

Host Report

10.10.10.222 - Linux 4.15 - 5.6

 Linux  Server - Shelled - Owned

Host Notes:

```
maildeliverer@Delivery:~$ cat user.txt
221a30fc0945b545cdae244f3bcd5c39
```

```
root@Delivery:/home/maildeliverer# cat /root/root.txt
7a45d541ae205e66534b0b5821645888
```

Ports:

Port	Proto	Service	Version	Status
22	tcp	ssh	OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)	Owned

Port Notes:

SSH using maildeliverer:Youve_G0t_Mail!

```
(kali㉿kali)-[~/Desktop/HTB/Delivery]
└─$ ssh maildeliverer@10.10.10.222
The authenticity of host '10.10.10.222 (10.10.10.222)' can't be established.
ED25519 key fingerprint is SHA256:AGdhHnQ749stJakbrtXVi48e6KTkaMj/+QNYMW+tyj8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.222' (ED25519) to the list of known hosts.
maildeliverer@10.10.10.222's password:
Linux Delivery 4.19.0-13-amd64 #1 SMP Debian 4.19.160-2 (2020-11-28) x86_64

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.
Last login: Tue Jan  5 06:09:50 2021 from 10.10.14.5
maildeliverer@Delivery:~$ █
```

```
maildeliverer@Delivery:~$ cat user.txt
221a30fc0945b545cdae244f3bcd5c39
```

Researching MatterMost, we discover this possible vector. <https://docs.mattermost.com/configuration/configuration-settings.html>

