Mini Project - Attack

Alexander Berg
Thomas Hoffmann Kilbak
Kristoffer Bruun Højelse
Emil Jäpelt
Adam Negaard
Oscar Gludsted Strange

November 2022

1 Steps

1.1 Target acquisition and Information gathering

Initially we used `nmap` to scan the ports on the target host of our opponent group (`secu13.itu.dk`). Here we see that port 22 is open for ssh, and port 5000 was open for tcp, which we assumed was for the MySecretNotes application. This can be seen in figure 1.

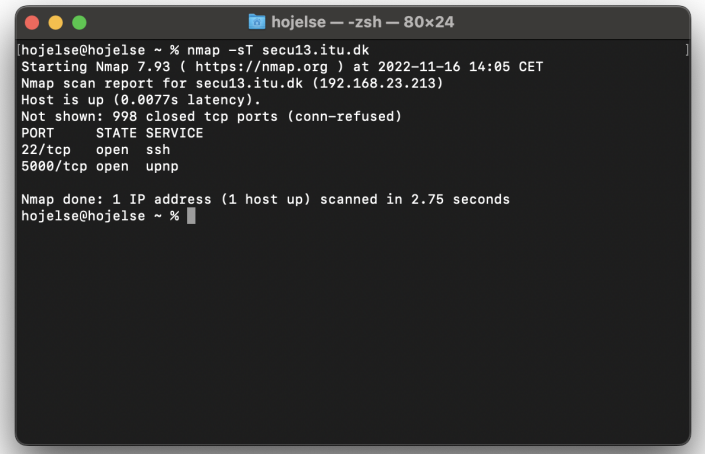

Figure 1: Ports 22 and 5000 are open

To verify our assumption, we used `curl` to see how the underlying service on port 5000 would respond to an HTTP GET request. It turned out that it responded with HTML content, i.e. the page from MySecretNotes. This can be seen in figure 2.

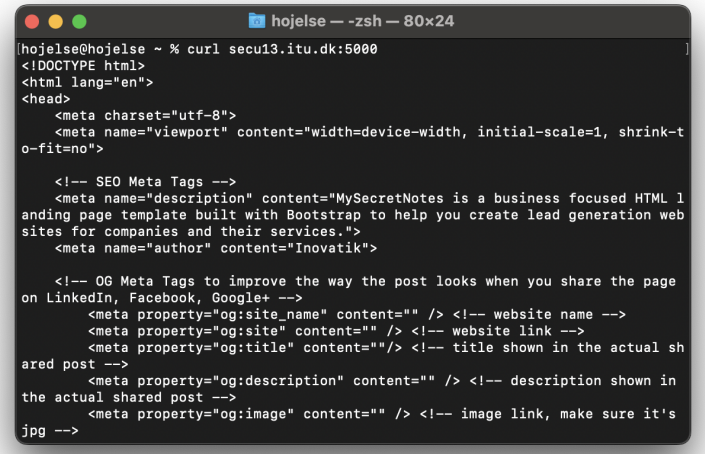

Figure 2: Port 5000 returns html

After creating a user, we saw the public note with ID 7030049051, which said "Bernardos favourit number is 0". Our intuition was to import the note with ID 0, which showed a note with the text "Hint - Admin likes: 53 76 65 6E 73 6B 65 4B 6F 65 64 62 6F 6C 6C 65 72 46 72 61 49 6B 65 61 32 2A". This can be seen in figure 3. We then used the website Online UTF-8 Tools to decode the byte array, which translated to the text "SvenskeKoedbollerFraIkea2*".

