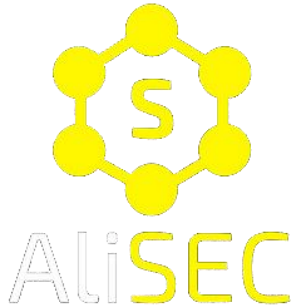
Jornadas de orientación laboral en ciberseguridad: Seguridad Ofensiva



David Álvarez Robles

Índice

1. Presentación
2. Cronología del camino hacia la empresa privada
3. Camino una vez dentro de la empresa privada
4. Seguridad ofensiva: día a día
5. Consejos para iniciar el camino

EPI Gijón
Universidad de Oviedo
GRUPO CIES

Presentación

C:\> whoami

- David Álvarez Robles (km0xu95/tdkmp4n4)
  - Responsable de seguridad ofensiva en Grupo CIES – AliSEC
  - Grado y Máster en Ingeniería de Telecomunicación
  - Doctorado en Informática (en progreso)
  - Experto Universitario en Seguridad Perimetral
  - OSEP, OSCP, OSWP, CRTO, CRTP, CRTE, eWPTX…

AliSEC

Universidad de Oviedo
Universidá d'Uviéu
University of Oviedo

Grupo CIES – AliSEC

- Empresa asturiana especializada en ciberseguridad
  - Instituto CIES + AliSEC Soluciones S.L.

Cumplimiento y legal	Seguridad ofensiva	Seguridad defensiva	Respuesta incidentes
Monitorización avanzada	Formación y sensibilización	I+D+i	Despliegues e infraestructura

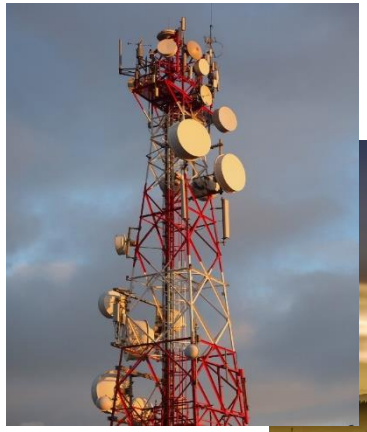
Cronología del camino hacia la empresa privada

Visión global

- Mi camino dio inicio en 2013, cuando empecé los estudios de grado
- Durante el camino se logran hitos (importantes y menos importantes)
- Actualmente, este camino todavía sigue su curso

Primeros años

- Grado en Ingeniería en Tecnologías y Servicios de Telecomunicación



tsc uniovi

En mis primeros años, comencé más enfocado a TSC

2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

Primer contacto con la ciberseguridad

- Grado en Ingeniería en Tecnologías y Servicios de Telecomunicación

Manuel Fernández, Xabiel García Pañeda, Gabriel Díaz, David Melendi, Sergio Cabrero

Seguridad en Redes y Servicios

Grado en Ingeniería en Tecnologías y Servicios de Telecomunicación

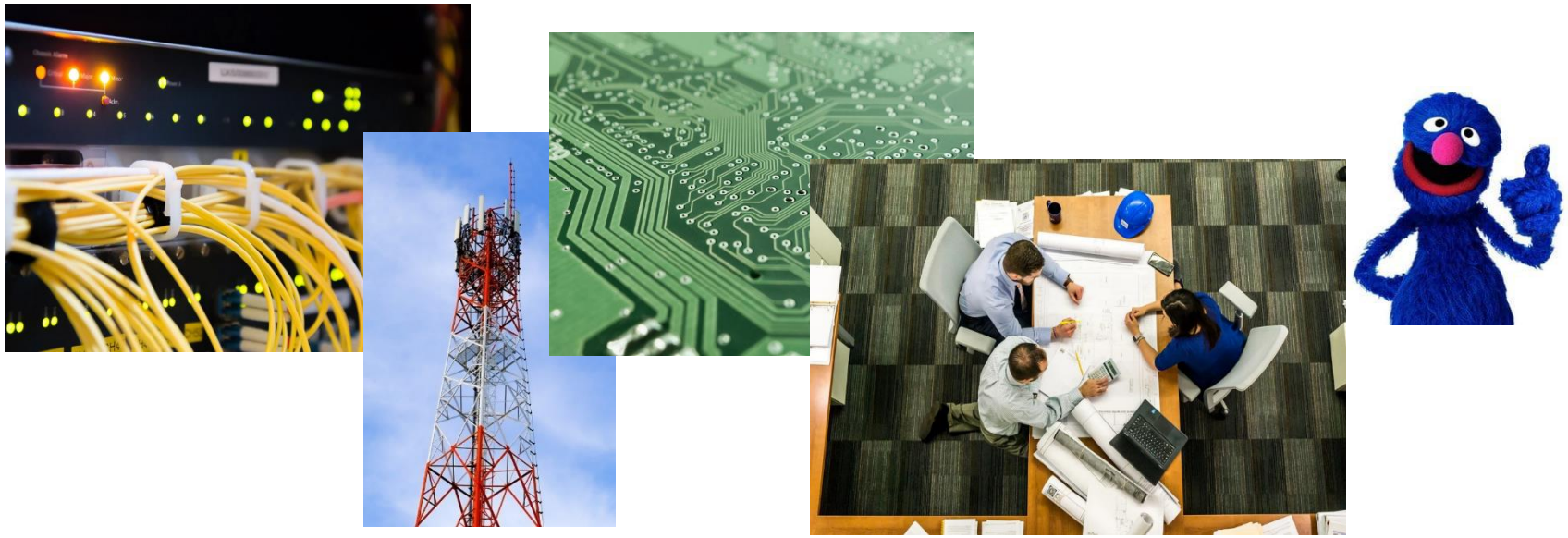
Mi primera toma de contacto con el mundo de la ciberseguridad fue en cuarto año de carrera

El camino ya lo había iniciado (sin saberlo…)

