# Foundations of computer security

Norbert Oláh

2022.

# Content

# X2Go Client

- Session->New session (or Ctrl+n)
- Session name: arbitrary value
- Host is the IP address below:
  172.22.194.191
  172.22.194.192
  172.22.194.193
  172.22.194.194
- SSH port: 10001 -10044
- Session type: Do not put a tick next to Run in X2GoKDrive (experimental) (!!!) and change the type to MATE

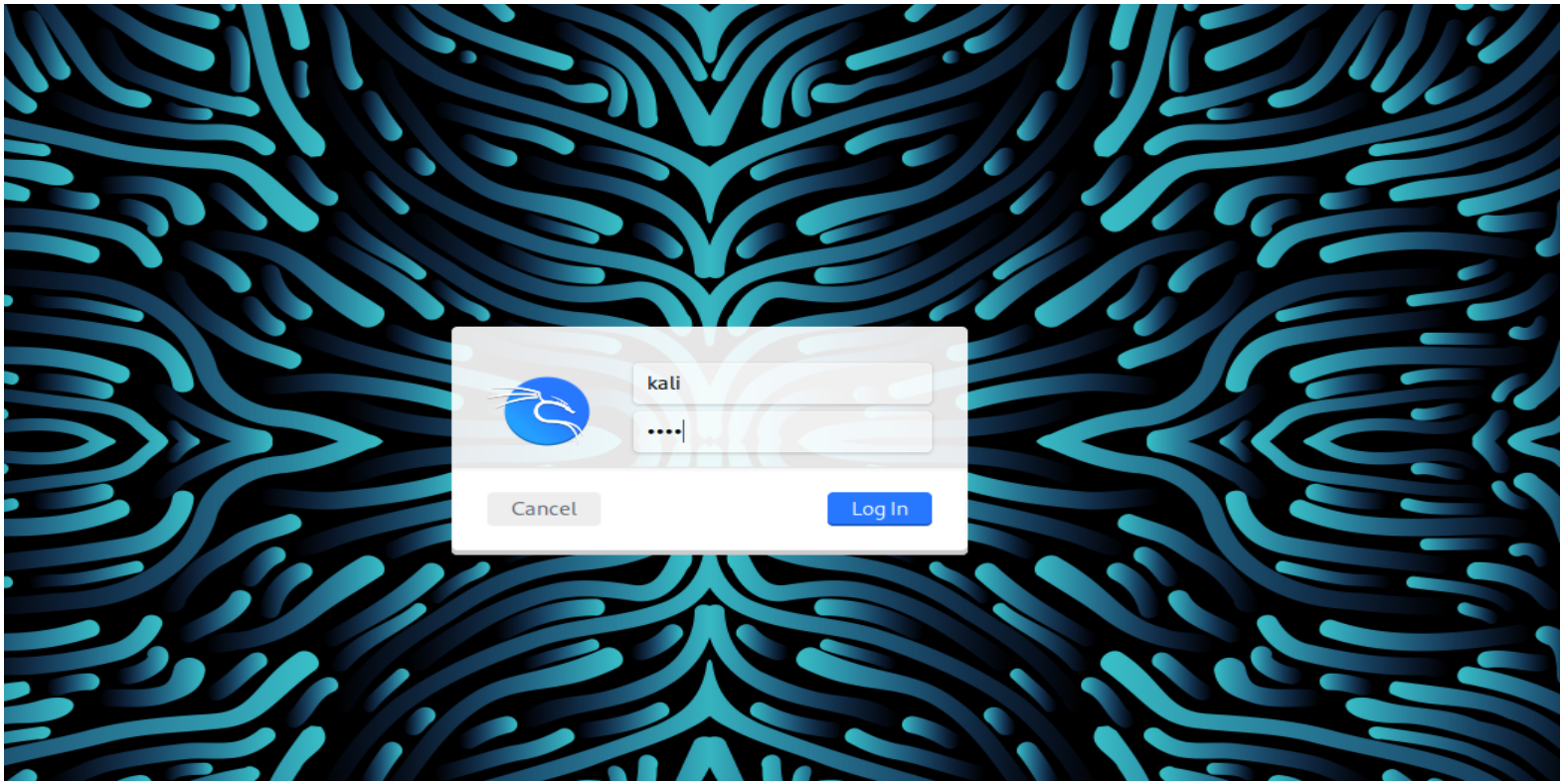
# X2Go Client

- student student1 172.22.194.191 10001
- student student2 172.22.194.192 10002
- student student3 172.22.194.193 10003
- student student4 172.22.194.194 10004
- student student5 172.22.194.191 10005
- ...
- student student44 172.22.194.194 10044

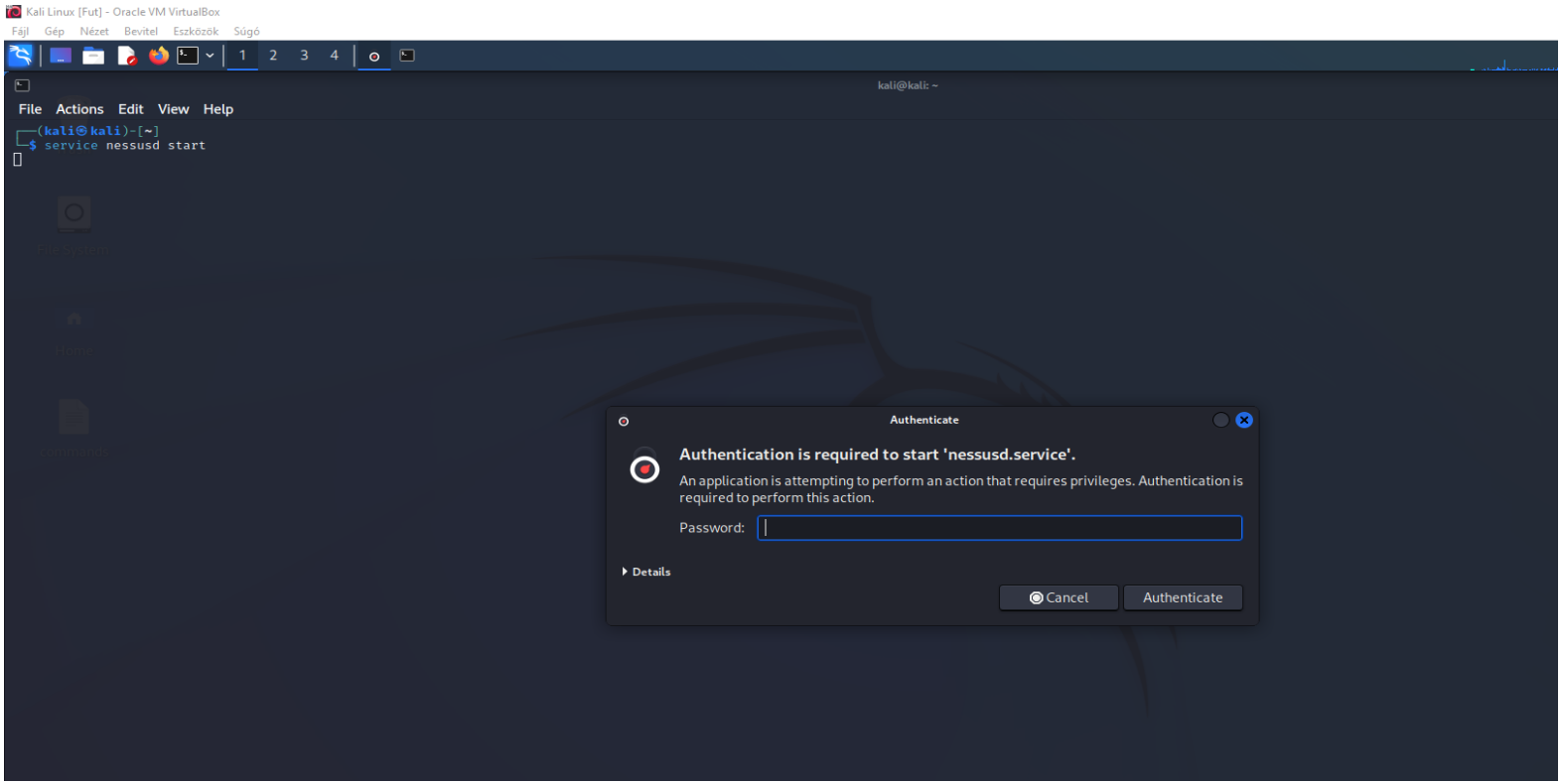
# First steps

- Start Parrot linux
- Open Terminal:
  service nessusd start
  password: studentx → x denotes your number at the end of the password
- Checking the nessus application:
  service nessusd status
- Open the web browser and go to
  https://parrot:8834/
  https://127.0.0.1:8834
- Log in to Nessus
  nessus / nessus

# First steps



# First steps


Kali Linux [Fut] - Oracle VM VirtualBox
Fájl Gép Nézet Bevitel Eszközök Súgó
1 2 3 4
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$ service nessusd start
Authenticate
Authentication is required to start 'nessusd.service'.
An application is attempting to perform an action that requires privileges. Authentication is required to perform this action.
Password:
Details
Cancel
Authenticate

