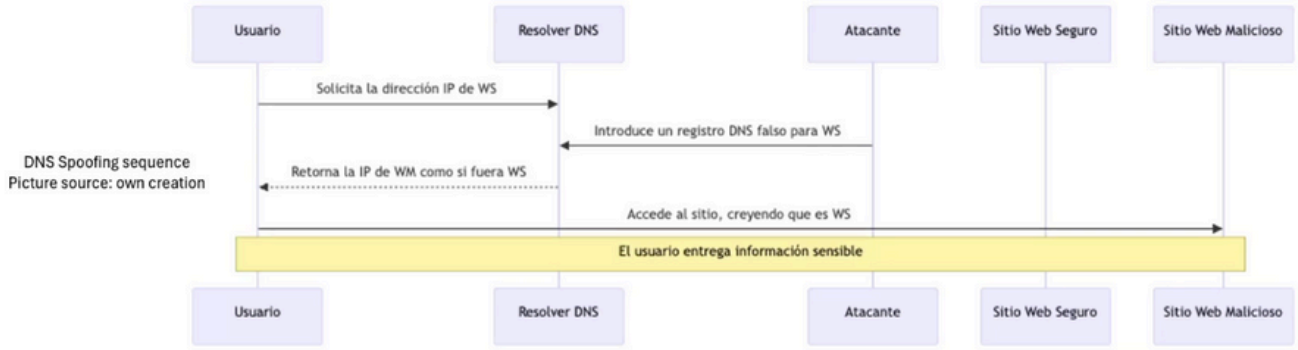
DNS Spoofing

DNS Spoofing is a cyber attack where false DNS records are introduced into a DNS resolver's cache, causing it to return an incorrect IP address and diverting traffic to a malicious site. This technique is often used for phishing attacks to steal sensitive information.

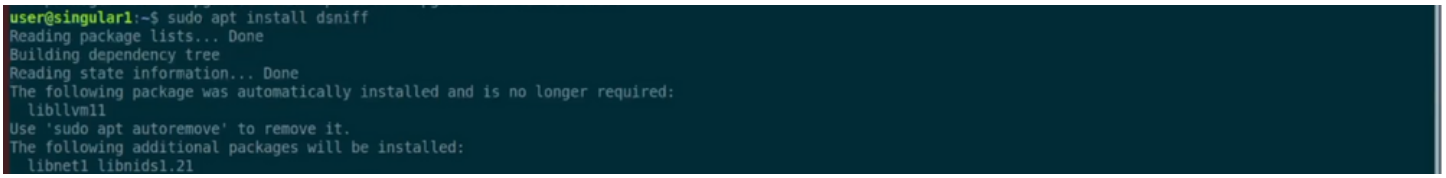


Maquina de ataque: 10.211.55.5

Maquina victima: 10.211.5.17

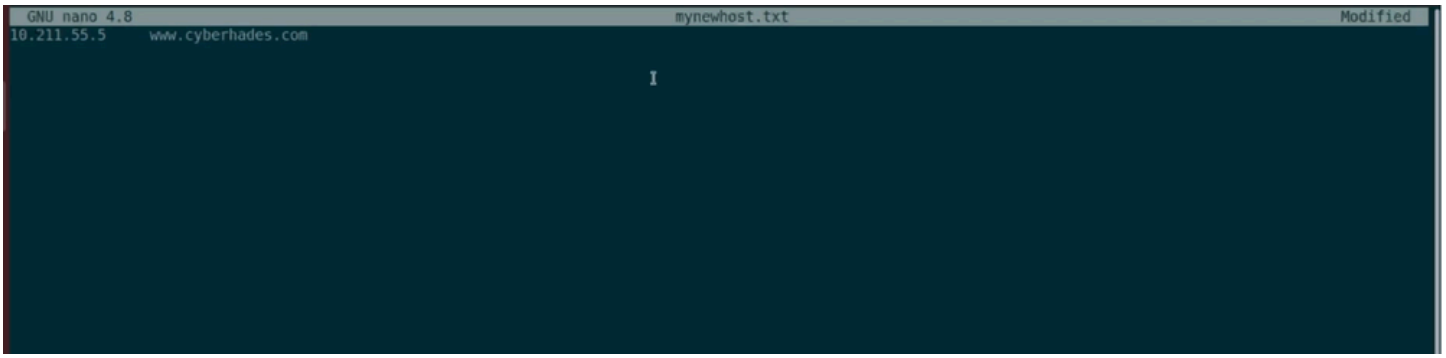
Usaremos herramientas cómo dnsspoof o ethercap para alterar el tráfico dns de una red.

