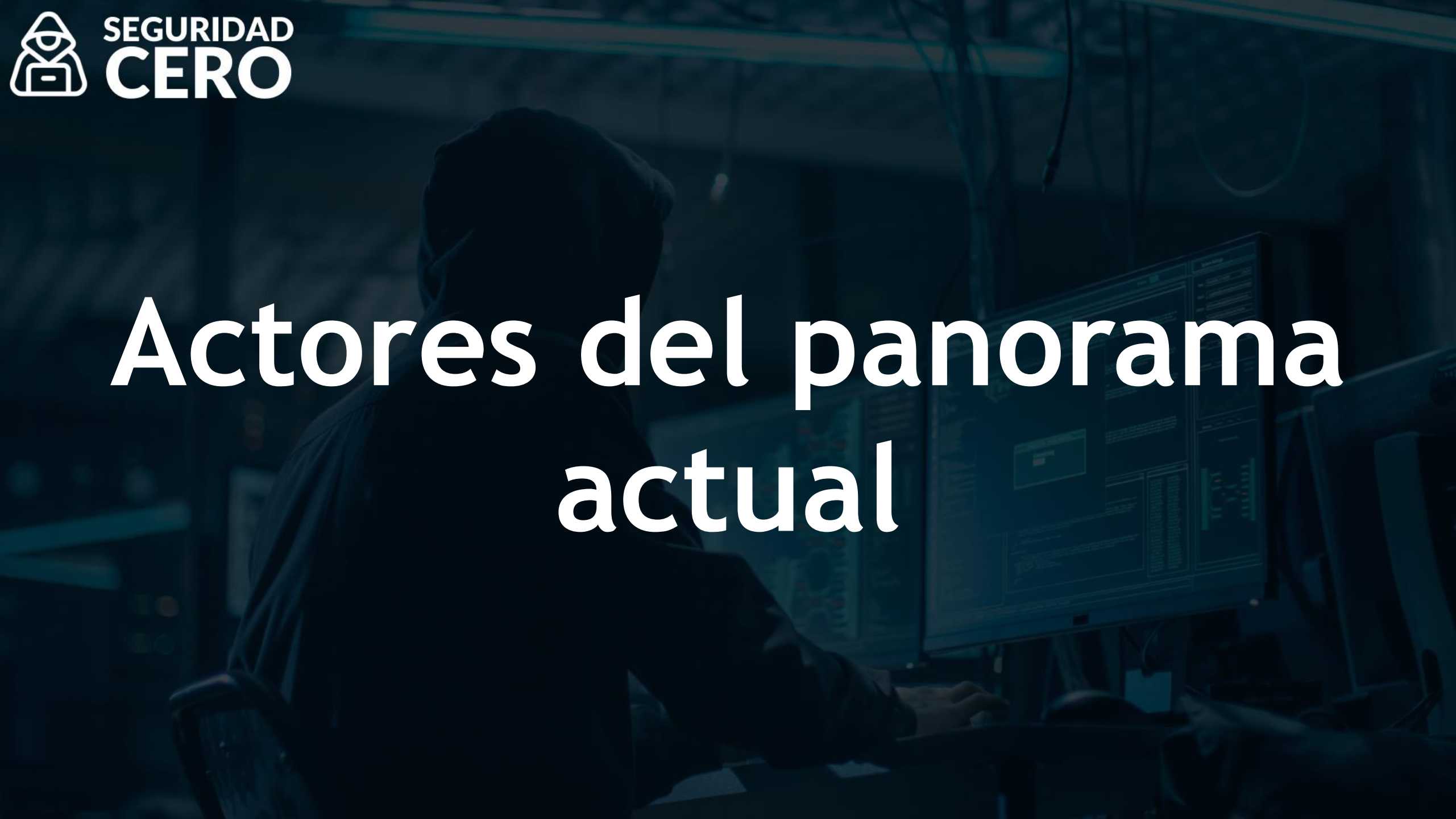
Hackers awarded $100 million in bug bounties on the HackerOne platform

HackerOne announced that hackers have earned $100 million in bug bounties on the HackerOne platform.



Better cybersecurity hinges on actual risks and addressing the
Business efficiency metrics are than detection metrics
Elasticsearch security: Understa and apply best practices
Data exfiltration: The art of dist
Cybersecurity software sales ar touch world

Spot light Elasticsearch securit your options and app practices



Actores del panorama actual

Conceptos Clave

Activo

Componente digital o físico que contiene información valorada de la organización.

Amenaza

Evento o acción que puede ocasionar un incidente de seguridad sobre un activo.

Hack Value

Nivel de atracción que tiene un activo para los cibercriminales.

Vulnerabilidad

Debilidad o fallo en la seguridad de un activo de información.

Exploit

Pieza de software diseñada para aprovechar una vulnerabilidad.

Payload

Sección de un exploit que especifica las acciones maliciosas a realizar.


SEGURIDAD
CERO
Ethical Hacking


afetypen


$3 000 000
3M Security Glass

SEGURIDAD CERO

Ethical Hacking

Es un proceso de identificación proactiva de vulnerabilidades mediante la simulación de un ataque informático con pruebas avanzadas de seguridad.

Las organizaciones se apoyan del ethical hacking ahorrar de forma efectiva el gasto asociado a las consecuencias de un ciberataque frente a la inversión efectuada para estos servicios.

