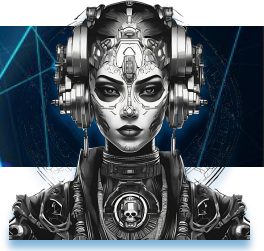
Confesiones y anécdotas de un ex-**APT**

Javier Marcos
@javutin
@jmpsec

Confesiones y anécdotas de un ~~ex~~-APT

Javier Marcos
@javutin
@jmpsec

Confesiones y anécdotas de un ~~ex~~-APT



```
$ whoami
```

Siemens (2006-2007)

IBM (2007-2011)

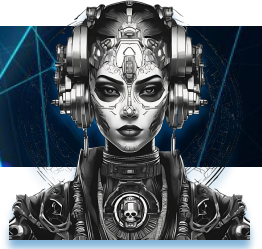
Facebook (2011-2016)

Uber (2016-2018)

Airbnb (2018-2019)

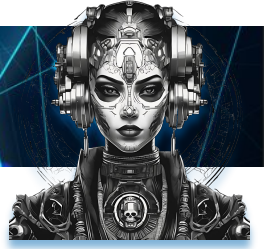
BitMEX (2019-2021)

JMP Security (2021-now)



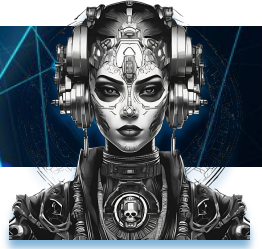
$ whoami

Staff Security Engineer



Agenda

- Desmitificando APTs
  - Definición, fases y ejemplos
- CCDC: Collegiate Cyber Defense Competition
  - Experiencia personal y APTs
- Stanza
  - Liberación de implante y C2
- Preguntas

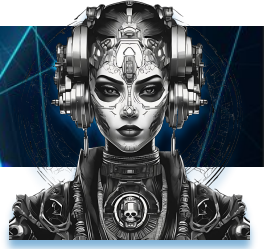


¿Qué es un APT?

- **A**dvanced **P**ersistent **T**hreat

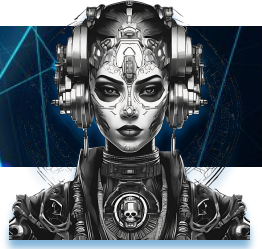
--> *"Ataque cibernético prolongado y dirigido, muchas veces respaldado por estados-nación o grupos organizados"*

ChatGPT



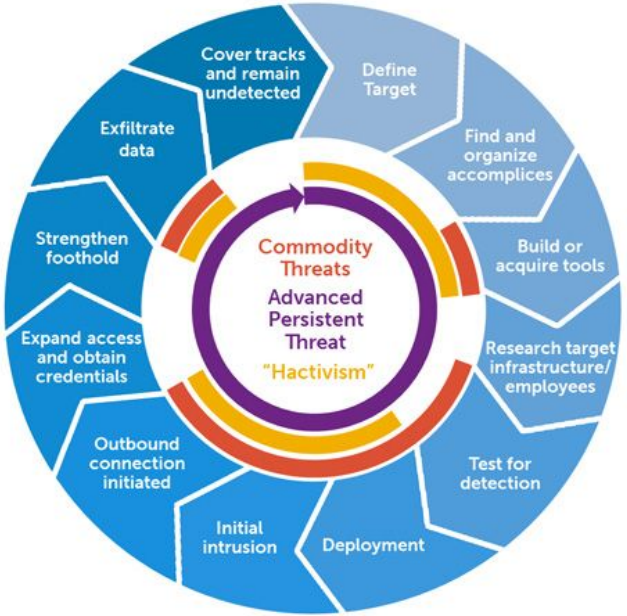
Características de un APT

- Uso de técnicas **sofisticadas**, a menudo con herramientas no públicas hechas a medida
- Mantienen el acceso durante un **largo periodo de tiempo**, sin ser detectados
- Buscan robar información, dinero, espiar o causar algún tipo de **daño**

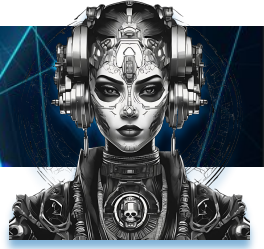


Ciclo de vida de un APT

- Infiltración Inicial y Establecimiento
  - ⇢ Reconocimiento, Entrega, Persistencia
- Expansión y Control
  - ⇢ Privesc, Movimiento lateral, C2
- Ejecución y Evasión
  - ⇢ Exfiltración, Borrado de huellas, Latencia

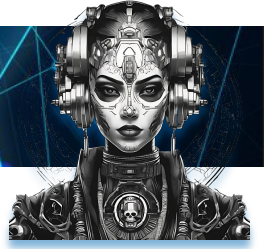


https://en.wikipedia.org/wiki/Advanced_persistent_threat



Clasificación de APTs

- Por **país**
  - China, Rusia, Irán, Corea del Norte, USA, Israel…
- Por **nombre**
  - Red Apollo, Elfin Team, Lazarus, Fancy Bear, Equation Group…
- Por **numeración**
  - APT[1-30], APT3[3-5], APT3[7-8]…



Clasificación de APTs

- Por APT-SIG (**Security Interest Group**)
  - Mandiant
  - CrowdStrike
  - MITRE
  - Kaspersky
  - FireEye
  - US-CERT
  - …

