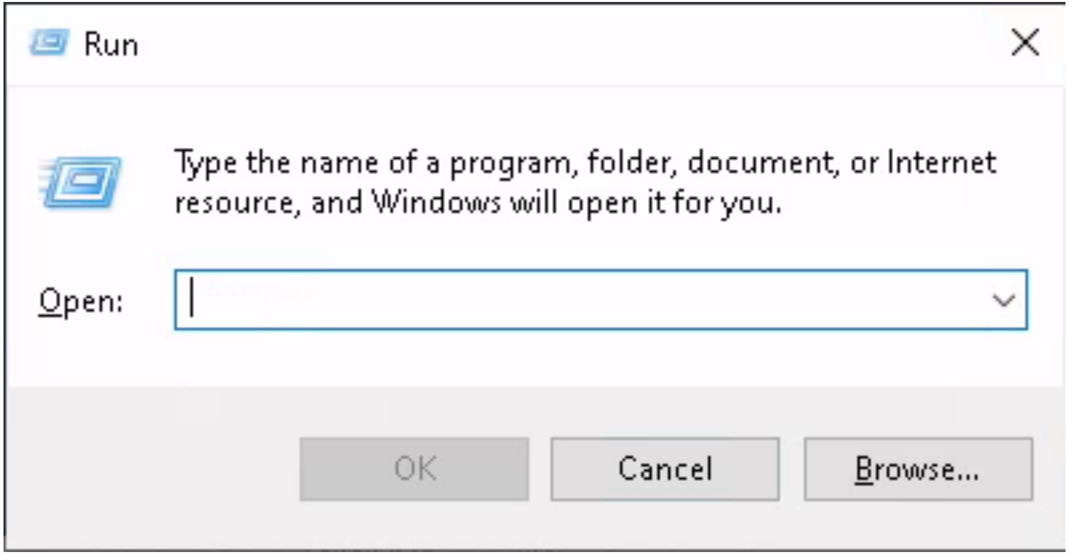
Rubber Ducky

Script

One of the first things you need to do for most RDPs to actually be able to work is to have a user with admin controls and to turn the firewall off. You are able to do this manually by navigating the system settings and control pannel, but we will be doing it by writing a script which will disable the firewall and add a new user with admin controls.

The first step to writing a script which can add a new user and turn off the firewall is to learn how to do both of those normally without the script.

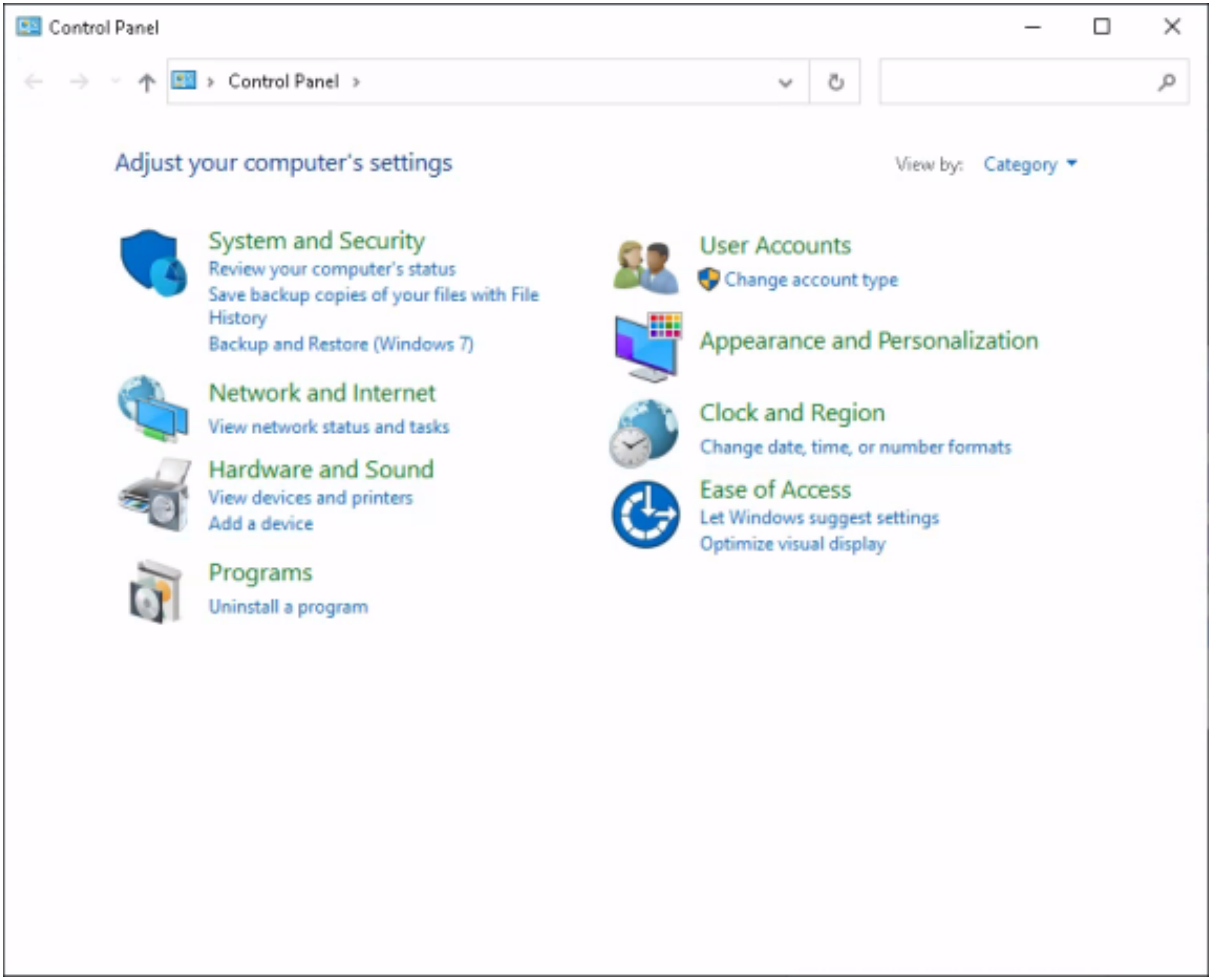
We will focus on turning the fire wall off. The first thing we will do for a windows machine is open the “run” panel, which can be done easily by holding the windows button and pressing the ‘r’ key.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

If done correctly it will pull up a panel like this.