Las ventajas de estas practicas implican la mejora de la postura de seguridad y la disminución del riesgo ocasionado por brechas o destrucción de datos, perdidas de disponibilidad por ataques, etc.


SEGURIDAD
CERO
Ethical Hacking

Activo

Componente digital o físico que contiene información valorada de la organización.

Amenaza

Evento o acción que puede ocasionar un incidente de seguridad sobre un activo.

Hack Value

Nivel de atracción que tiene un activo para los cibercriminales.

Vulnerabilidad

Debilidad o fallo en la seguridad de un activo de información.

Exploit

Pieza de software diseñada para aprovechar una vulnerabilidad.

Payload

Sección de un exploit que especifica las acciones maliciosas a realizar.

1
Reconocimiento

2
Escaneo

3
Enumeración

4
Analisis de Vulnerabilidades

5
Explotación

6
Reporte

ETHICAL HACKING

METODOLOGIA

Reconocimiento

SEGURIDAD CERO

Reconocimiento

Adquisición de información acerca del objetivo bajo ataque buscan información a través de fuentes abiertas de internet e interacción sigilosa con el objetivo.

Found 769 Website HTMLs, 604 Text Files, 486 PDF Files, 400 Pastes, 218 HTML Files, 32 Excel Files, 20 Word Files, 5 Database Files

Разбитая база 2018.18.07_15-23-32/225.txt [Part 15 of 39]

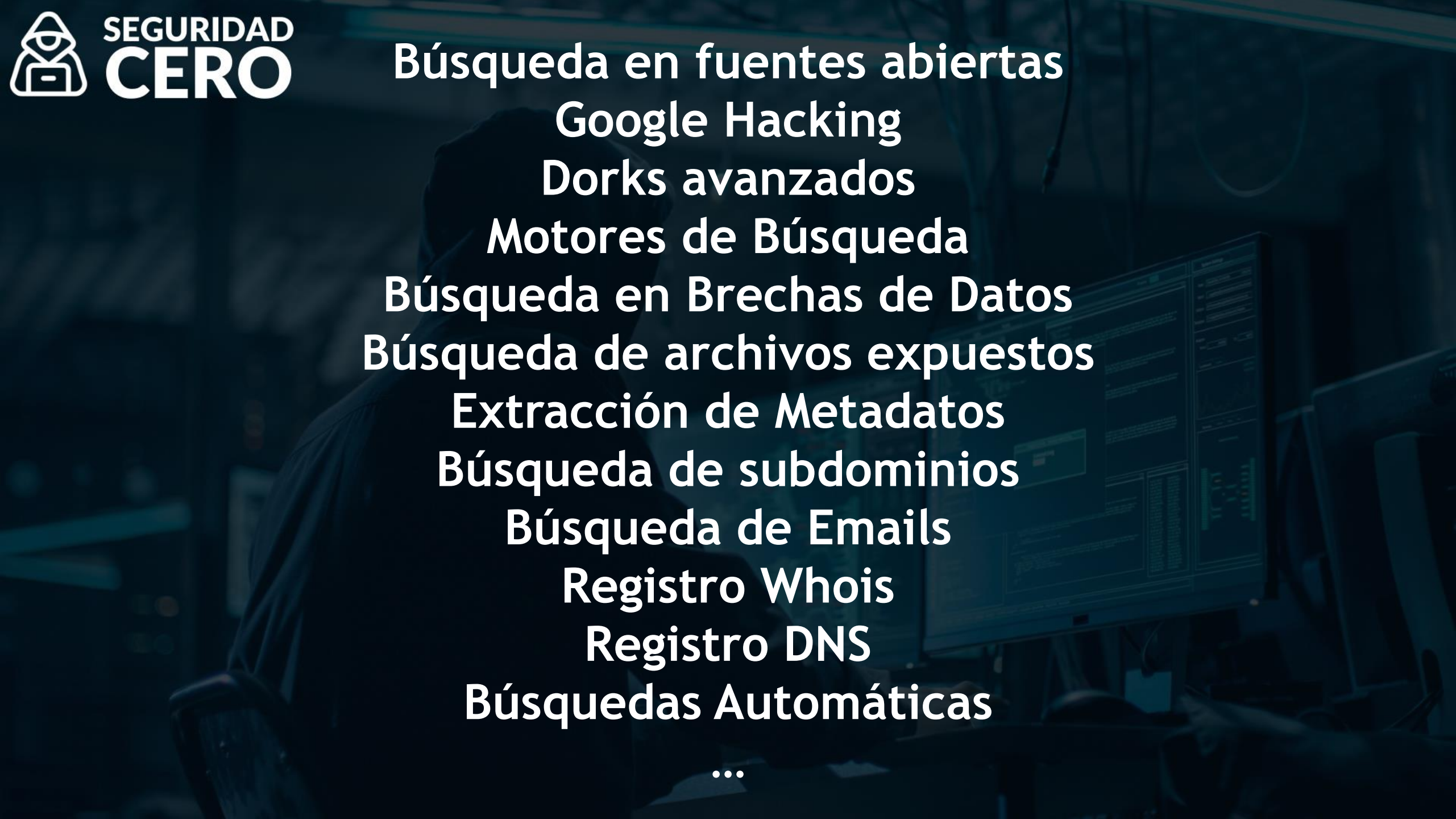
```
kevykreator@yahoo.com:paris
ramjet62@themail.com:labtech
pokerman82863@aol.com:111111
charlie@nexttonothing.net:punkfry
skyheather@neo.rr.com:pandora
hengshenwui@gmail.com:aqswdefr1234
deguinan@speakeasy.org:squirrel
daniel503@hotmail.com:deoppresso
```