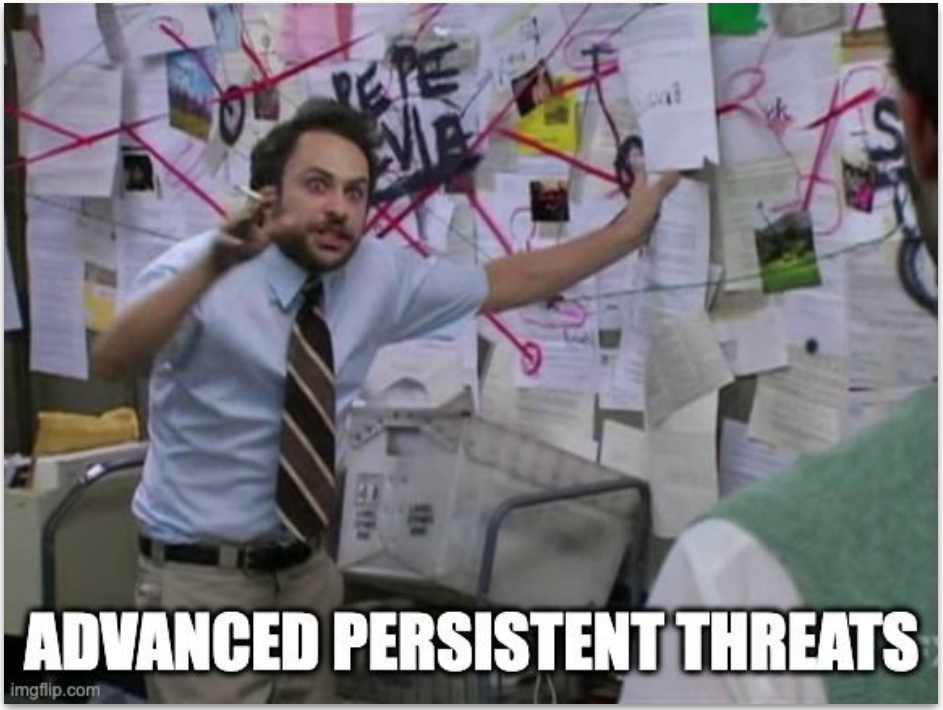
https://attack.mitre.org/groups/

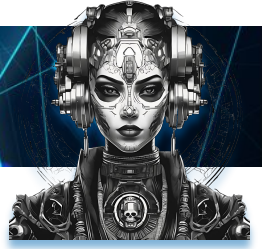
https://www.crowdstrike.com/adversaries/

https://apt.securelist.com/

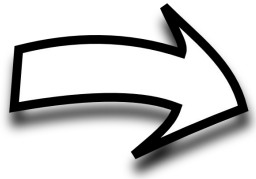
https://cloud.google.com/security/resources/insights/apt-groups

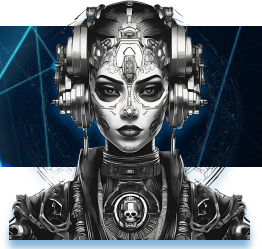
Confesiones y anécdotas de un ~~ex~~-APT



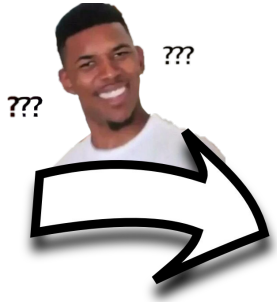


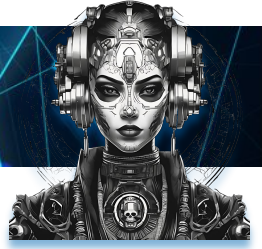
Entrenamiento contra APTs





Entrenamiento contra APTs?





(CTF inverso)

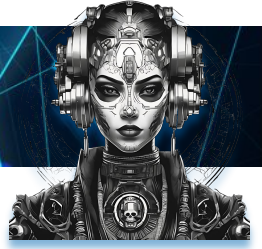
Collegiate Cyber Defense Competition

- *Campeonato de Ciberdefensa Universitaria*

  - → Estudiantes tienen que **defender** una red empresarial realista bajo ataque (2 días)
  - → Rondas clasificatorias regionales y finales nacionales
  - → Sponsors institucionales y privados

CCDC

https://www.nationalccdc.org/



(CTF inverso)

Collegiate Cyber Defense Competition

- *Campeonato de Ciberdefensa Universitaria*

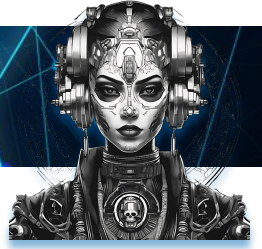
→ 10 **Blue** Teams de 8-10 estudiantes

→ Cada **Blue** Team tiene 2 personas del **Red** Team
  - Windows / Linux

→ Se realiza durante 2 días, limitado a 8 horas
  - Se corta el acceso a los participantes

CCDC

https://www.nationalccdc.org/

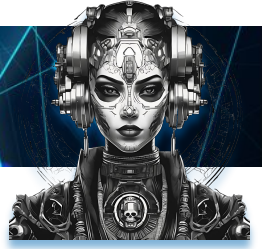


CCDC: Equipos

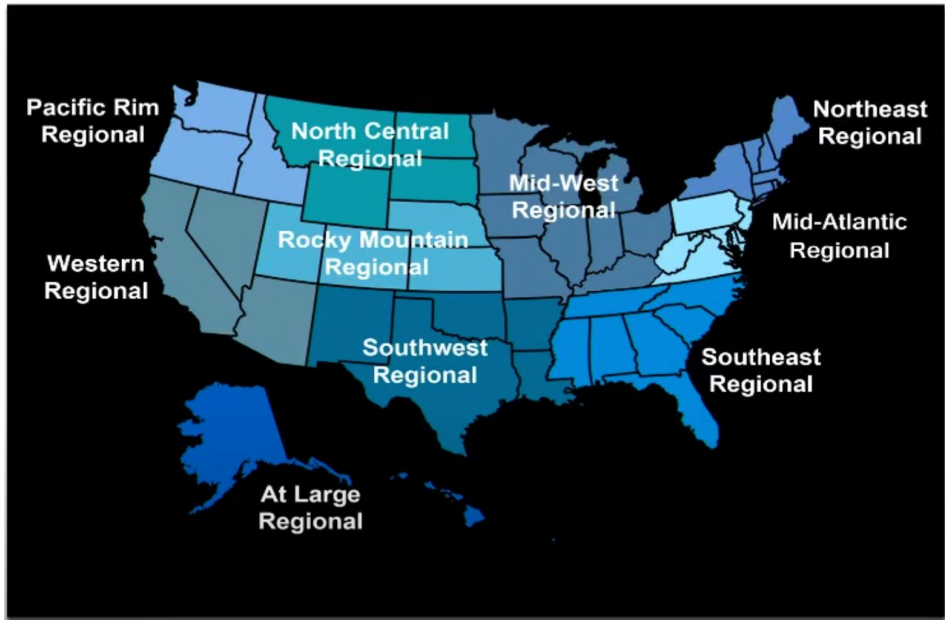
- **Blue** Teams (Defensa)
- **Red** Team (Ataque, APT)
- **Black** Team (Infra)
- **White** / **Gold** / **Orange** (Operaciones)

