Reconnaissance Fundamentals – Exam

Execution Summary

- You are hired to perform a digital investigation for the following target: **185.218.124.165**
- This is a template for **uploading your screenshots and data**.
- The exam objective is to utilize active and passive reconnaissance to identify stored online ssh private key.
- Finding exposed public ssh key does not complete the exam objective.
- You are free to report vulnerabilities if you find any along the way. Each vulnerability gives extra points.
- Not all vulnerabilities are giving the same number of points.
- The order of the vulnerabilities **DO NOT MATTER**, nor the tools used to get to them.
- You are free to upload multiple **screenshots** for each **vulnerability**, including your **path** and how did you **find** it.
- **No network breach or local privilege escalation is needed!**

Do not overstress or overcomplicate it. The time is enough, you can do it.

Scope

Scope is open, meaning you can perform your own information gathering and you are free to enumerate the target for vulnerabilities from every angle.

Appendix

This is the data section. Make sure to **detail each finding**. The overall vulnerability count is unknown, try to **find as much as possible** while following the **main objective**. It is a good practice to **explain your finding**.

When describing your finding, make sure to be as clear as possible by **answering** the following **questions**:

1. What is the vulnerability I found?
2. How did I find it?
3. What "bad" can happen, what risk does it carry?

After the description, make sure to **drop** your **screenshots** below.

Vulnerability 1

Description: Old Verison
1. Initial Nmap Scan **Conducted a basic port scan using:**

sudo nmap -p- 185.218.124.165 -vv

Open Port Detected: Port 80 (HTTP) was accessible.

2. Version Detection

Performed service version scanning with:

sudo nmap –sC –sV 185.218.124.165 –p 80 -vv

Identified Software: Apache 2.4.62 (outdated).

3. Vulnerability Assessment

Searched for known exploits using:

searchsploit Apache 2.4.62

Critical Vulnerabilities Found:

CVE-2023-25690 – HTTP Request Smuggling (potential RCE/DoS).

CVE-2023-27522 – Mod_proxy misconfiguration (possible SSRF).

Additional risks due to unpatched CVEs and misconfigurations.

4. Risk Evaluation

Severity: High (exploitable for remote code execution or service disruption).

Recommendations:

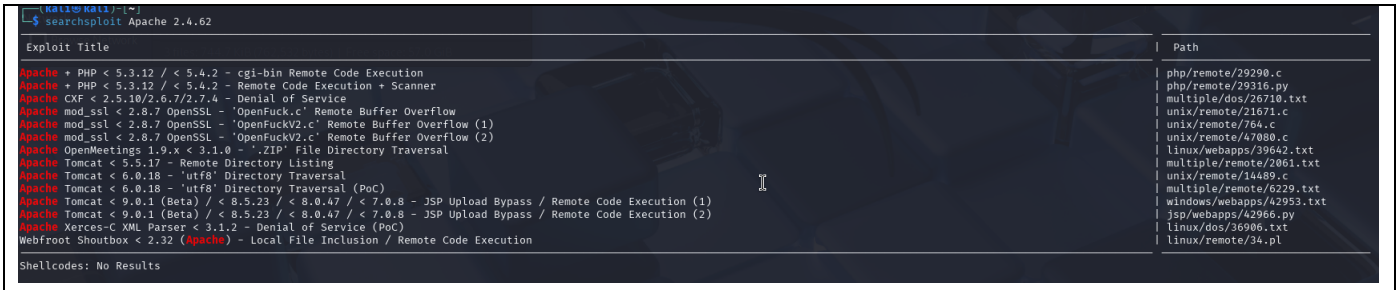
Immediate Action: Upgrade to the latest stable Apache version.

Hardening: Review and secure server configurations (e.g., disable unused modules).

Mitigation: Deploy a WAF (Web Application Firewall) as an interim measure.

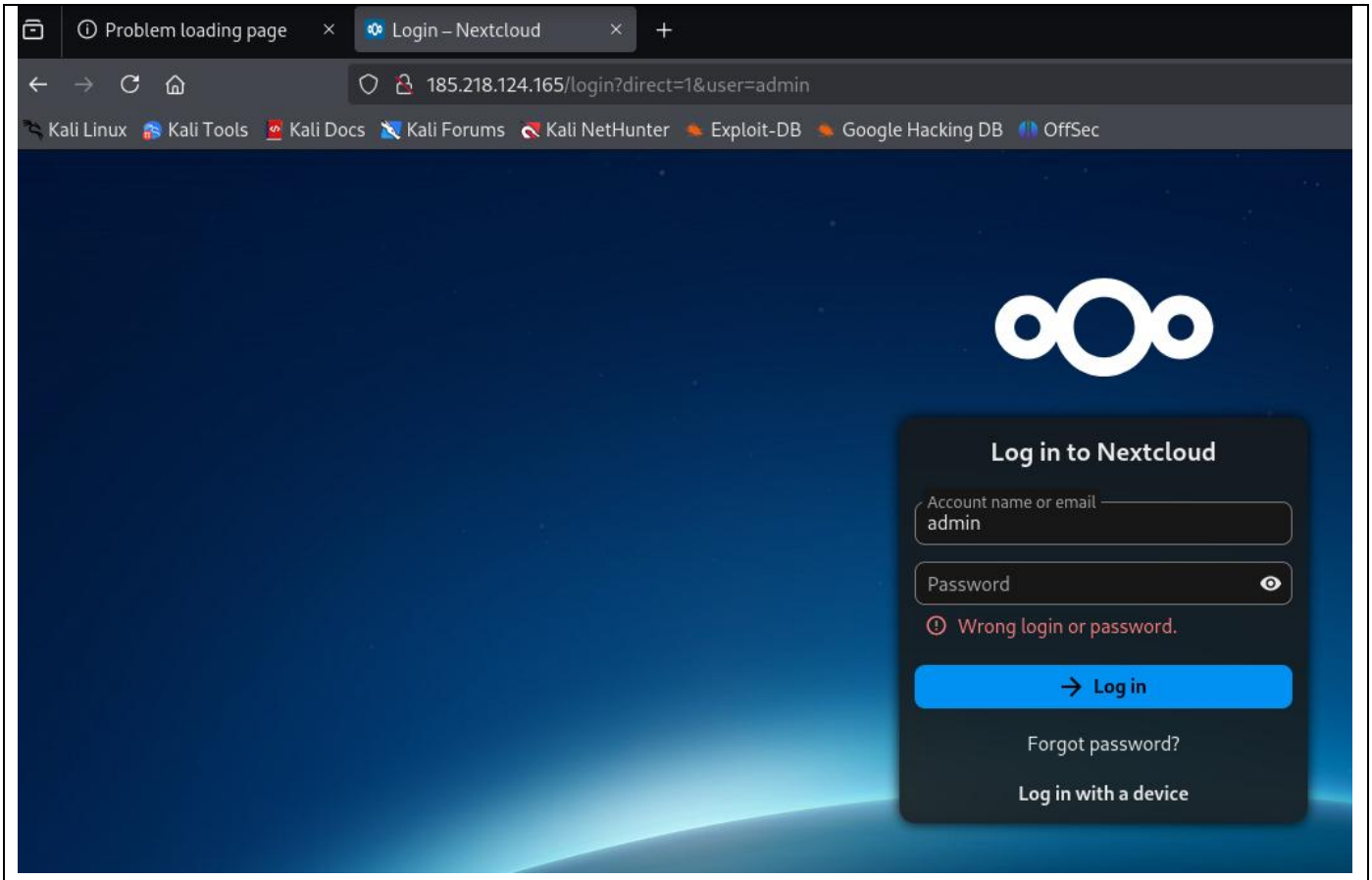
Screenshots:

```
PORT   STATE SERVICE REASON         VERSION
80/tcp open  http    syn-ack ttl 56 Apache httpd 2.4.62 ((Debian))
|_http-title: Nextcloud
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.4.62 (Debian)
```