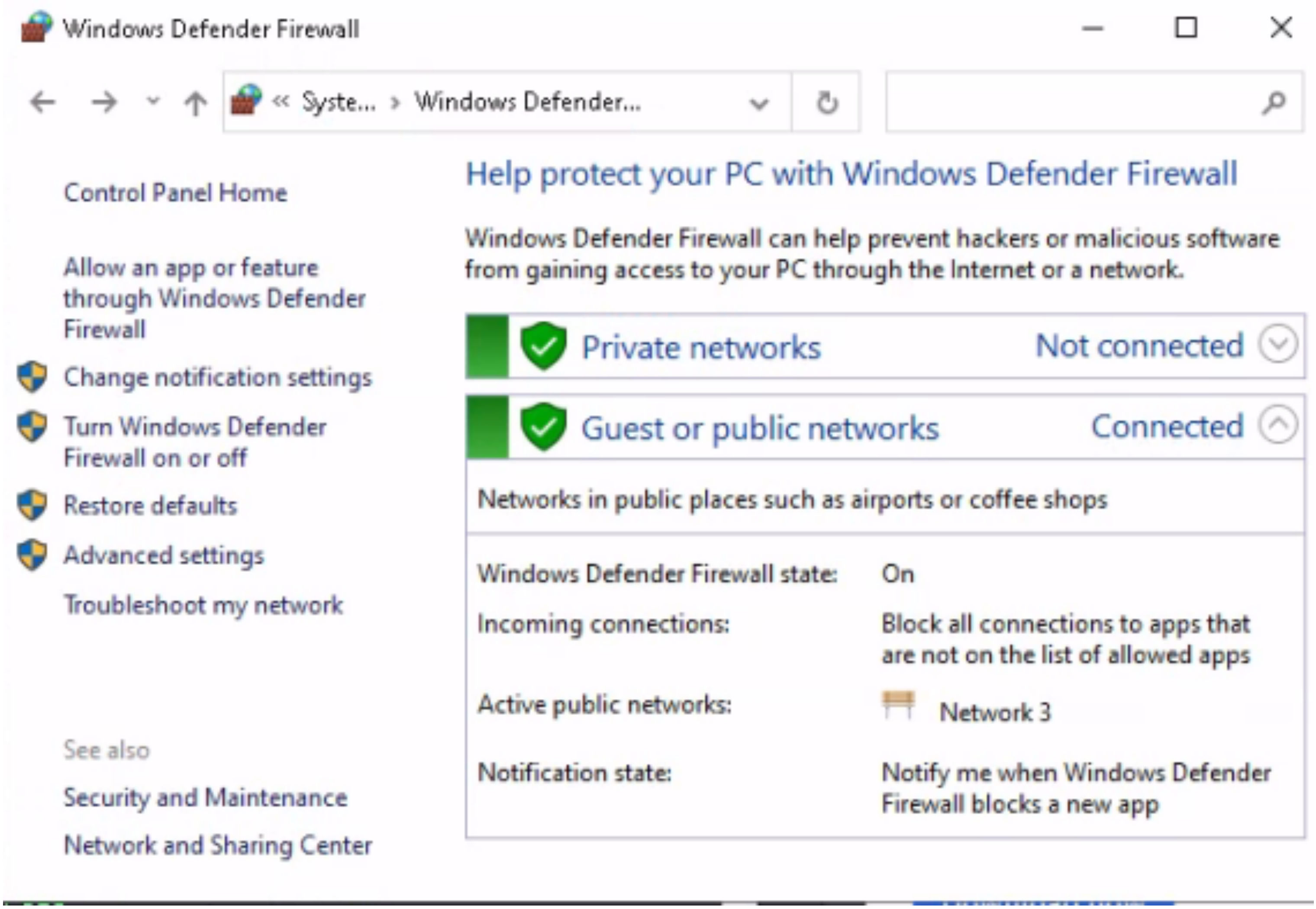
From here we will type “control panel” and press OK, this should pull up the control panel.


Control Panel
Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Save backup copies of your files with File History
Backup and Restore (Windows 7)
Network and Internet
View network status and tasks
Hardware and Sound
View devices and printers
Add a device
Programs
Uninstall a program
User Accounts
Change account type
Appearance and Personalization
Clock and Region
Change date, time, or number formats
Ease of Access
Let Windows suggest settings
Optimize visual display

It should look like this, if it doesnt then check the “View by: ” and change it to ‘Category’

From here we should go to the “System and Security” tab

inside the System and Security tab there should be a section that says “Windows Defender Firewall”. under the firewall section in small text there is some that says “Check firewall status” click on it.



Windows Defender Firewall
« Syste... › Windows Defender...
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network
See also
Security and Maintenance
Network and Sharing Center

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Private networks — Not connected

Guest or public networks — Connected

Networks in public places such as airports or coffee shops

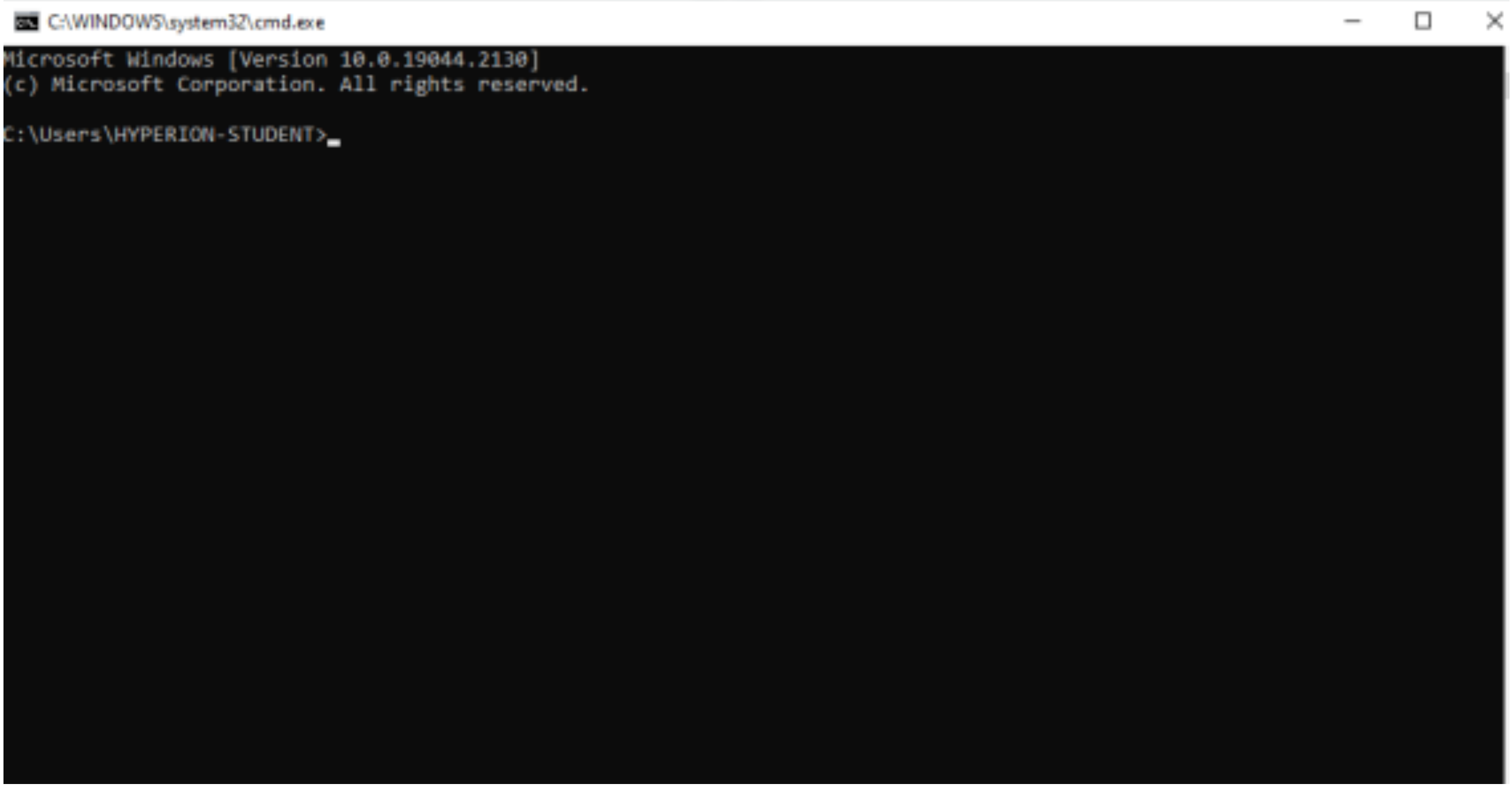
Windows Defender Firewall state: On

Incoming connections: Block all connections to apps that are not on the list of allowed apps

Active public networks: Network 3

Notification state: Notify me when Windows Defender Firewall blocks a new app

This window will pull up.
With this window we can to go the Turn Windows Defender Firewall on or off. We turn it off.
(This will let us connect to the computer later.)
Next we close Windows defender and open cmd using Run (make sure to open in Administrator)



```
Microsoft Windows [Version 10.0.19044.2130]
(c) Microsoft Corporation. All rights reserved.

C:\Users\HYPERION-STUDENT>_
```