GMAIL.COM.txt [Part 42 of 273]

```
macafull@gmail.com:220166
jamilmurad8@gmail.com:159532532
amateurgrlairpkt@gmail.com:KiwIPoC3
tubetone@gmail.com:01020304
yariv.nis@gmail.com:letmeinnow
tomas.samulis@gmail.com:patranka
asoberirishman32@gmail.com:typewriter
xuelongmu@gmail.com:snowdragon
```

GMAIL.COM.txt [Part 42 of 273]

```
macafull@gmail.com:220166
jamilmurad8@gmail.com:159532532
amateurgrlairpkt@gmail.com:KiwIPoC3
tubetone@gmail.com:01020304
yariv.nis@gmail.com:letmeinnow
```


SEGURIDAD
CERO
Búsqueda en fuentes abiertas
Google Hacking
Dorks avanzados
Motores de Búsqueda
Búsqueda en Brechas de Datos
Búsqueda de archivos expuestos
Extracción de Metadatos
Búsqueda de subdominios
Búsqueda de Emails
Registro Whois
Registro DNS
Búsquedas Automáticas
...

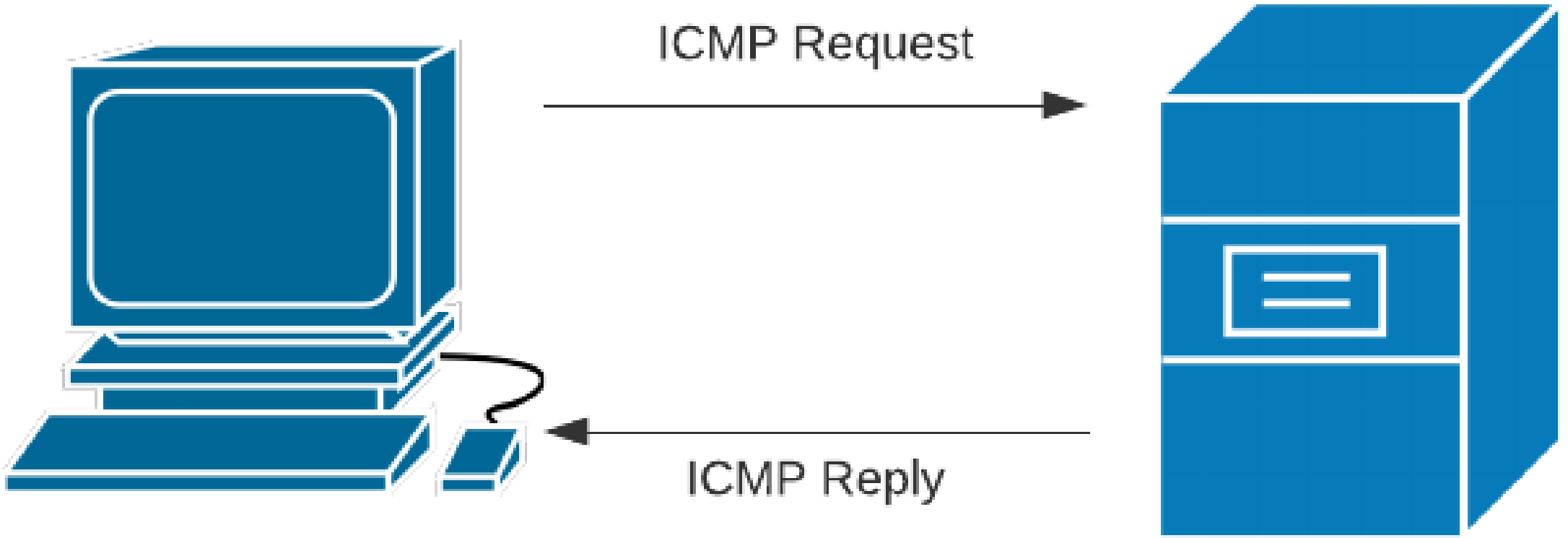
Escaneo

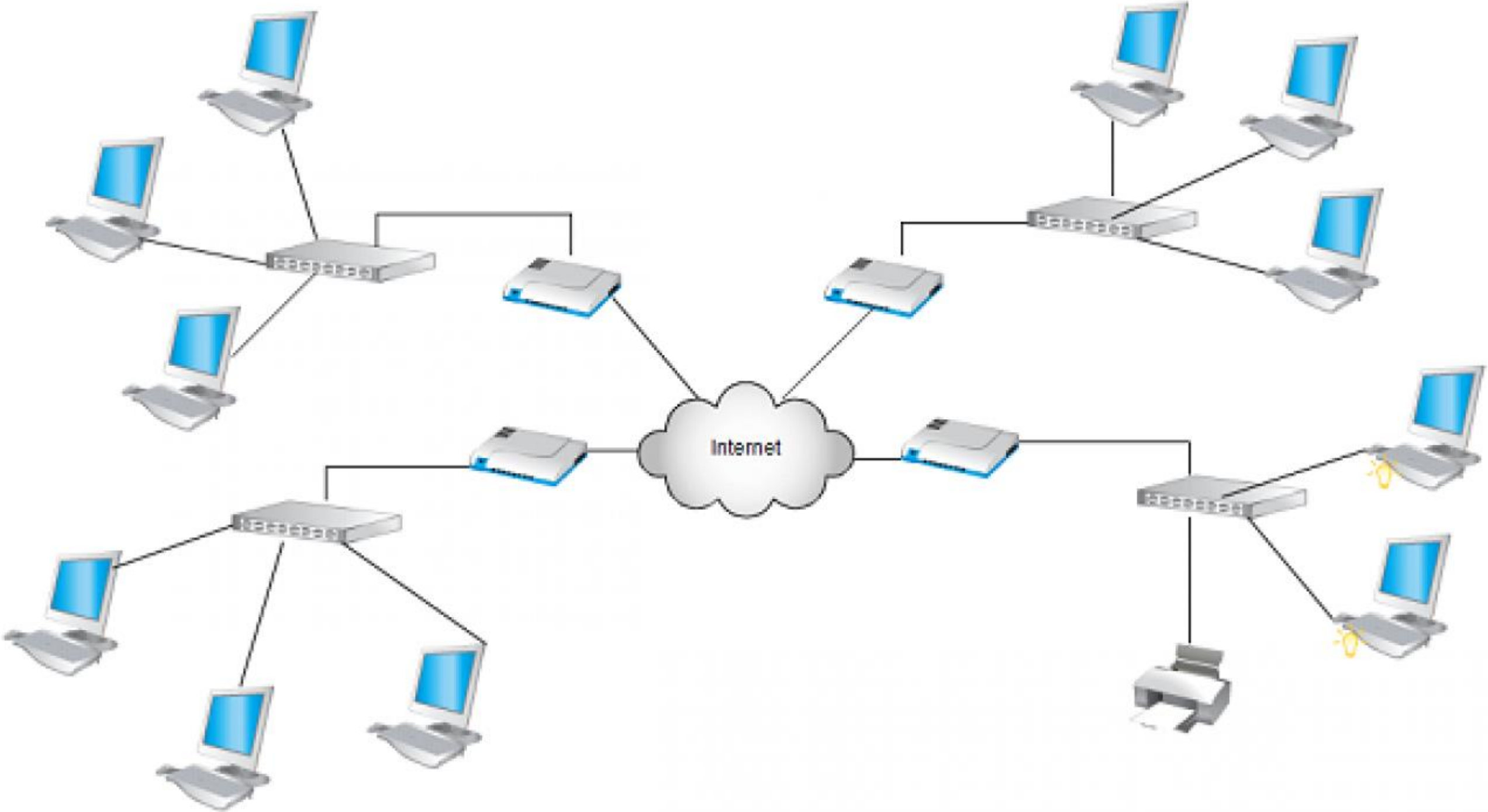

97.5
98.2
16:55:51
97.5
98.2
16:55:51
MEDICORE
Alarm(°F)
Alarm Sound
99.5
Display(°F)
Bell Sound
94.1
Auto Save
SAVE

SEGURIDAD CERO

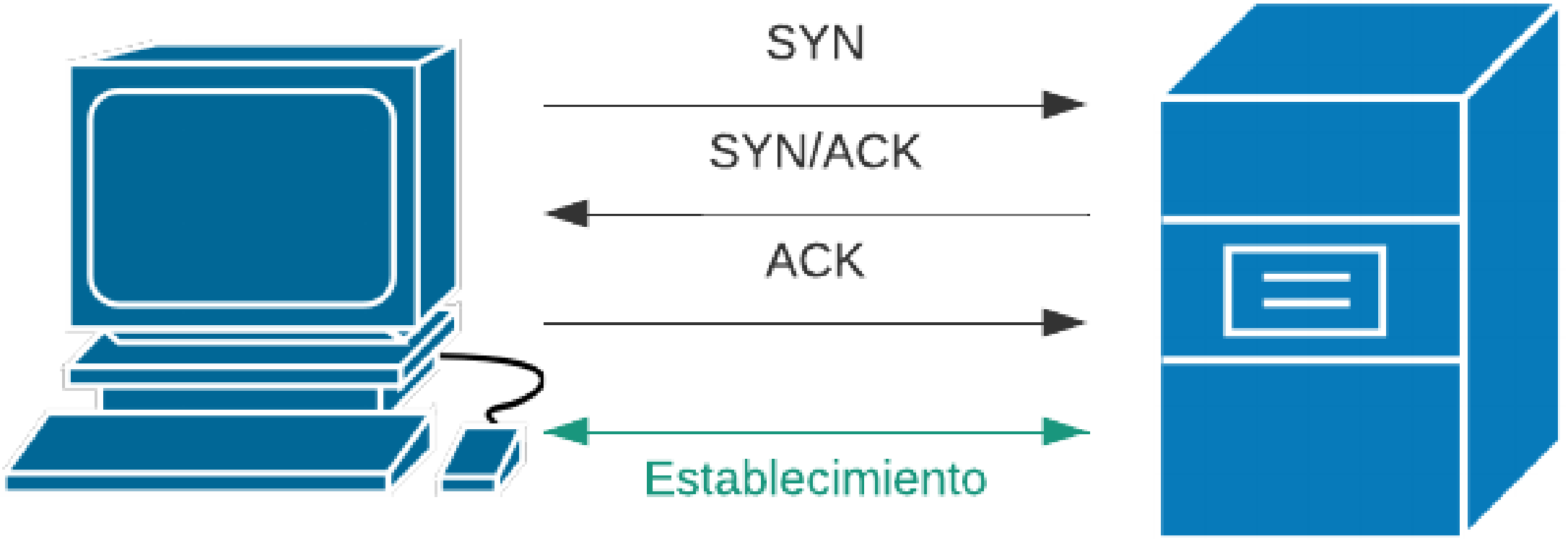
Escaneo

Escaneo de red sobre el objetivo en base a la información obtenida en la etapa de reconocimiento en busca de dispositivos, sistemas operativos, puertos y servicios