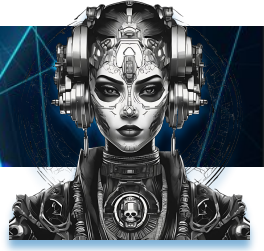
CCDC NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

https://www.nationalccdc.org/

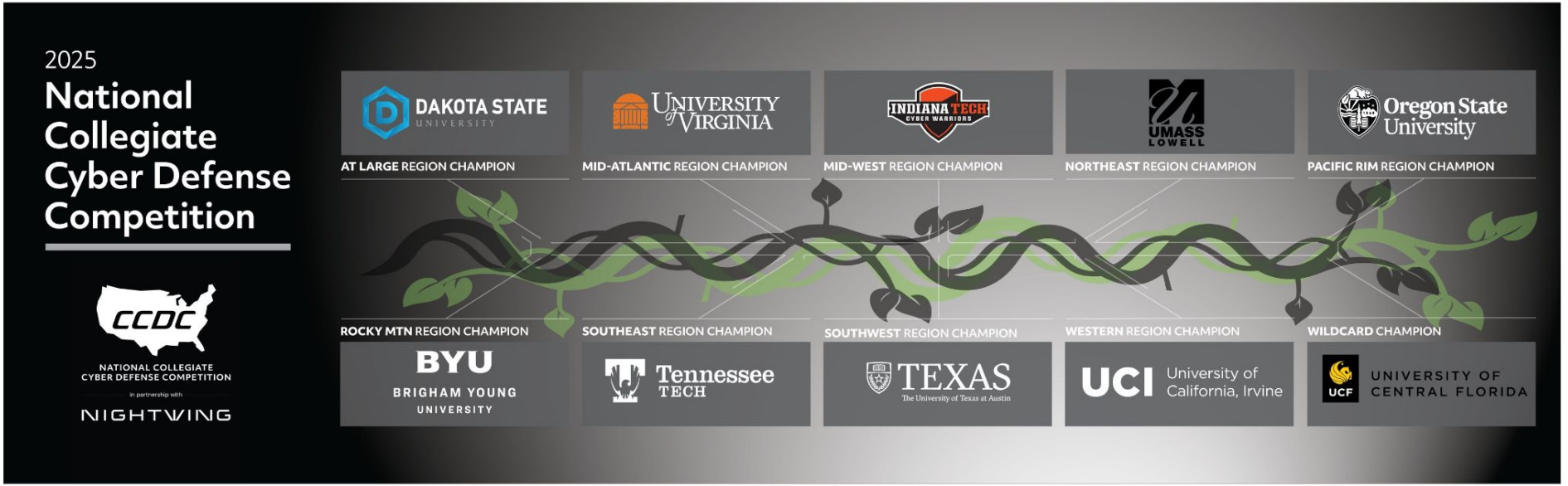


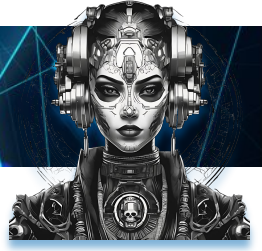
CCDC: Clasificatorias Regionales



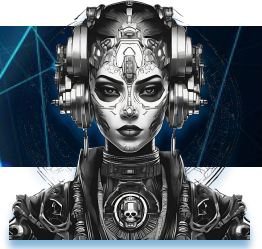


CCDC: Finales Nacionales

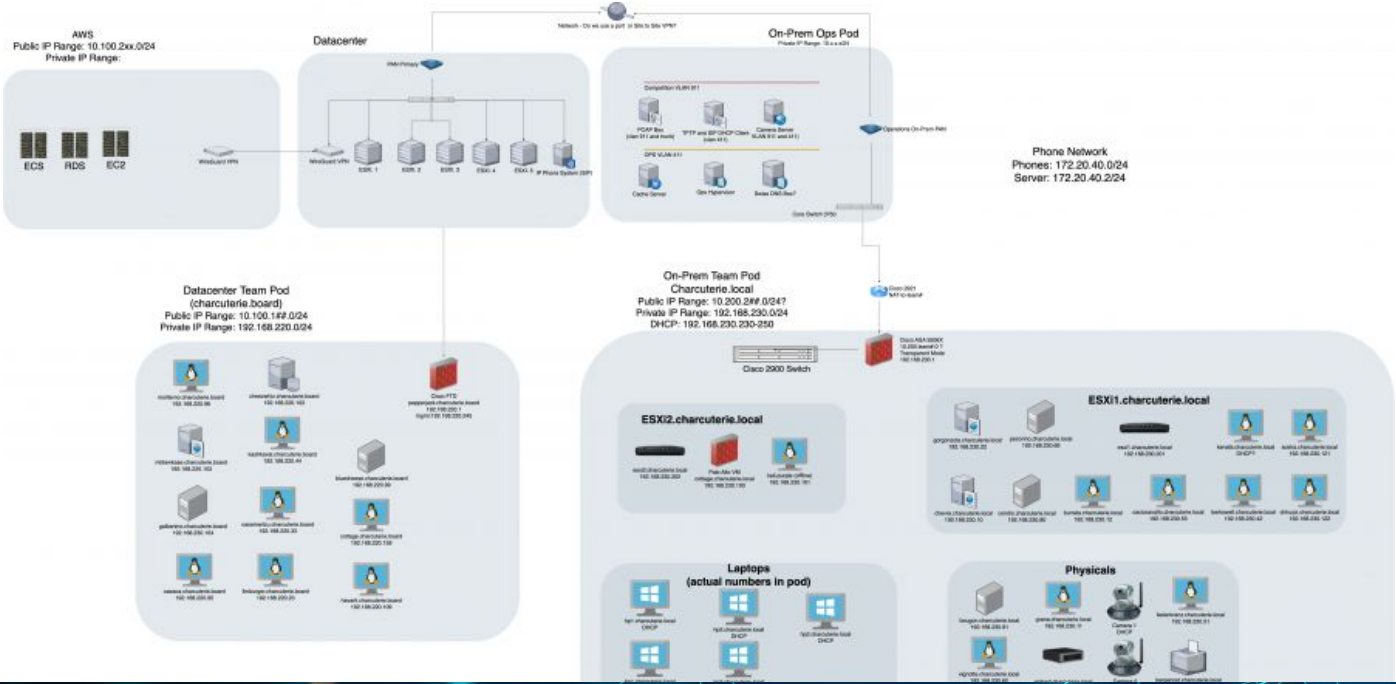


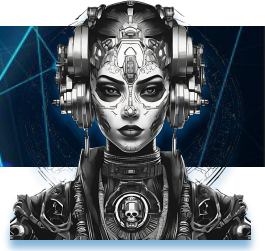


CCDC: Sponsors

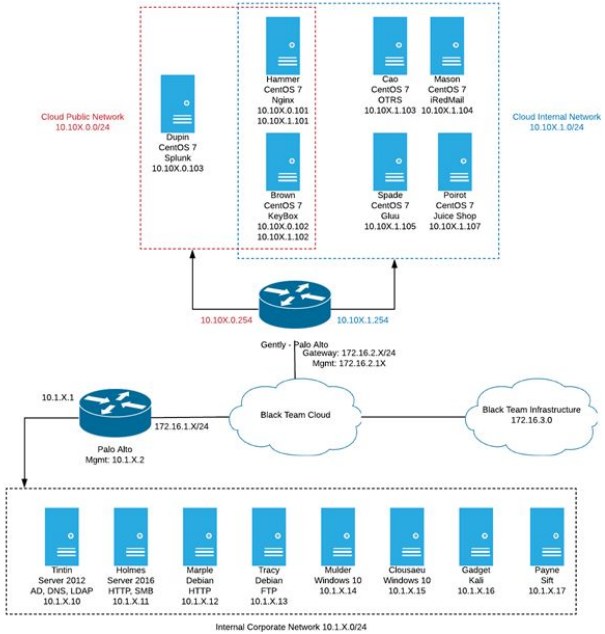


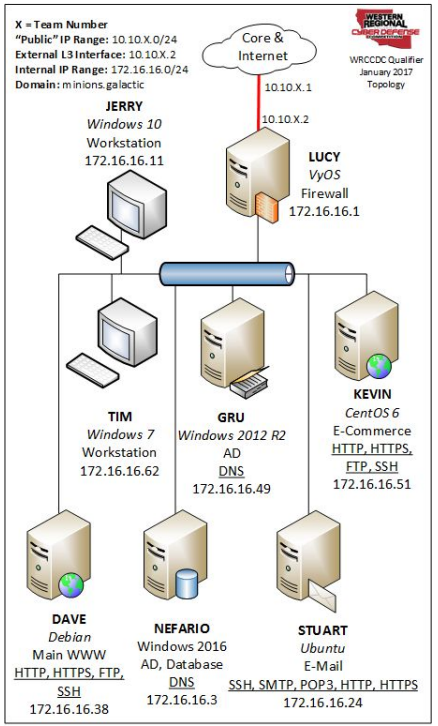
CCDC: Infra (Blue Team)

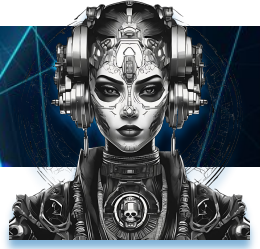




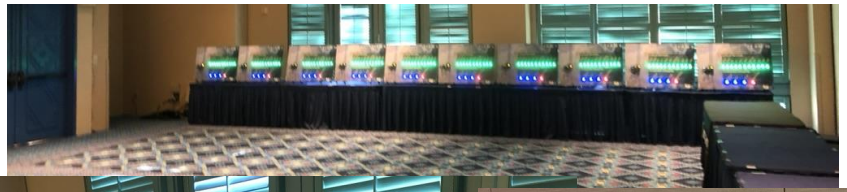
CCDC: Infra (Blue Team)







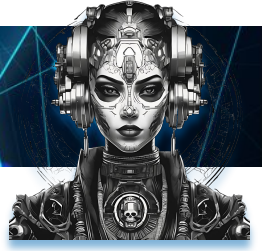
CCDC: Infra




TEAM 5
VOLITECH
Critical Services
WWW
E-COM
DNS
FTP
POP3
SMTP
Help Desk
SSH1
SSH2
SSH3
HRM
Corporate Integrity
Intellectual Property
HIPAA
Financial
Active Incident

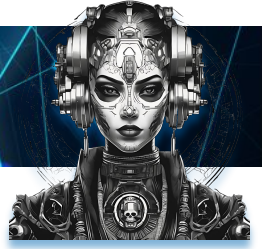

TEAM 4
Critical Services
Corporate Integrity


TEAM 1
Critical Services
Retail Locations



