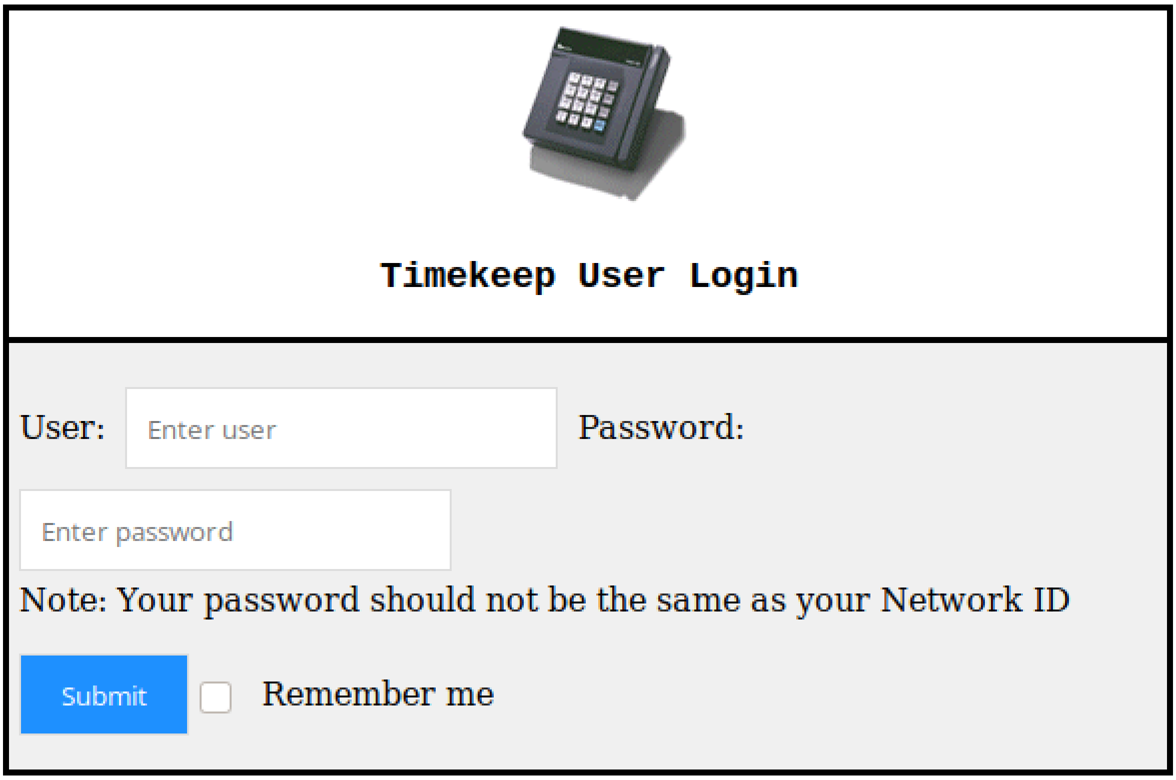
25

After doing everything that you can with your initial footholds your team thinks that it is time to look at other resources and services that we have opened while moving through the network. Since these are internal server we will need to run your browser through a proxychain with FoxyProxy to forward your traffic through the proxy server.
We can use crackmapexec again along with the proxy server to find all open servers. Run crackmapexec again to find what devices are open.

Enumerating THROWBACK-TIME Timekeep Server
Upon initial access we can see that it appears to be a timekeeping software that requires a login.


Timekeep User Login

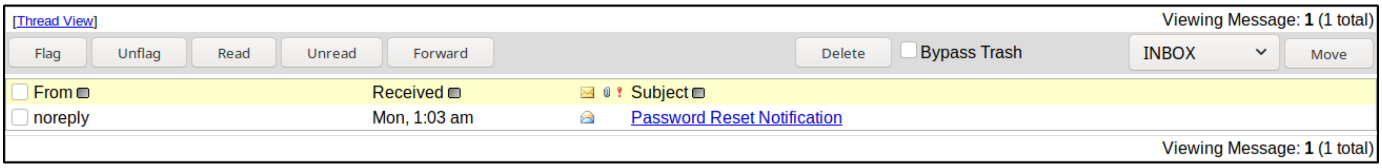
User: Enter user Password:

Enter password

Note: Your password should not be the same as your Network ID

Timekeep user login

Going back in time
Your team has informed you that you could password spray the login however there may be account lockout policies in place. Instead your team has informed you to look back at your previously compromised mail server accounts.
When looking back through the compromised accounts you find that there is a noreply email about a password reset on the timekeep server.