2013 2014 2015 **2016** 2017 2018 2019 2020 2021 2022 2023

Siguientes años de Universidad

- Máster en Ingeniería de Telecomunicación

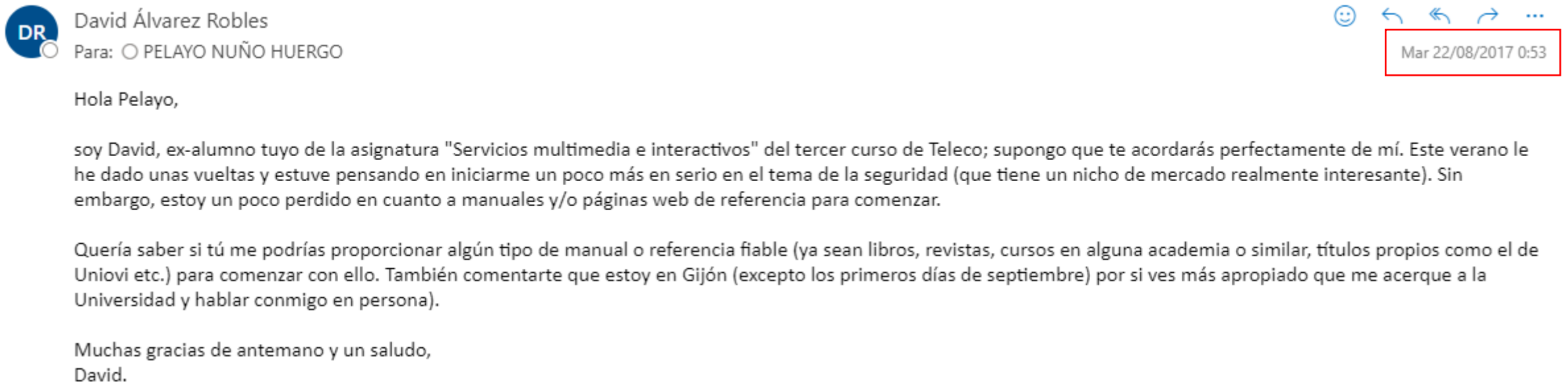


Vuelta a los orígenes para descartarlos por completo

Necesario para acceder al doctorado

2013 | 2014 | 2015 | **2016** | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

El hito más importante de mi camino



David Álvarez Robles
Para: PELAYO NUÑO HUERGO

Mar 22/08/2017 0:53

Hola Pelayo,

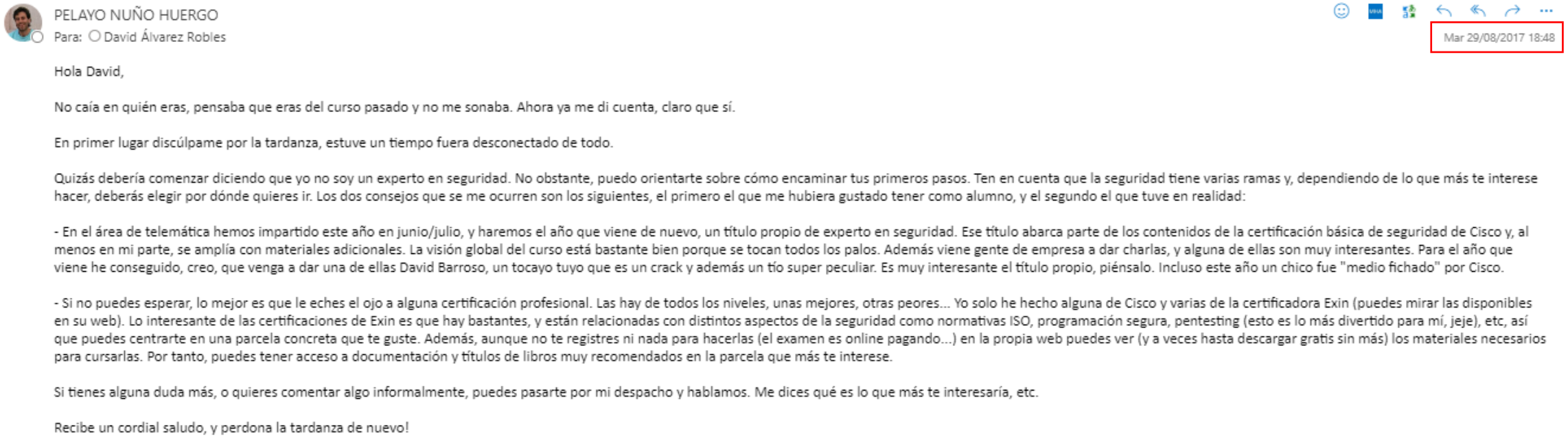
soy David, ex-alumno tuyo de la asignatura "Servicios multimedia e interactivos" del tercer curso de Teleco; supongo que te acordarás perfectamente de mí. Este verano le he dado unas vueltas y estuve pensando en iniciarme un poco más en serio en el tema de la seguridad (que tiene un nicho de mercado realmente interesante). Sin embargo, estoy un poco perdido en cuanto a manuales y/o páginas web de referencia para comenzar.

Quería saber si tú me podrías proporcionar algún tipo de manual o referencia fiable (ya sean libros, revistas, cursos en alguna academia o similar, títulos propios como el de Uniovi etc.) para comenzar con ello. También comentarte que estoy en Gijón (excepto los primeros días de septiembre) por si ves más apropiado que me acerque a la Universidad y hablar conmigo en persona).

Muchas gracias de antemano y un saludo,
David.

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

El hito más importante de mi camino



PELAYO NUÑO HUERGO
Para: David Álvarez Robles

Mar 29/08/2017 18:48

Hola David,

No caía en quién eras, pensaba que eras del curso pasado y no me sonaba. Ahora ya me di cuenta, claro que sí.

En primer lugar discúlpame por la tardanza, estuve un tiempo fuera desconectado de todo.

Quizás debería comenzar diciendo que yo no soy un experto en seguridad. No obstante, puedo orientarte sobre cómo encaminar tus primeros pasos. Ten en cuenta que la seguridad tiene varias ramas y, dependiendo de lo que más te interese hacer, deberás elegir por dónde quieres ir. Los dos consejos que se me ocurren son los siguientes, el primero el que me hubiera gustado tener como alumno, y el segundo el que tuve en realidad:

- En el área de telemática hemos impartido este año en junio/julio, y haremos el año que viene de nuevo, un título propio de experto en seguridad. Ese título abarca parte de los contenidos de la certificación básica de seguridad de Cisco y, al menos en mi parte, se amplía con materiales adicionales. La visión global del curso está bastante bien porque se tocan todos los palos. Además viene gente de empresa a dar charlas, y alguna de ellas son muy interesantes. Para el año que viene he conseguido, creo, que venga a dar una de ellas David Barroso, un tocayo tuyo que es un crack y además un tío super peculiar. Es muy interesante el título propio, piénsalo. Incluso este año un chico fue "medio fichado" por Cisco.