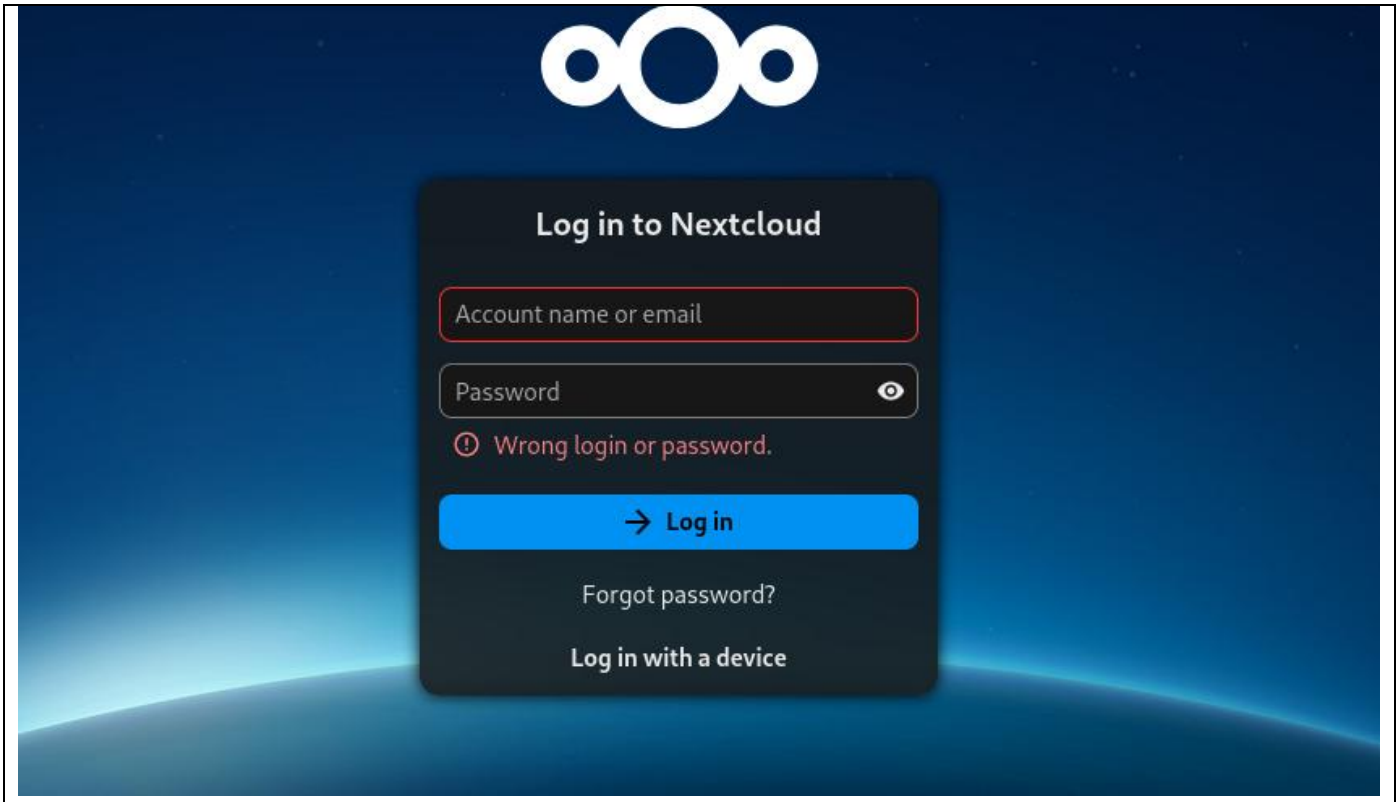
Vulnerability 2

Description: Lack of HTTPS Encryption
Risk Level: Medium/High (depending on data sensitivity) **Affected Service: Apache 2.4.62 (Port 80 - HTTP)** **Description** **The web server does not enforce HTTPS, transmitting all data over unencrypted HTTP. This exposes sensitive information (e.g., credentials, session tokens) to:** **Eavesdropping (Man-in-the-Middle attacks).** **Session hijacking (via network sniffing).** **Stripping attacks (downgrading HTTPS → HTTP).**
Screenshots:
->



Vulnerability 3

Description: Lack of Login Attempt Restrictions (Brute Force Possible)
->Risk Level: Medium/High (depending on authentication sensitivity) **Affected Page: http:// 185.218.124.165 /login** **Description** **The login page does not enforce account lockout or rate-limiting mechanisms, allowing:** **Unlimited password guesses (brute force/dictionary attacks).** **Credential stuffing (testing leaked passwords).** **Enumeration of valid usernames (via error messages).**
Screenshots:
->



Vulnerability 4

Description: Exposed SSH Service (OpenSSH 8.2p1 with Weak Configurations)

->Risk Level: High (Attack Surface Expansion)

Affected Service: OpenSSH 8.2p1 Ubuntu 4ubuntu0.5 (Port 22/TCP)

1. Discovery Evidence

sudo nmap –sC –sV 185.218.124.165 –p 22 –vv

2. Key Exposure Analysis

Public Host Keys Exposed:

RSA (4096-bit)

- **Fingerprint: ea:1e:52:90:7f:f5:c2:e1:9f:5f:8e:24:56:45:dd:17**
- **Full Public Key:**
  AAAAB3NzaC1yc2EAAAADAQABAAACAQC6fl7CgasnpSQF438esBoZW2dnpfAJYnuUcaMenUuhT1ukrIBa+z+5Vp7WCgEzfuJRczNumpi397NAr7L/+SHwP4T/ULSYjQEFc0vj4u1Nfys7Q/74j/qBEiO8E/WZ+ywS3E2QobpuFIloxFHVqDmxjpxzer8IBTwjxoh4KsAmFzvTf/7aAUUC0aNBYL6G10l0zImw0gjVMRsgj3Z4+khy/u04KBB9Rhwd2l33qGMqdyzBcN1K2CSNf4nHnm32qw2azj5gPsXV4k2MPbGPRdE9shjjR1zKqfmirQ1MP7NcM/6L/6YfwN1L4wccGlnUR+VwNJVfHRQ0hpeMfSB6ScFHA1yyxKxUczCGYO6/2aQn9kw0d1zAGBAHHHvssc8gMlmMXW7PNOoggcBsAF6MD5PLWiT7LzO80dnCU5dbL4yJiCXUVZdk7uXywKr8Oz9LBSQv5bnIuFYc6+wcC932j8OfPfhpM20xfSQY9hN7HVp/rjRn4wGrUh36TfYpQU0jnHsgD0z18aEoUqCstUsqUP3I1dKaILqNERQbMMzzwmkZFWxJrsbaspIl058Ht74Hvn7IxdVkclUL675H7+2AWipFCn+S9OIuLCWwqOHDJly9lWp4BCBw4trNjDCJYsuYwQCBHPm1yzVLueroFKgbWj52XuDn4HC8XXBe5Kb+9goZqQ==