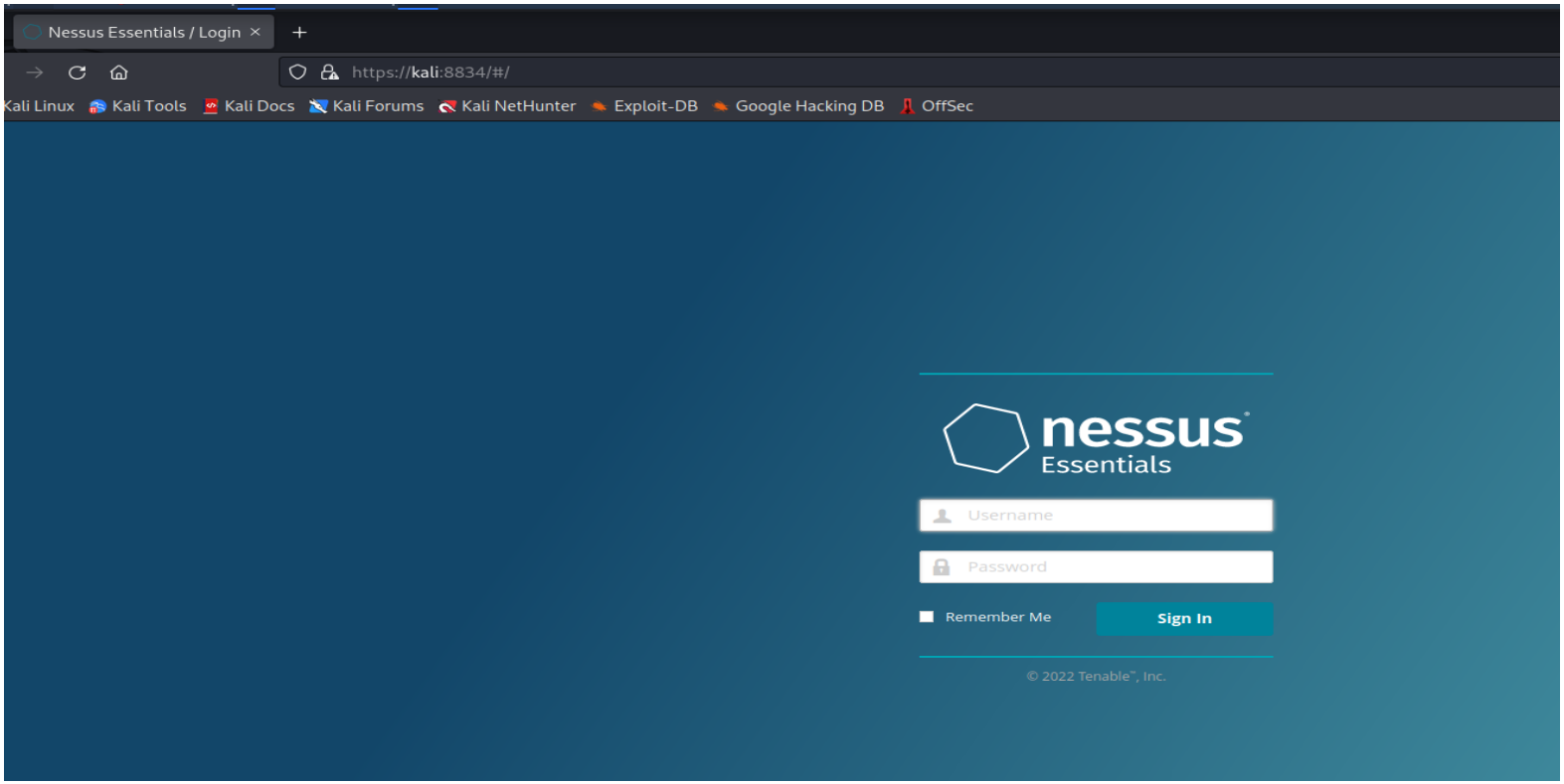
# First steps

```
┌──(kali㉿kali)-[~]
└─$ service nessusd status
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: disabled)
     Active: active (running) since Mon 2022-11-14 02:12:17 EST; 18s ago
   Main PID: 3458 (nessus-service)
      Tasks: 12 (limit: 2292)
     Memory: 1.0G
        CPU: 14.979s
     CGroup: /system.slice/nessusd.service
             ├─3458 /opt/nessus/sbin/nessus-service -q
             └─3460 nessusd -q

Nov 14 02:12:17 kali systemd[1]: Started The Nessus Vulnerability Scanner.
Nov 14 02:12:33 kali nessus-service[3460]: Cached 253 plugin libs in 158msec
Nov 14 02:12:33 kali nessus-service[3460]: Cached 253 plugin libs in 72msec

┌──(kali㉿kali)-[~]
└─$
```

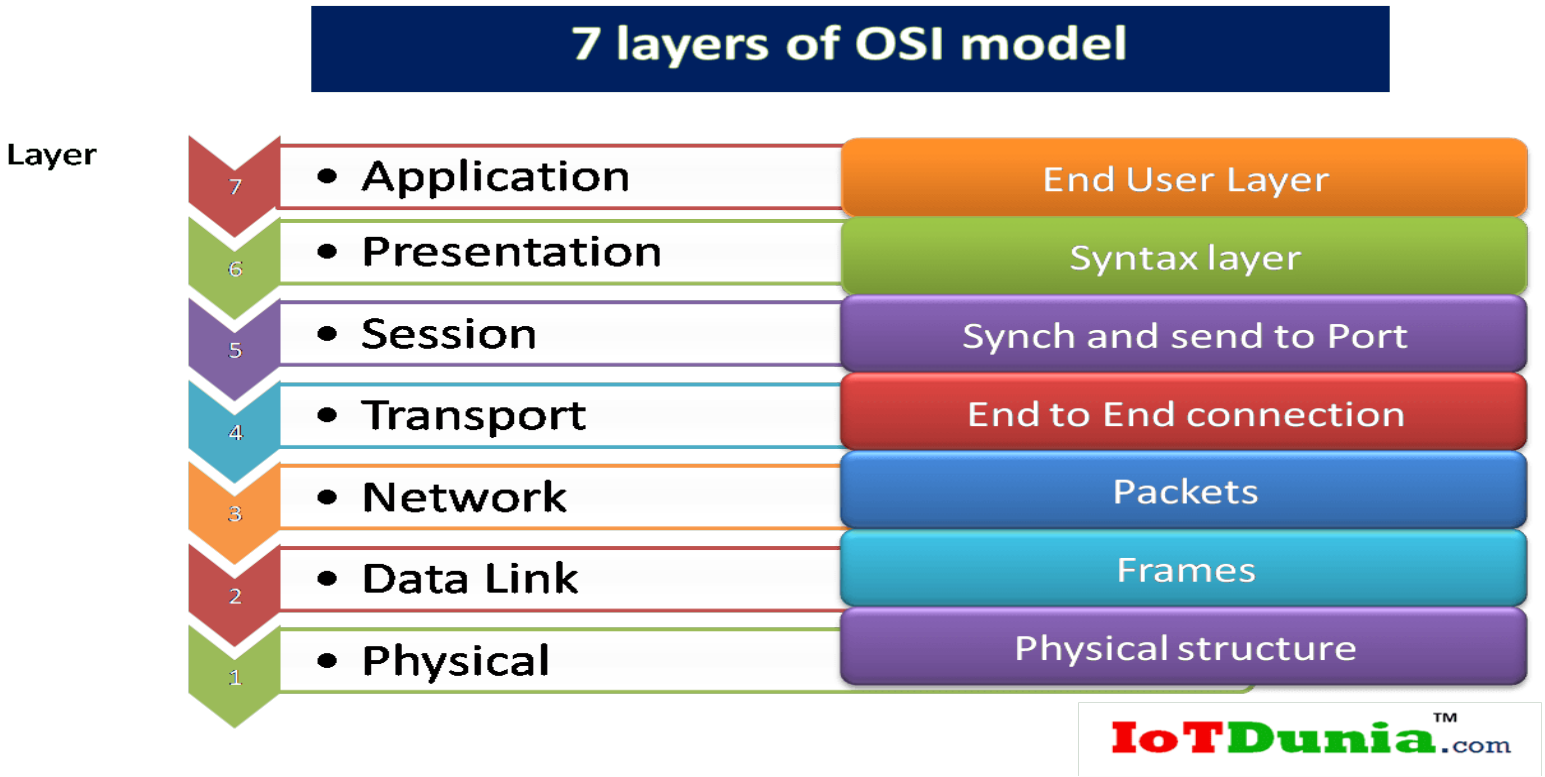
# First steps


Nessus Essentials / Login
https://kali:8834/#/
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
nessus
Essentials
Username
Password
Remember Me
Sign In
© 2022 Tenable™, Inc.

# Create your website scan

- Create New Scan
- Use Basic Scan
- Target: demo.testfire.net
- Generate a PDF from the result and write the IP Address and ports of the target

# OSI model


7 layers of OSI model
Layer
7
• Application
End User Layer
6
• Presentation
Syntax layer
5
• Session
Synch and send to Port
4
• Transport
End to End connection
3
• Network
Packets
2
• Data Link
Frames
1
• Physical
Physical structure
IoTDunia™.com

# OSI modell

- Open Systems Interconnection
- Interoperability of communication systems with standard communication protocols
- It groups the functions provided by different protocols into layers that build on each other
- ISO 7498-1
- A layer can rely only and exclusively on the functions provided by the layers below it, and the functions it provides can only be provided by the layer above it
- Ensure network interoperability between different products from different vendors, using different platforms, without it mattering which components are made by whom.