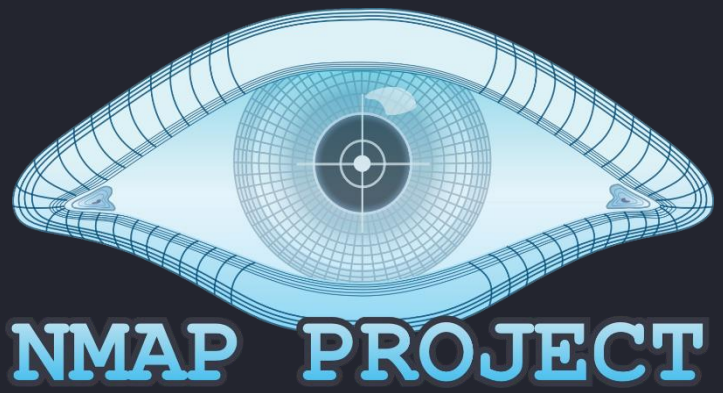

ICMP Request
ICMP Reply


Internet

TCP 1-65535
UDP 1-65535



```
kali@kali:~$ nmap -sV -p- -T5 10.0.2.4
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 19:44 EDT
Nmap scan report for 10.0.2.4
Host is up (0.00094s latency).
Not shown: 65506 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)
111/tcp   open  rpcbind     2 (RPC #100000)
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)
512/tcp   open  exec        netkit-rsh rexecd
513/tcp   open  login       OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell   Metasploitable root shell
2049/tcp  open  nfs         2-4 (RPC #100003)
2121/tcp  open  ftp         ProFTPD 1.3.1
3306/tcp  open  mysql       MySQL 5.0.51a-3ubuntu5
3632/tcp  open  distccd     distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc         VNC (protocol 3.3)
6000/tcp  open  X11         (access denied)
6667/tcp  open  irc         UnrealIRCd (Admin email admin@Metasploitable.LAN)
6697/tcp  open  irc         UnrealIRCd
8180/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
8787/tcp  open  drb         Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
33466/tcp open  nlockmgr    1-4 (RPC #100021)
```



Enumeración

SEGURIDAD CERO

Enumeración

Obtención de información detallada del objetivo bajo ataque interactuando profundamente con los punto de entrada que ofrece. Esta es el paso mas importante.

```
kali@kali:~$ nmap -script smb-os-discovery 10.0.2.9 -p445 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 22:55 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00078s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: LUISRODRIGUEZ; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: luisrodriguez
|   NetBIOS computer name: LUISRODRIGUEZ\x00
kali@kali:~$ nmap -script smb-protocols 10.0.2.9 -p445 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 22:48 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00073s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
Service Info: Host: LUISRODRIGUEZ; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb-protocols:
|   dialects:
|     NT LM 0.12 (SMBv1) [dangerous, but default]
|     2.02
|_    2.10
```

Análisis

SEGURIDAD CERO

Análisis de Vulnerabilidades

En esta etapa se identifican y categorizan las vulnerabilidades asociadas a nuestro objetivo utilizando como base toda la información recopilada en los pasos anteriores.

SEGURIDAD CERO

Common Vulnerability Score System (CVSS)

Sistema de valoración de la criticidad de las vulnerabilidades basada en las características y propiedades de la vulnerabilidad y se obtiene como resultado una puntuación numérica.
https://www.first.org/cvss/calculator/3.1

Severity / Severidad	Puntuación
None / Ninguna	0.0
Low / Baja	0.1 – 3.9
Medium / Media	4.0 – 6.9
High / Alta	7.0 – 8.9
Critical / Critica	9.0 – 10.0

FOLDERS
My Scans
All Scans
Trash

RESOURCES
Policies
Plugin Rules
Scanners

TENABLE
Community
Research

Tenable News

Tenable Research Discloses Multiple Vulnerabilitie...

Read More

metasploitable2

‹ Back to My Scans

Configure | Audit Trail | Launch | Report

Nessus® vulnerability scanner

Hosts 1 | **Vulnerabilities** 55 | Remediations 4 | History 1

Filter | Search Vulnerabilities | 55 Vulnerabilities

Sev	Name	Family	Count
CRITICAL	Bind Shell Backdoor De...	Backdoors	1
CRITICAL	Debian OpenSSH/Ope...	Gain a shell remotely	1
CRITICAL	NFS Exported Share Inf...	RPC	1
CRITICAL	rexecd Service Detection	Service detection	1
CRITICAL	Unix Operating System ...	General	1
CRITICAL	VNC Server 'password' ...	Gain a shell remotely	1
MIXED	4 ISC Bind (Multiple...	DNS	4
MIXED	3 Apache Tomcat (...	Web Servers	3
MIXED	3 Web Server (Multi...	Web Servers	3