ECDSA (256-bit)

- **Fingerprint: 30:88:10:70:db:8d:98:cc:8e:b6:c5:45:f4:5c:1e:da**
- **Full Public Key:**
  AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHfFgQijun8oK4a3El5kOjRgSaEdIAV

2rt/b0Na7KT98L2GrxrPk9g74lFna9HbBdQG7BtaSuHT/Ayqz3HmD3Po=

ED25519 (256-bit)

- **Fingerprint: 37:b8:44:8e:d2:8a:3a:d8:e9:dc:56:a9:4a:a7:c3:d6**
- **Full Public Key: AAAAC3NZaC11ZDI1NTESAAAATDrWxHT3RN/KKPeJNJCE5ZLB4FAODSFUTEINSXAdFFjd**

Screenshots:

->

Vulnerability 5

Description: MySQL Root Account with Weak Password (Unauthenticated Access)

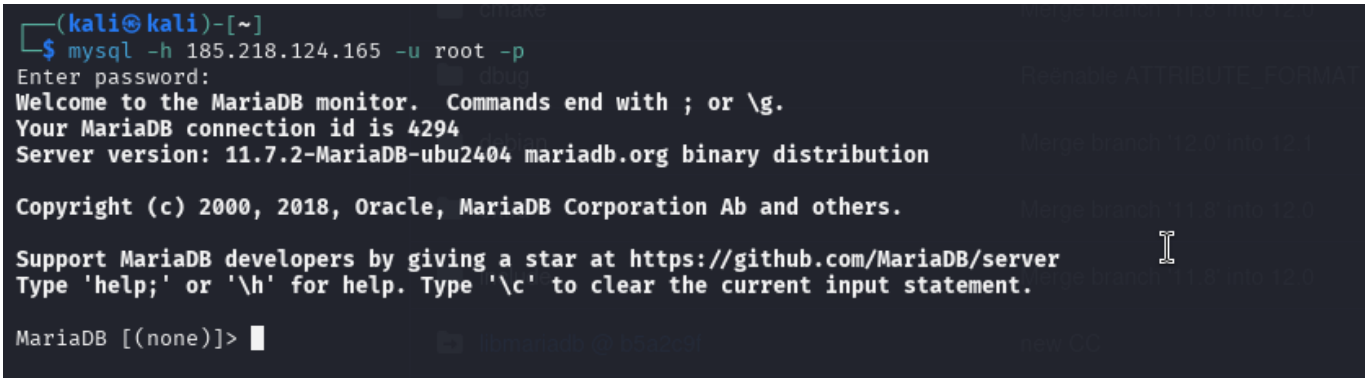
-> Risk Level: Critical (9.8/10 CVSS)

Affected Service: MySQL (Port 3306/TCP)

I scan with command:

mysql -h 185.218.124.165 -u root –p → Then I access the database with password: admin

Screenshots:



Vulnerability 6

Description: Public Exposure of SSH KEY in Pastebin

1.I started by accessing the MySQL database using the password "admin."

2.I executed the command **`SHOW DATABASES;`** to review the available databases.

3.Then, I used the command **`SELECT * FROM oc_users;`** to retrieve a list of all users and their corresponding passwords (encrypted).

4.Using the information from the database, I logged into the “netcloud” website on port 80 with the

username “admin” and a password that was the same as the user “rambo” (from the attached screen-shot).This is also a weak configuration because both of them are using same passwords in database.

5.I accessed the site’s admin panel and opened the file **example.md.**

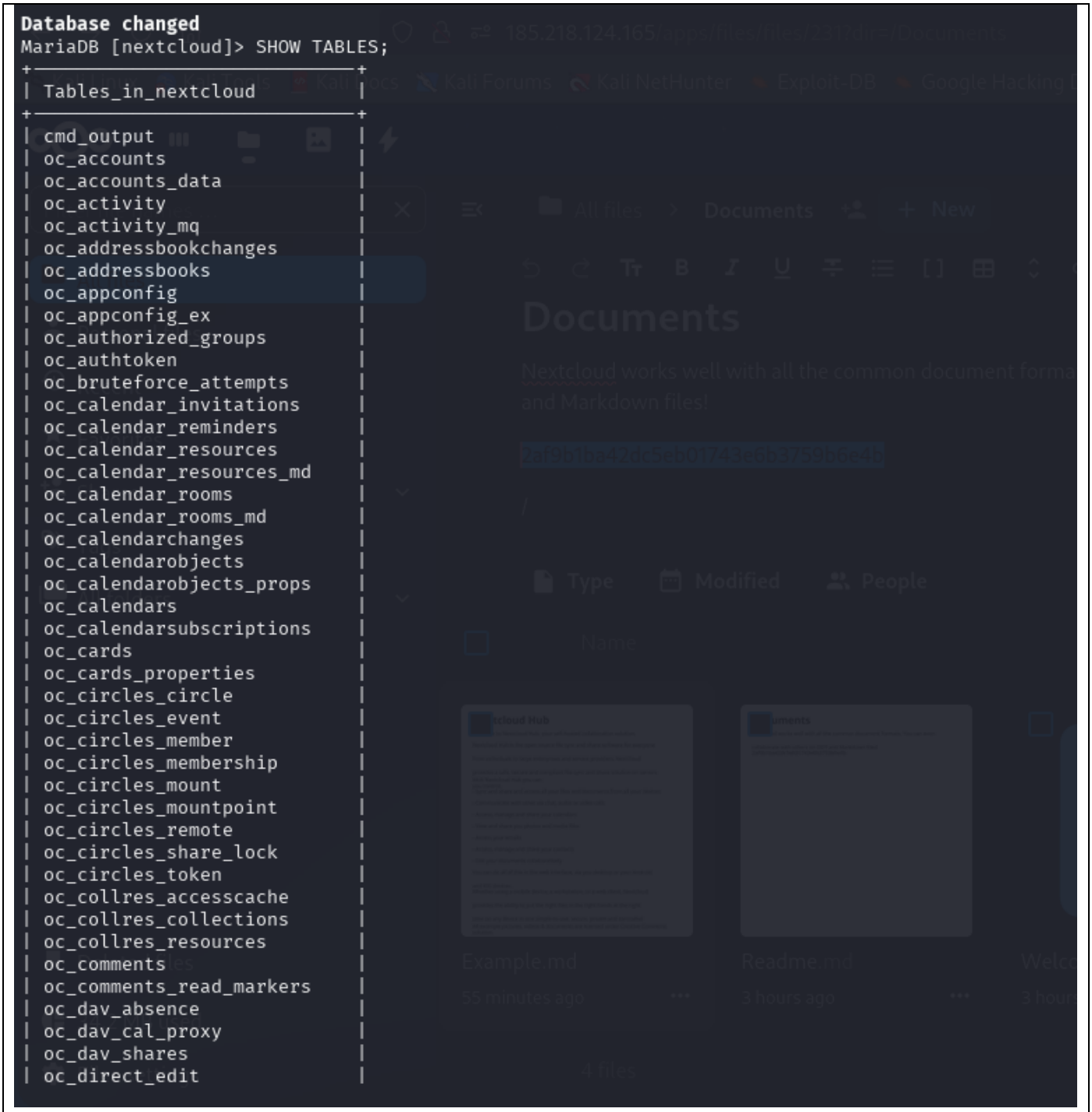
6.In that file, I found a link to Pastebin, which contained additional information.