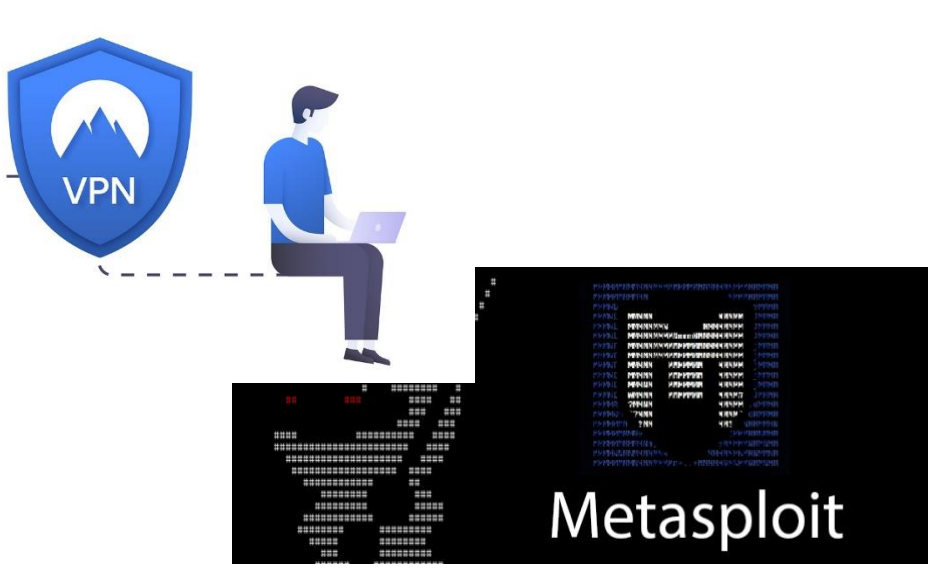
- Si no puedes esperar, lo mejor es que le eches el ojo a alguna certificación profesional. Las hay de todos los niveles, unas mejores, otras peores... Yo solo he hecho alguna de Cisco y varias de la certificadora Exin (puedes mirar las disponibles en su web). Lo interesante de las certificaciones de Exin es que hay bastantes, y están relacionadas con distintos aspectos de la seguridad como normativas ISO, programación segura, pentesting (esto es lo más divertido para mí, jeje), etc, así que puedes centrarte en una parcela concreta que te guste. Además, aunque no te registres ni nada para hacerlas (el examen es online pagando...) en la propia web puedes ver (y a veces hasta descargar gratis sin más) los materiales necesarios para cursarlas. Por tanto, puedes tener acceso a documentación y títulos de libros muy recomendados en la parcela que más te interese.

Si tienes alguna duda más, o quieres comentar algo informalmente, puedes pasarte por mi despacho y hablamos. Me dices qué es lo que más te interesaría, etc.

Recibe un cordial saludo, y perdona la tardanza de nuevo!

Formación universitaria adicional

- Título Propio Experto Universitario en Seguridad Perimetral

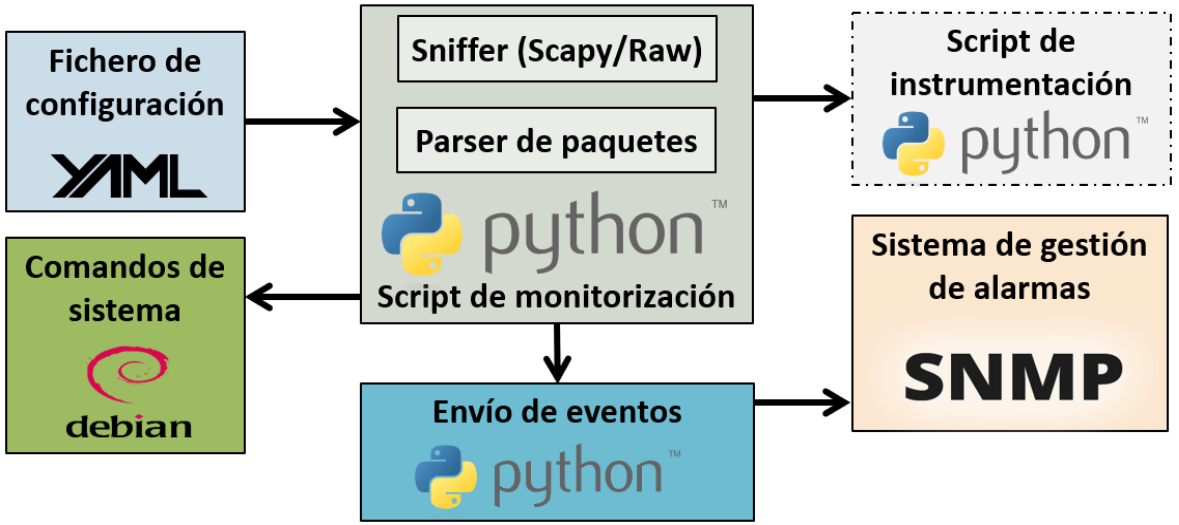


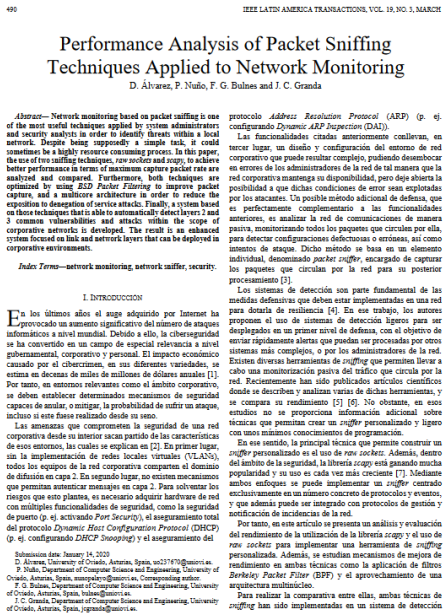
Título MUY BUENO para ampliar y sentar bases de carrera y máster

2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

Formación universitaria adicional

- Proyecto IUTA





490 IEEE LATIN AMERICA TRANSACTIONS, VOL. 19, NO. 3, MARCH

Performance Analysis of Packet Sniffing Techniques Applied to Network Monitoring

D. Álvarez, P. Nuño, F. G. Bulnes and J. C. Granda

Abstract— Network monitoring based on packet sniffing is one of the most useful techniques applied by system administrators and security analysts in order to identify threats within a local network. Despite being supposedly a simple task, it could sometimes be a highly resource consuming process. In this paper, the use of two sniffing techniques, *raw sockets* and *scapy*, to achieve better performance in terms of maximum capture packet rate are analyzed and compared. Furthermore, both techniques are optimized by using *BSD Packet Filtering* to improve packet capture, and a multicore architecture in order to reduce the exposition to denegation of service attacks. Finally, a system based on those techniques that is able to automatically detect layers 2 and 3 common vulnerabilities and attacks within the scope of corporative networks is developed. The result is an enhanced system focused on link and network layers that can be deployed in corporative environments.

Index Terms—network monitoring, network sniffer, security.

I. INTRODUCCION

En los últimos años el auge adquirido por Internet ha provocado un aumento significativo del número de ataques informáticos a nivel mundial. Debido a ello, la ciberseguridad se ha convertido en un campo de especial relevancia a nivel gubernamental, corporativo y personal. El impacto económico causado por el cibercrimen, en sus diferentes variedades, se estima en decenas de miles de millones de dólares anuales [1]. Por tanto, en entornos relevantes como el ámbito corporativo, se deben establecer determinados mecanismos de seguridad capaces de anular, o mitigar, la probabilidad de sufrir un ataque, incluso si este fuese realizado desde su seno.