# OSI modell

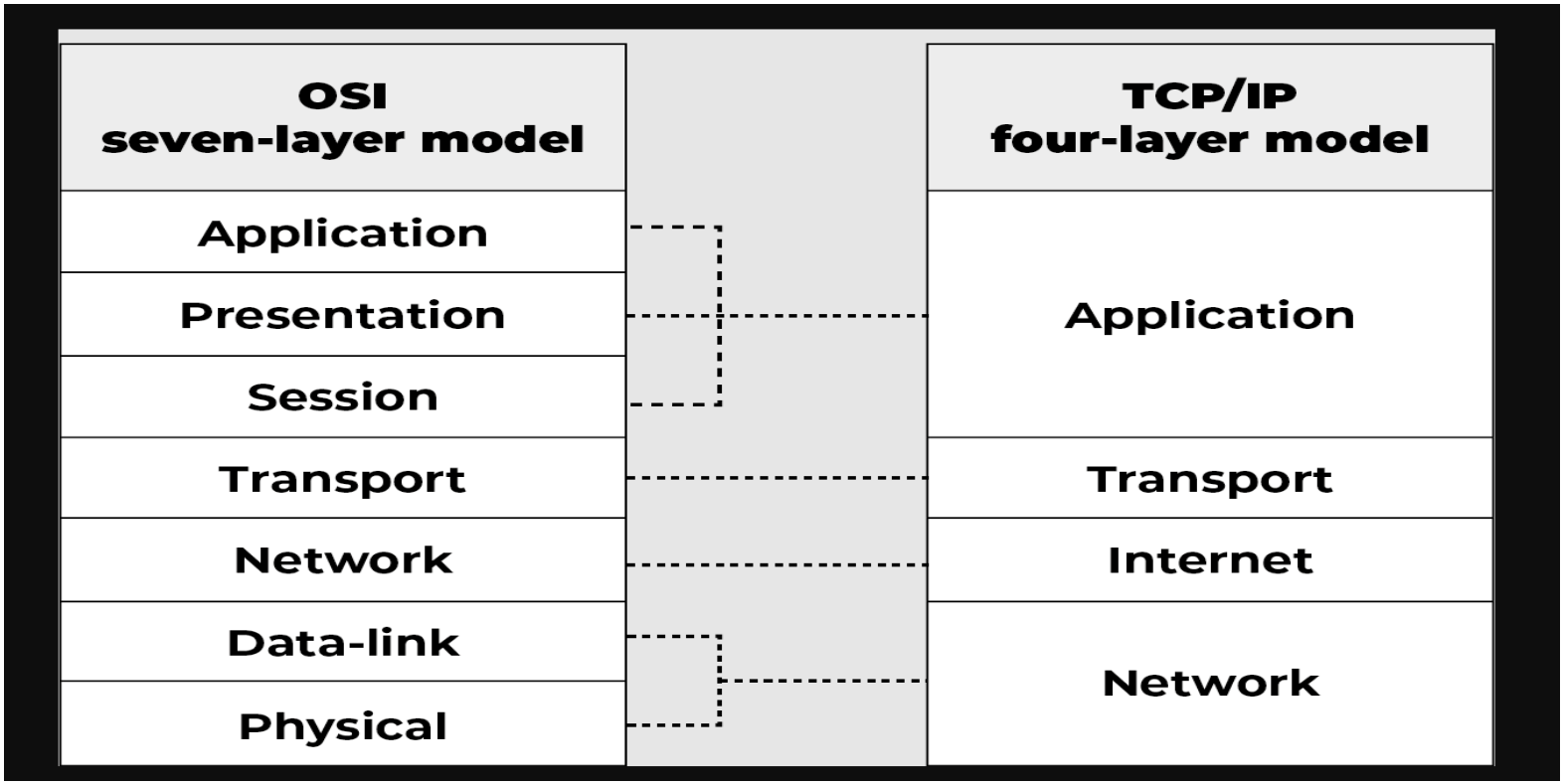
- HTTP, TLS, SSL, SMTP, FTP, TCP, UDP IPsec, MAC, PHY

**TCP/IP** stands for Transmission Control Protocol/Internet Protocol and is a suite of communication protocols used to interconnect network devices on the internet. TCP/IP is also used as a communications protocol in a private computer network (an intranet or extranet).

The TCP/IP model differs slightly from the seven-layer Open Systems Interconnection (OSI) networking model designed after it. The OSI reference model defines how applications can communicate over a network.

**Port**: In computer networking, a port is a number assigned to uniquely identify a connection endpoint and to direct data to a specific service.

# OSI vs. TCP/IP model



**Audit**: A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to an established set of criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes and user practices.

# Nmap

Nmap is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap features include:

- Host discovery
- Port scanning
- Version detection
- TCP/IP stack fingerprinting

# Nmap

Typical uses of Nmap:

- Auditing the security of a device or firewall by identifying the network connections which can be made to, or through it.
- Identifying open ports on a target host in preparation for auditing.
- Network inventory, network mapping, maintenance and asset management.
- Auditing the security of a network by identifying new servers.
- Generating traffic to hosts on a network, response analysis and response time measurement.
- Finding and exploiting vulnerabilities in a network.
- DNS queries and subdomain search

# Nmap task

Run the nmap command in the terminal, looking at the following address: 172.22.204.184
Which ports are open and what services are connected to the ports?
(If you get stuck, it helps to type nmap in the terminal, or if you need more help use the -h switch)

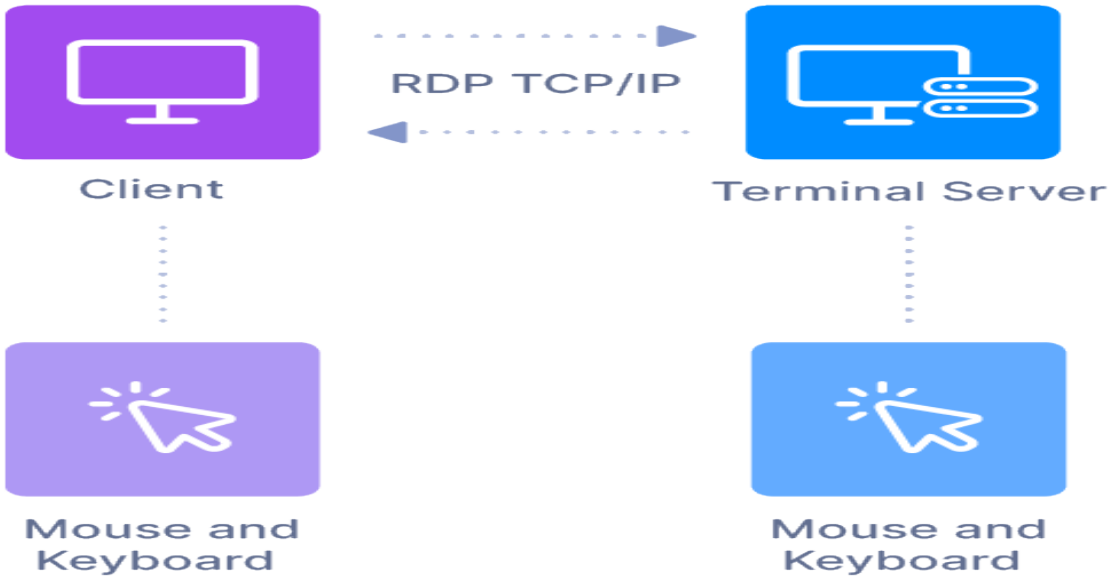
# Remmina

**Remmina** is a remote desktop client. It supports the Remote Desktop Protocol (RDP), VNC, NX, XDMCP, SPICE, X2Go and SSH protocols and uses FreeRDP as foundation. A common use is to connect to Windows machines, to use servers and computers remotely via Remote Desktop Services, by system administrators and novice users.

# Create and prepare your OS scan

- Try to log in to XP with RDP
  Use Remmina in Linux and Remote Desktop in Windows
  **ip address: 172.22.204.184**
  **username: User**
  **password: password**

# Remote Desktop Protocol- RDP



# RDP

- Remote Desktop Protocol (RDP) is a Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389.
- It provides network access for a remote user over an encrypted channel. Network administrators use RDP to diagnose issues, login to servers, and to perform other remote actions.
- Remote users use RDP to log into the organization's network to access email and files.
- Encrypted channel is used (SSL/TLS)

# RDP

- The activity involved in sending and receiving data through the RDP stack is essentially the same as the seven-layer OSI model standards for common LAN networking today.
- Data from an application or service to be transmitted is passed down through the protocol stacks. It's sectioned, directed to a channel (through MCS), encrypted, wrapped, framed, packaged onto the network protocol, and finally addressed and sent over the wire to the client. The returned data works the same way only in reverse. The packet is stripped of its address, then unwrapped, decrypted, and so on.