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

```
(kali㉿kali)-[~/Desktop/HTB/Delivery]
└─$ john ./root_hash --wordlist=./wordlist.txt
Using default input encoding: UTF-8
Loaded 1 password hash (bcrypt [Blowfish 32/64 X3])
Cost 1 (iteration count) is 1024 for all loaded hashes
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
PleaseSubscribe!21 (?)
1g 0:00:00:00 DONE (2022-01-17 07:01) 2.631g/s 189.4p/s 189.4c/s 189.4C/s PleaseSubscribe!..PlesPles
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

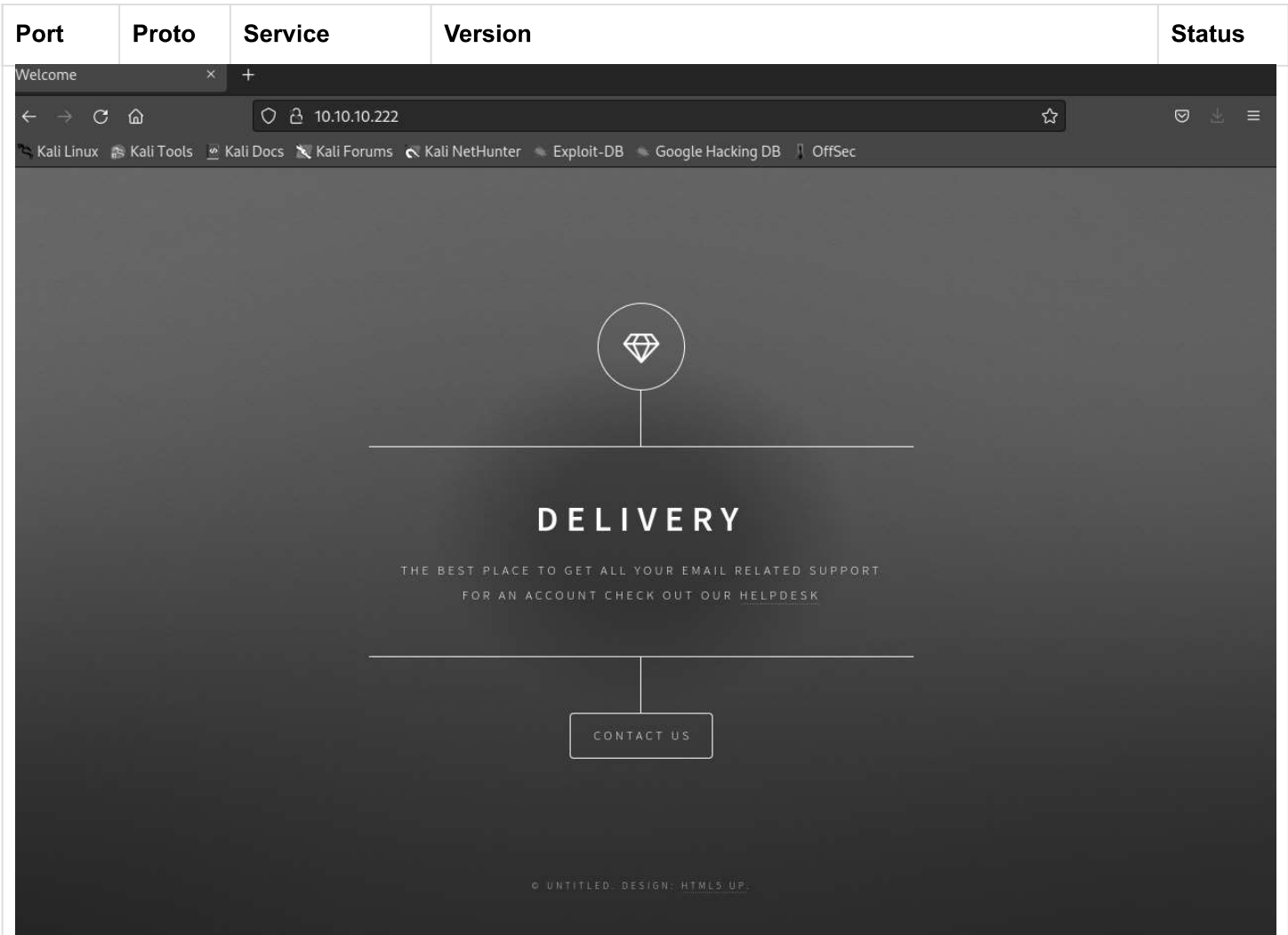
```
maildeliverer@Delivery:~$ su root
Password:
root@Delivery:/home/maildeliverer# whoami
root
root@Delivery:/home/maildeliverer# hostname
Delivery
root@Delivery:/home/maildeliverer# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group default qlen 1000
    link/ether 00:50:56:b9:af:ee brd ff:ff:ff:ff:ff:ff
    inet 10.10.10.222/24 brd 10.10.10.255 scope global ens192
        valid_lft forever preferred_lft forever
    inet6 fe80::250:56ff:feb9:afee/64 scope link
        valid_lft forever preferred_lft forever
root@Delivery:/home/maildeliverer# cat /root/root.txt
7a45d541ae205e66534b0b5821645888
root@Delivery:/home/maildeliverer#
```