Las amenazas que comprometen la seguridad de una red corporativa desde su interior sacan partido de las características de esos entornos, las cuales se explican en [2]. En primer lugar, sin la implementación de redes locales virtuales (VLANs), todos los equipos de la red corporativa comparten el dominio de difusión en capa 2. En segundo lugar, no existen mecanismos que permitan autenticar mensajes en capa 2. Para solventar los riesgos que esto plantea, es necesario adquirir hardware de red con múltiples funcionalidades de seguridad, como la seguridad de puerto (p. ej. activando *Port Security*), el aseguramiento total del protocolo *Dynamic Host Configuration Protocol* (DHCP) (p. ej. configurando *DHCP Snooping*) y el aseguramiento del protocolo *Address Resolution Protocol* (ARP) (p. ej. configurando *Dynamic ARP Inspection* (DAI)).

Las funcionalidades citadas anteriormente conllevan, en tercer lugar, un diseño y configuración del entorno de red corporativo que puede resultar complejo, pudiendo desembocar en errores de los administradores de la red de tal manera que la red corporativa mantenga su disponibilidad, pero deje abierta la posibilidad a que dichas condiciones de error sean explotadas por los atacantes. Un posible método adicional de defensa, que es perfectamente complementario a las funcionalidades anteriores, es analizar la red de comunicaciones de manera pasiva, monitorizando todos los paquetes que circulen por ella, para detectar configuraciones deficitosas o erróneas, así como intentos de ataque. Dicho método se basa en un elemento individual, denominado *packet sniffer*, encargado de capturar los paquetes que circulan por la red para su posterior procesamiento [3].

Los sistemas de detección son parte fundamental de las medidas defensivas que deben estar implementadas en una red para dotarla de resiliencia [4]. En ese trabajo, los autores proponen el uso de sistemas de detección ligeros para ser desplegados en un primer nivel de defensa, con el objetivo de enviar rápidamente alertas que puedan ser procesadas por otros sistemas más complejos, o por los administradores de la red. Existen diversas herramientas de *sniffing* que permiten llevar a cabo una monitorización pasiva del tráfico que circula por la red. Recientemente han sido publicados artículos científicos donde se describen y analizan varias de dichas herramientas, y se compara su rendimiento [5] [6]. No obstante, en esos estudios no se proporciona información adicional sobre técnicas que permitan crear un *sniffer* personalizado y ligero con unos mínimos conocimientos de programación.

En ese sentido, la principal técnica que permite construir un *sniffer* personalizado es el uso de *raw sockets*. Además, dentro del ámbito de la seguridad, la librería *scapy* está ganando mucha popularidad y su uso es cada vez más creciente [7]. Mediante ambos enfoques se puede implementar un *sniffer* centrado exclusivamente en un número concreto de protocolos y eventos, y que además puede ser integrado con protocolos de gestión y notificación de incidencias de la red.

Por tanto, en este artículo se presenta un análisis y evaluación del rendimiento de la utilización de la librería *scapy* y el uso de *raw sockets* para implementar una herramienta de *sniffing* personalizada. Además, se estudian mecanismos de mejora de rendimiento en ambas técnicas como la aplicación de filtros *Berkeley Packet Filter* (BPF) y el aprovechamiento de una arquitectura multinúcleo.

Para realizar la comparativa entre ellas, ambas técnicas de *sniffing* han sido implementadas en un sistema de detección

Submission date: January 14, 2020
D. Álvarez, University of Oviedo, Asturias, Spain, uo237670@uniovi.es.
P. Nuño, Department of Computer Science and Engineering, University of Oviedo, Asturias, Spain, nunopalacios@uniovi.es, Corresponding author.
F. G. Bulnes, Department of Computer Science and Engineering, University of Oviedo, Asturias, Spain, fbulnes@uniovi.es.
J. C. Granda, Department of Computer Science and Engineering, University of Oviedo, Asturias, Spain, jcgranda@uniovi.es.

Oportunidad única para investigar y seguir creciendo

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

Primeros cursos específicos

- Cursos en The Security Sentinel
  - Certificado Profesional de Hacking Ético (CPHE)
  - Certificado de Hacking Ético Experto (CHEE)
  - Certificado de Pentesting con PowerShell (HCPP)
  - Certificado de Hacking de Aplicaciones Web (HCAHW)

NO hacer ningún curso de estos ni parecidos. No merecen la pena

Otras plataformas de aprendizaje

Microsoft Active Directory

DVWA

Hack The Box
PEN-TESTING LABS

Explorar estos recursos, son muy buenos y muchas veces GRATIS o muy baratos

2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023

Camino una vez dentro de la empresa privada

Primer trabajo

- Analista SOC
  - Aprendizaje idiomas
  - Certificación de inglés
  - Aprendizaje mundo laboral
  - Aprendizaje SOC

Primera certificación relevante

- Offensive Security Certified Professional (OSCP)

Certificación base fundamental para pentesting y red teaming

2013 | 2014 | 2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022 | 2023

Formación continua

- Offensive Security Wireless Professional (OSWP)
- Certified Red Team Professional (CRTP)
- Nessus Certificate of Proficiency
- Virtual Hacking Labs Advanced/Advanced+

** AÑO DE PANDEMIA

Formación continua

- Certified Red Team Expert (CRTE)
- SecurityTube Linux Assembly Expert x86 (SLAE32)
- SecurityTube GNU Debugger Expert (SGDE)

** AÑO DE CIERRES PARCIALES

Comienzo del doctorado

- Doctor en Informática – Diseño y evaluación de técnicas para mejorar la seguridad en redes corporativas
  - *Performance Analysis of Packet Sniffing Techniques Applied to Network Monitoring (*IEEE Latin America Transactions · Mar 3, 2021*)*
  - *Performance Analysis of Software-Defined Networks to Mitigate Private VLAN Attacks (MDPI Sensors · Feb 4, 2023)*