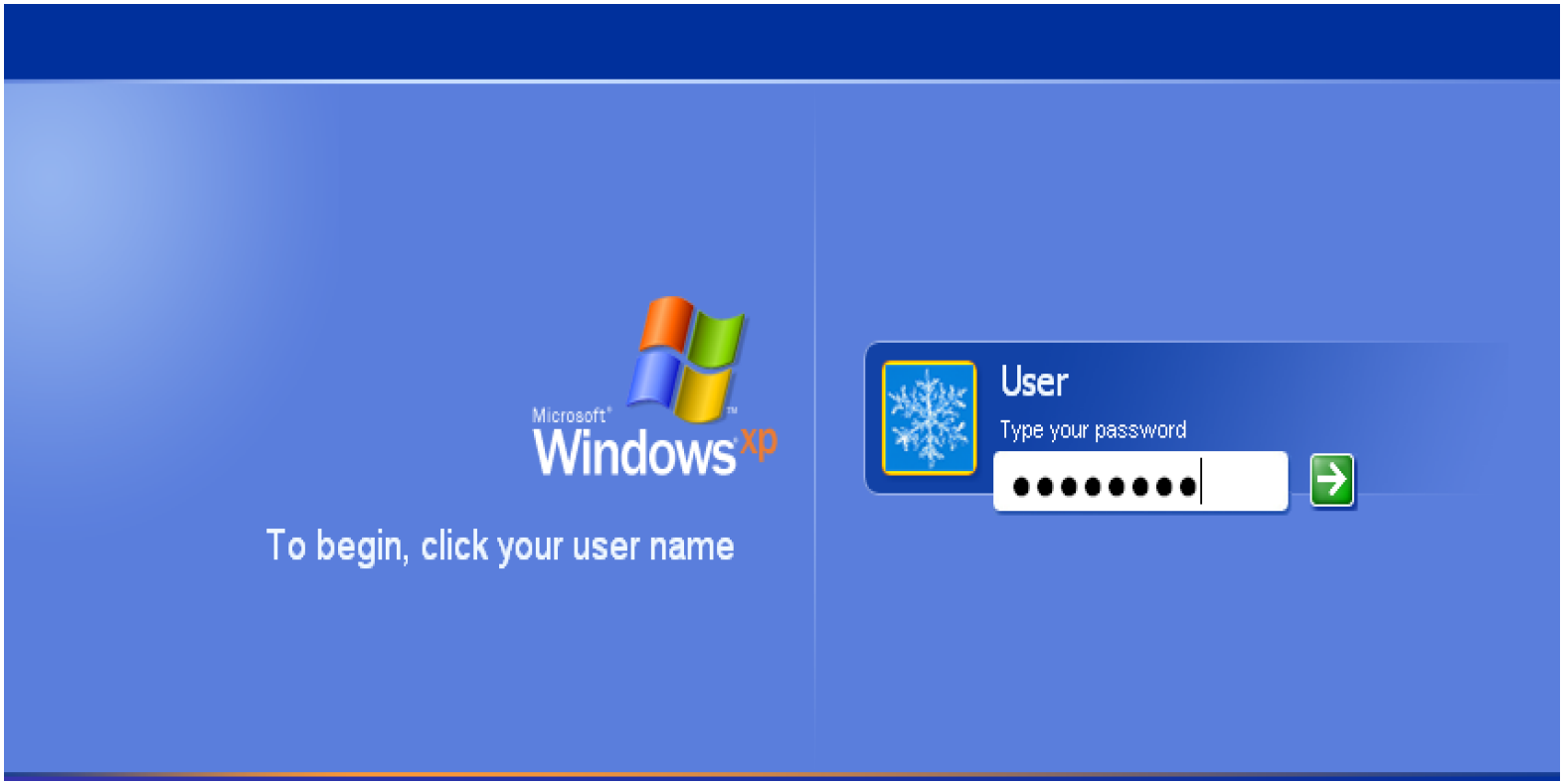
# Hydra

**Hydra** is a parallelized login cracker which supports numerous protocols to attack. It is very fast and flexible, and new modules are easy to add. This tool makes it possible for researchers and security consultants to show how easy it would be to gain unauthorized access to a system remotely.

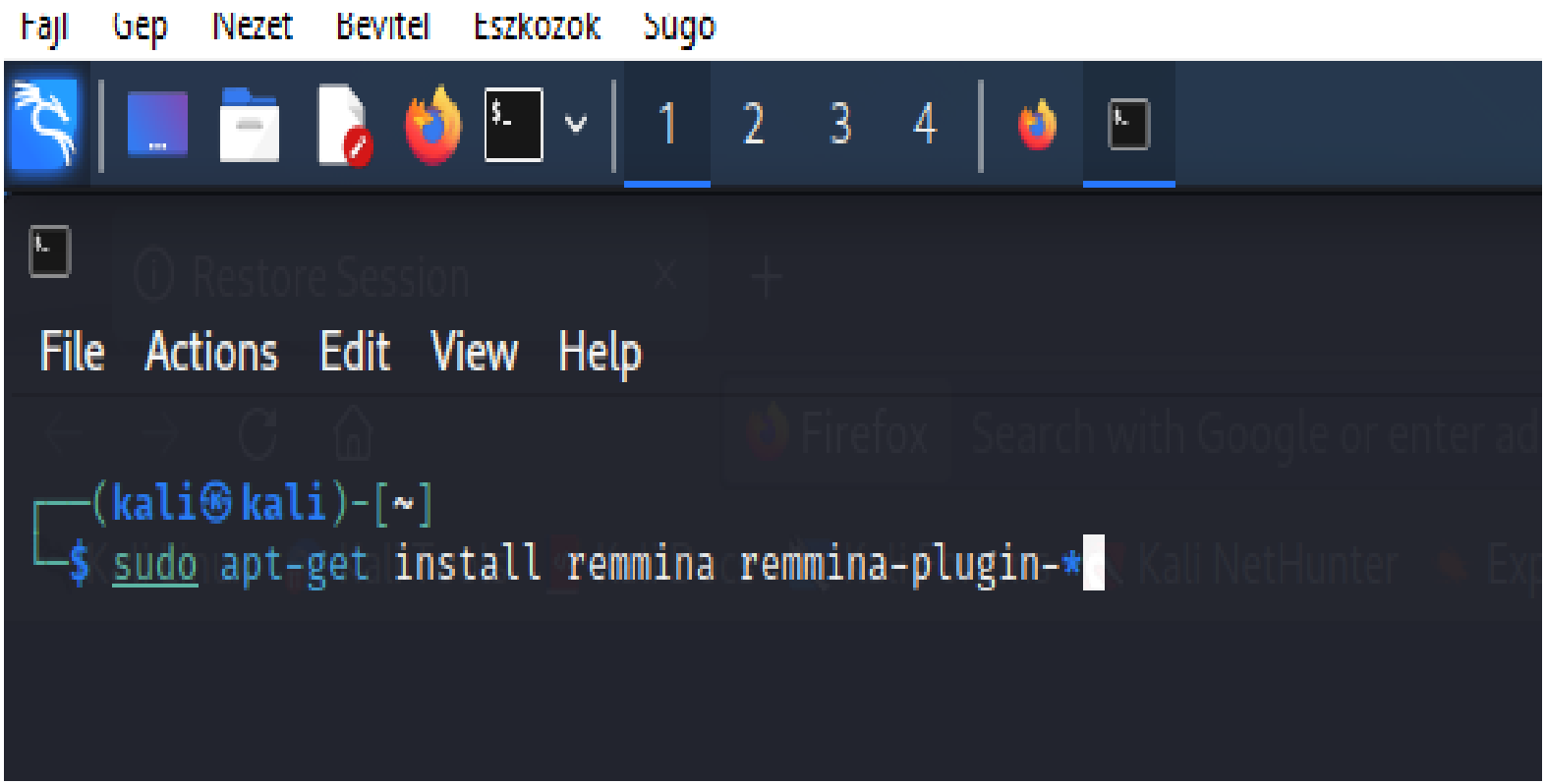
# Create and prepare your OS scan

- Try to apply Hydra in Parrot Linux
  hydra -L user.txt -P rockyou.txt 172.22.204.184 rdp
  Rockyou: https://github.com/brannondorsey/naive-hashcat/releases/download/data/rockyou.txt