```
root@Delivery:/home/maildeliverer# cat /root/root.txt
7a45d541ae205e66534b0b5821645888
```

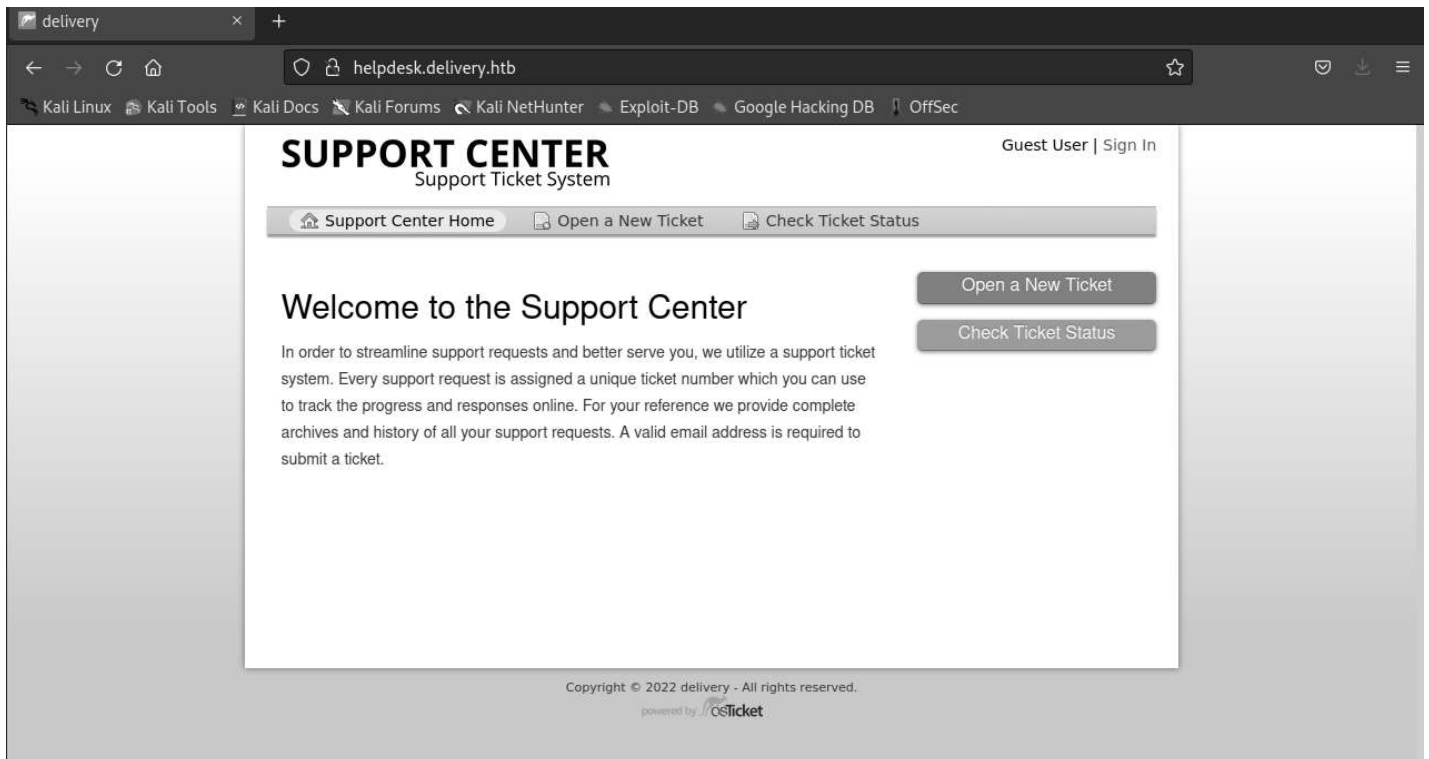
53	udp	domain		
67	udp	dhcps		
68	udp	dhcpc		
69	udp	tftp		
80	tcp	http	nginx 1.14.2	Owned

Port Notes:

http://10.10.10.222 provides us a landing page with 2 links. Contact Us and HelpDesk. Go for HelpDesk first.



Hitting the HelpDesk link wants to take us to <http://helpdesk.delivery.htb>. Add 10.10.10.222 delivery.htb helpdesk.delivery.htb to the /etc/hosts file and the page will render.



Port	Proto	Service	Version	Status
<p>From here, we can create a ticket with dummy information, if successful, we will get an @dilivery.htb email address that we can use to register for the link on the Contact Us Page.</p>				

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

SUPPORT CENTER

Support Ticket System

Guest User | Sign In

- [Support Center Home](#)
- [Open a New Ticket](#)
- [Check Ticket Status](#)

Open a New Ticket

Please fill in the form below to open a new ticket.

Contact Information

Email Address *

Full Name *

Phone Number

 Ext:

Help Topic

 *

Ticket Details

Please Describe Your Issue

Issue Summary *

<> | | Aa | B | / | U | | | | | | |

Testing reg link|

unsaved

Drop files here or choose them

CAPTCHA Text:



Enter the text shown on the image. *

-
-
-

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

SUPPORT CENTER

Support Ticket System

Guest User | [Sign In](#)

[Support Center Home](#) [Open a New Ticket](#) [Check Ticket Status](#)

✔ Support ticket request created


Neocount,

You may check the status of your ticket, by navigating to the Check Status page using ticket id: 9916822.

If you want to add more information to your ticket, just email 9916822@delivery.htb.

Thanks,

Support Team

Copyright © 2022 delivery - All rights reserved.
powered by 

Now we need to check the status of the ticket, register for the MatterMost link on the Contact Us page and then recheck the ticket status.

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------

[Guest User](#) | [Sign Out](#)

SUPPORT CENTER

Support Ticket System

[Support Center Home](#)
[Open a New Ticket](#)
[View Ticket Thread](#)

Looking for your other tickets?
[Sign In](#) or [register for an account](#) for the best experience on our help desk.

Contact Us #9916822 [Print](#) [Edit](#)

Basic Ticket Information	User Information
Ticket Status: Open	Name: Neocount