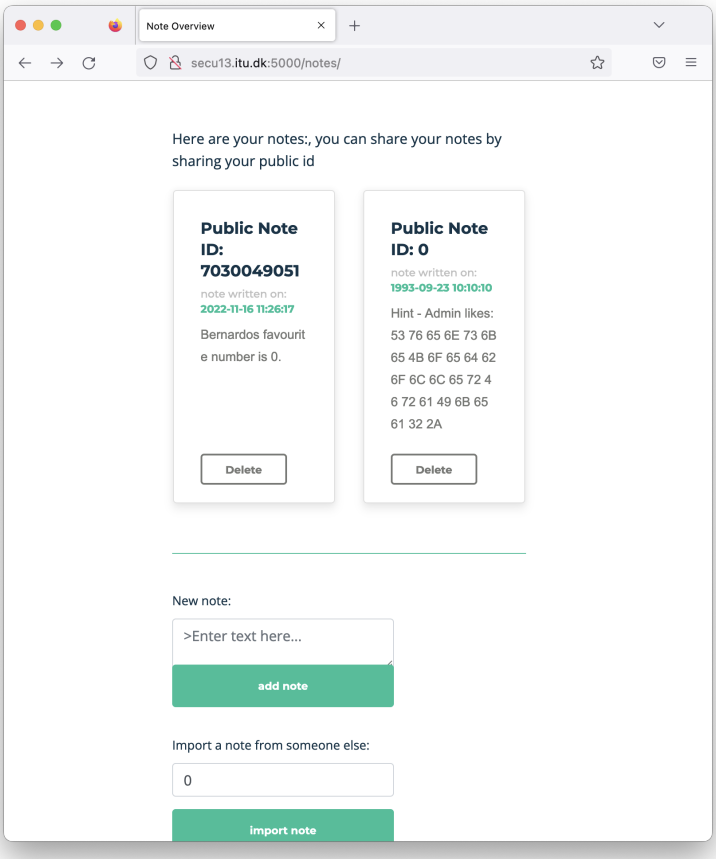

Figure 3: The notes page after importing note 0

We used this password to log in to MySecretNotes with the username "admin" and the password

”SvenskeKoedbollerFraIkea2*” which were valid credentials for the site. This can be seen in figure 4.

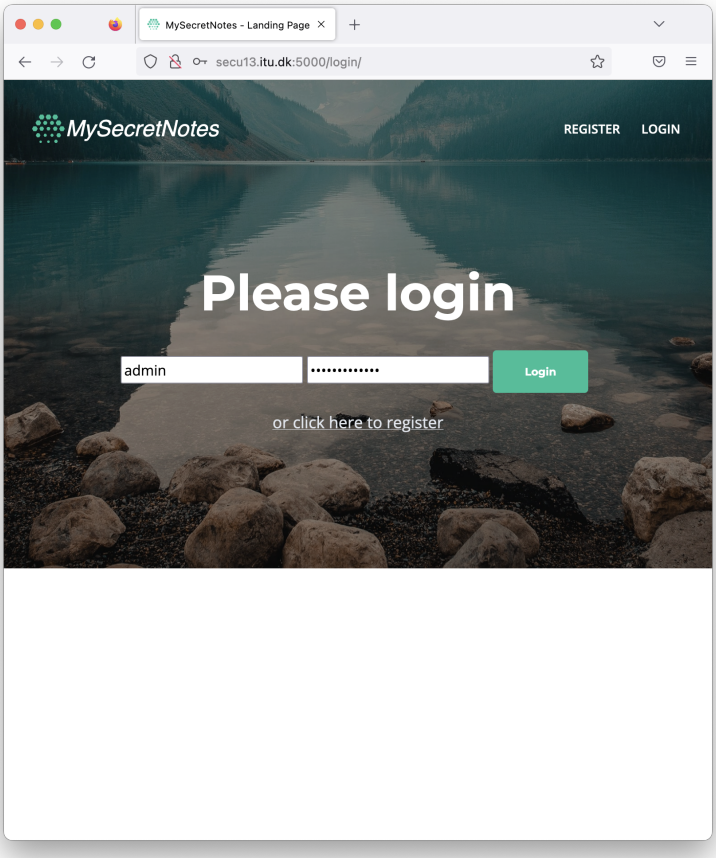

Figure 4: Login as admin

We then read the notes page when logged into the admin user. This user had a note that said ”Don’t forget terminal password: isgvmavnnb22*”, which can be seen in figure 5.