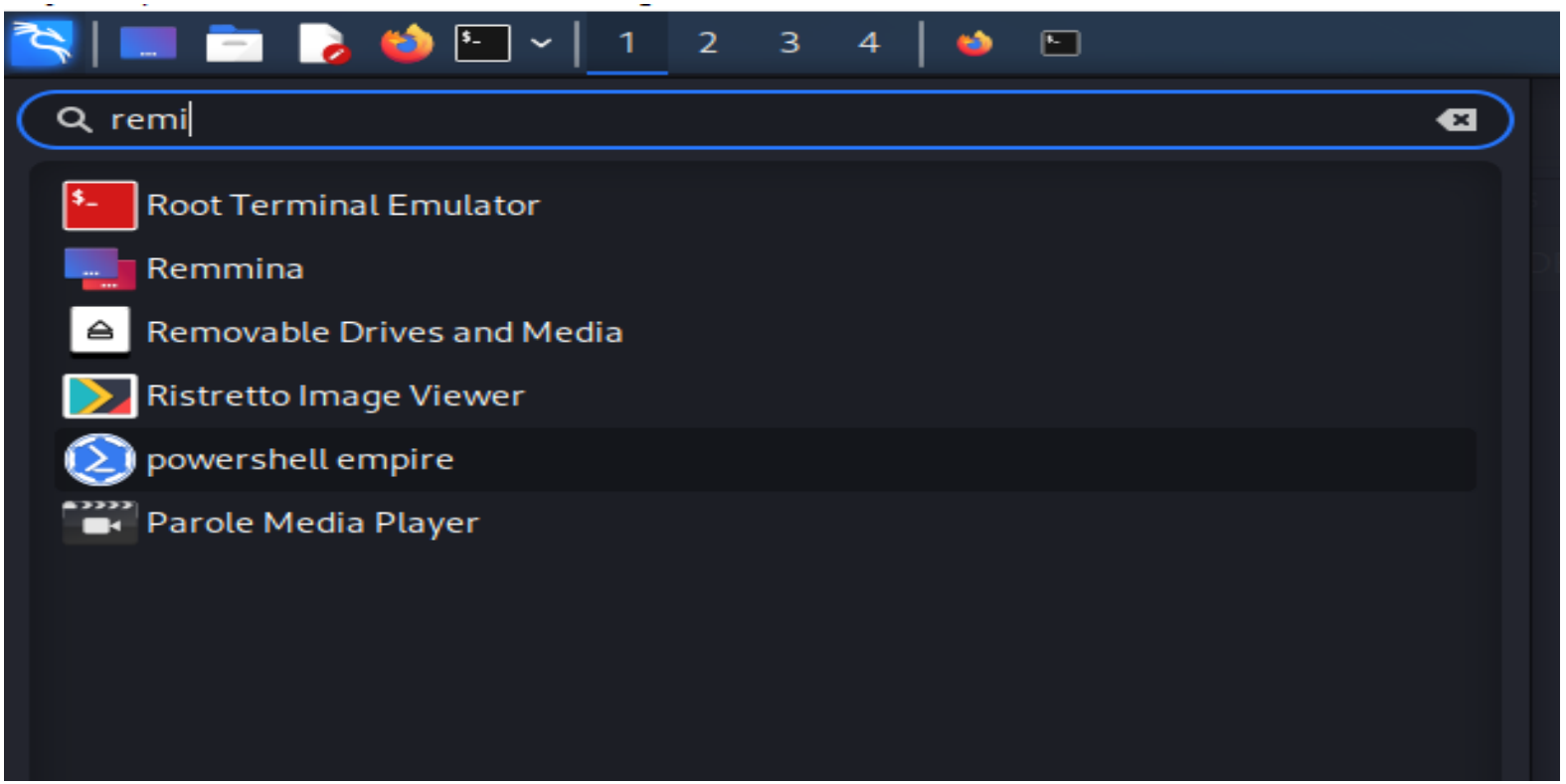
# Create your OS scan



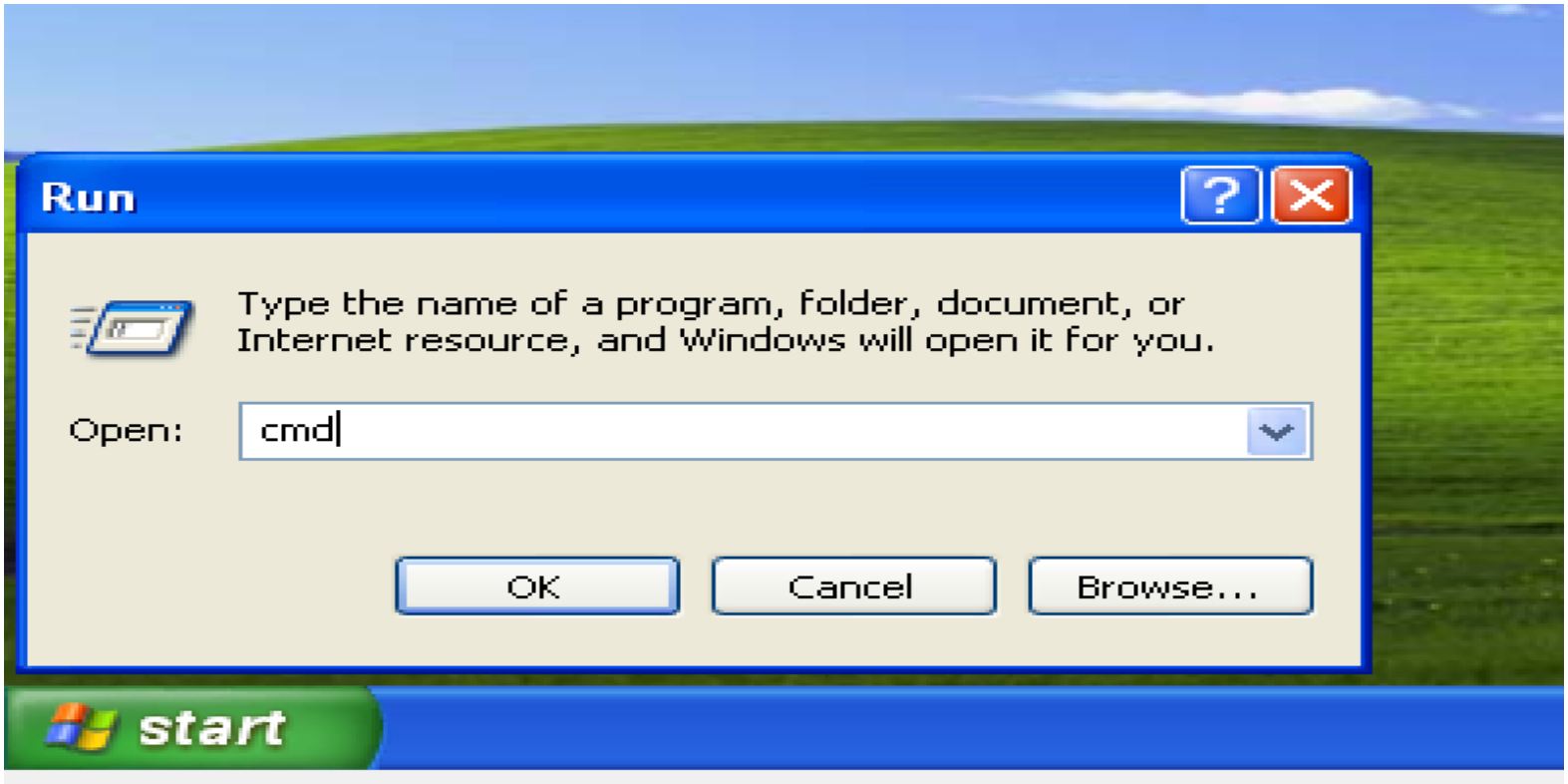
# Create your OS scan



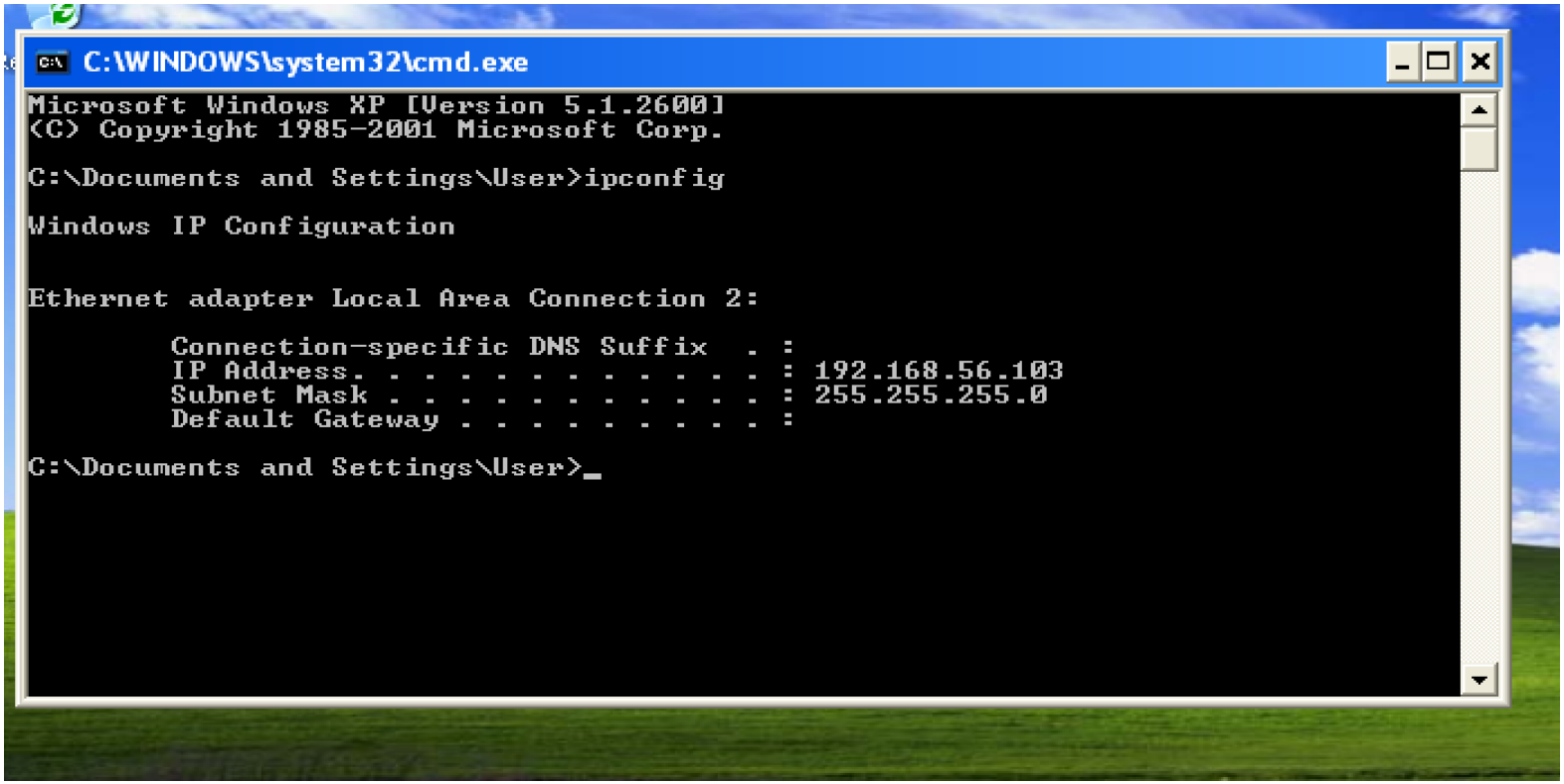
# Create your OS scan



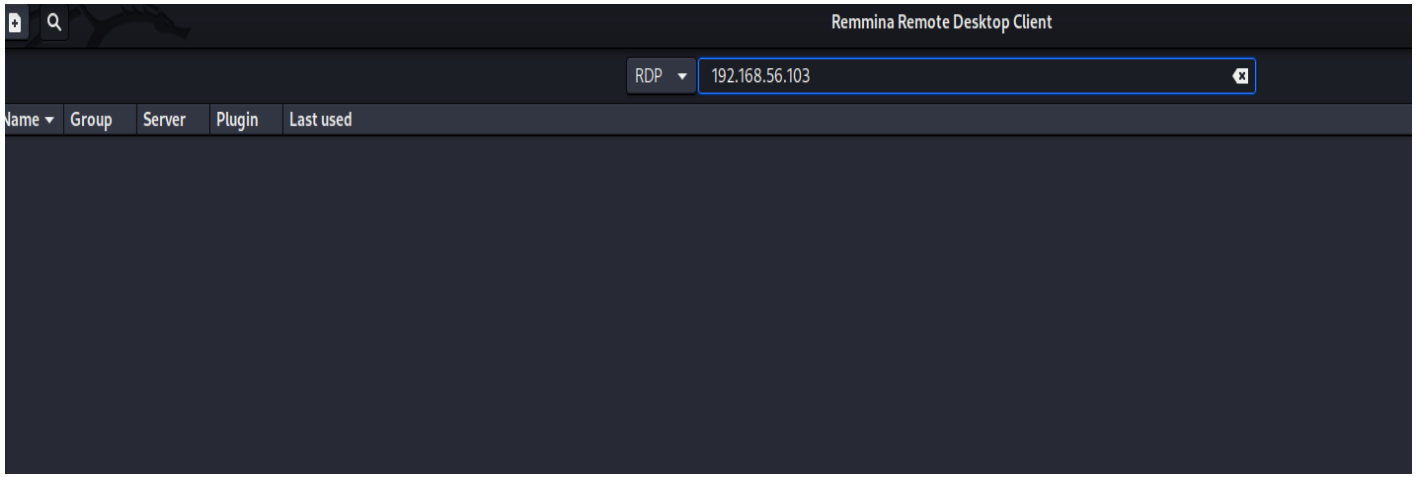
# Create your OS scan



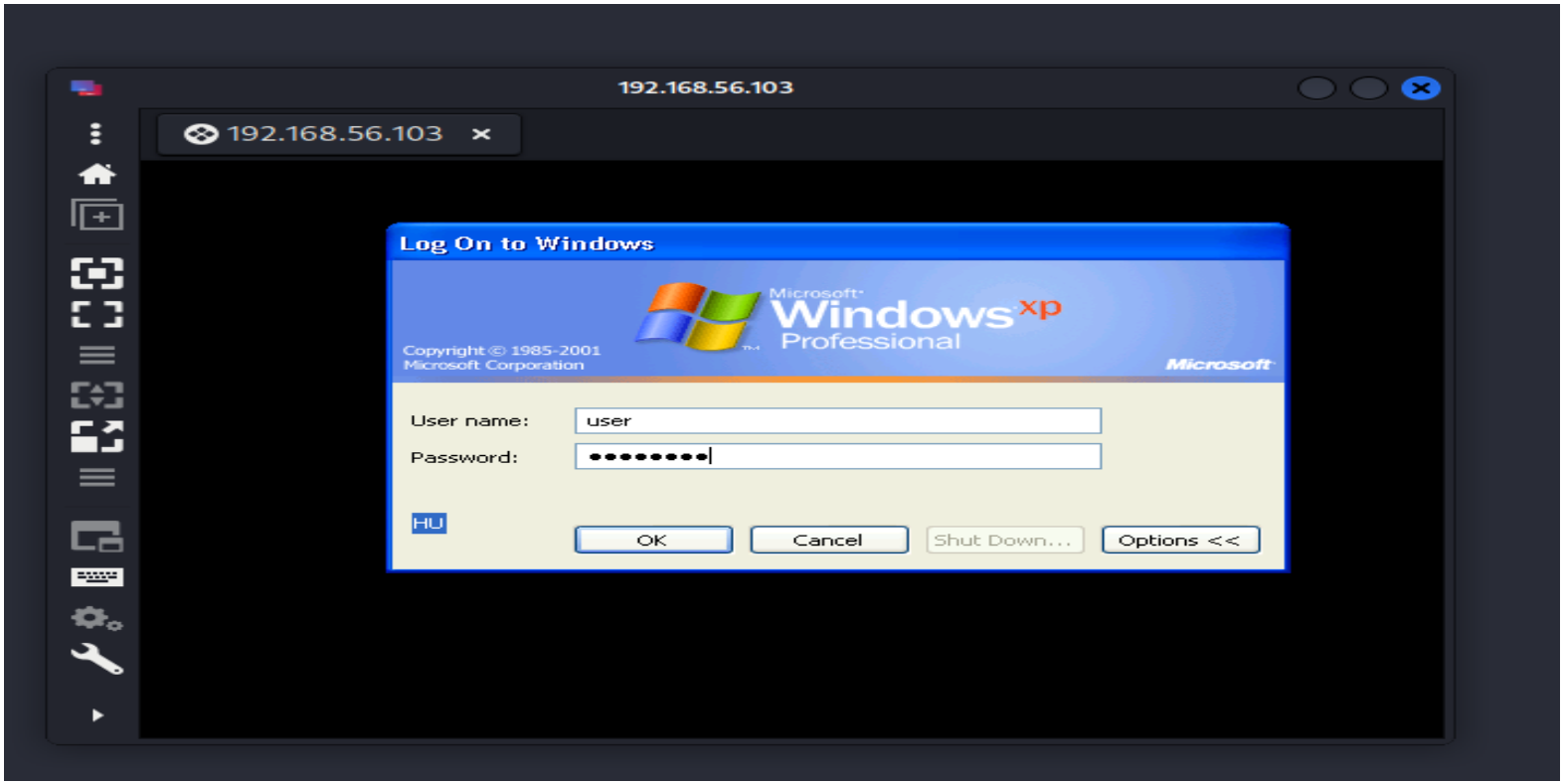