CCDC: Red Team

- Regionales (**Voluntarios**) y Nacionales (**Selección**)
  - --> Profesionales de Seguridad Ofensiva
  - --> Profesionales de Seguridad
  - --> Profesionales++

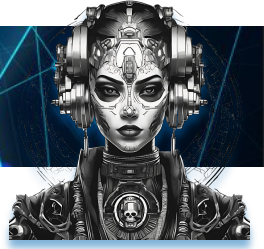


CCDC: Red Team

- Regionales (**Voluntarios**) y Nacionales (**Selección**)
  - --> Profesionales de Seguridad Ofensiva
  - --> Profesionales de Seguridad
  - --> Profesionales++

WRCCDC: 2014-2018

NCCDC: 2017-2020, 2025!



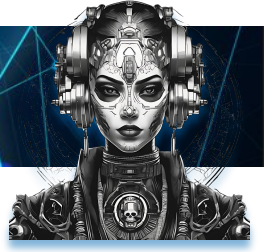
CCDC: Infra (Red Team)

NATIONAL COLLEGIATE CYBER DEFENSE COMPETITION

There will be 10 teams in this year's NCCDC with the following subnets:

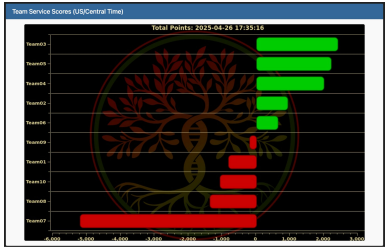
Team 1 - 10.10.10.X, 172.16.10.X
Team 2 - 10.20.20.X, 172.16.20.X
Team 3 - 10.30.30.X, 172.16.30.X
Team 4 - 10.40.40.X, 172.16.40.X
Team 5 - 10.50.50.X, 172.16.50.X
Team 6 - 10.60.60.X, 172.16.60.X
Team 7 - 10.70.70.X, 172.16.70.X
Team 8 - 10.80.80.X, 172.16.80.X
Team 9 – 10.90.90.X, 172.16.90.X
Team 10 – 10.100.100.X, 172.16.100.X