7.In Pastebin, I found a password that was hashed — I decrypted it using a suitable tool.

8.Next, I took the hash obtained from Pastebin and decoded it again using the website https://www.base64decode.org/.

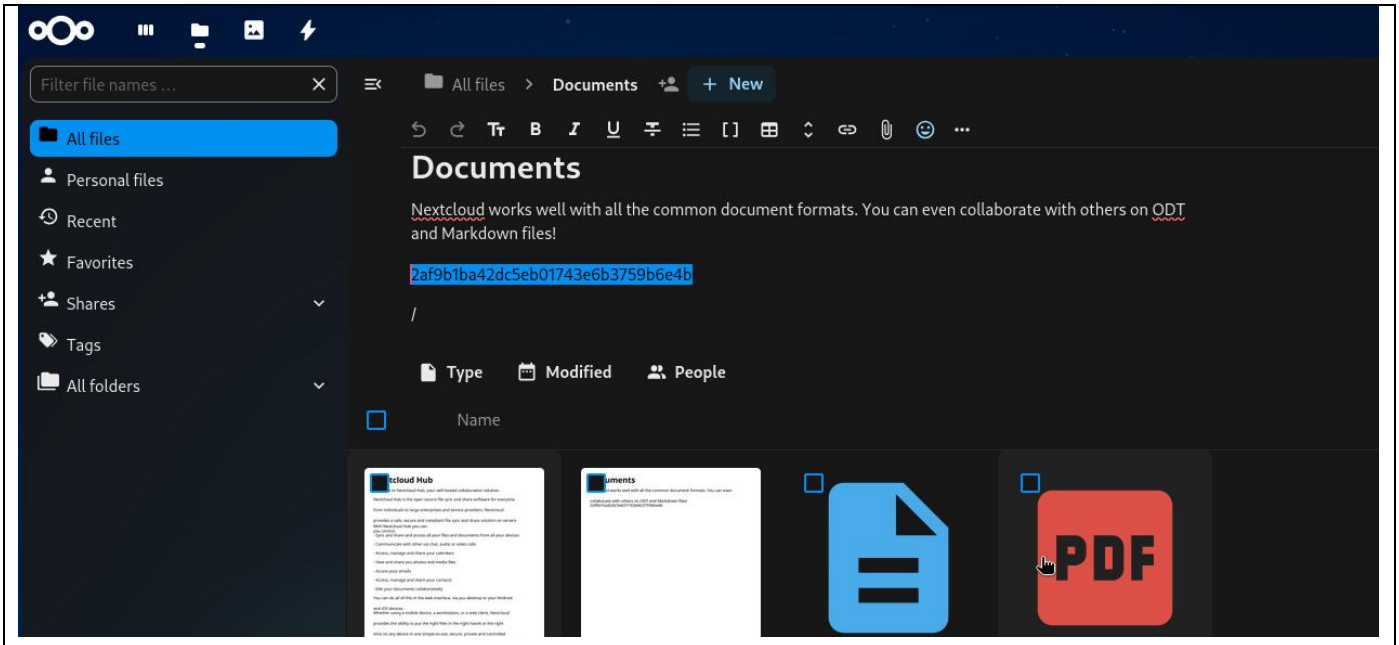
9.As a result, I obtained a private SSH key, which was necessary to pass the exam.

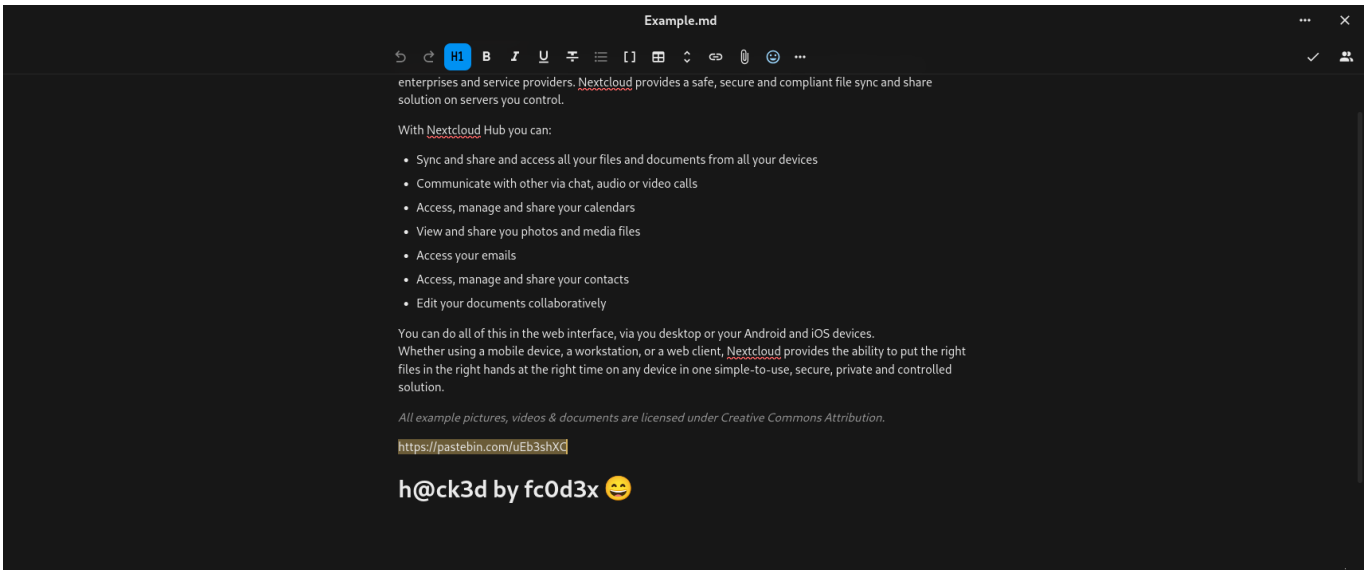
Screenshots:



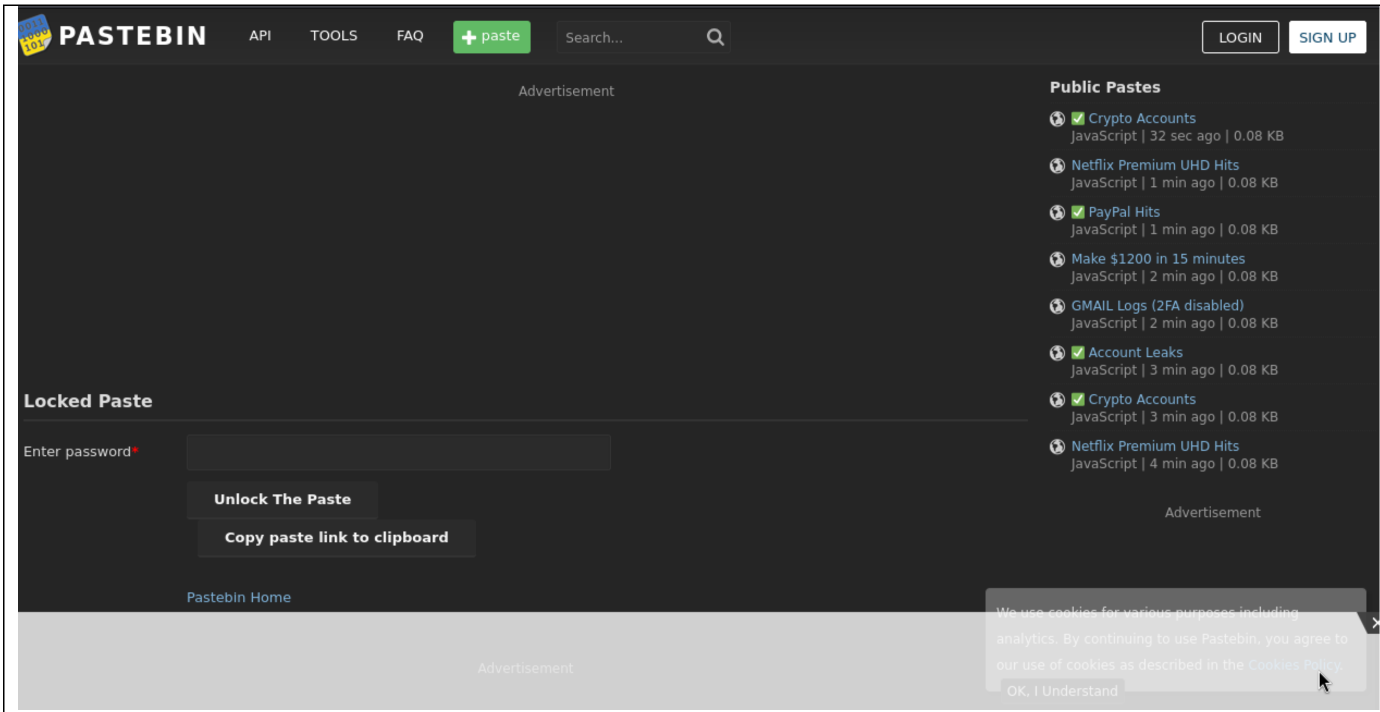
```
Database changed
MariaDB [nextcloud]> SHOW TABLES;
+-------------------------------+
| Tables_in_nextcloud           |
+-------------------------------+
| cmd_output                    |
| oc_accounts                   |
| oc_accounts_data              |
| oc_activity                   |
| oc_activity_mq                |
| oc_addressbookchanges         |
| oc_addressbooks               |
| oc_appconfig                  |
| oc_appconfig_ex               |
| oc_authorized_groups          |
| oc_authtoken                  |
| oc_bruteforce_attempts        |
| oc_calendar_invitations       |
| oc_calendar_reminders         |
| oc_calendar_resources         |
| oc_calendar_resources_md      |
| oc_calendar_rooms             |
| oc_calendar_rooms_md          |
| oc_calendarchanges            |
| oc_calendarobjects            |
| oc_calendarobjects_props      |
| oc_calendars                  |
| oc_calendarsubscriptions      |
| oc_cards                      |
| oc_cards_properties           |
| oc_circles_circle             |
| oc_circles_event              |
| oc_circles_member             |
| oc_circles_membership         |
| oc_circles_mount              |
| oc_circles_mountpoint         |
| oc_circles_remote             |
| oc_circles_share_lock         |
| oc_circles_token              |
| oc_collres_accesscache        |
| oc_collres_collections        |
| oc_collres_resources          |
| oc_comments                   |
| oc_comments_read_markers      |
| oc_dav_absence                |
| oc_dav_cal_proxy              |
| oc_dav_shares                 |
| oc_direct_edit                |
```

```
MariaDB [nextcloud]> SELECT * FROM oc_users;
+--------+--------------+------------------------------------------------------------------------------------------------------------------------------------+-------------+
| uid    | displayname  | password                                                                                                                           | uid_lower   |
+--------+--------------+------------------------------------------------------------------------------------------------------------------------------------+-------------+
| admin  | NULL         | 3|$argon2id$v=19$m=65536,t=4,p=1$VldNTWkwZzNCazAvbVhIbQ$eIle8UIi/feDDEYfdsoFwtOer2w6d8rKHARcdqUQ3Rs | admin       |
| john   | john         | OtEdnoDoOsem                                                                                                                       |             |
| rambo  | rambo        | MySuperSecretPass1                                                                                                                 |             |
| test   | test         | 3|$argon2id$v=19$m=65536,t=4,p=1$Gv2XBvWBlfKZgA0APUlc9w$wlwTkloPUXx6fKo1bVjxEjOZ2JuJxk6N9H35dfGiP+8 | test        |
| test-a | Test User A | $2y$10$VSlU.vxN3eQQz4SYQxRYWO9TOcwZYG7pJvjR9HkQ4BzKfNUeHzXlu                                                                       | test-a      |
+--------+--------------+------------------------------------------------------------------------------------------------------------------------------------+-------------+
5 rows in set (0.041 sec)
```


Filter file names ...
All files
Personal files
Recent
Favorites
Shares
Tags
All folders
All files
Documents
New
Documents
Nextcloud works well with all the common document formats. You can even collaborate with others on ODT and Markdown files!
2af9b1ba42dc5eb01743e6b3759b6e4b
/
Type
Modified
People
Name
PDF


Example.md
H1
enterprises and service providers. Nextcloud provides a safe, secure and compliant file sync and share solution on servers you control.
With Nextcloud Hub you can:
Sync and share and access all your files and documents from all your devices
Communicate with other via chat, audio or video calls
Access, manage and share your calendars
View and share you photos and media files
Access your emails
Access, manage and share your contacts
Edit your documents collaboratively
You can do all of this in the web interface, via you desktop or your Android and iOS devices.
Whether using a mobile device, a workstation, or a web client, Nextcloud provides the ability to put the right files in the right hands at the right time on any device in one simple-to-use, secure, private and controlled solution.
All example pictures, videos & documents are licensed under Creative Commons Attribution.
https://pastebin.com/uEb3shXC
h@ck3d by fc0d3x