# Create your OS scan



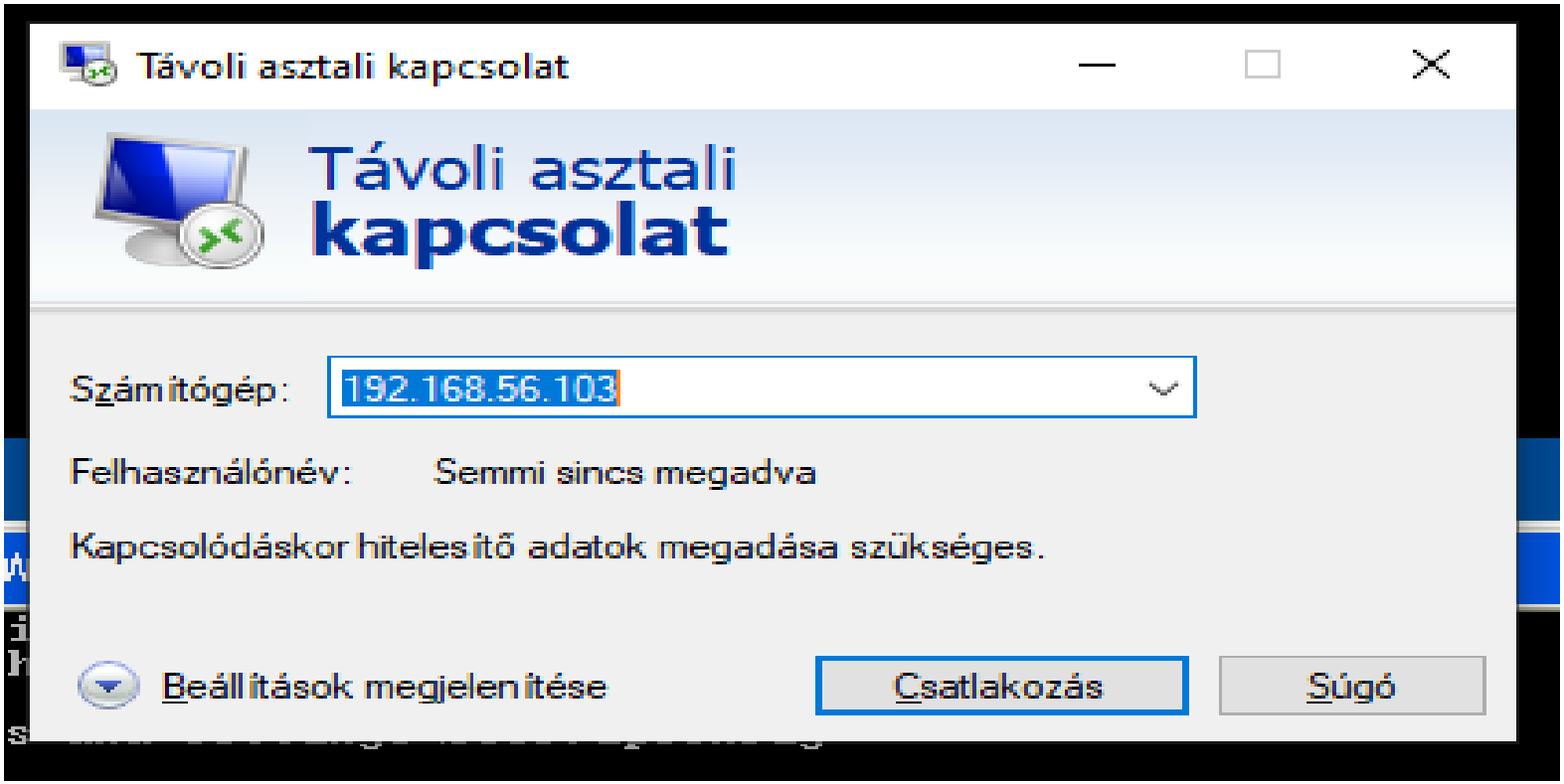
# Create your OS scan



# Create your OS scan



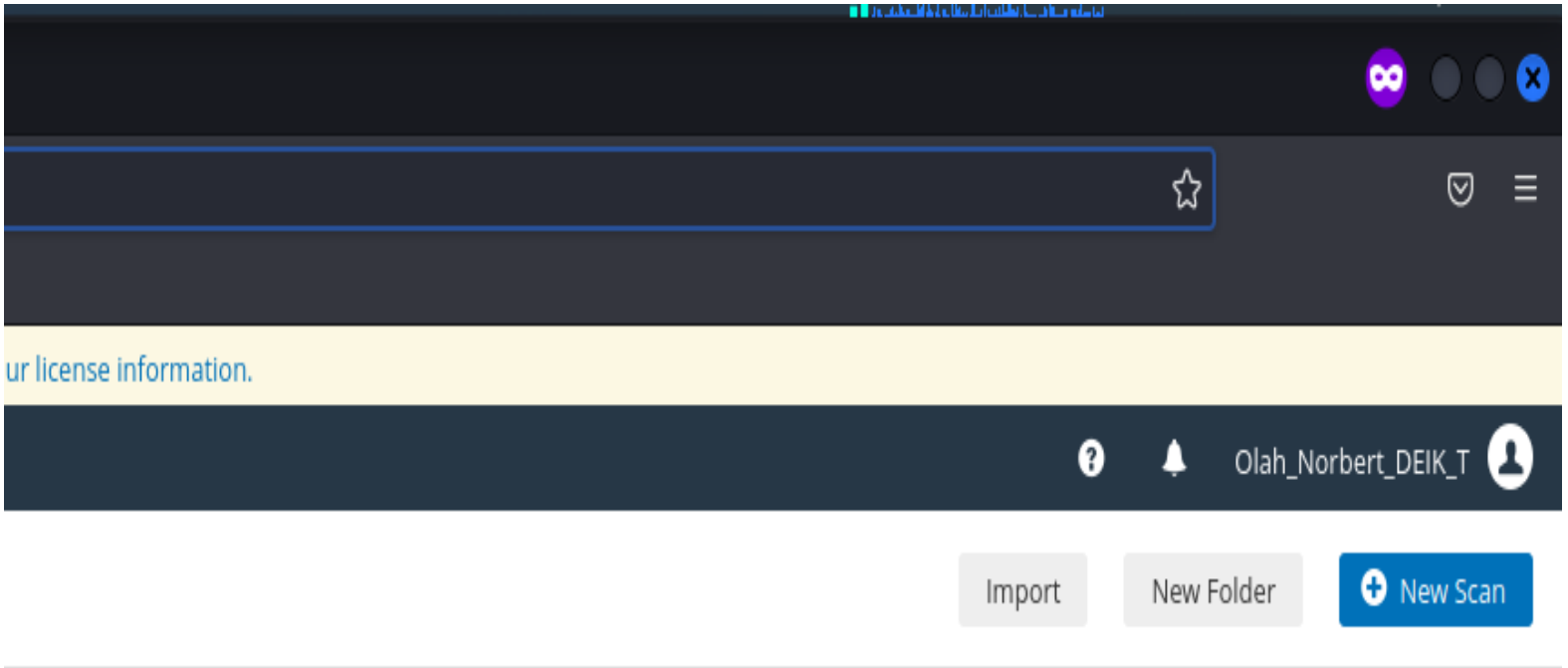
# Create your OS scan



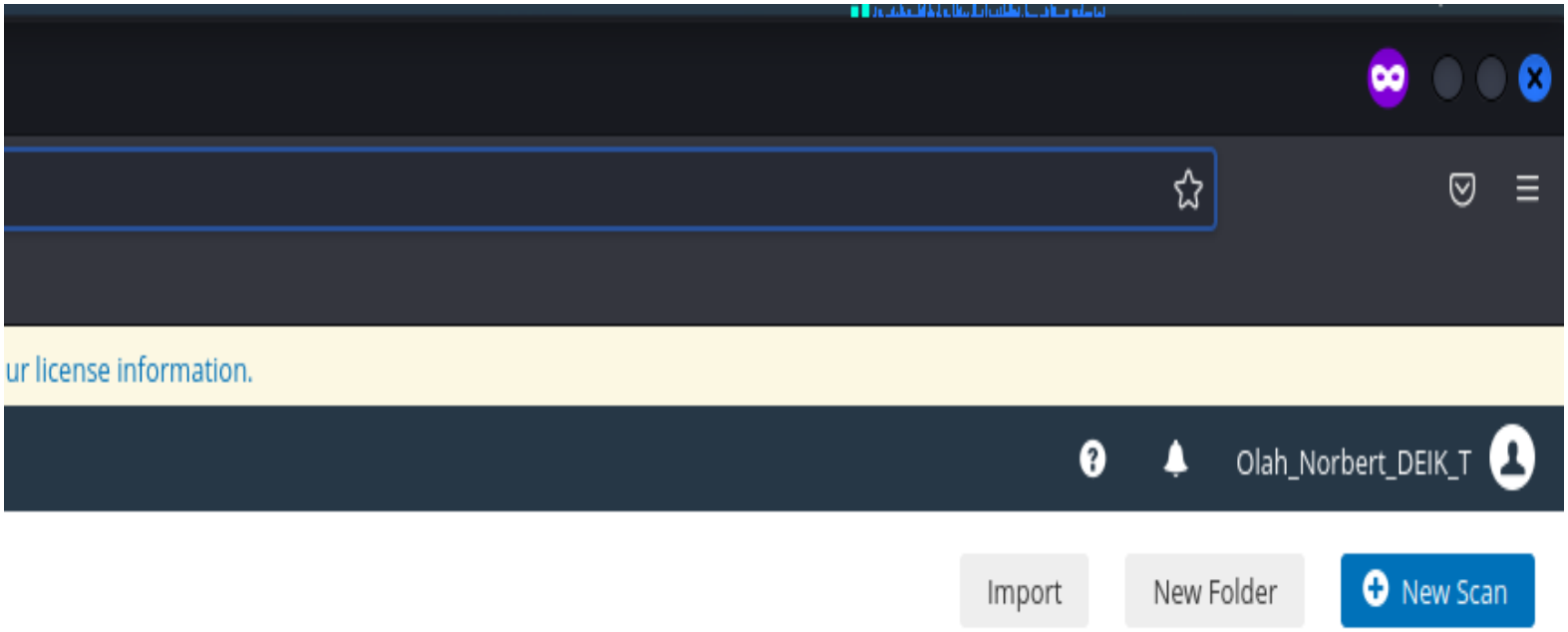