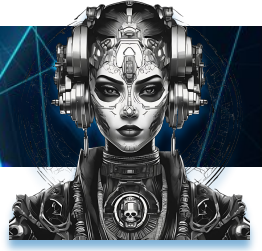
```
arctu-ssh2 - Linux - 172.16.X0.110 - Port 22
blog-http - Windows - 172.16.X0.125 - Port 80
ceres-ssh2 - Linux - 10.X0.X0.26 - Port 22
doli-http - Linux - 172.16.X0.105 - Port 80
emr-http - Linux - 172.16.X0.120 - Port 80
fin-http - Linux - 10.X0.X0.18 - Port 80
galaA-http - Linux - 172.16.X0.115 - Port 80
galax-http - Linux - 172.16.X0.115 - Port 8080
ganym-ssh2 - Linux - 10.X0.X0.21 - Port 22
gemini-pop3 - Linux - 10.X0.X0.6 - Port 110
gemini-smtp - Linux - 10.X0.X0.6 - Port 25
hrm-http - Linux - 10.X0.X0.12 - Port 80
labs-http - Linux - 172.16.X0.135 - Port 80
polar-ssh2 - Linux - 172.16.X0.115 - Port 22
rigel-ftp - Linux - 10.X0.X0.27 - Port 21
rigel-ssh2 - Linux - 10.X0.X0.27 - Port 22
sable-ssh2 - Linux - 172.16.X0.140 - Port 22
shop-http - Linux - 10.X0.X0.24 - Port 80
sirius-dns - Windows - 10.X0.X0.5 - Port 53
supp-http - Windows - 10.X0.X0.33 - Port 80
tools-http - Linux - 172.16.X0.110 - 80
tools-Mhttp - Linux - 172.16.X0.110 - 9090
www-http - Linux - 10.X0.X0.9 - Port 80
```



CCDC: Reglas y Puntuación

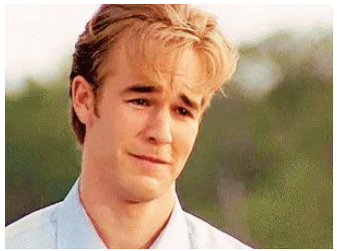
- T0 - Día 1
  - Comienzo de la competición (**Blue** / **Red**)
  - Momento de más importancia para Red Team
- Sistema de puntuación
  - **+** Servicios críticos, Incident Response, Inserts, Otros
  - **-** Servicios críticos, Red Team Reports y Flags
- **Reglas muy estrictas!**



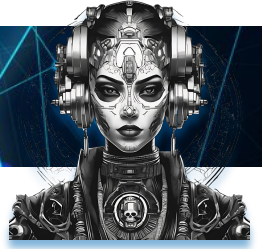


CCDC: Reglas y Puntuación

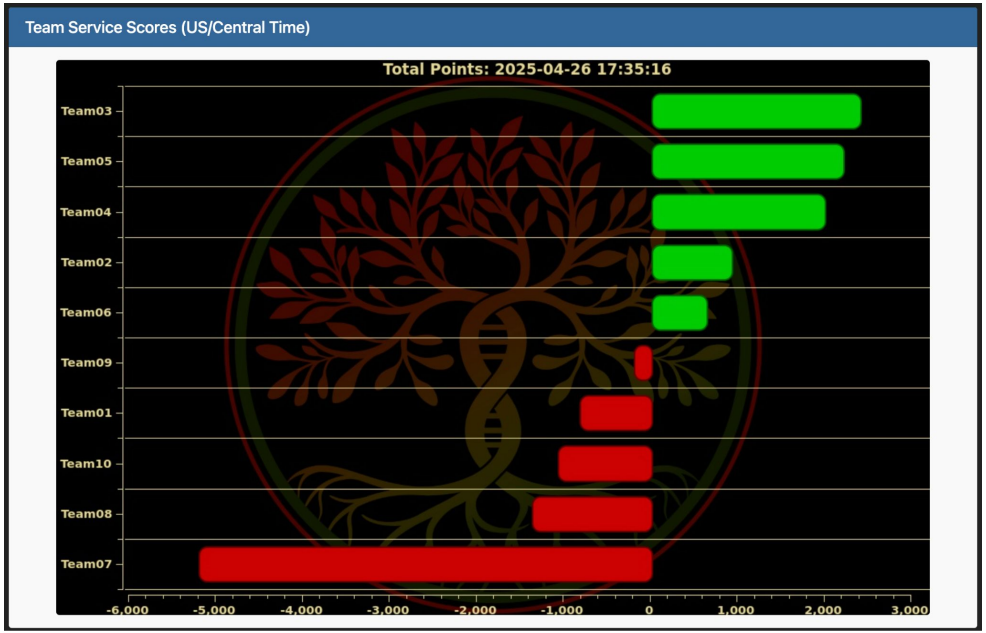
- Día **1** = Calma
  - Reconocimiento, Infiltración, Persistencia…
  - Movimiento Lateral, **Latencia**, Preparación
- Día **2** = Kaos
  - Ejecución, Exfiltración, **Destrucción**
- Lo que nunca te dejan hacer en un Red Team!