Instalamos el paquete.

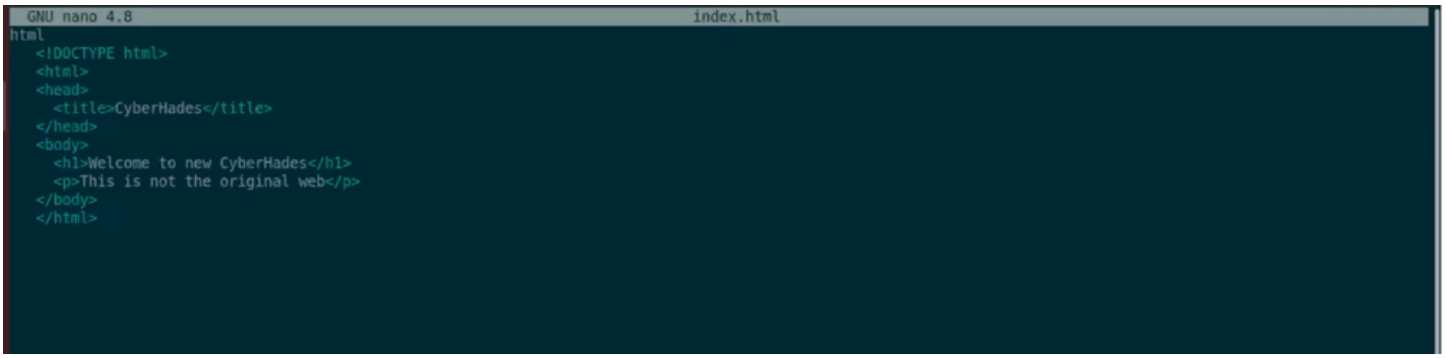


Creamos un fichero host con un dominio y una dirección ip, para que cuando accedemos al dominio se redireccione a la dirección ip seleccionada. Y en esa dirección ip montaremos un servidor web para que la persona que piensa que va a la pagina del dominio web vaya a la pagina de la ip que nosotros montamos, y en éste momento la victima estaría en nuestra página web y se piensa que está en la correcta página web, podríamos obtener así sus credenciales de login y password, etc.

usamos nano para crear el fichero mynewhost.txt y redireccionar el dominio a la ip indicada.



Ahora haremos un html para simular la página indicada y engañar a la victima, con nano index.html, es un ejemplo y lo más básico.

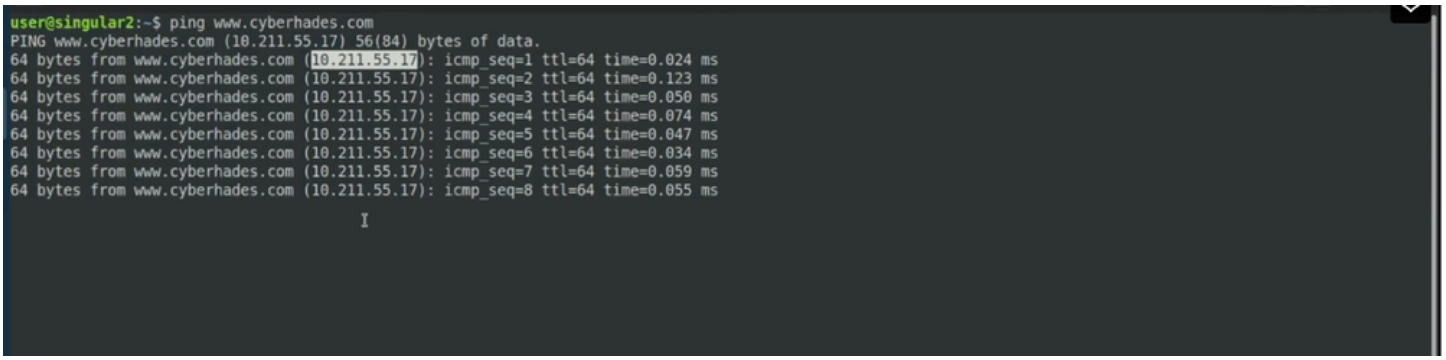


Levantamos un servidor web con python:

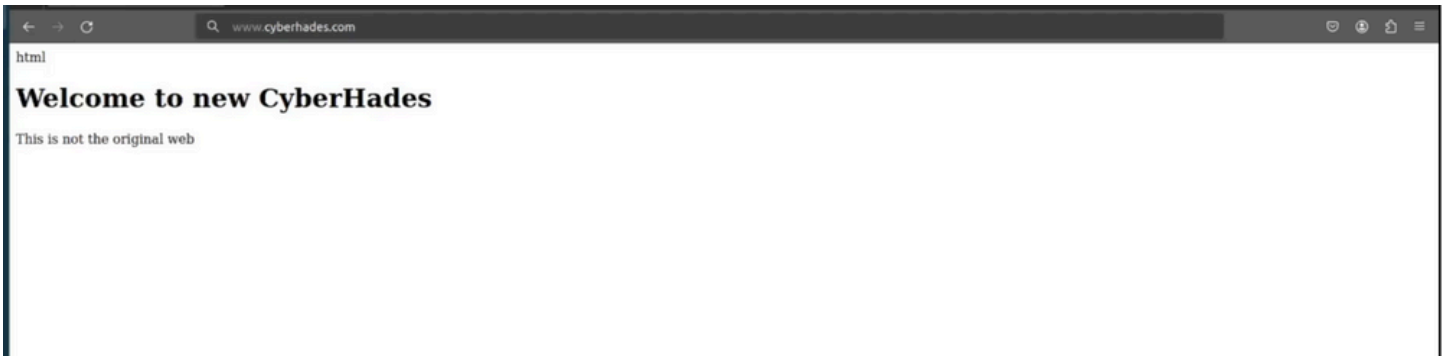
Ésta seria la pagina que hemos creado para engañar al usuario, ya está lanzada:

Abrimos otra terminal para no parar el servidor web y levantamos dnsspoof.

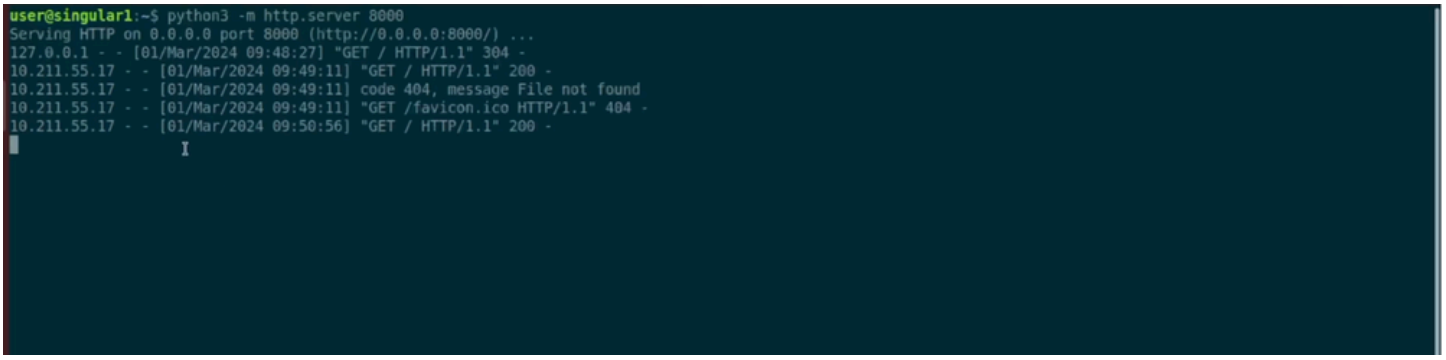
Vamos a la maquina victima y hacemos un ping a la pagina web de ciberhades, pero vemos que la ip es la otra, la que hemos hecho spoof, la maquina atacante. El dns spoof ha sido un exito, redirecciona la victima a la web falsa:



También lo vemos en el servidor web, muy potente para suplantar la pagina web y obtener información de la victima.



Volvemos al servidor de ataque y vemos las peticiones internas y remotas



Y vemos también el dns spoof en marcha

Mitigación de dns spoofing:

DNS Spoofing mitigations

- **Implement DNSSEC (DNS Security Extensions)** to add a layer of authentication to DNS responses, ensuring their integrity and authenticity.
- **Use DNS servers with DNSSEC validation** to verify the digital signature of DNS responses and prevent spoofed responses.
- **Configure firewalls and IDS/IPS filters** to detect and block suspicious or malicious DNS traffic.
- **Keep DNS server software up to date** to fix known vulnerabilities that could be exploited for spoofing attacks.