# Create your OS scan

# Create and prepare your OS scan

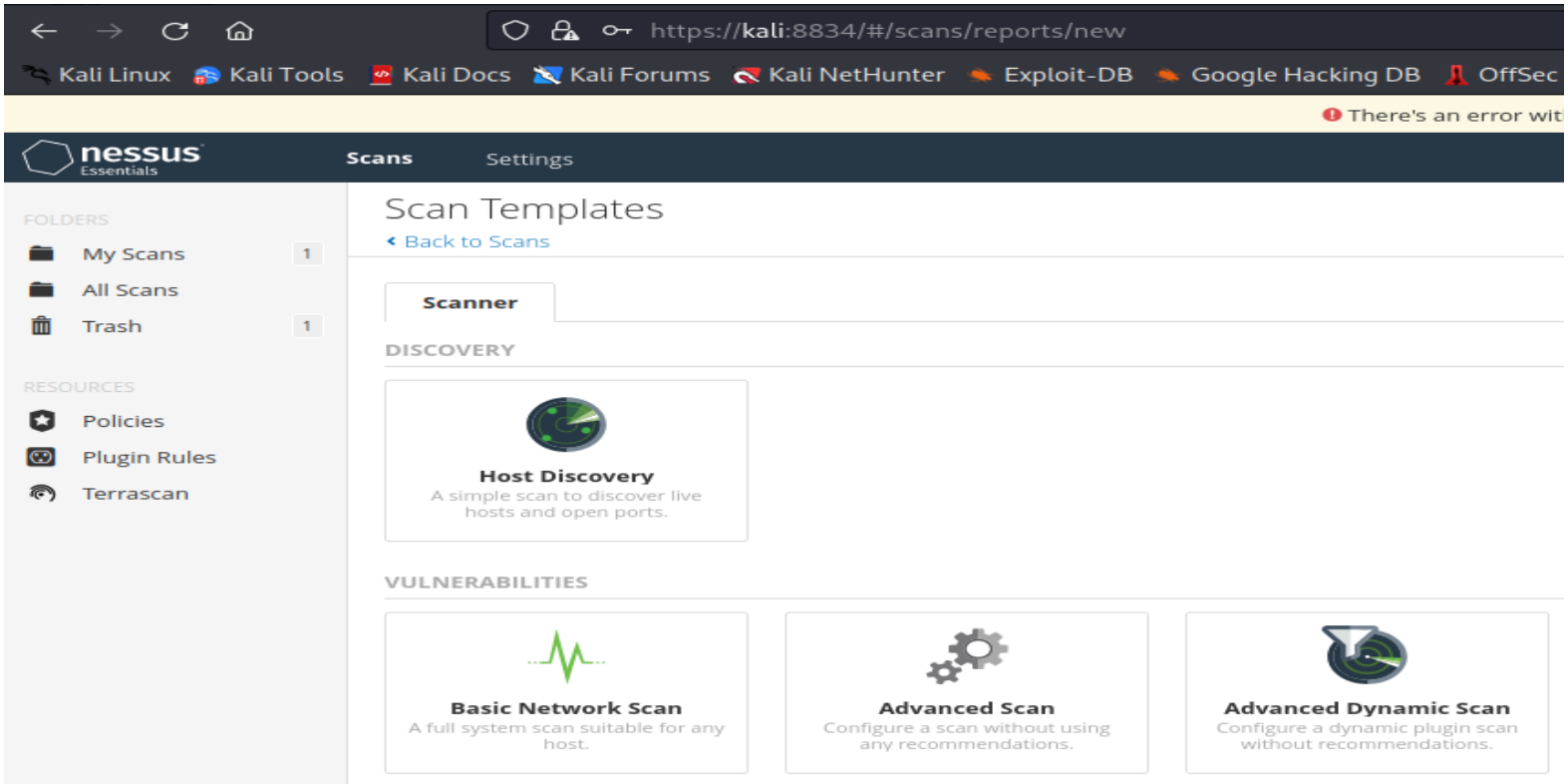
- Create New Scan
- Basic Scan
- Start XP VM **username: User password: password**
- Start cmd
- Use ipconfig
- Copy the IP address to the target box
- Configure the credentials (See the picture)