Scan Details

Policy:	Advanced Scan
Status:	Completed
Scanner:	Local Scanner
Start:	June 20 at 3:09 PM
End:	June 20 at 3:14 PM
Elapsed:	4 minutes

Vulnerabilities

```
kali@kali:~$ nmap -script vuln 10.0.2.9 -p445 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 22:43 EDT
Nmap scan report for 10.0.2.9
Host is up (0.0011s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
Service Info: Host: LUISRODRIGUEZ; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.20 seconds
```

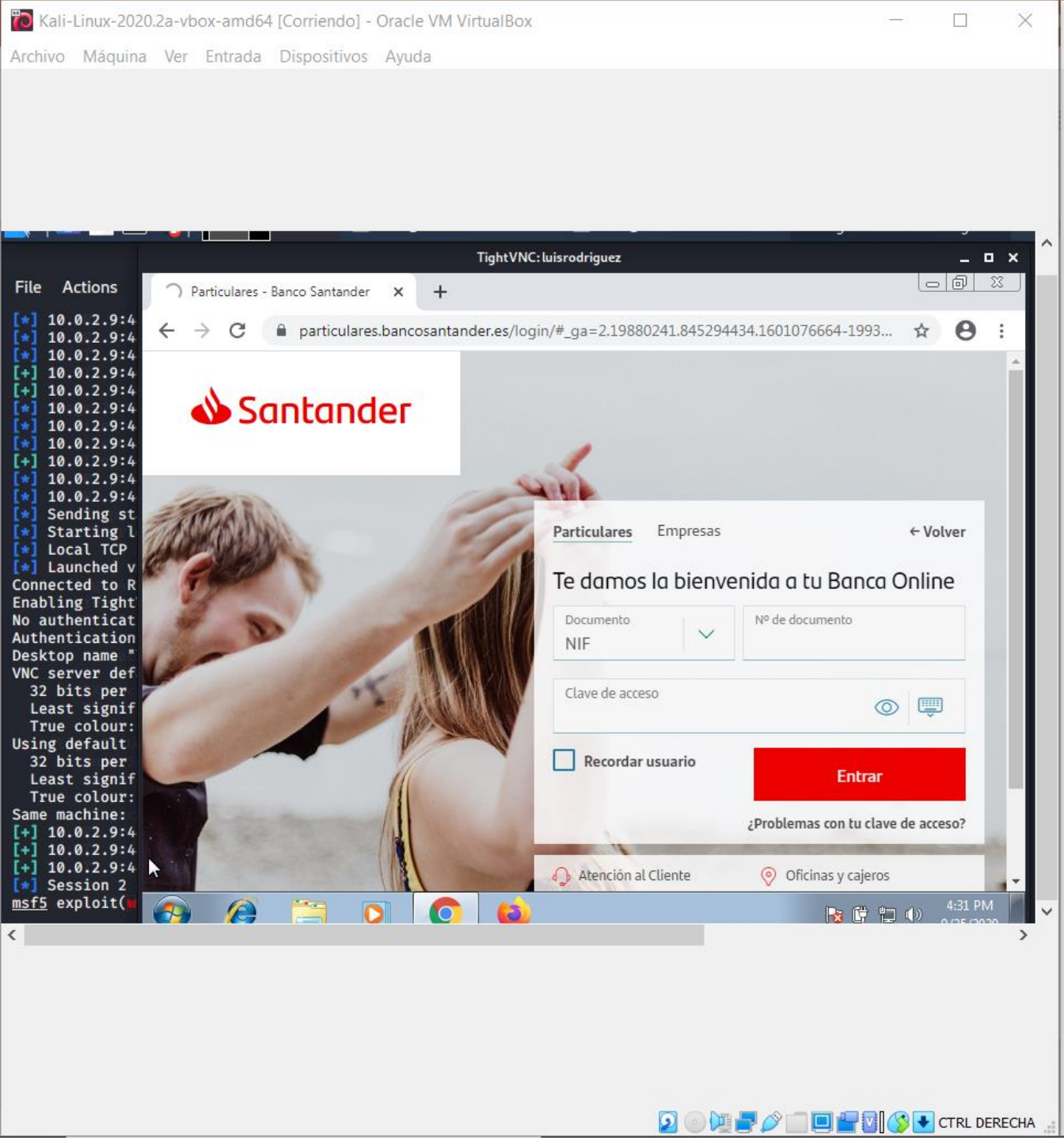
Explotación

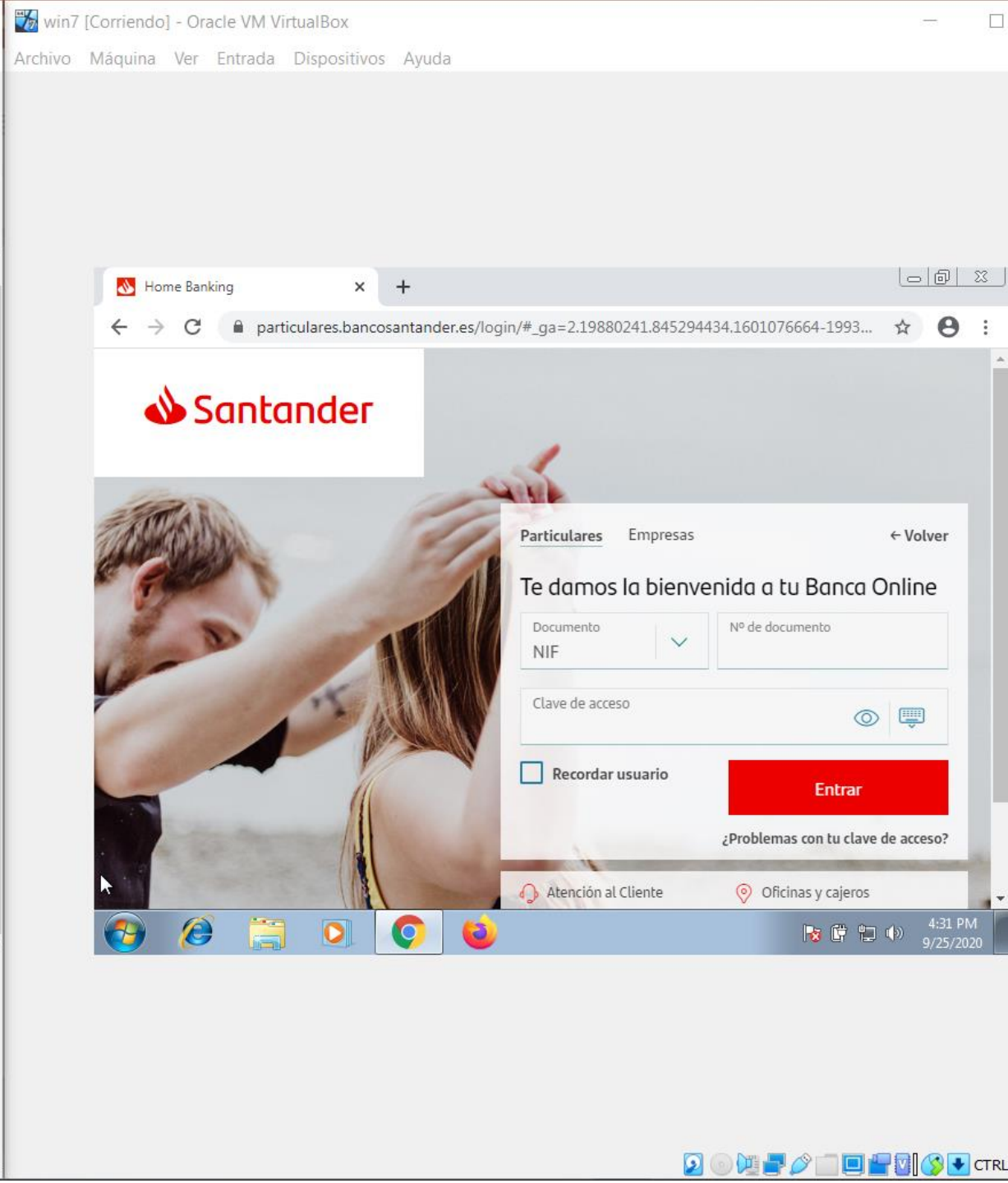
SEGURIDAD CERO

Explotación

Ejecución del ataque explotando las vulnerabilidades identificadas. Esta etapa es de ejecución delicada, debe ser coordinada y realizada de manera milimétrica.

```
kali@kali:~$ msfconsole


                 .                                         .
 .

     dBBBBBBb  dBBBP dBBBBBBP dBBBBBb  .                       o
      '   dB'                     BBP
    dB'dB'dB' dBBP     dBP     dBP BB
   dB'dB'dB' dBP      dBP     dBP  BB
  dB'dB'dB' dBBBBP   dBP     dBBBBBBB

                                   dBBBBBP  dBBBBBb  dBP    dBBBBP dBP dBBBBBBP
          .                  .                  dB' dBP    dB'.BP
                             |       dBP    dBBBB' dBP    dB'.BP dBP    dBP
                           --o--    dBP    dBP    dBP    dB'.BP dBP    dBP
                             |     dBBBBP dBP    dBBBBP dBBBBP dBP    dBP

                                                                    .
                .