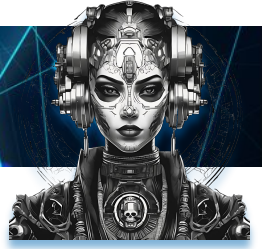


Blue Team

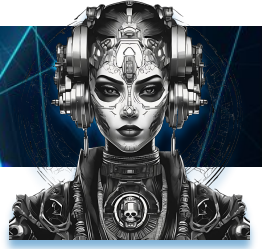


CCDC: Reglas y Puntuación

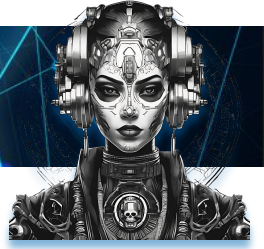




CCDC: Reglas y Puntuación



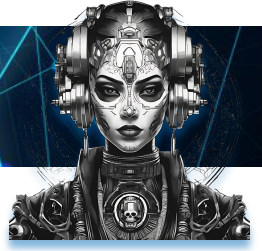
CCDC: Reglas y Puntuación



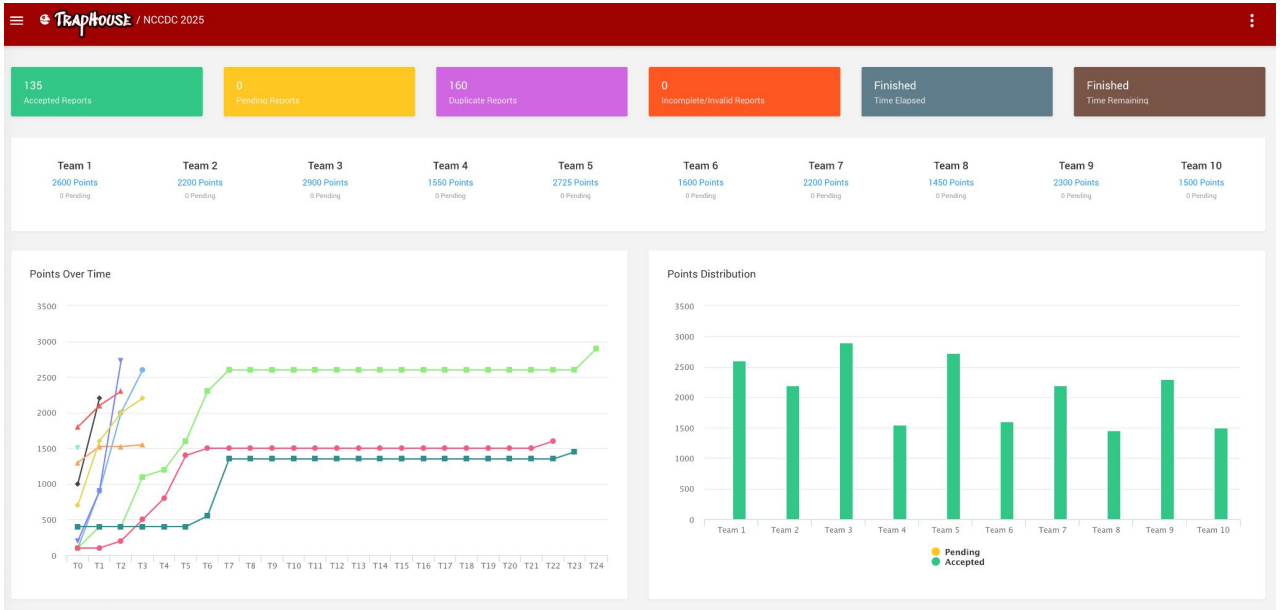
CCDC: Reglas y Puntuación

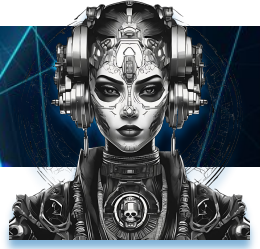
Red Team actions include:

- Obtaining root/administrator level access to a team system: -100 points
- Obtaining user level access to a team system (shell access, non anonymous access to an FTP service, or equivalent): -25 points
- Recovery of userids and passwords from a team system (encrypted or unencrypted): -50 points
- Recovery of one or more sensitive files or pieces of information from a team system (configuration files, corporate data, etc.): -25 points
- Recovery of customer credit card numbers: -50 points
- Recovery of personally identifiable customer information (name, address, and credit card number): -200 points