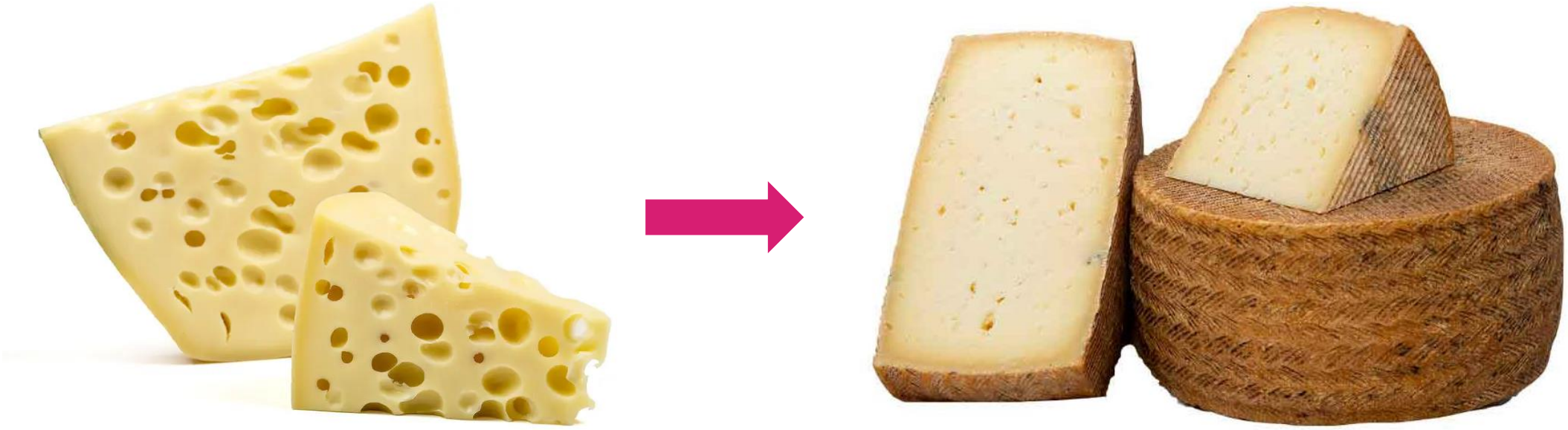
Formación más avanzada

- eLearnSecurity Web Penetration Testing eXpert (eWPTX)
- Offensive Security Experienced Penetration Tester (OSEP)
- Certified Red Team Operator (CRTO)
  - --- ongoing Certified Red Team Lead (CRTL)
  - --- ongoing Malware Development

Seguridad ofensiva: día a día

Descripción básica

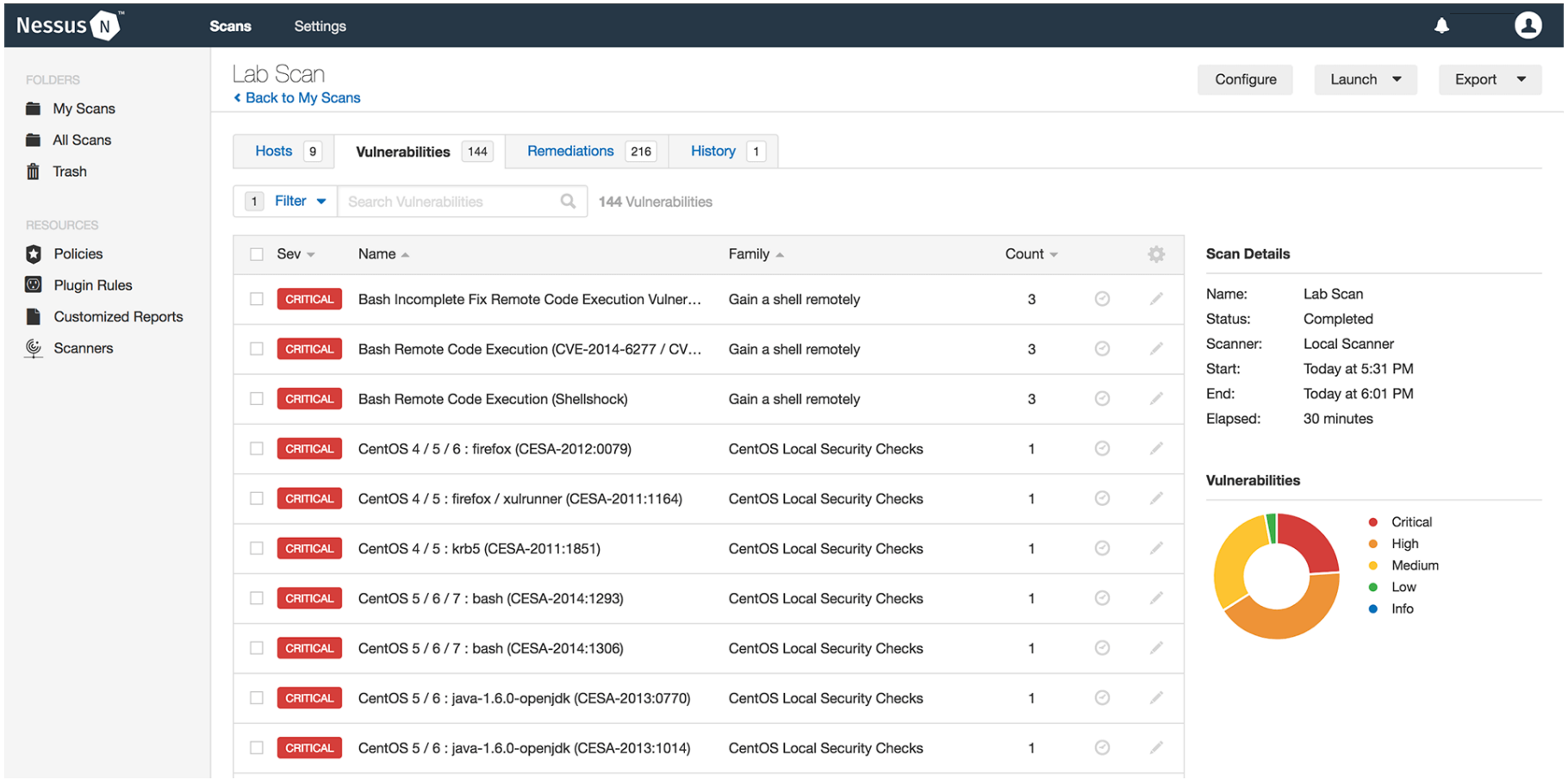
- Buscar problemas de seguridad para su reporte y posterior corrección por parte de los equipos oportunos



Análisis de vulnerabilidades

- Búsqueda de vulnerabilidades que puedan afectar potencialmente al cliente **sin explotarlas**
  - Revisión de actualizaciones y/o parches
  - Revisión de errores de configuración
  - Revisión de exposiciones innecesarias
  - Nivel interno (redes LAN) como externo (red WAN)