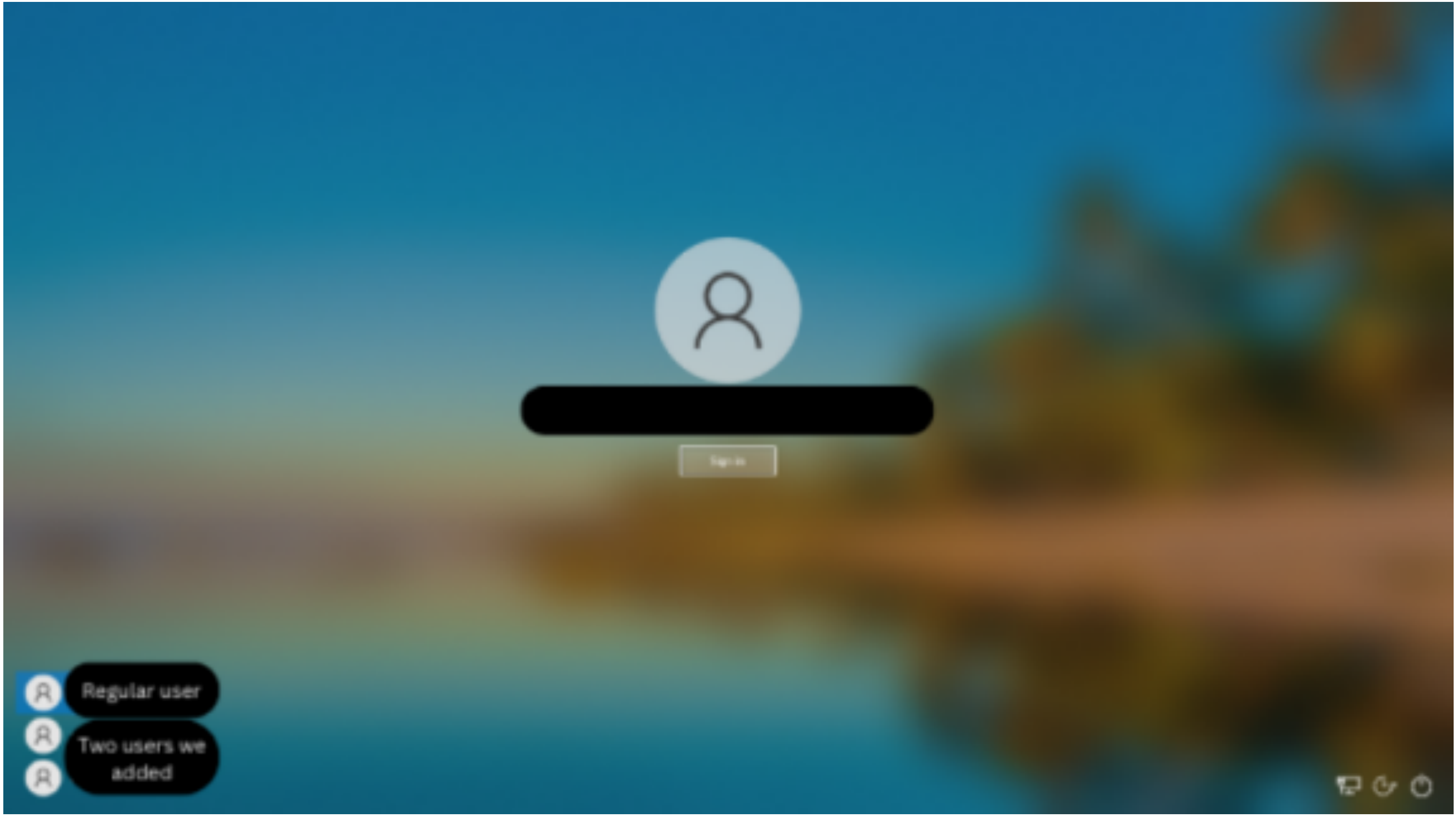
Now we are going to add ourselves as a user on their computer.

To do so, we are going to run the command “net user (username) (password) /add"

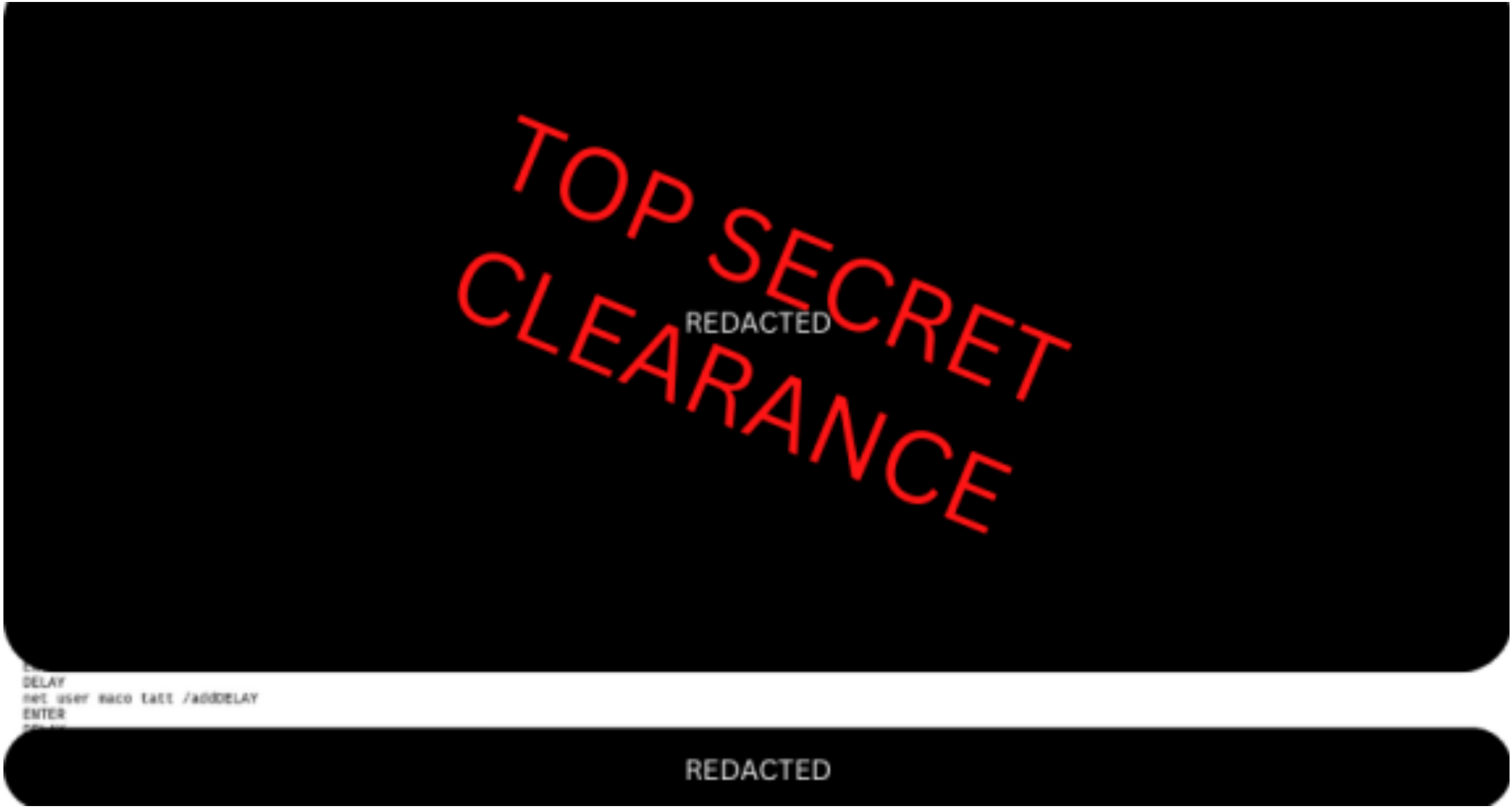
This will add us to the user list, now we are going to take it a step further and add ourselves as administrators.