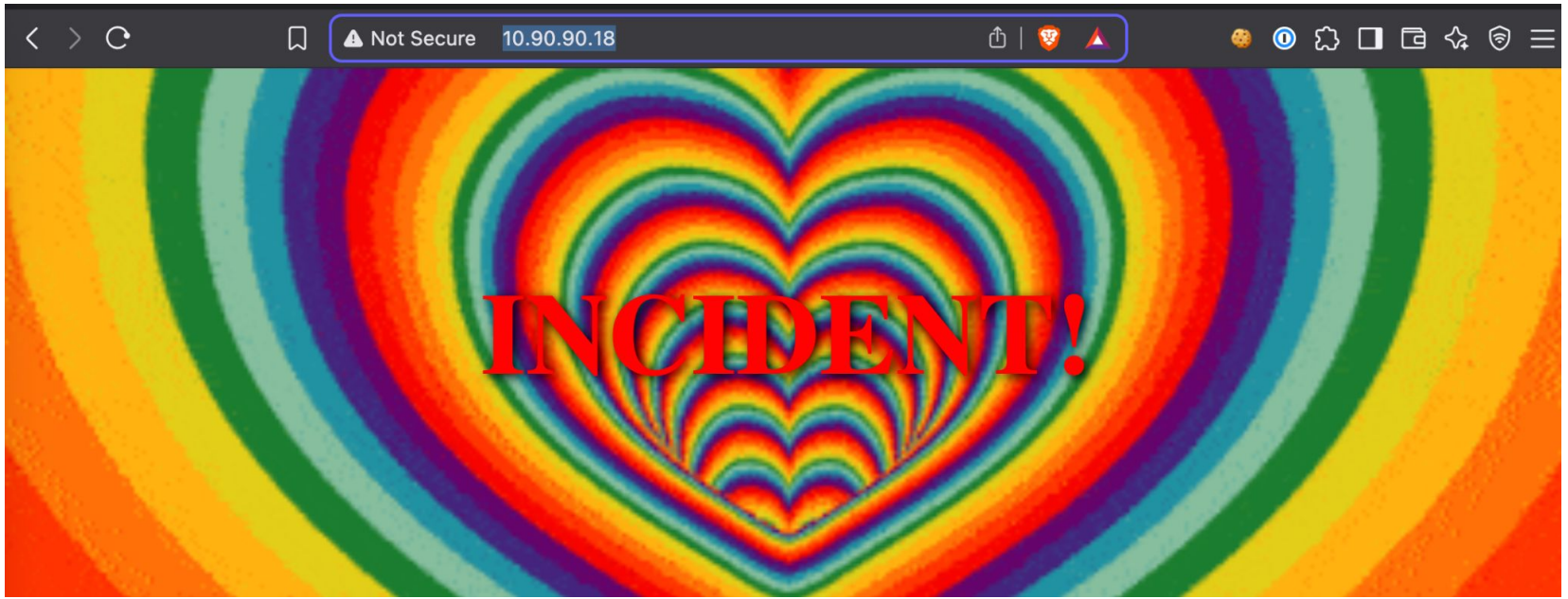


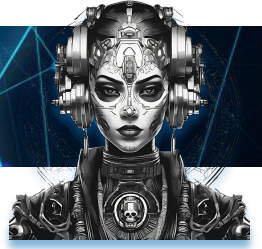
CCDC: Reglas y Puntuación



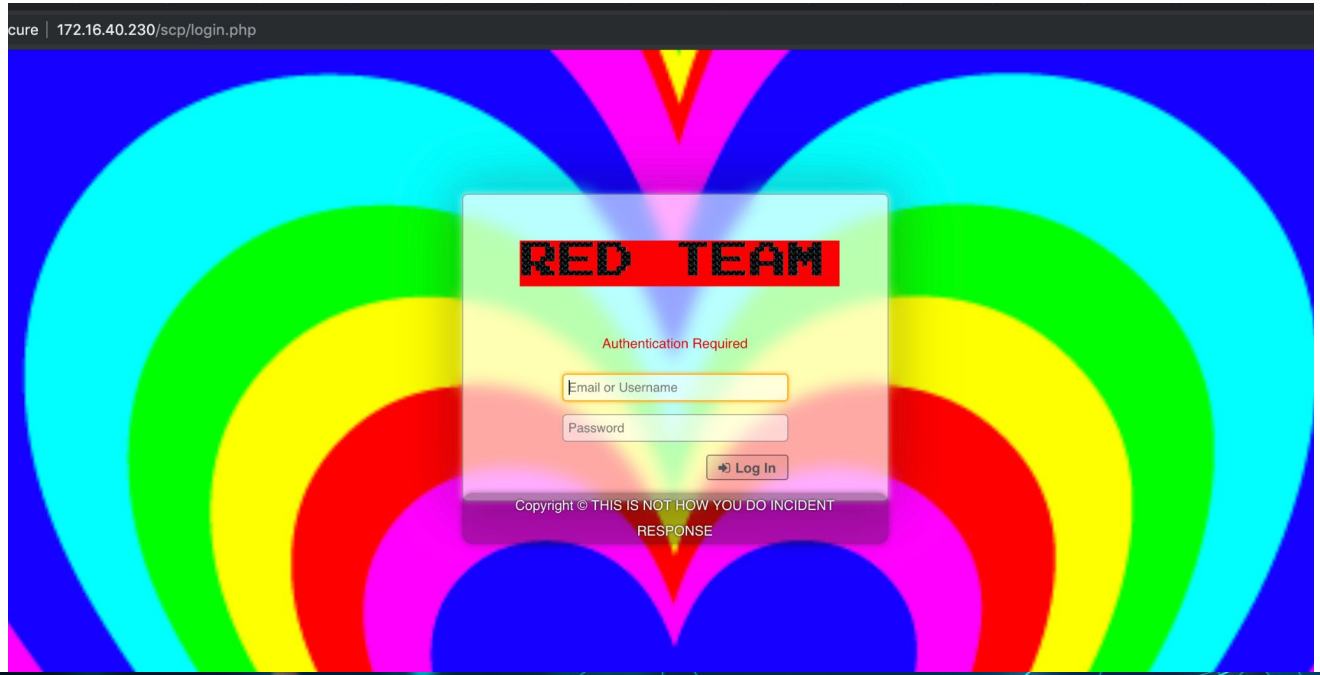


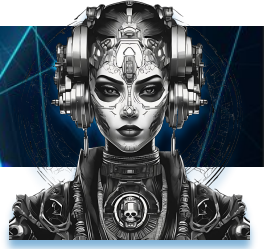
CCDC: Ejemplos Día 2



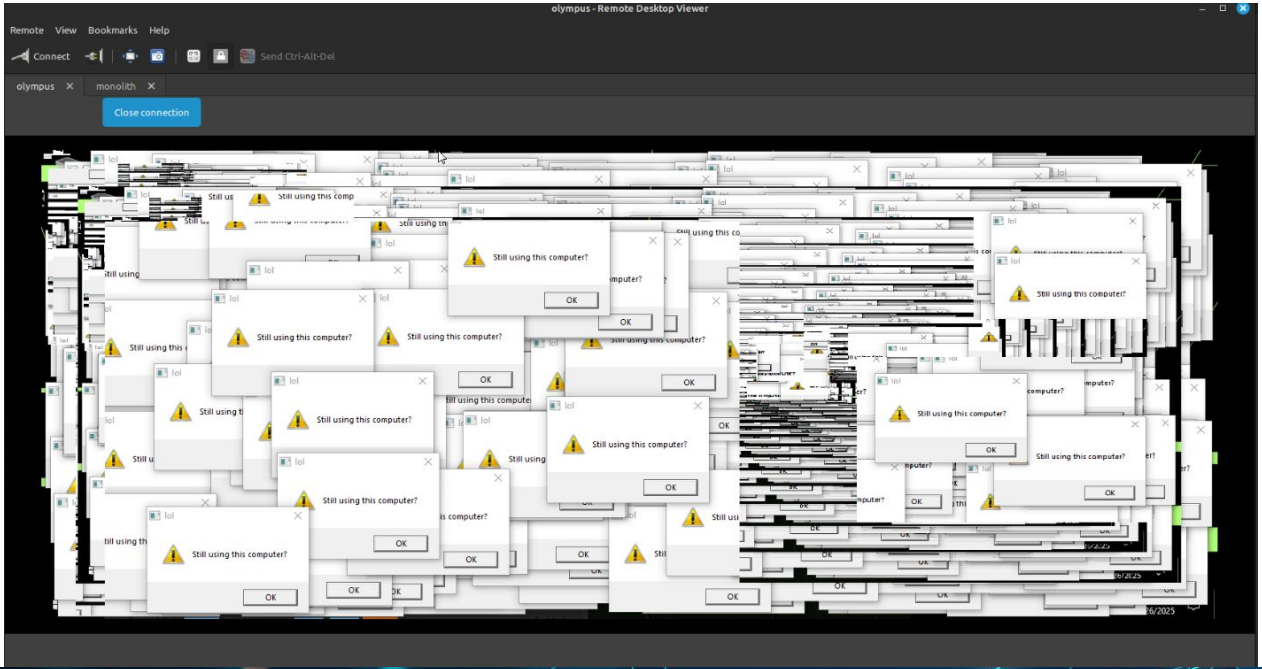


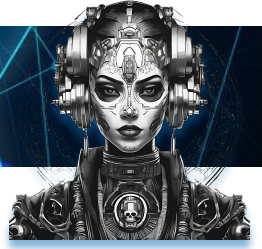
CCDC: Ejemplos Día 2



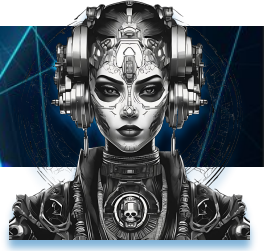


CCDC: Ejemplos Día 2



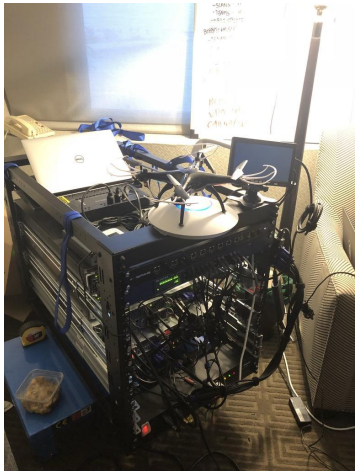


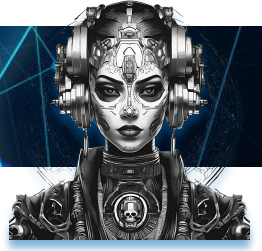
CCDC: Ejemplos Día 2



CCDC Red Team Toolkit

- Herramientas Públicas
  - → Metasploit, sliver, realm, Cobalt Strike, Mimikatz…
- Herramientas Privadas
  - → [REDACTED], [REDACTED], [REDACTED]…

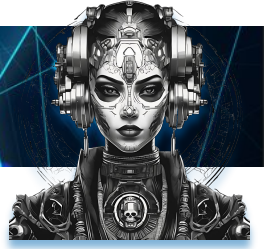




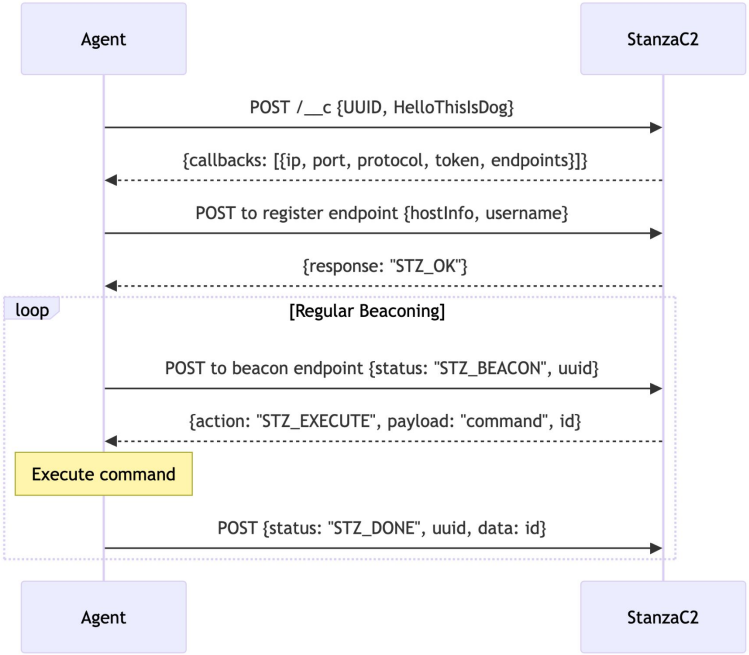
CCDC Red Team Toolkit

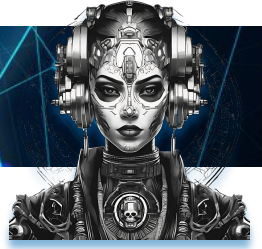
- Nuevo implante y C2: **Stanza**
  - Implante multiplataforma (go)
