Dag:
5 - Nisse Alliance

Kategori:
Steganografi

Opgavebeskrivelse:
Vi har fået info omkring en server som måske ejes af Brunbjørnene. Den findes på IP: 20.240.4.10. Se om du kan få adgang, og skaffe informationer omkring denne nisse alliance.

1. Jeg starter med at lave en port scan på IP'en

```
└─$ nmap 20.240.4.10 -p- -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-05 05:35 EST
Nmap scan report for 20.240.4.10
Host is up (0.062s latency).
Not shown: 65533 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 356.53 seconds
```

2. Det første jeg gør er at se om FTP tillader anonymous login, hvilket det gør.
   ftp anonymous@20.240.4.10

```
└─$ ftp anonymous@20.240.4.10
Connected to 20.240.4.10.
220 (vsFTPd 3.0.5)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||32117|)
150 Here comes the directory listing.
drwxr-xr-x    2 1001     0            4096 Nov 25 18:44 bearfun
drwxr-xr-x    2 1001     0            4096 Nov 25 18:44 bearsecrets
drwxr-xr-x    2 1001     0            4096 Nov 25 18:50 documents
drwxr-xr-x    2 1001     0            4096 Nov 25 19:12 notsecret
drwxr-xr-x    2 1001     0            4096 Nov 25 18:43 private
drwxr-xr-x    2 1001     0            4096 Nov 25 18:50 sagalabs_secrets
226 Directory send OK.
```

   Jeg logger ind og ser en række forskellige directories - for bekvemmelighedens skyld henter jeg det hele ned på min egen maskine med
   wget -r ftp://anonymous:@20.240.4.10/

```
┌──(kali㉿kali)-[~/Desktop/5]
└─$ wget -r ftp://anonymous:@20.240.4.10/
```

3. Jeg kigger filerne i gennem manuelt og ser der er en række billedfiler. Jeg uploader dem til https://www.aperisolve.com/ og i billedet i

notsecret/alliance_med_nisserne.jpg er der gemt en .txt fil som er passwordprotected.

```
└─$ steghide extract -sf alliance_med_nisserne.jpg
Enter passphrase:
```

Det viser sig så at julemanden kom tidligt i år, for AperiSolve har angiveligt selv bruteforcet sig frem til koden og jeg kan downloade txt filen direkte derfra.

4. Jeg kopierer den mærkeligt string og bruger “Magic” i Cyberchef (https://gchq.github.io/CyberChef/) på den og får flaget

```
1 I en fortryllet skov, dybt inde i bjergene, levede en stolt stamme af brune
  bjørne og en festlig flok nisser. Hvert år, når vinteren dækkede skoven i et
  tæppe af sne, begyndte bjørnene og nisserne at mærke julemagien i luften. En
  dag, under det magiske julelys, besluttede de to samfund at danne en
  alliance for at sprede glæde og juleånd til alle skovens væsener.
2
3 Det startede med et møde mellem Bjørnekongen, en mægtig og klog leder blandt
  bjørnene, og Nisseoverhovedet, den erfarne leder af nisserne. De satte sig
  sammen i en cirkel af sne og talte om deres fælles ønske om at gøre skoven
  til et endnu mere magisk sted i juletiden
4
5
6 RkRDQXtBbGxJYU5jZV9NRURfTkkkNWVybmV9
7
```