2af9b1ba42dc5eb01743e6b3759b6e4b



This was the hash I found:

**SSBob3BlIHRoaXMgbGV0dGVyIGZpbmRzIHlvdSB3ZWxsLCBwZXJoYXBzIGV2ZW4gaW4gdGhlIG1pZHN0IG9mIHNv
bWUgZXhjaXRpbmcgY29kaW5nIGFkdmVudHVyZXMhCgpJIHdhbnRlZCB0byB0YWtlIGEgbW9tZW50IHRvIGV4dGV
uZCBhIHdhcm0gZ3JlZXRpbmcgeW91ciB3YXkuIEhhY2tpbmcsIGFmdGVyIGFsbCwgaXMgYSBjcmFmdCB0aGF0IHJlc
XVpcmVzIGluZ2VudWl0eSwgY3JlYXRpdml0eSwgYW5kIGEga2VlbiBzZW5zZSBvZiBleHBsb3JhdGlvbi4gWW91ciBh
YmlsaXR5IHRvIG5hdmlnYXRlIHRoZSBkaWdpdGFsIHdvcmxkIHdpdGggZmluZXNzZSBhbmQgY3VyaW9zaXR5IGlzIH
RydWx5IHJlbWFya2FibGUuCgpXaGlsZSBvdXIgcGF0aHMgbWF5IG5vdCBhbHdheXMgaW50ZXJzZWN0IGluIHRoZS
Btb3N0IGNvbnZlbnRpb25hbCBvZiBjaXJjdW1zdGFuY2VzLCBJIGFkbWlyZSB0aGUgcGFzc2lvbiBhbmQgc2tpbGwge
W91IGJyaW5nIHRvIHlvdXIgZW5kZWF2b3JzLiBZb3VyIGtuYWNrIGZvciB1bnJhdmVsaW5nIGNvbXBsZXhpdGllcyBh
bmQgcHVzaGluZyBib3VuZGFyaWVzIGlzIGJvdGggaW1wcmVzc2l2ZSBhbmQgaW50cmlndWluZy4KCkFzIHlvdSBuY
XZpZ2F0ZSB0aGUgdmFzdCBleHBhbnNlcyBvZiBjeWJlcnNwYWNlLCBJIGVuY291cmFnZSB5b3UgdG8gY29udGludW
UgeW91ciBxdWVzdCBmb3Iga25vd2xlZGdlIGFuZCBtYXN0ZXJ5LiBSZW1lbWJlciwgd2l0aCBncmVhdCBwb3dlciBjb2
1lcyBncmVhdCByZXNwb25zaWJpbGl0eSwgYW5kIHRoZSBjaG9pY2VzIHlvdSBtYWtlIGNhbiBzaGFwZSB0aGUgZGln
aXRhbCBsYW5kc2NhcGUgaW4gcHJvZm91bmQgd2F5cy4KClNvLCBoZXJlJ3MgdG8geW91LCBkZWFyIGhhY2tlciwg
bWF5IHlvdXIga2V5c3Ryb2tlcyBiZSBzd2lmdCwgeW91ciBhbGdvcml0aG1zIGVsZWdhbnQsIGFuZCB5b3VyIGV4cGx
vaXRzIGV0aGljYWxseSBzb3VuZC4gS2VlcCBjb2RpbmcsIGtlZXAgZXhwbG9yaW5nLCBhbmQgbWF5IHlvdXIgZGlnaX
RhbCBhZHZlbnR1cmVzIGJlIGZpbGxlZCB3aXRoIGV4Y2l0ZW1lbnQgYW5kIGRpc2NvdmVyeS4KClllcywgdGhpcyBpc
yBmcm9tIEdQVC0zLjUKCk5ldmVybWluZCwgeW91IFBBU1MsIGhlcmUgaXMgeW91ciBrZXk6CgotLS0tLUJFR0lOIE9
QRU5TU0ggUFJJVkFURSBLRVktLS0tLQpiM0JsYm5OemFDMXJaWGt0ZGpFQUFBQUFCRzV2Ym1VQUFBQUVibTl1
WlFBQUFBQUFBQUFCQUFBQmx3QUFBQWR6YzJndGNuCk5oQUFBQUF3RUFBUUFBQVlFQXNpN3lNNzhJUEQzL3J
SRm9scVpUi9xejRFUktUTlp0R0ZRZnVSSlZhNjV3Z0rM3hQZVYKbGZlNU9mNkF6Q2NRamt2Vm1MRnBYRDdmcz
NEUzY0M2t2b1JOSHFLN2J3VUdXeTJid2RRYnJiQzNvUjc2VlFjSUFDRytDQgozVUxkSUlXdjVkMHF5Y3FteStLcDFUait
iUXhSNWd2bHB4UG56Z1kvSXpMREdWcU9YNDlKeVZlN3ZnRThjcWxERWdRM1NTCkptRzBaa1kzMHB1WUdPOV
M5emJUSTYyeHZjbm1lL05idlBWZThoRXN4TDBPU0tHYk8vQ05LY0pHcFBYWnJhL2FtQUlWY2UKUFNvMEg4L2dFR
nJjNm1qVFdMVXBvTHM2L3ZobzZnUENsSklwQmhkZGsrRkd3Qk5sVUFLRENVU0NkSVorVlBsWnRqc0RnNnprTEd
0ZGk1WkF6YVJpOFZuak1zeUR1bEpNcE85VG1ST2NiMWF2RlJ5QzBZVjN5dVIyWlRMRmlFRlNJdVRMRnpzenZWM
TA0CndGN25rdEx5b0FrYncd1Vva1BFVHA0RUFSVCtiTzZNNDBSMFB4YmJnaXJMUWlzaVBSWGpMekxLUm9JZ3R
1QXRSb1B6a3oKRkEvS1IzWkFpMnZUMTdvbkphM0tqNlF2eVljSU1UQkY4M254S3BNbkFBQUZrSFNNSZEVOMGtYU
kRBQUFBQjNOemFDMXljMgpFQUFBR0JBTEl1OGpPL0NEdkpSYUtFdzkvNjBSYUpFU2NTYUFpN2ZNNGxZaFFhVVZIN2tVWld1dW
NJQi90OFQzbFpYM1VbitnTXduCkVJNUwxWml4YVZZZ3KzM3TncwdXVONUw2RVRSNml1MjhGQmxzdG04SFVHN**