  - Soporte multiprotocolo: HTTP(S), TCP, UDP
  - Diseñado para resistencia e invisibilidad
  - Mínimas dependencias externas

https://github.com/jmpsec/stanza-c2

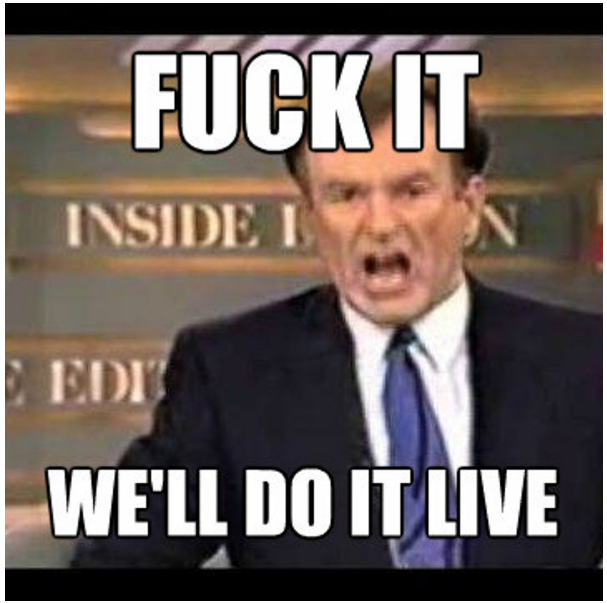


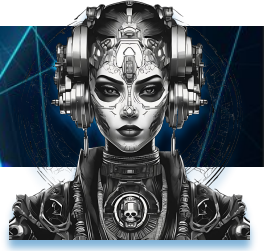
CCDC Red Team Toolkit: Stanza





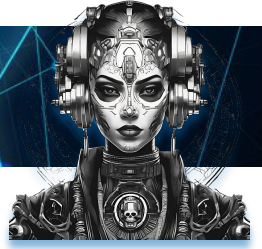
CCDC Red Team Toolkit: Stanza demo





Conclusiones

- Los APT representan una amenaza **real**, **sofisticada** y **persistente**, que requiere preparación técnica y mental.
- CCDC ofrece un entorno práctico realista para simular este tipo de ataques y poner a prueba las habilidades de defensa.
- No es solo cuestión de tecnología, también de trabajo en equipo, toma de decisiones bajo presión y comunicación.



¿Preguntas?

Confesiones y anécdotas de un ~~ex~~-APT

@jmpsec

@javutin

¡MUCHAS GRACIAS!

ESKERRIK ASKO!

EuskalHack Security Congress VIII