For that we just run one more command “net localgroup administrators (username) /add”

Now we can login under our own profile with the abillity to do anything we want.


[redacted]

(picture of part of the script we ran)



TOP SECRET CLEARANCE

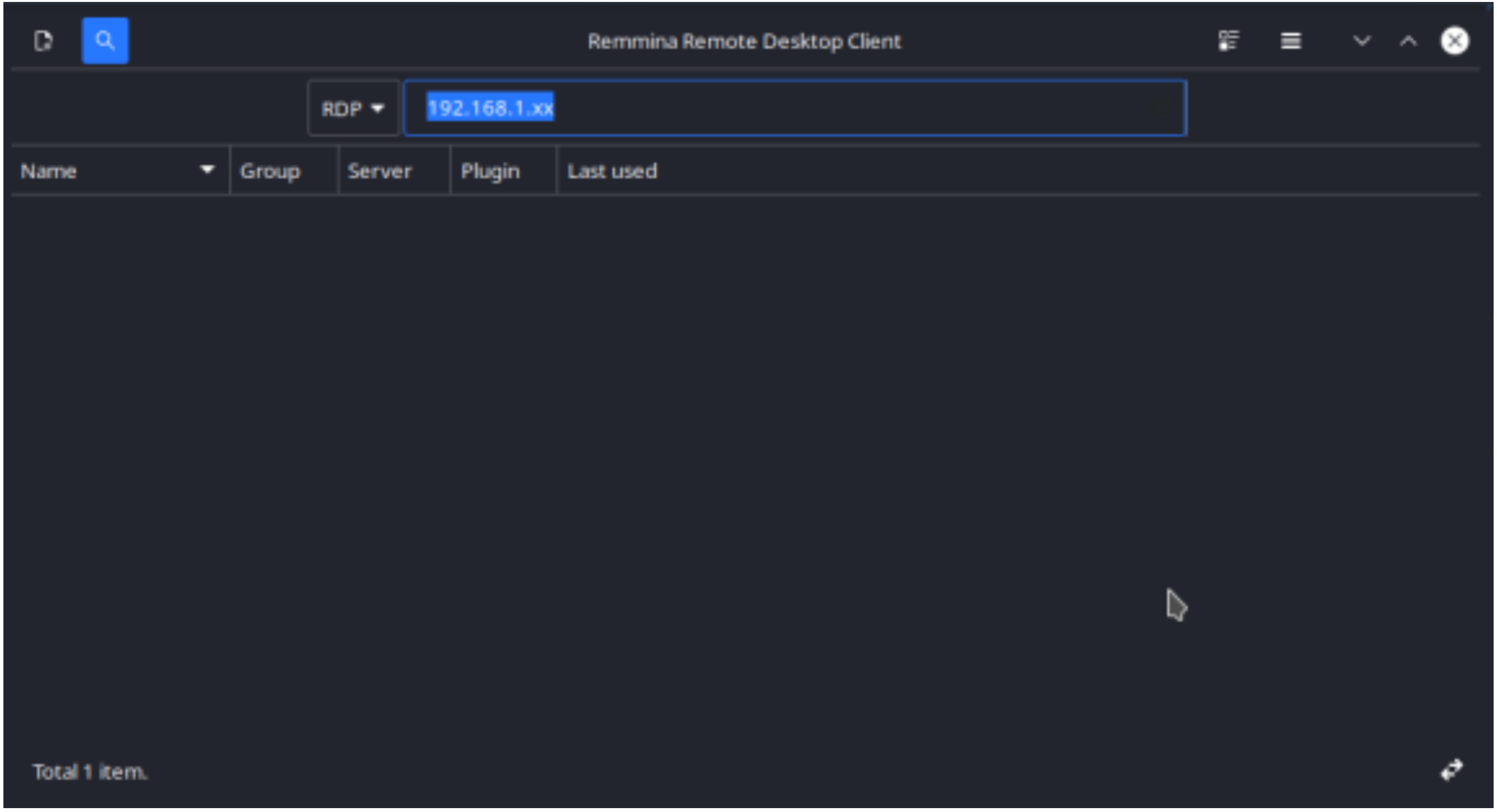
REDACTED

```
DELAY
net user maco tatt /addDELAY
ENTER
```

REDACTED

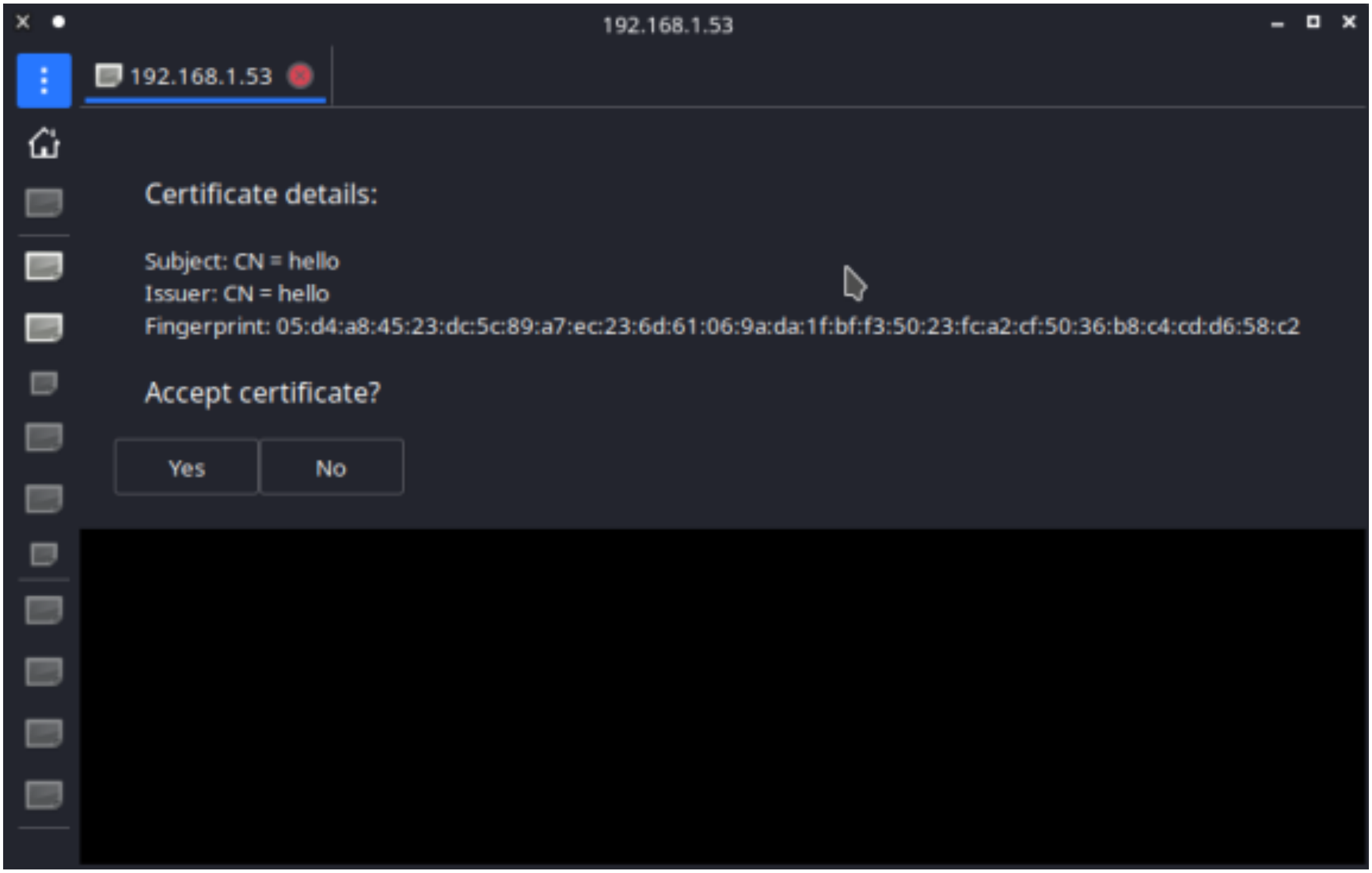
RDP

A remote desktop is a process of taking someones computer and connecting to it from another location.
Most of the time people use a Remote Desktop to connect to their own computer so they can work from home or a buisness trip.
We are going to use this process to install a type of spyware to a victims computer.
We are going to connect to the victims computer using a application named Remmina.