J3dDZFZStsVUhDQUFodmdnZDFDM1NDRnIrWGQKS3NuS3BzdmlxZFU0L20wTVVlWUw1YWNUNTg0R1B5TXl3eG
xhamwrUFNjbFh1NzRCUEhLcFF4SUVOMGtpWmh0R1pHTjlLYgptQmp2VXZjMjB5T3RzYjNKNW52elc3ejFYdklSTE
1TOURraWhtenZ3alNuQ1JxVDEyYTJ2MnBnQ0ZYSGowcU5CL1A0QkJhCjNPcG8wMWkxS2FDN092NzRhT29Ed3BT
U0tRWVhYWlBoUnNBVFpWQUNnd2xFZ25TR2ZsVDVXYlk3QTRPNUN4clhZdVdRTTIKa1l2Rlo0ekxNZzdwU1RLVH
ZVNWtUbkc5V3J4VWNndEdGZDhya2RtVXl4WWhCVWlMa3l4YzdNNzFkZE9NQmU1NUxTOHFBSgpHOFA4RktKR
HhFNmVCQUVVL216dWpPTkVkRDhXMjRJcXkwSXJJajBWNHk4eXlrYUNJTGJnTFVhRDg1TXhRUHlrZDJRSXRyCjA5
ZTZKeVd0eW8ra0w4bUhDREV3UmZONThTcVRKd0FBQUFNQkFBRUFBQUdBRDlwZHdkMHZET083NXppRGRIL1k
xZTZ3RS8KWFBkeXI1YXRtS2pGWHdFLzYyL2dwMFNGOGt4OEo4dXR4YUM0L2dNN1lyTmdUTUtjdTRReDFOenNK
VzhJZThoWFlYWDF4MApRU2JRMHZ2SVRmbWVqNFJvNDZsci9LTUQ1c2RNbjVwWkZFdDBWVEJNQWdlMGNGTX
VET3dOZFY3clh1bVV1MmxkM05hVUxLCkdVRTFlMEFOakdTS0RNWWh0dGFPRHBZaHhjSjhrTlJWb3krNWNoL3Zu
d0NPbXZwYlFvVDdQeWF6aHUyRG1CTGQvNXBUUVMKM01NYXczTDJydTZjM1c2NE9YRko4YWFDR2xjeEdFc2Rs
WEZub0dFQmxxUW1NUWQrNVhuY3hKemEvSVdwUW5MTGlkV1JVTQpURnhGcUFBRVdyZm05eFlQeVZJTDBkbn
BxSDZyVElZamkzQ05QbnkxblZTbUxlczdpclVZT1Rvems1K1JHZml0elpjbmNTCmZRaHZkM1l5QXkvRlJLT0s3YlBYel
pyalFOWFI2QjlvTVFwOWtyY0RhRmNNbzIvVTlmK1lhTmxxQmZWM2w4K3paTFc5K2wKQ1FhNUs0WkNmYmV6e
U9PTWtvNlVRZXhkYVB4R3JUb0p4anpDMzZ1ZzkrMHlPalZzRDBQZlNzblJJNWpLZUhERnBoQUFBQQp3UUNnUWd
PNVVvZG1MSHppUFJqZVhTVzRJbGg1Zmo0d1hzcGlMejMxYnBnVTl2RkUvTUhEdVcrOVlhN0dRVEthTUx0T3ROCl
N3cEgreTA1WCsxQnIzS0owNG5ZSWtMdGRvWXhCWDgwQVRMaWQyU3IxT1FEOXJZdWF4dWxMdEFjbXdhSDQ2
am5ZV1RvdVMKMlo3MS9XczBSVWpnSXV4T2J3S21tK2taUG45VnF4N1QzclFJcVh2N2RDZEx5dUpEaEZDSklkcUhy
OElUK0F4MEQ0U21HMAphS1JkOXhQNXpFYjNGUkhpbm5yL2x0UGNpSERUOEhsTVFxZ2FDaDNDTkM5eGwzYmZ
zQUFBREJBTGpFSHdzcGhLeDZCOHFQCnBzbGpSeG84cFlNc3hMQk4vMEgxSWFWZjJiZHorTCtRK2lOTmFVUG1iOG
dwaHBJaTdtOWJKZFArV1JNZ0xjeXpDQmRFS2wKYkdDYzEwZzZTQUM1RXZrV2h3Q3l3Y1BjNHY3TlpldlB0TU1kZlp
FTFduNWtKNENnNGlmMFA1Q05IMmYzUlZ1b09ZTng5dwozczJDQ2kwNTI5Z3lvVDlMZnVhbHFqa1ZlcVgrMUl5M
mhRTlgvM3J2L24zZ0NqUWZiRlY0N0dPVjNKUGtrVFFKL3VxTS84ClZKSHZoMDZXeHZmbVBUOHJiVE9EeHFBM1cw
OUs0cllRQUFBTUVBOXVFaFFGMDhzZzNPMlFkL3lVZlZaR1NROXRoTVJwTU0KdUIxREkrMFdoWVJqNGxtMzIyWEV
2dnhySjNFV0FSeDB0Rm12L3JRR1BpcHZLaXFhNkJyVEdmdm9PaDBrZnZlRUF0WERqRQpoVnQyRkR6Ni9hVmZVcX
RKYUhqY0VFL1hyV25UNGN4blBIdXQ4SkJFYVZqMW1tS2VTdjFvOE5QVXd5akU4Y2NXMVJJYmV4CjdDSmhENHNz
QVBDTzdxUFplTCtacTkyQWJkTVhNcmg2WmNESnBwTXkrZ1BJNmhvWFNLOWVjV3liK2YzREl1RVl0SVR2WncKK3
hzOVVGWDhsZ0NaT0hBQUFBR0d4elpXTkFiSE5sWXkxUWNtVmphWE5wYjI0dE56Y3hNQUVDCi0tLS0tRU5EIE9Q
RU5TU0ggUFJJVkFURSBLRVktLS0tLQ==

Then I got the answer:

-----BEGIN OPENSSH PRIVATE KEY-----

b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn

NhAAAAAwEAAQAAAYEAsi7yM78IPD3/rRFolqZTN/qz4ERKTNZtGFQfuRJVa65wgH+3xPeV

lfe5Of6AzCcQjkvVmLFpXD7fs3DS643kvoRNHqK7bwUGWy2bwdQbrbC3oR76VQcIACG+CB

3ULdIIWv5d0qycqmy+Kp1Tj+bQxR5gvlpxPnzgY/IzLDGVqOX49JyVe7vgE8cqlDEgQ3SS

JmG0ZkY30puYGO9S9zbTI62xvcnme/NbvPVe8hEsxL0OSKGbO/CNKcJGpPXZra/amAIVce

PSo0H8/gEFrc6mjTWLUpoLs6/vho6gPClJIpBhddk+FGwBNlUAKDCUSCdIZ+VPlZtjsDg7

kLGtdi5ZAzaRi8VnjMsyDulJMpO9TmROcb1avFRyC0YV3yuR2ZTLFiEFSIuTLFzszvV104

wF7nktLyoAkbw/wUokPETp4EART+bO6M40R0PxbbgirLQisiPRXjLzLKRoIgtuAtRoPzkz

FA/KR3ZAi2vT17onJa3Kj6QvyYcIMTBF83nxKpMnAAAFkHSRdEN0kXRDAAAAB3NzaC1yc2

EAAAGBALIu8jO/CDw9/60RaJamUzf6s+BESkzWbRhUH7kSVWuucIB/t8T3lZX3uTn+gMwn

EI5L1ZixaVw+37Nw0uuN5L6ETR6iu28FBlstm8HUG62wt6Ee+lUHCAAhvggd1C3SCFr+Xd

KsnKpsviqdU4/m0MUeYL5acT584GPyMywxlajl+PSclXu74BPHKpQxIEN0kiZhtGZGN9Kb

```
mBjvUvc20yOtsb3J5nvzW7z1XvIRLMS9DkihmzvwjSnCRqT12a2v2pgCFXHj0qNB/P4BBa
3Opo01i1KaC7Ov74aOoDwpSSKQYXXZPhRsATZVACgwlEgnSGfIT5WbY7A4O5CxrXYuWQM2
kYvFZ4zLMg7pSTKTvU5kTnG9WrxUcgtGFd8rkdmUyxYhBUiLkyxc7M71ddOMBe55LS8qAJ
G8P8FKJDxE6eBAEU/mzujONEdD8W24Iqy0Irlj0V4y8yykaCILbgLUaD85MxQPykd2QItr
09e6JyWtyo+kL8mHCDEwRfN58SqTJwAAAAMBAAEAAAGAD9pdwd0vDOO75ziDdH/Y1e6wE/
XPdyr5atmKjFXwE/62/gp0SF8kx8J8utxaC4/gM7YrNgTMKcu4Qx1NzsJW8Ie8hXYXX1x0
QSbQ0vvITfmej4Ro46lr/KMD5sdMn5pZFEt0VTBMAge0cFMuDOwNdV7rXumUu2ld3NaULK
GUE1e0ANjGSKDMYhttaODpYhxcJ8kNRVoy+5ch/vnwCOmvpbQoT7Pyazhu2DmBLd/5pTQS
3MMaw3L2ru6c3W64OXFJ8aaCGlcxGEsdlXFnoGEBlqQmMQd+5XncxJza/IWpQnLLidWRUM
TFxFqAAEWrfm9xYPyVIL0dnpqH6rTIYji3CNPny1nVSmLes7irUYOTozk5+RGfitzZcncS
fQhvd3YyAy/FRKOK7bPXzZrjQNXR6B2/MQp9krcDaFcMo2/U9f+YaNlqBfV3l8+zZLW9+l
CQa5K4ZCfbezyOOMko6UQexdaPxGrToJxjzC36ug9+0yOjVsD0PfSsnRI5jKeHDFphAAAA
wQCgQgO5UodmLHziPRjeXSW4Ilh5fj4wXspiLz31bpgU9vFE/MHDuW+9Ya7GQTKaMLtOtN
SwpH+y05X+1Br3KJ04nYIkLtdoYxBX80ATLid2Sr1OQD9rYuaxulLtAcmwaH46jnYWTouS
2Z71/Ws0RUjgIuxObwKmm+kZPn9Vqx7T3rQIqXv7dCdLyuJDhFCJIdqHr8IT+Ax0D4SmG0
aKRd9xP5zEb3FRHinnr/ltPciHDT8HlMQqgaCh3CNC9xl3bfsAAADBALjEHwsphKx6B8qP
psljRxo8pYMsxLBN/0H1IaVf2bdz+L+Q+iNNaUPmb8gphpIi7m9bJdP+WRMgLcyzCBdEKl
bGCc10g6SAC5EvkWhwCywcPc4v7NZevPtMMdfZELWn5kJ4Cg4if0P5CNH2f3RVuoOYNx9w
3s2CCi0529gyoT9LfualqjkVeqX+1Iy2hQNX/3rv/n3gCjQfbFV47GOV3JPkkTQJ/uqM/8
VJHvh06WxvfmPT8rbTODxqA3W09K4rYQAAAMEA9uEhQF08sg3O2Qd/yUfVZGSQ9thMRpMM
uB1DI+0WhYRj4lm322XEvvxrJ3EWARx0tFmv/rQGPipvKiqa6BrTGfvoOh0kfveEAtXDjE
hVt2FDz6/aVfUqtJaHjcEE/XrWnT4cxnPHut8JBEaVj1mmKeSv1o8NPUwyjE8ccW1RIbex
7CJhD4ssAPCO7qPZeL+Zq92AbdMXMrh6ZcDJppMy+gPI6hoXSK9ecWyb+f3DIuEYtITvZw
+xs9UFX8lgCZOHAAAAGGxzZWNAbHNlYy1QcmVjaXNpb24tNzcxMAEC
-----END OPENSSH PRIVATE KEY-----
```

Writeup

Step-by-step summary of my reconnaissance process Step 1: Initial scan with active nmap scan. **1.Command: sudo nmap -p- 185.218.124.165 –vv**

2. Command: sudo nmap –sC –sV 185.218.124.165 –p 80 -vv

Determine the version of the server hosted on port 80. Then report a vulnerability for an old version of the server that was hosted.

Step 2: 1. Initial Observation

When visiting the website (http://185.218.124.165) I noticed that the connection is made only via HTTP protocol - there is no automatic redirection to HTTPS. The address does not start with "https://".

2. Verification with Nmap and Browser

When scanning with nmap, port 443 (HTTPS) was not found open:

sudo nmap -p 443 185.218.124.165

Result: port 443 closed/unavailable.

Step 3:

Search for the login page at:

http://185.218.124.165/login

When manually trying to enter incorrect usernames and passwords, I noticed that there is no limit to the number of attempts (no temporary blocking or maintenance after several incorrect entries).

Attempts to make several consecutive unsuccessful logins without getting an error when blocking the account or saving.

Consequences:

Allows unlimited login attempts with different passwords (brute force or dictionary attacks).

Can be used to fill in credentials - automatically testing leaked passwords from other sites.

For various errors when entering a username, an enumeration (enumeration) of valid accounts can be done.

Step 4:

Methodology:

I used nmap to detect and analyze the SSH service running on port 22 of the IP address 185.218.124.165.

The command executed:

sudo nmap -sC -sV 185.218.124.165 -p 22 -vv

-sC for default scripts scan

-sV for service/version detection

-p 22 to scan only port 22 (SSH)

-vv for verbose output

Step 5:

Methodology:

I tested if the MySQL service was accessible on port 3306 by attempting to connect directly to the database.

Command used:

mysql -h 185.218.124.165 -u root -p

At the password prompt, I entered admin.

Findings:

Successfully logged into the MySQL database using the root user with the password admin.

This indicates that the main administrative account uses a weak and easily guessable password.

Step 6:

I accessed the admin panel in http://185.218.124.165/login . Then I went into all the files. I saw that there was text with a hash 2af9b1ba42dc5eb01743e6b3759b6e4b. After I unhash the text I noticed that this was the password that I needed. I started digging around the site and found a file called "Example.md". There was a pastebin link there, which I accessed. The unhash password that I found helped me log in to the pastebin link. From there I received another hashed message, which was the private ssh key that they required from us to pass the exam.

Tools Used: • gobuster • nmap • Browser • MySQL • searchsploit

The engagement concluded with direct discovery of an SSH private key, completing the exam objective. Thank you, Lachezar – this was a very interesting