Caso práctico 1 hacking ético.

1.

- Entrando en la web iep.edu.es encontramos que la empresa se dedica a la educación y opera en EEUU, España, México, Argentina y Colombia. También vemos que tiene como instituciones asociadas Summa University, CUA, UEM y EAN.

-Como dominio principal tiene www.iep.edu.es y utilizando la herramienta DNSdumbster vemos que maneja también campusvirtual.iep.edu.es, info.iep.edu.es, pagoseguro.iep.edu.es, sg.iep.edu.es, ss.iep.edu.es, staging-nuevo.iep.edu.es, vpn.iep.edu.es.

-Tras esto obteniendo la ip de DNSdumbster que es 104.26.0.115 la introducimos en trusted IP obteniendo de ahí el AS que en este caso es AS13335.

-de DNSdumbster tambien obtenemos las direcciones IP correspondientes campusvirtual.iep.edu.es (185.77.132.133), info.iep.edu.es (104.26.1.115), pagoseguro.iep.edu.es (188.164.199.122), sg.iep.edu.es (172.67.73.221), ss.iep.edu.es (34.107.54.19), staging-nuevo.iep.edu.es (104.26.0.115), vpn.iep.edu.es (212.81.147.156).

-Tras utilizar shodan y dorks de google se puede obtener acceso a cientos de archivos PDF de la institución con cursos casos prácticos y demás documentación del campus virtual.

2. **Herramientas utilizadas**: Utilicé Nmap para realizar el escaneo de puertos abiertos y servicios en ejecución, y Metasploit para explorar posibles vulnerabilidades.

Escaneo de puertos: Ejecuté el comando `nmap -sT -p- -Pn 192.168.1.240` y obtuve los siguientes puertos abiertos: 21/tcp (ftp), 22/tcp (ssh), 23/tcp (telnet), 25/tcp (smtp), 80/tcp (http), 3306/tcp (mysql) y 8180/tcp (unknown).

Vulnerabilidades identificadas: Encontré varias vulnerabilidades potenciales. El puerto 21 (FTP) está ejecutando vsftpd, que tiene una vulnerabilidad conocida de puerta trasera. El puerto 22 (SSH) podría ser vulnerable a ataques de fuerza bruta si no se han configurado credenciales fuertes. El puerto 23 (Telnet) es inseguro y podría exponer información en texto plano. En el puerto 3306 (MySQL), la utilización de credenciales predeterminadas podría permitir acceso no autorizado a la base de datos.