Práctica 3 – Máquina Cybox

<https://www.youtube.com/watch?v=TAry1aYIaBg> → Ejemplo de uso de la máquina cybox

La máquina simula un servidor interno en una organización llamada Cybox, el objetivo es conseguir la flag de user.txt y de root.txt.

1. Descargar la máquina en Kali Linux y comprobar la integridad de la ova descargada.
2. Instalarla en Virtual Box. La máquina Kali Linux y la Máquina Cybox deben tener comunicación.
3. Realizar escaneo de puertos con Nmap y Wireshark para que muestre las versiones de los servicios y lance scripts para obtener más información. Pantallazo del resultado.

# Recursos adicionales

[Repositorio en github con la práctica](https://github.com/jayanezj/ceti-hacking-etico/tree/master/lesson-1/practice-3)

# Análisis completo con nmap

[Video en Asciinema](https://asciinema.org/a/AHIstAgMjzZ1yzsrZpyUGRsTv)

# Descubrimiento de FTP (21) en Wireshark

|  |
| --- |
| Descubrimiento del puerto 21 en Wireshark con información de la aplicación |

# Descubrimiento de SMTP (25) en Wireshark

|  |
| --- |
| Descubrimiento del puerto 25 en Wireshark con información de la aplicación |

# Descubrimiento de HTTP (80) en Wireshark

|  |
| --- |
| Descubrimiento del puerto 80 en Wireshark con información de la aplicación |

# Descubrimiento de POP (110) en Wireshark

|  |
| --- |
| Descubrimiento del puerto 110 en Wireshark con información de la aplicación |

# Descubrimiento de IMAP (143) en Wireshark

|  |
| --- |
| Descubrimiento del puerto 143 en Wireshark con información de la aplicación |

# Descubrimiento de HTTPS (443) en Wireshark

|  |
| --- |
| Recogiendo claves de encriptación para el puerto 443 |

|  |
| --- |
| Añadiendo las claves de encriptación a Wireshark |

|  |
| --- |
| Descubrimiento del puerto 443 en Wireshark con información de la aplicación |