192.168.1.xx

(This is not a real IP number please do not try and connect)
If needed you can go into settings and change aspect ratios or other graphics settings but after you are done, you just hit enter and connect.
We should be able to connect because we turned off the firewall to our victims computer.
If done correctly, you will be asked to accept the certificate, just hit yes.

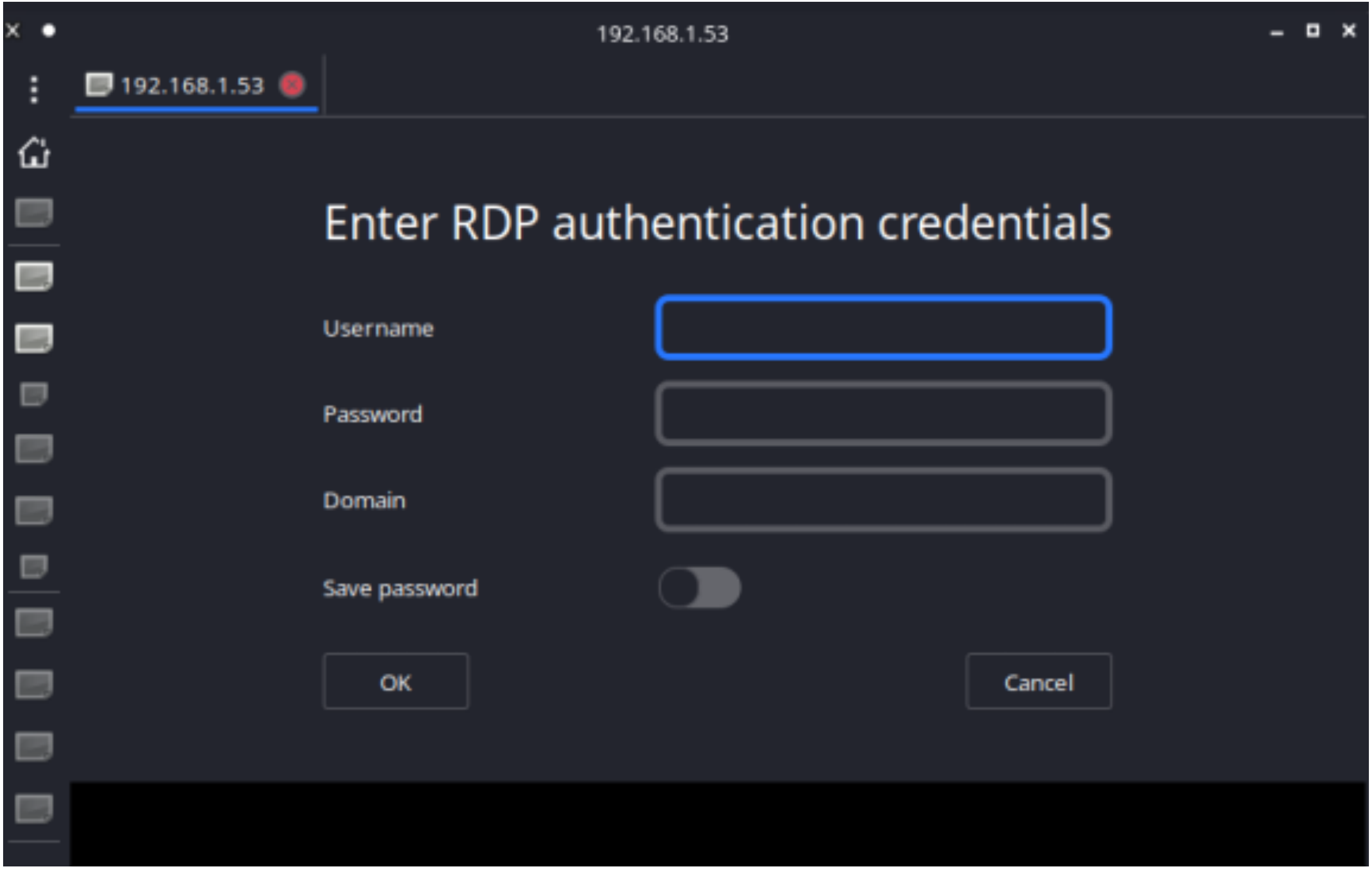


Certificate details:

Subject: CN = hello
Issuer: CN = hello
Fingerprint: 05:d4:a8:45:23:dc:5c:89:a7:ec:23:6d:61:06:9a:da:1f:bf:f3:50:23:fc:a2:cf:50:36:b8:c4:cd:d6:58:c2

Accept certificate?

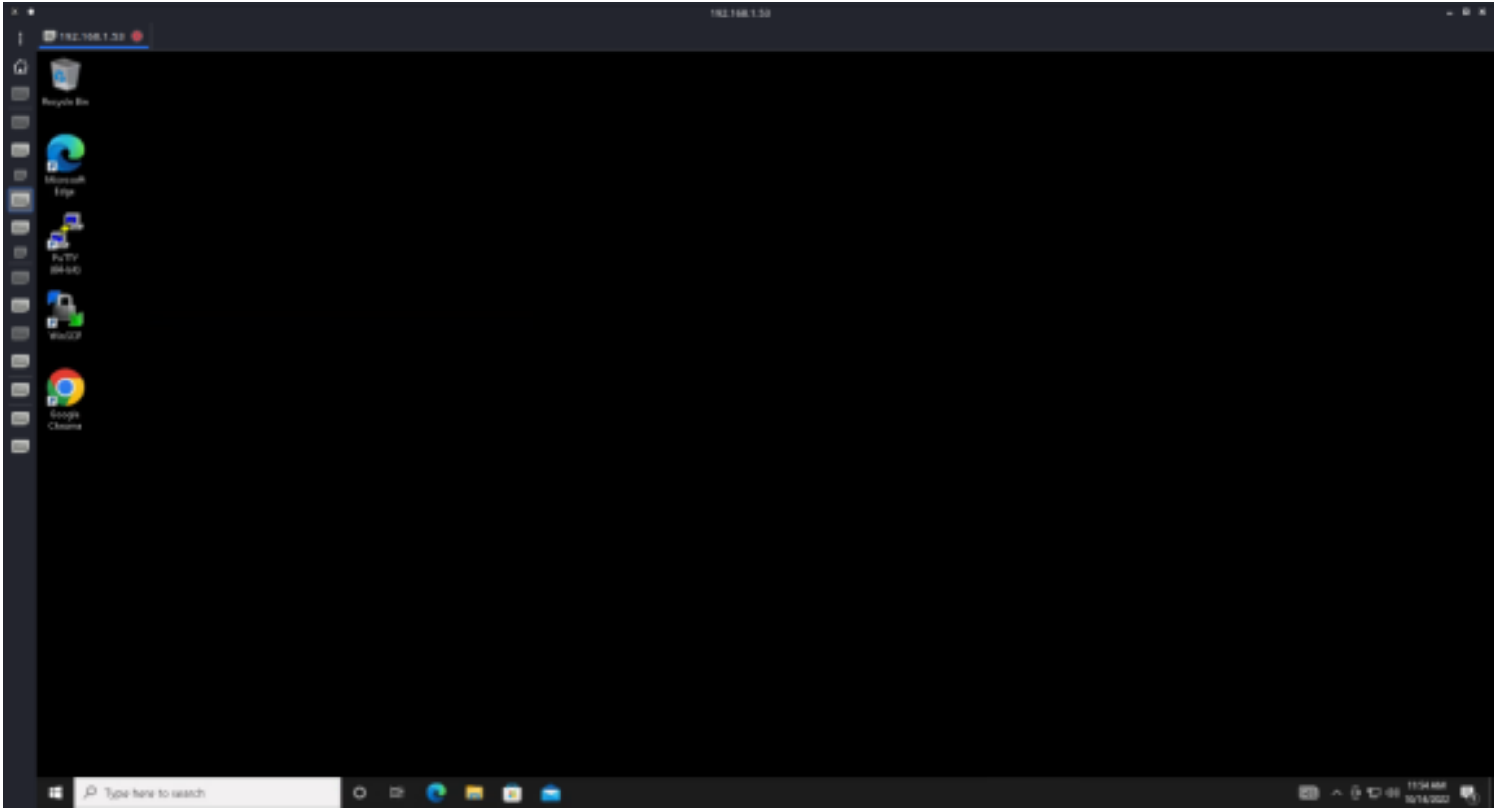
After yes is hit, you will be propted to put in a username, password and domain.