ur license information.
Olah_Norbert_DEIK_T
Import
New Folder
New Scan

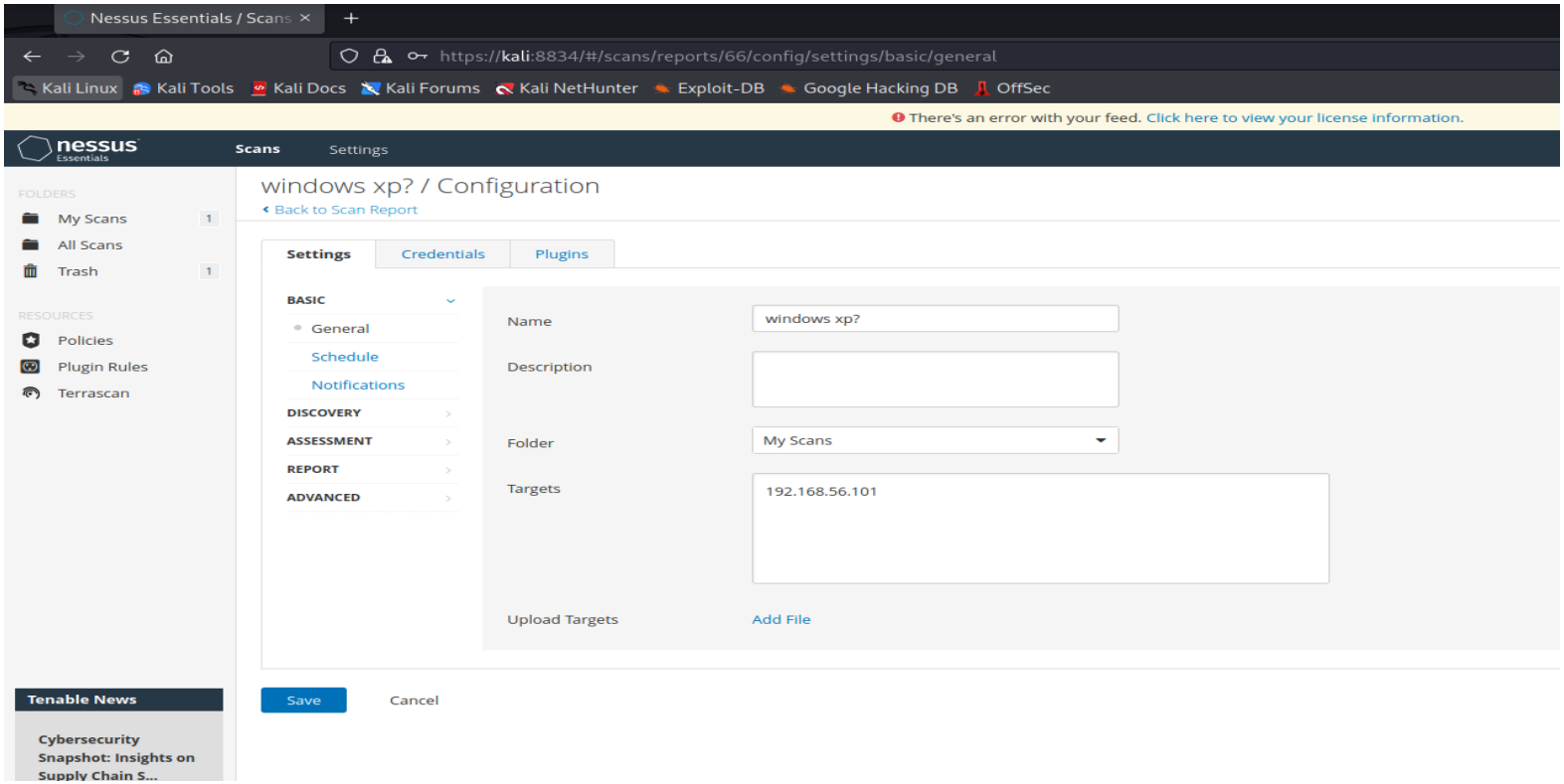
# Create your OS scan



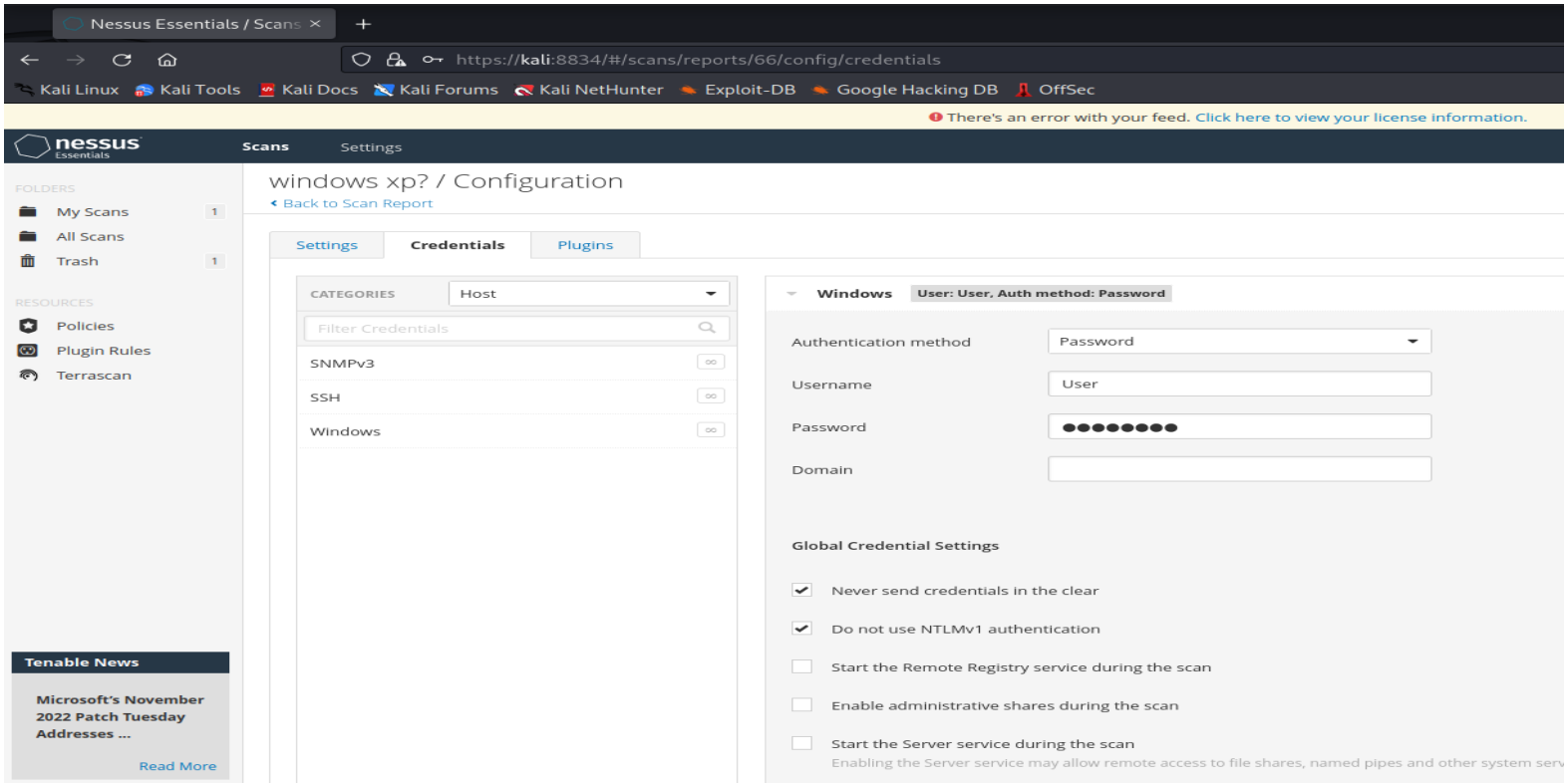
# Create your OS scan



# Create your OS scan



# Create your OS scan



# Create your OS scan

- Create New Scan
- Use Basic Scan / Advanced Scan
- Target: XP
- Generate a PDF from the result and write the IP Address and ports of the target

# Create your OS scan

- Set This policy setting is: Computer Configuration → Administrative Templates → Windows Components → Remote Desktop Services → Remote Desktop Session Host → Security → Require use of specific security layer for remote (RDP) connections
- Run the scan again
- What happens when a firewall is switched on?
- Run the scan again

Thank you for your attention!