Department: Support	Email: neocount@delivery.htb
Create Date: 1/17/22 5:50 AM	Phone: (999) 999-9999

Neocount posted 1/17/22 5:50 AM

Testing reg link

Created by **Neocount** 1/17/22 5:50 AM

Post a Reply

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

Rich text editor toolbar: <> | [Text] | [Bold] | [Italic] | [Underline] | [List] | [Image] | [Video] | [Link] | [Unlink]

Drop files here or choose them

Post Reply Reset Cancel

Copyright © 2022 delivery - All rights reserved.
 powered by OSticket

And After, when MatterMost sends the registration confirmation email to the generated address from your ticket.

Copying the Validation Link : http://delivery.htb:8065/do_verify_email?token=naay75cky4ahmax8zrotpfwuh4omtp7uy7wwcednpzngoy518u99r756ajdqbd&email=9916822%40delivery.htb into a new tab, will validate your address and allow to log into MatterMost and allow us to view the Internal Team's chat chanell.

Port	Proto	Service	Version	Status
------	-------	---------	---------	--------



Beginning of Internal

Welcome to Internal!

Post messages here that you want everyone to see. Everyone automatically becomes a permanent member of this channel when they join the team.

Invite others to this team Set a Header

December 26, 2020

System 9:25 AM @root joined the team.

System 9:28 AM @root updated the channel display name from: Town Square to: Internal

root 9:29 AM @developers Please update theme to the OSTicket before we go live. Credentials to the server are maildeliverer:Youve_G0t_Mail! Also please create a program to help us stop re-using the same passwords everywhere.... Especially those that are a variant of "PleaseSubscribe!" (edited)

root 10:58 AM PleaseSubscribe! may not be in RockYou but if any hacker manages to get our hashes, they can use hashcat rules to easily crack all variations of common words or phrases. (edited)

Today

System 5:54 AM You joined the team.

From here, we can SSH as maildeliverer:Youve_G0t_Mail!

123	udp	ntp		
135	udp	msrpc		
137	udp	netbios-ns		
138	udp	netbios-dgm		

Port	Proto	Service	Version	Status
139	udp	netbios-ssn		
161	udp	snmp		
162	udp	snmptrap		
445	udp	microsoft-ds		
500	udp	isakmp		
514	udp	syslog		
520	udp	route		
631	udp	ipp		
1434	udp	ms-sql-m		
1900	udp	upnp		
4500	udp	nat-t-ike		
8065	tcp	unknown		
49152	udp	unknown		

Credentials:

Service	Username	Password	Full Name	Hash
mysql/mariadb	mmuser	Crack_The_MM_Admin_PW		
SSH	maildeliverer	Youve_G0t_Mail!		
su	root	PleaseSubscribe!21		