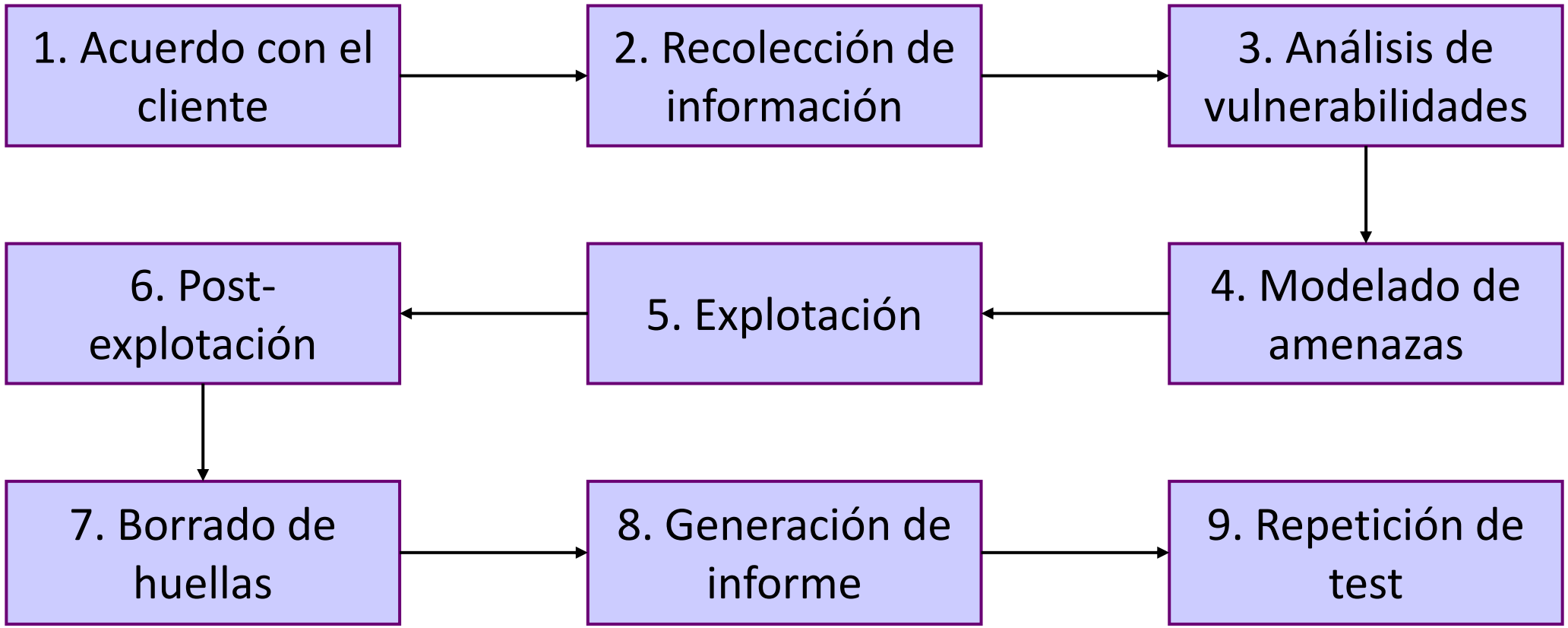
Análisis de vulnerabilidades



Pentesting

- Búsqueda de problemas de seguridad que puedan afectar a una organización al completo (redes, apps…). En este caso **SÍ se explotan**
  - El objetivo es buscar el mayor número de problemas posible
  - Metodologías OSSTMM, NIST o PTES
  - Debe reportarse al cliente cada problema de seguridad junto a su mitigación

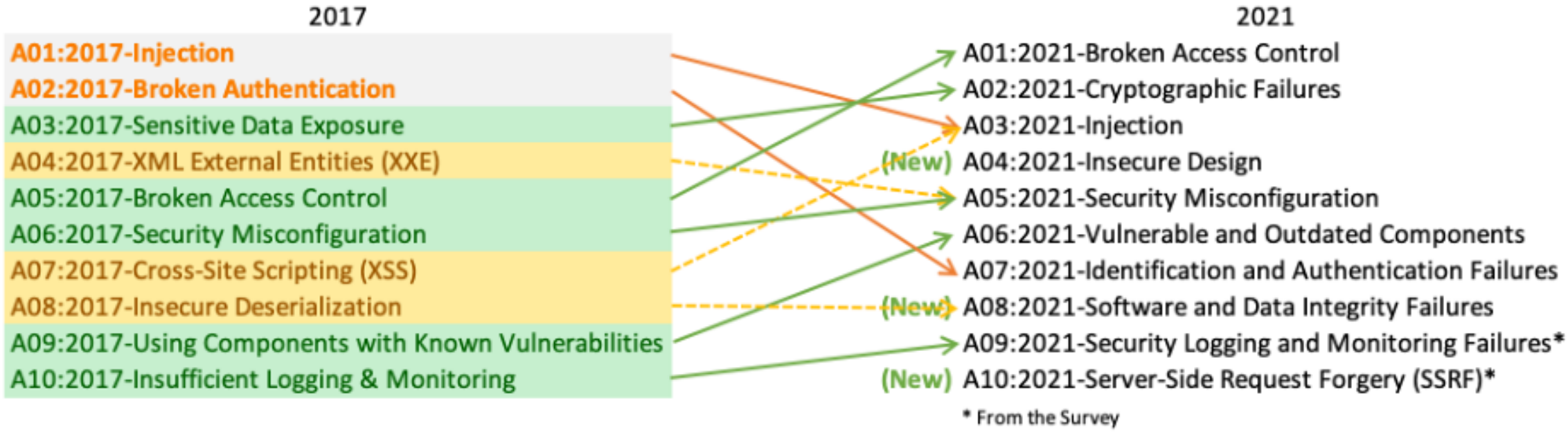
Pentesting


1. Acuerdo con el cliente
2. Recolección de información
3. Análisis de vulnerabilidades
4. Modelado de amenazas
5. Explotación
6. Post-explotación
7. Borrado de huellas
8. Generación de informe
9. Repetición de test

Auditoría de aplicaciones

- Búsqueda de problemas de seguridad que puedan afectar a una aplicación (web, móvil, nativa, API…). **SÍ se explotan**
  - El objetivo es buscar el mayor número de problemas posible
  - Metodologías OWASP WSTG, OWASP MSTG
  - Debe reportarse al cliente cada problema de seguridad junto a su mitigación

