
Hack The Box - Writeup

Forge

c1sc0



c1sc0 Guru

Rank: 399  462 ★ 19

hackthebox.eu

September 22, 2021

Table of Content

Overview	3
Nmap	3
/etc/hosts	3
Website	3
Subdomain enumeration	4
admin.forge.htb	5

Overview

IP	Difficulty
10.10.11.111	Medium

Nmap

```
sudo nmap -sC -sV -oA nmap/forge -vvv 10.10.11.111
```

```

1 PORT      STATE      SERVICE REASON          VERSION
2 21/tcp    filtered  ftp      no-response
3 22/tcp    open      ssh      syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu
    ↪ Linux; protocol 2.0)
4 | ssh-hostkey:
5 |   3072 4f:78:65:66:29:e4:87:6b:3c:cc:b4:3a:d2:57:20:ac (RSA)
6 | ssh-rsa
    ↪ AAAAB3NzaC1yc2EAAAADAQABAAQGC2sK9Bs3bKpmIER8QE1FzWwM0V/pval09g7BOCYMOZihHpPeE4S2aCt0oe9/KH
7 |   256 79:df:3a:f1:fe:87:4a:57:b0:fd:4e:d0:54:c6:28:d9 (ECDSA)
8 | ecdsa-sha2-nistp256
    ↪ AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBH67/BaxpvT3XsefC62xfP5fvtdKxG2J2di6u8wup
9 |   256 b0:58:11:40:6d:8c:bd:c5:72:aa:83:08:c5:51:fb:33 (ED25519)
10 | _ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAILcTSbyCdqkw29aShdKmVhnudyA2B6g6ULjspAQpHLIC
11 80/tcp    open      http      syn-ack ttl 63 Apache httpd 2.4.41 ((Ubuntu))
12 |_http-title: Did not follow redirect to http://forge.htb
13 |_http-server-header: Apache/2.4.41 (Ubuntu)
14 | http-methods:
15 |_ Supported Methods: GET HEAD POST OPTIONS
16 Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

/etc/hosts

80 redirects to `forge.htb`. So adding it to `/etc/hosts`

[[Pasted image 20210922093500.png]]

Website

[[Pasted image 20210922093610.png]]

Interesting “Upload an image” button top right

[[Pasted image 20210922094015.png]]

Looks like you can either provide file or enter URL.

Uploading images works, whereas uploading a cmd shell for example doesn't.

If you try and choose to upload from URL the box will callback to you:

```

1 > sudo ncat -lnvp 80
2 [sudo] password for patrick:
3 Ncat: Version 7.92 ( https://nmap.org/ncat )
4 Ncat: Listening on :::80
5 Ncat: Listening on 0.0.0.0:80
6 Ncat: Connection from 10.10.11.111.
7 Ncat: Connection from 10.10.11.111:38550.
8 GET /foo.png HTTP/1.1
9 Host: 10.10.14.8
10 User-Agent: python-requests/2.25.1
11 Accept-Encoding: gzip, deflate
12 Accept: */*
13 Connection: keep-alive

```

Subdomain enumeration

Wfuzz will reveal another subdomain:

```

1 > wfuzz -c -w
   ↪ ~/tools/wordlists/SecLists/Discovery/DNS/subdomains-top1million-5000.txt -u
   ↪ 'http://forge.htb' -H "Host: FUZZ.forge.htb" --hw 26
2 *****
3 * Wfuzz 3.1.0 - The Web Fuzzer *
4 *****
5
6 Target: http://forge.htb/
7 Total requests: 4989
8
9 =====
10 ID           Response  Lines  Word  Chars  Payload
11 =====
12
13 000000024:  200        1 L    4 W    27 Ch  "admin"
14
15 Total time: 0
16 Processed Requests: 4989
17 Filtered Requests: 4988
18 Requests/sec.: 0

```

So adding it to `/etc/hosts` and again look at the resulting page.

admin.forge.htb

[[Pasted image 20210922094923.png]]

So the idea is to leverage a vulnerability at the upload from URL part to look at `admin.forge.htb` from internally.

[[Pasted image 20210922095028.png]]