Enter RDP authentication credentials

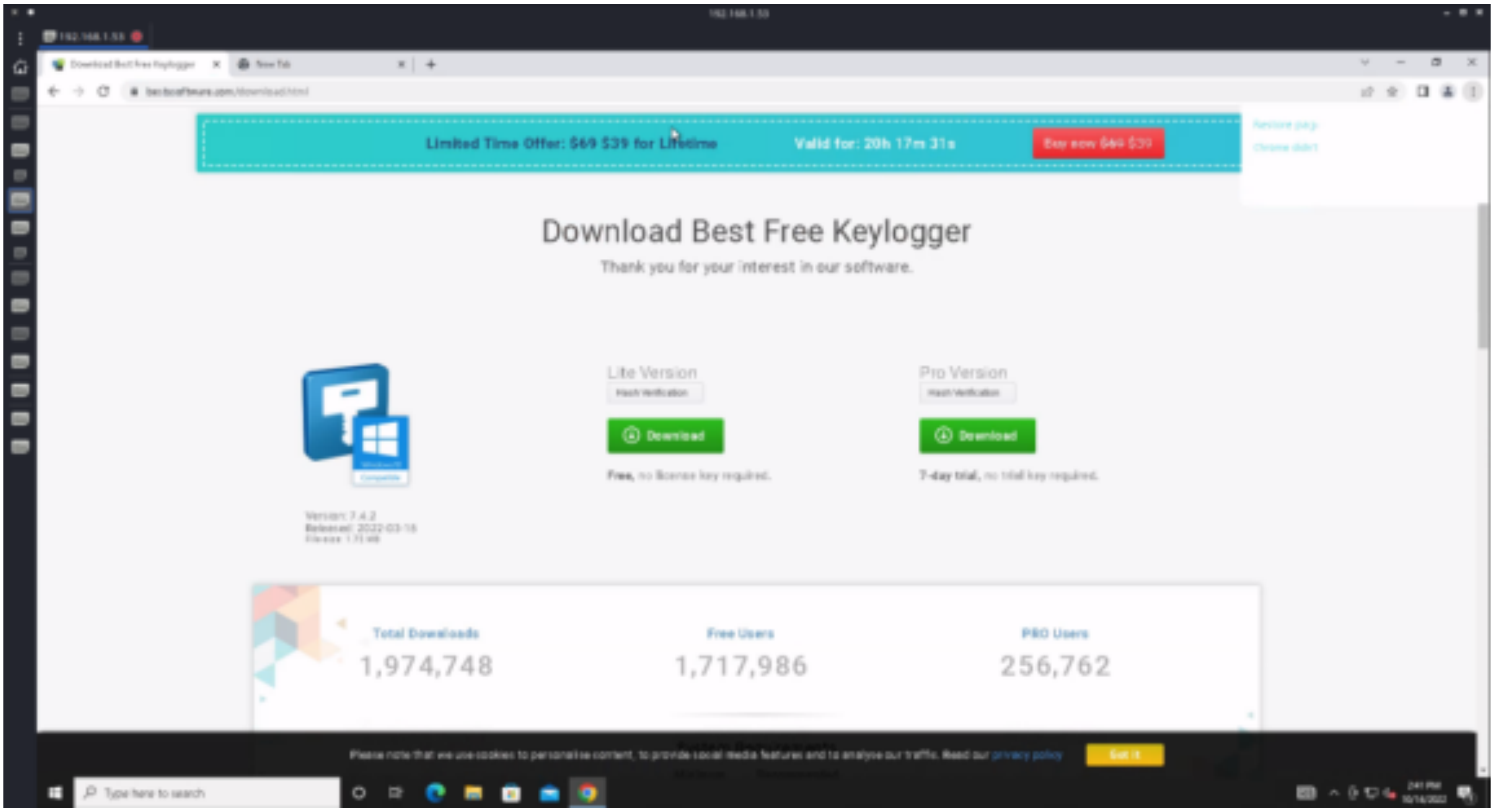
Username
Password
Domain
Save password

We use the credentials from the script we created on their computer to login. (leave the domain empty)
After about 30 seconds we will be logged in with adminstrative privlages.



Keylogger

A keylogger is a type of spyware that takes everything you type, all aplications you open, and randomly takes screenshots of what you are doing on your computer.
For this process to be carried out, we are going to take the computer we set up a remote desktop on and download a keylogger to steal their passwords to their personall accounts.
For this we are going to set up a keylogger named Best Keylogger.



Limited Time Offer: $69 $39 for Lifetime

Valid for: 20h 17m 31s

Download Best Free Keylogger

Thank you for your interest in our software.

Lite Version

Free, no license key required.

Pro Version

7-day trial, no trial key required.