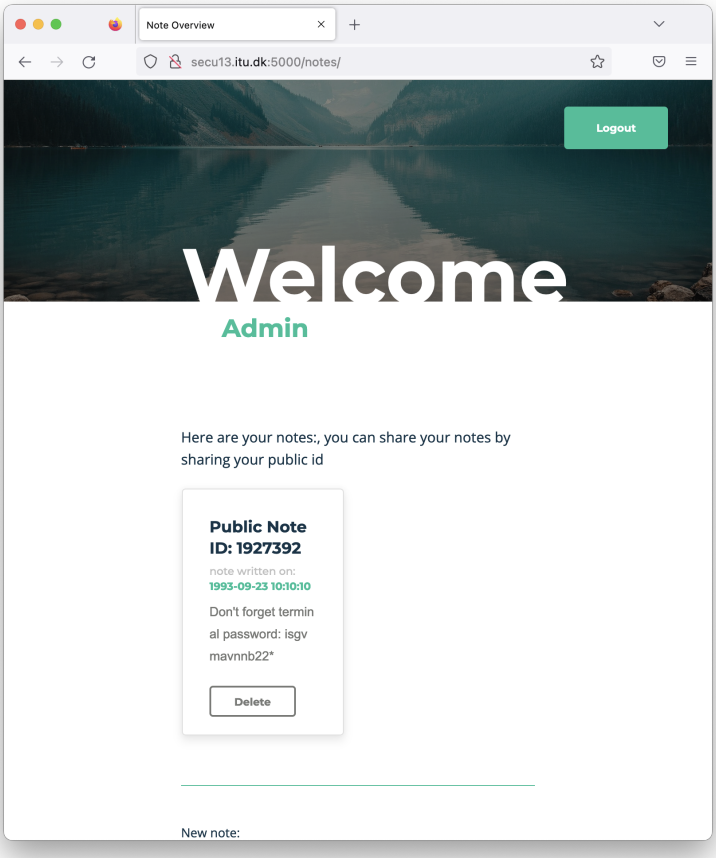

Figure 5: Admin page has user password to stud

1.2 Initial access

Having retrieved a password from the admins notes, we attempted to login to the server remotely with the user stud, using the command: `ssh stud@secu13.itu.dk`, with the retrieved password `isgvmavnnb22*`. We chose the user stud, since we knew that every group was initially given this user. This worked and we therefore had user access on the server, as seen in figure 6.

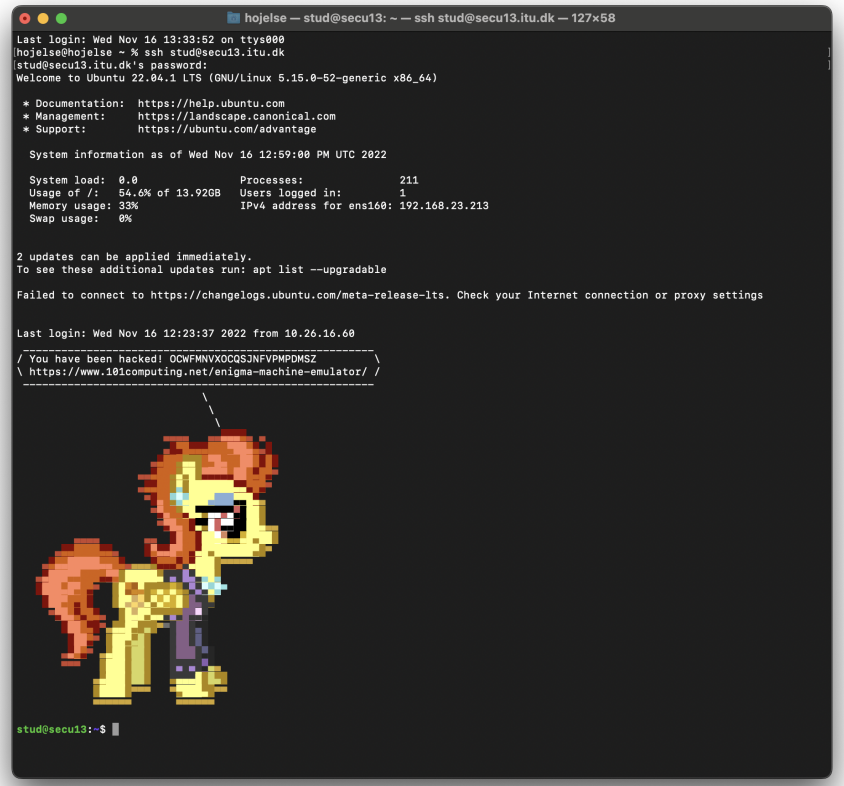

Figure 6: Command outputs unicorns with a text bubble

1.3 Privilege escalation

Having achieved user access, specifically with the `stud` user, we executed `groups stud`, to figure out what kind of privileges we had. It turns out that `stud` was in the `sudo` group, i.e. was allowed to execute commands with root privileges, only having to enter the password for `stud` itself, which we of course knew at this point. With this we could execute `sudo su root` to switch to the root user. This can be seen done in figure 7. We later figured out that this was not the path that group 13 had intended.