        o                  To boldly go where no
                            shell has gone before


       =[ metasploit v5.0.87-dev                          ]
+ -- --=[ 2006 exploits - 1096 auxiliary - 343 post       ]
+ -- --=[ 562 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: View missing module options with show missing

msf5 >
```


Kali-Linux-2020.2a-vbox-amd64 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
TightVNC: luisrodriguez
File Actions
[*] 10.0.2.9:4
[+] 10.0.2.9:4
[*] Starting l
[*] Local TCP
[*] Launched v
Connected to R
Enabling Tight
No authenticat
Authentication
Desktop name "
VNC server def
32 bits per
Least signif
True colour:
Using default
32 bits per
Least signif
True colour:
Same machine:
[*] Session 2
msf5 exploit(
Particulares - Banco Santander
particulares.bancosantander.es/login/#_ga=2.19880241.845294434.1601076664-1993...
Santander
Particulares
Empresas
← Volver
Te damos la bienvenida a tu Banca Online
Documento
NIF
Nº de documento
Clave de acceso
Recordar usuario
Entrar
¿Problemas con tu clave de acceso?
Atención al Cliente
Oficinas y cajeros
4:31 PM
CTRL DERECHA


win7 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Home Banking
particulares.bancosantander.es/login/#_ga=2.19880241.845294434.1601076664-1993...
Santander
Particulares
Empresas
← Volver
Te damos la bienvenida a tu Banca Online
Documento
NIF
Nº de documento
Clave de acceso
Recordar usuario
Entrar
¿Problemas con tu clave de acceso?
Atención al Cliente
Oficinas y cajeros
4:31 PM
9/25/2020
CTRL