Version: 7.4.2

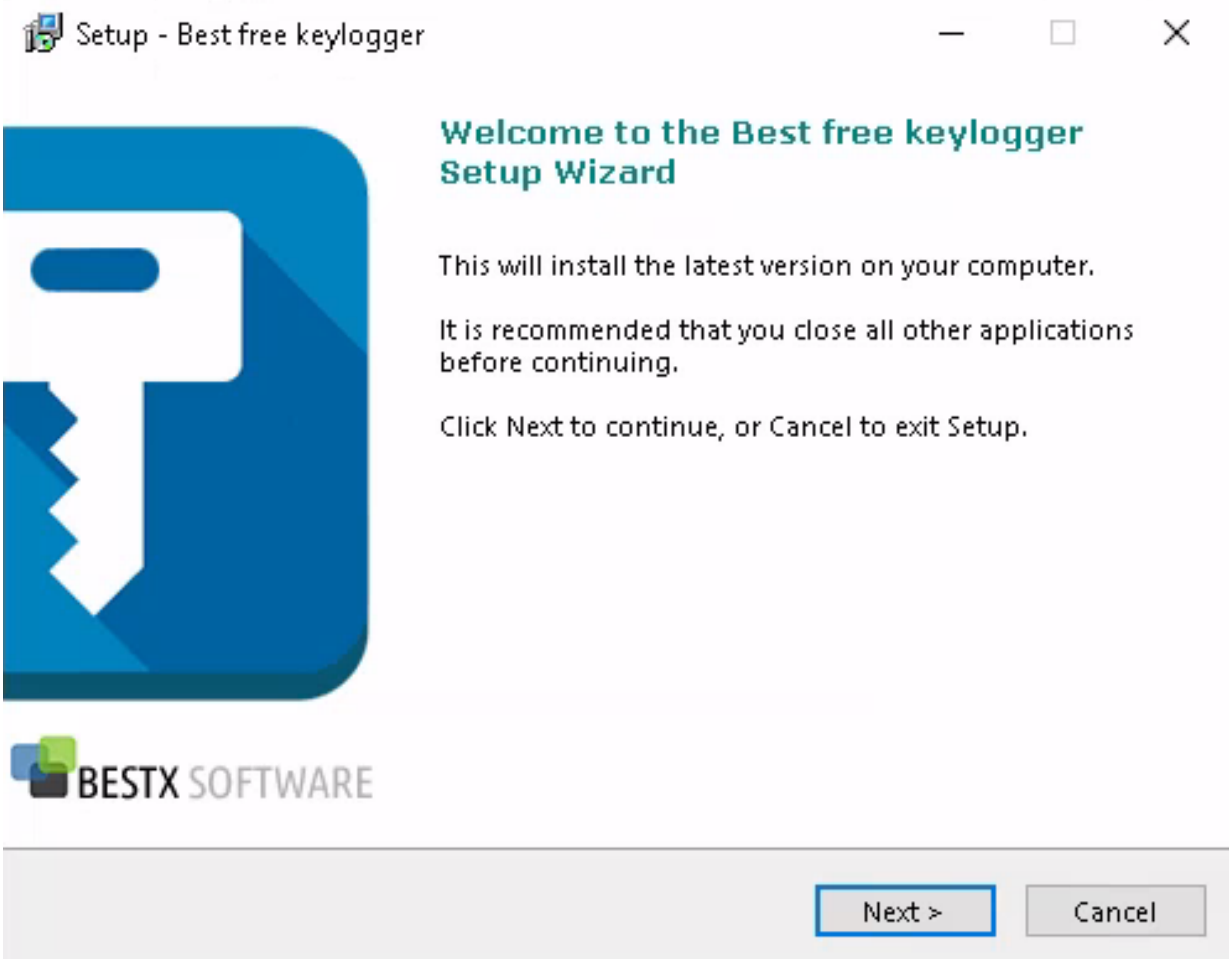
Released: 2022-03-16

Total Downloads 1,974,748

Free Users 1,717,986

PRO Users 256,762

(https://bestxsoftware.com/download.html)
For this purpose we used the free download.
To start the download,hit the download button under the free version.
This will give you a link and you just copy and paste it into the browser.
After download run the file.



Setup - Best free keylogger

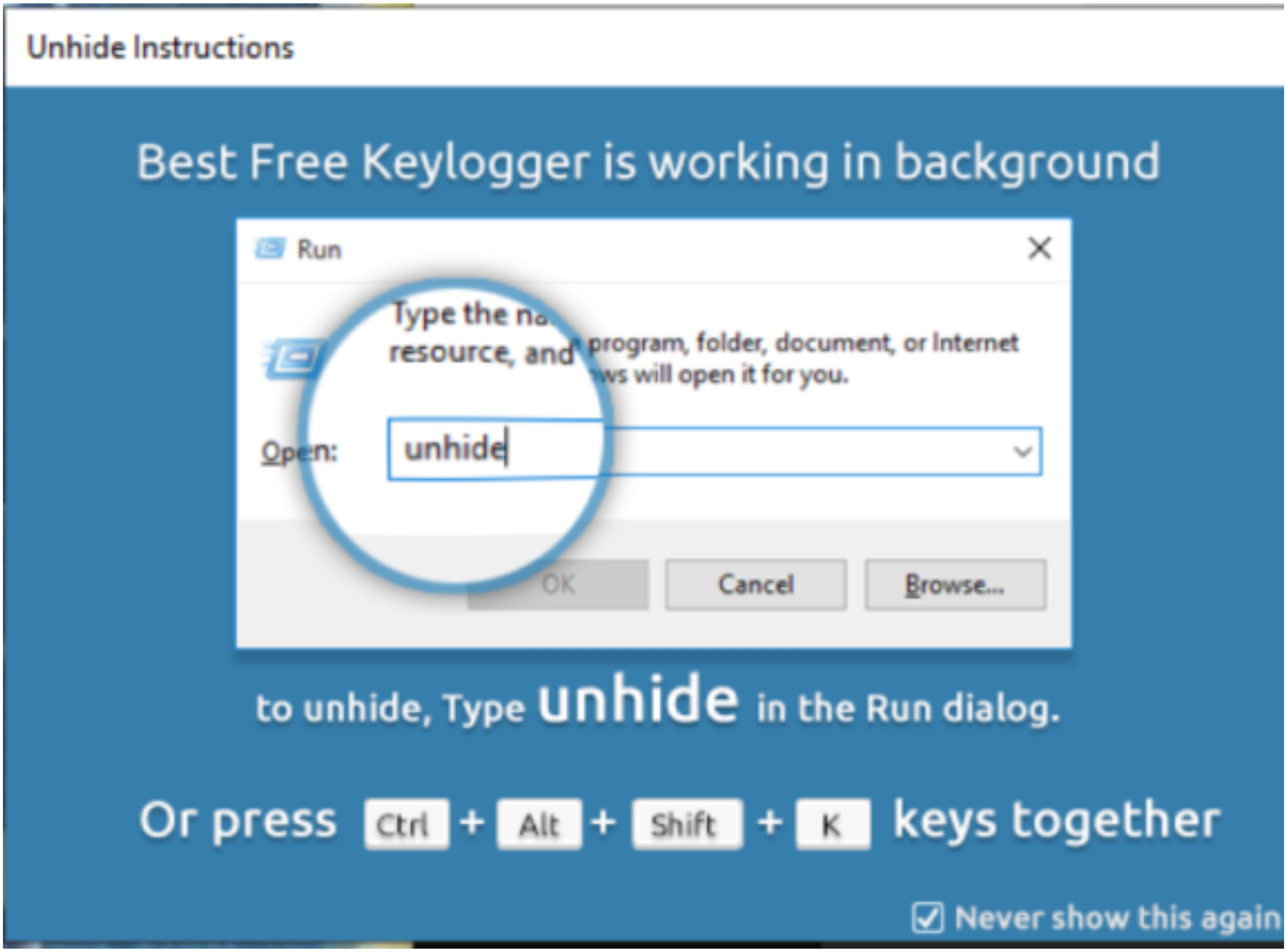
Welcome to the Best free keylogger Setup Wizard

This will install the latest version on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

Now you have to set up the actuall keylogger and download the rest of the files.
Once installed, This is the screen will pop up.



Unhide Instructions

Best Free Keylogger is working in background

Type the na resource, and program, folder, document, or Internet ws will open it for you.