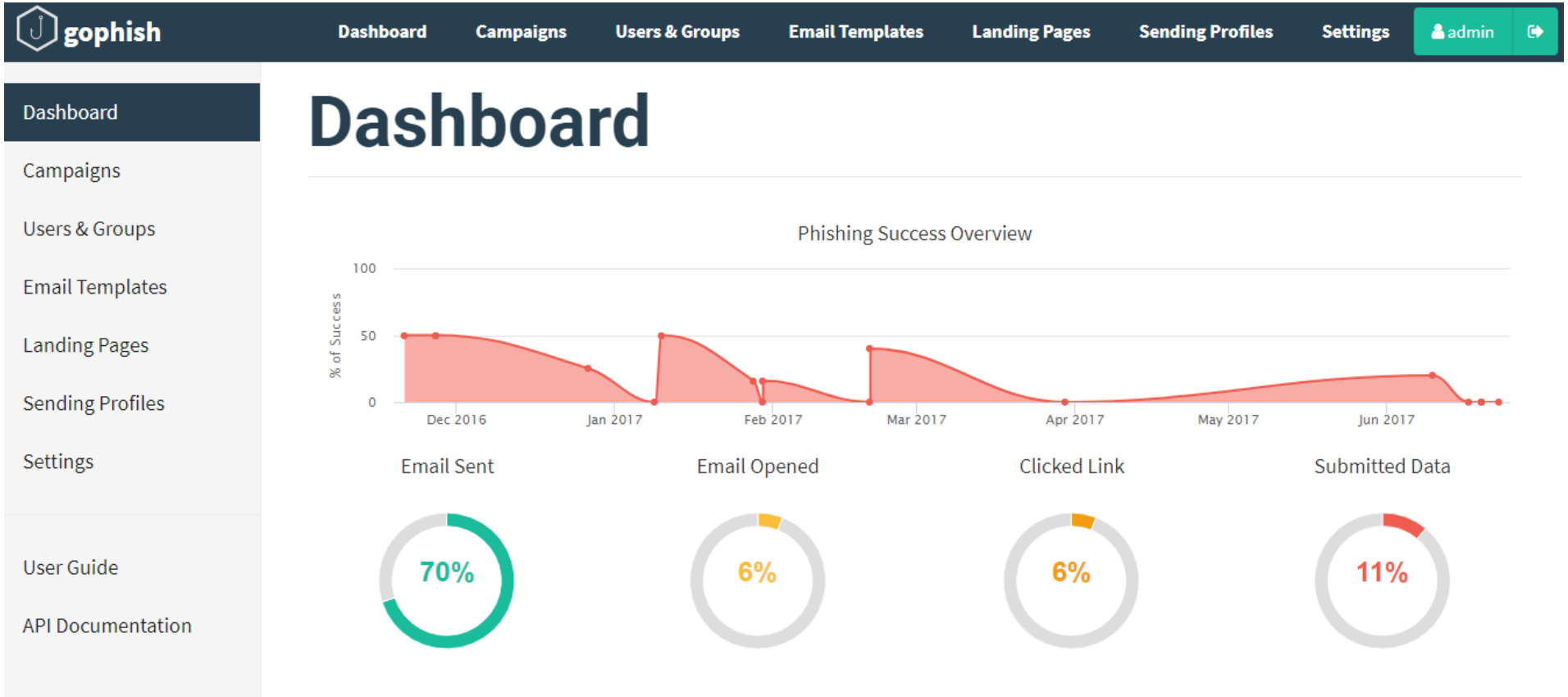
Auditoría de aplicaciones



Ejercicios de ingeniería social

- Búsqueda mediante OSINT de correos electrónicos y puntos de entrada a la organización y generación de campañas de ingeniería social (phishing, smishing, vishing…) para robo de credenciales o envío de malware
  - El objetivo es puramente estadístico -> Ver cómo se comportan los usuarios estadísticamente y formarlos

Ejercicios de ingeniería social

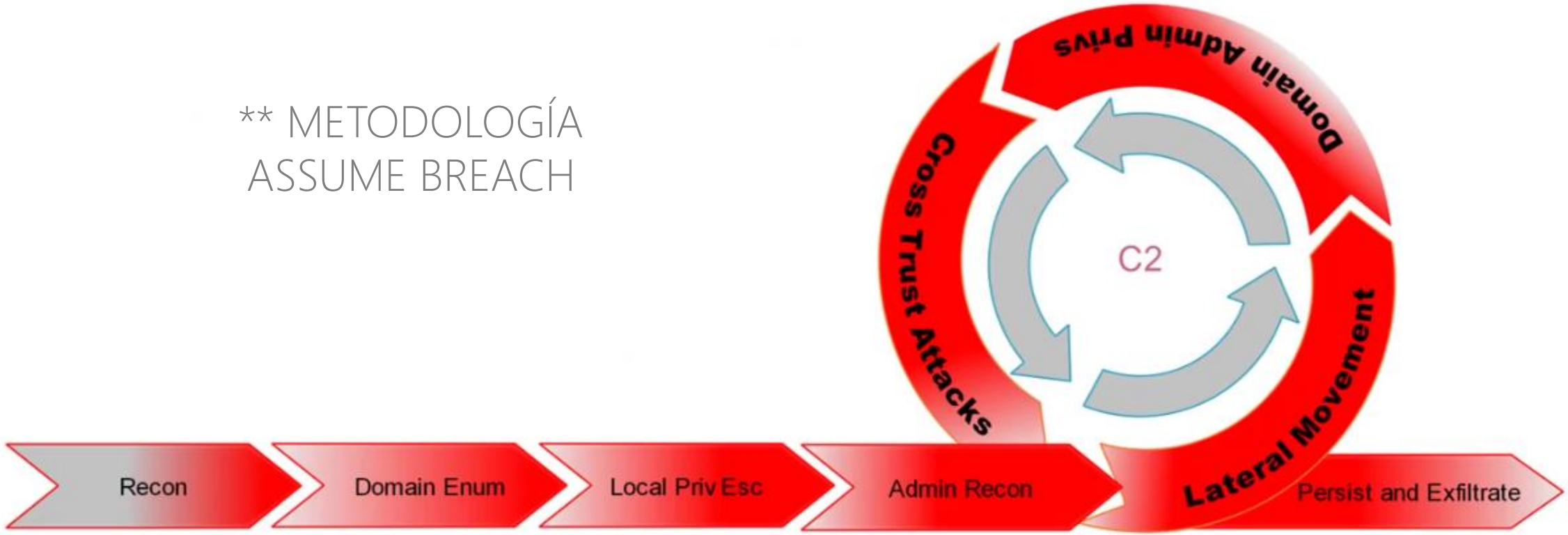


Red Teaming

- Emulación de adversarios reales, así como sus técnicas, tácticas y procedimientos (TTPs) para comprometer aquello que la organización estime como vital (documento, usuario, servidor…)
  - El objetivo es comprometer dicho activo sea como sea y medir la capacidad de respuesta de la organización
  - El equipo de seguridad defensiva puede y debe responder