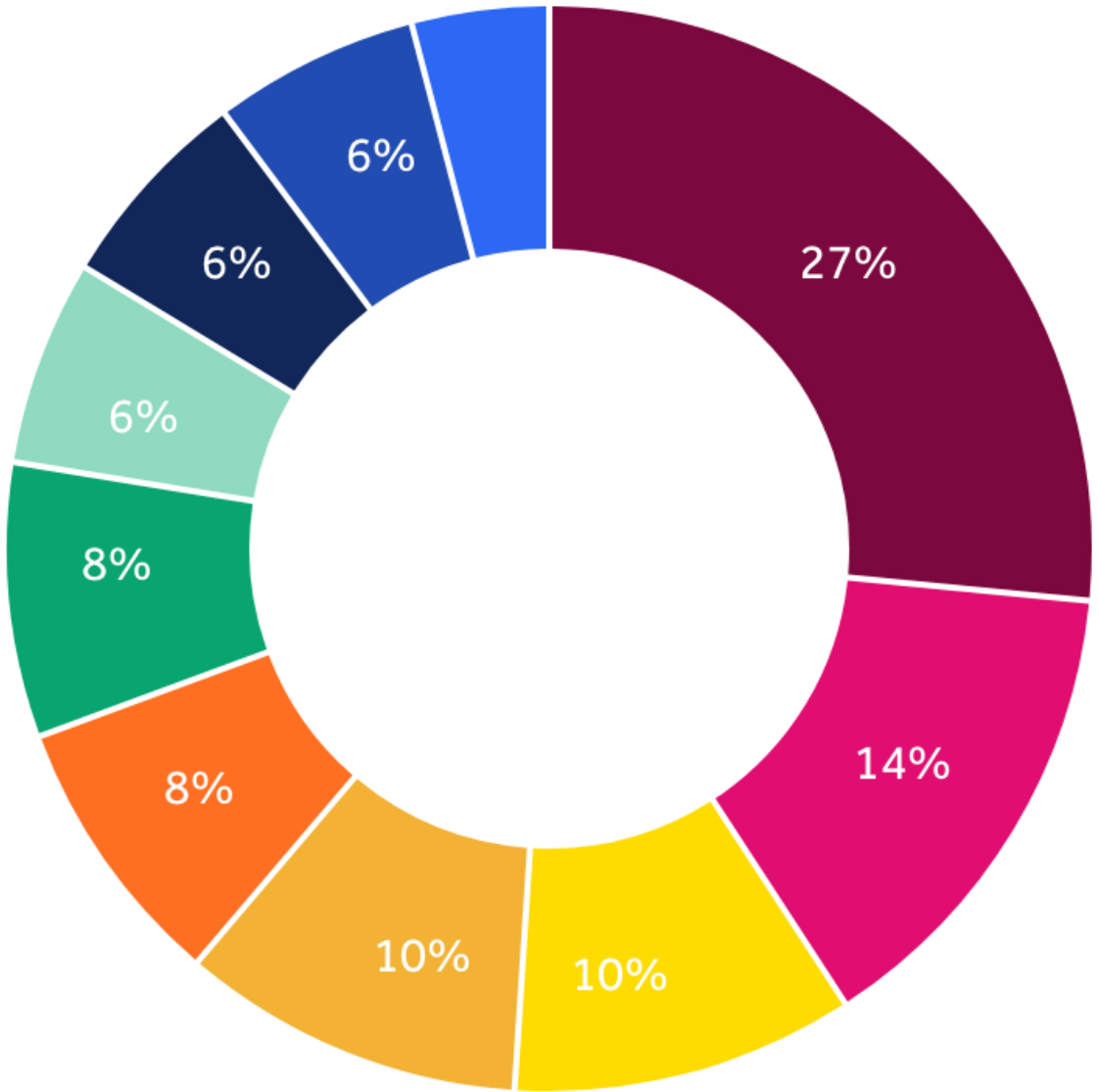
Reporte

SEGURIDAD CERO

Reporte

Durante el reporte todas las vulnerabilidades validadas, sus respectivas evidencias y recomendaciones son documentadas y presentadas

Valid Reports Bounty Amounts



- Other
- No Weakness
- Improper Authentication - Generic
- Open Redirect
- Improper Access Control - Generic
- Violation of Secure Design Principles
- Business Logic Errors
- Information Disclosure
- Server-Side Request Forgery (SSRF)
- Cross-Site Request Forgery (CSRF)

SEGURIDAD CERO

CLASE 1

LA METODOLOGÍA

LUNES 28 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM


Curso Online
Ethical Hacking
Professional
Más Información Aquí

SEGURIDAD CERO

CURSO GRATIS
ETHICAL HACKING

LUNES 28 SEPTIEMBRE MARTES 29 SEPTIEMBRE
MIÉRCOLES 30 SEPTIEMBRE

CRI	GTM	HND	MEX	PER
6:00 PM	6:00 PM	6:00 PM	7:00 PM	7:00 PM
				

COL	ECU	PAN	PRY	CHL
7:00 PM	7:00 PM	7:00 PM	8:00 PM	8:00 PM
				

BOL	VEN	DOM	ARG	URY
8:00 PM	8:00 PM	8:00 PM	9:00 PM	9:00 PM