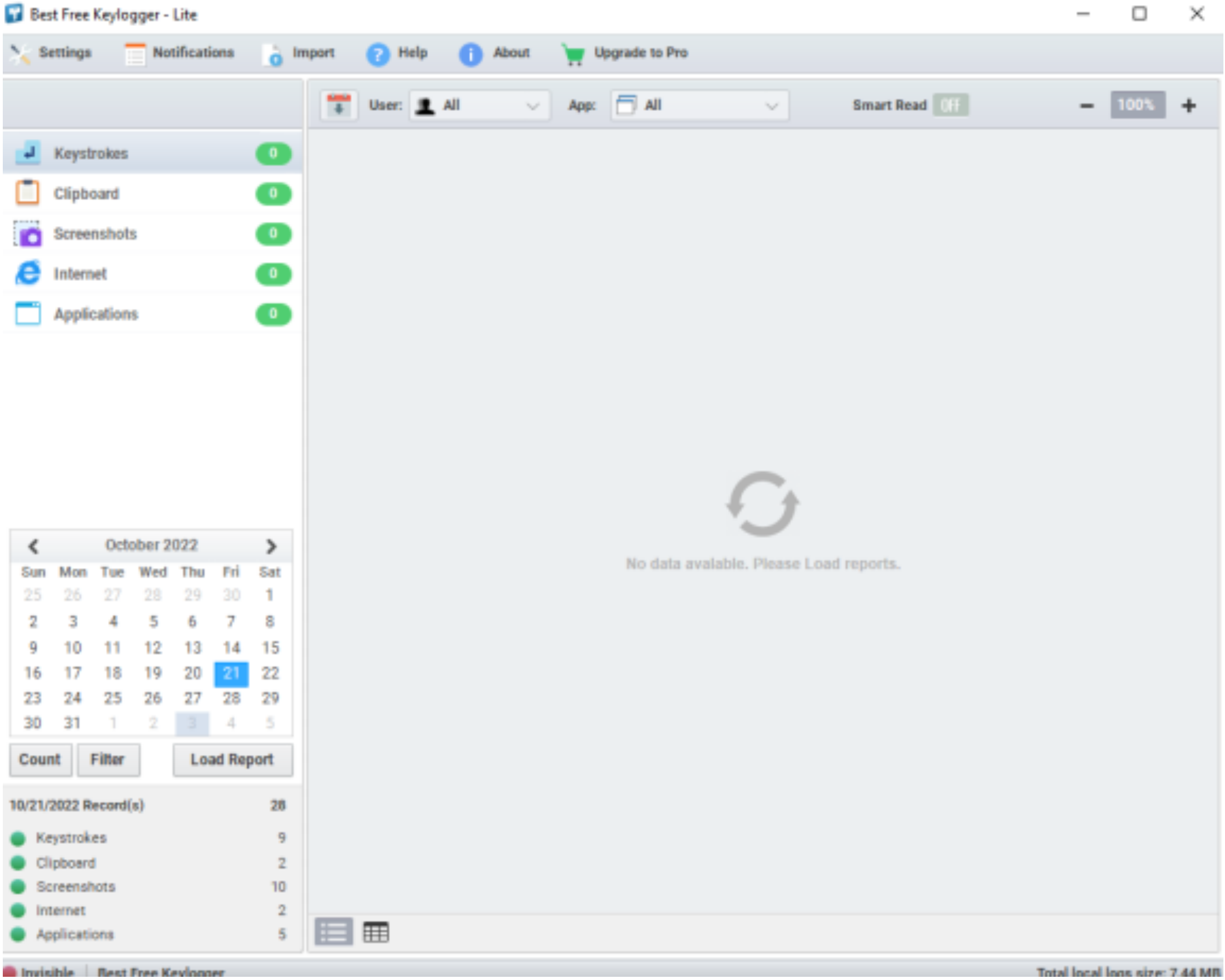
Open: unhide

to unhide, Type unhide in the Run dialog.

Or press Ctrl + Alt + Shift + K keys together

☑ Never show this again

This specific keylogger has a stealth feature that can record the information from someones computer, like keystrokes, and send them to my personal email.
To set this up we preform one of the actions to unhide it.
Once unhidden we get a dashboard of everything the keylogger records.



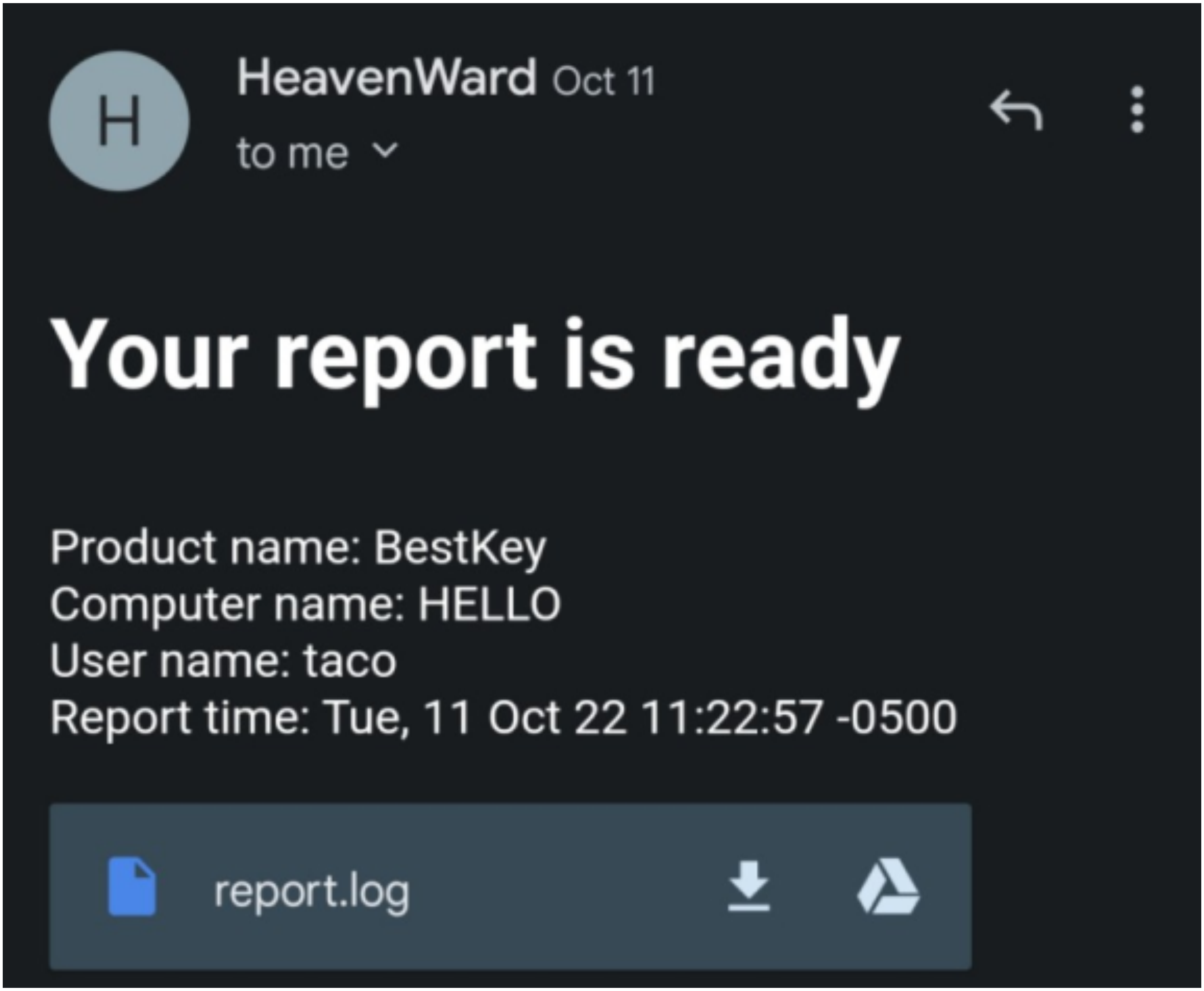
No data available. Please Load reports.

October 2022

Sun	Mon	Tue	Wed	Thu	Fri	Sat
25	26	27	28	29	30	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31	1	2	3	4	5

10/21/2022 Record(s)	28
● Keystrokes	9
● Clipboard	2
● Screenshots	10
● Internet	2
● Applications	5

If we want, every so often we can log into their computer and steal any info they type on their computer but that might be a little dangerous if they are on their computer.
Lasty we can set up an email so it sends us reports every so often.



Your report is ready

Product name: BestKey
Computer name: HELLO
User name: taco
Report time: Tue, 11 Oct 22 11:22:57 -0500

email of report