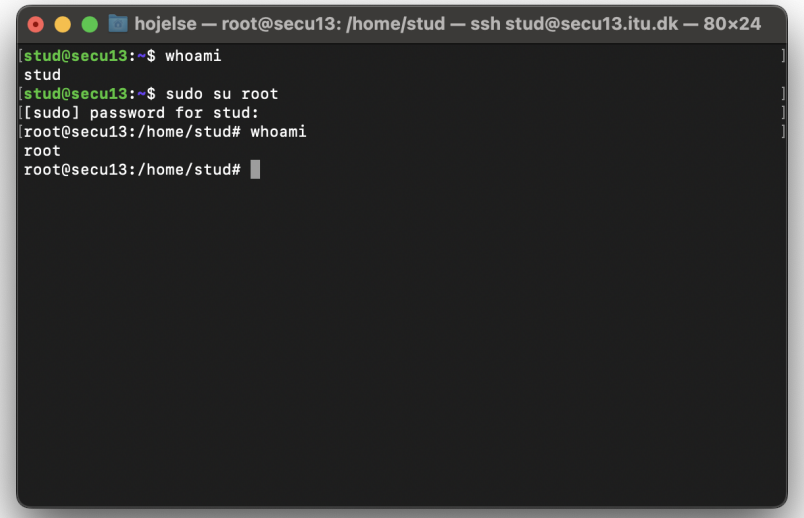

Figure 7: Login as root with stud password

1.3.1 Intended path

As seen in figure 6, every command on the server would show pixelart (in the figure its a pony), which had a speech bubble which said: "OCWFMNVXOCQSJNFVPMPDMSZ https://www.101computing.net/enigma-machine-emulator/". We then visited the website, and entered the specified code into the enigma machine. The code translated to "TRYTH ESAME PASSW ORDAG AIN" (see figure 8).

Figure 8: Enigma

Trivially, when logged into stud, we were able to gain access to the root user by executing `su root` with the same password, `isgvmavnnb22*`, as seen in figure 9.

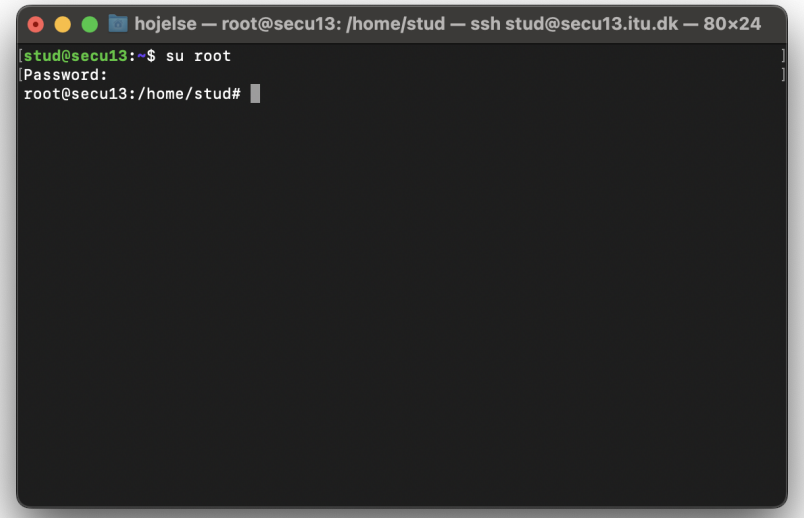

Figure 9: Login as root with the same password as the stud user password: `isgvmavnnb22*`

1.4 Security goal violations

1.4.1 Insecure connection

The service is simply an HTTP service, i.e. it sends all data over the network with no encryption, or integrity checks. This is of course quite problematic, as the contents of the notes, and user credentials, will be visible to packet sniffers. Thus, confidentiality and integrity is broken.

1.4.2 Public secrets

The ID of each note registered in the service, is selected at random from the range 1 000 000 000 to 9 999 999 999. Additionally, every note is allowed to be viewed by anyone, i.e. it is not possible for a note to have a non-public ID. This makes it very easy to find all users notes, by simple brute force, and is thus breaking confidentiality.

1.4.3 Non-minimal access

The user `stud`, was in the sudo group, which enables execution of commands, with escalated privileges. Specifically, this allowed stud to execute `sudo passwd`, changing the root password and then switching to the root user using the command: `su root`.

1.5 Maintaining access

To maintain access, we created a new user `secu03` with the command `sudo adduser secu03`, and gave it the password "fb2b59ef65d54df29ac634588af9aea0". Then we added the user to the sudoers group using the command `usermod -aG sudo secu03`. With this, even if the service maintainers were to patch the system and change passwords, we would still have access, unless they were to discover the new user and modify it.