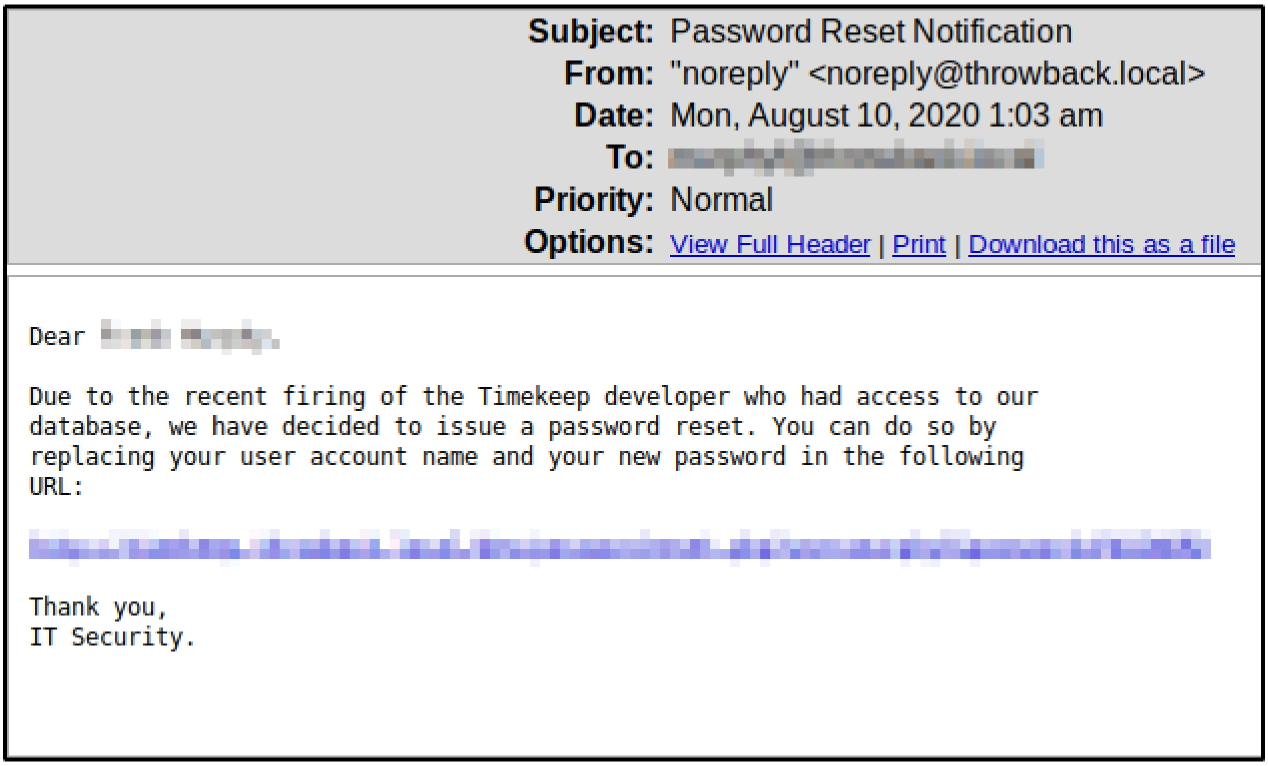
Viewing Message: **1** (1 total)

□ From	Received	Subject
□ noreply	Mon, 1:03 am	Password Reset Notification

Viewing Message: **1** (1 total)

Password reset email

Upon opening the email you find that they have sent you a password reset link for the server. This how you can get into the timekeep server.



Subject: Password Reset Notification
From: "noreply" <noreply@throwback.local>
Date: Mon, August 10, 2020 1:03 am
To: [redacted]
Priority: Normal
Options: View Full Header | Print | Download this as a file

```
Dear [redacted]

Due to the recent firing of the Timekeep developer who had access to our
database, we have decided to issue a password reset. You can do so by
replacing your user account name and your new password in the following
URL:

[redacted]

Thank you,
IT Security.
```

noreply password reset email

From the email we get a link. The link is a vhost on the timekeep server, to access it we need to set our /etc/hosts file to the fully qualified domain name in the link. After updating our hosts configuration we can navigate to the link and reset a user's password.

Answer the questions below

What is the hostname of the device?

Correct Answer

What is the title of the web page?

Submit

What user was the password reset for?

Correct Answer