Red Teaming

** METODOLOGÍA
ASSUME BREACH

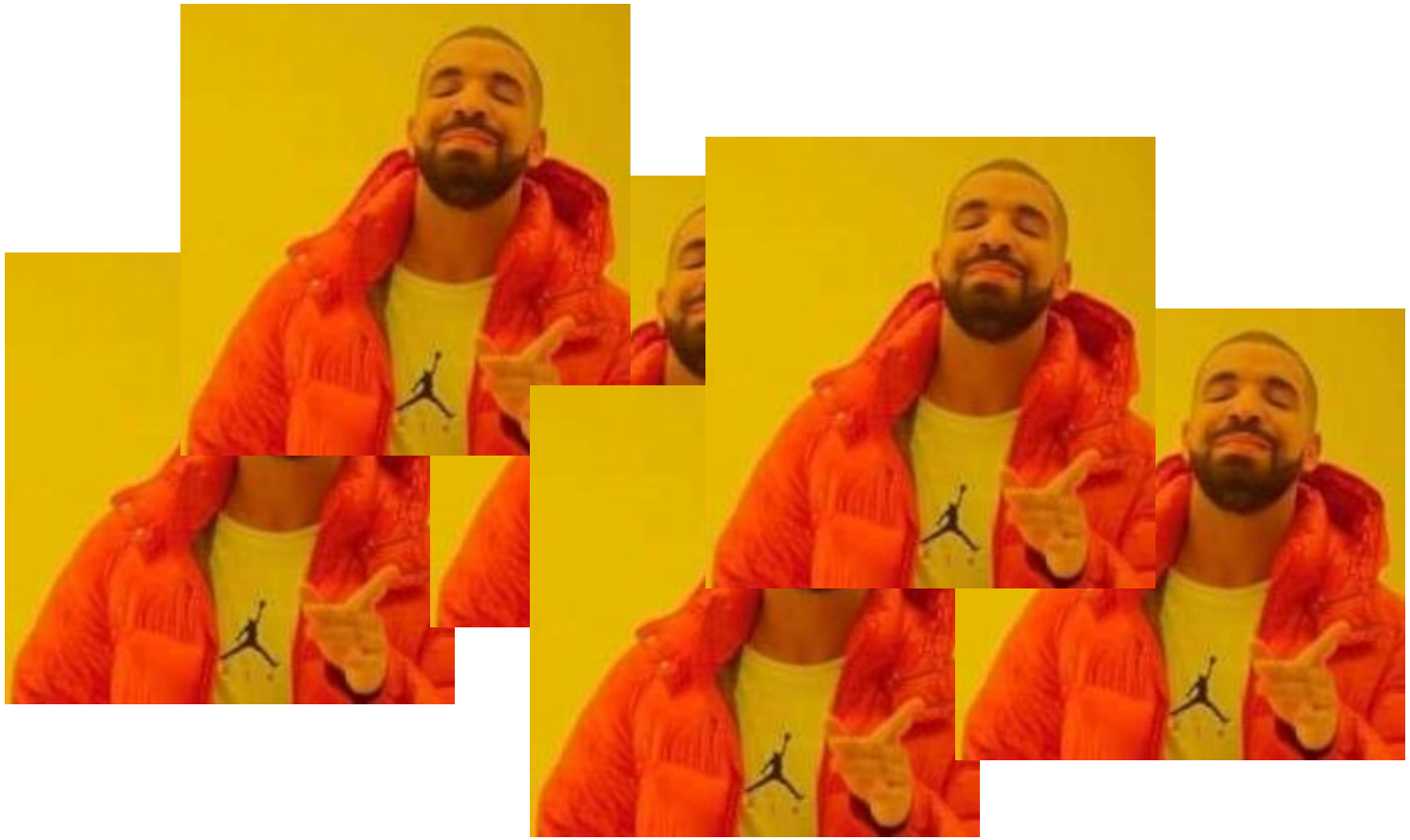


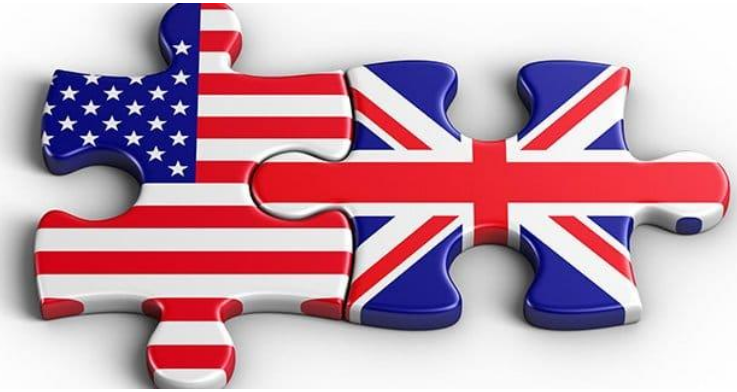
Otras tareas

- Formaciones técnicas y de sensibilización/concienciación
- Auditorías de activos (accesos remotos, Active Directory…)
- Auditoría de redes Wi-Fi
- Verificaciones de productos de ciberseguridad (EDR, NAC, FW…)
- Desarrollo de herramientas propias (scripting, programación…)
- Investigación y publicación de nuevas vulnerabilidades

Consejos para iniciar el camino

Lo primero de todo...





Lo primero de lo segundo…

- La ciberseguridad es "muy amplia". ¿Qué me gusta?

Seguridad ofensiva	Seguridad defensiva	Monitorización/SOC
Ciberinteligencia	Legal	Forense

Para empezar gratis…

- **Libros**: 0xWORD, Wiley, O'Reilly, No Starch Press…
- **Vídeos**: ippsec (pentesting)
- **Redes Sociales**: Benjamin Delpy, Kevin Beaumont, Vicent Le Toux (AD), Vadmin Khrykov (Threat Hunting)…
- **Foros**: AsturHackers, HackPlayers, Flu-Project, FWHibbit…
- **Canales**: Telegram, Discord, Slack…
- **Plataformas de hacking**: HackTheBox, TryHackMe, PicoCTF…

Para empezar con poca inversión…

- VIP HackTheBox/TryHackMe: Pentesting y retos
- Pentester Academy: Licencia de acceso a cursos
- Cursos de iniciación: TSS, Securízame, Mastermind, Udemy -> No los recomiendo mucho
- PentesterLab: Hacking web
- ProLabs HackTheBox: Active Directory

Salto de la Universidad a la empresa

- Buscad prácticas en empresas que se dediquen a ciberseguridad
  - Priorizar el conocimiento que vayáis a adquirir antes que otras cosas
  - Elegir en base a vuestros gustos (si se puede)

En AliSEC somos actualmente 11 en plantilla, de los cuales 4 empezaron haciendo prácticas en la empresa y se quedaron posteriormente (+35%)

Contacto

- Aquí o si no os atrevéis…
  - davidalvarezrobles@gmail.com
  - info@blog.asturhackers.es
  - Redes sociales
  - Telegram (km0xu95)
  - Discord
  - …

Jornadas de orientación laboral en ciberseguridad: Seguridad Ofensiva

EPI GIJÓN Universidad de Oviedo

GRUPO CIES

AliSEC

David Álvarez Robles