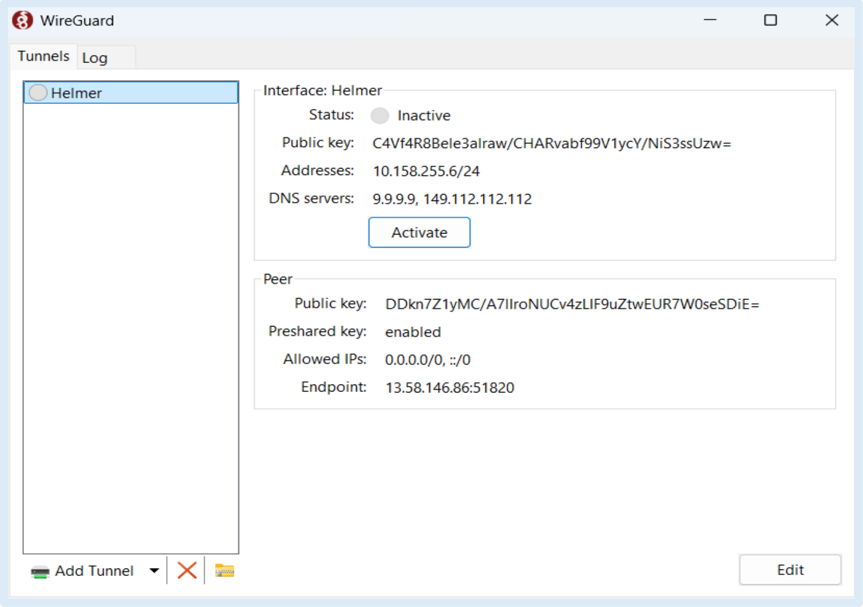
KNIGHT

USER MANUAL

TABLE OF CONTENTS

VPN Connection

Open WireGuard



Interface: Helmer

Status: ○ Inactive

Public key: C4Vf4R8Bele3alraw/CHARvabf99V1ycY/NiS3ssUzw=

Addresses: 10.158.255.6/24

DNS servers: 9.9.9.9, 149.112.112.112

Activate

Peer

Public key: DDkn7Z1yMC/A7IlroNUCv4zLIF9uZtwEUR7W0seSDiE=

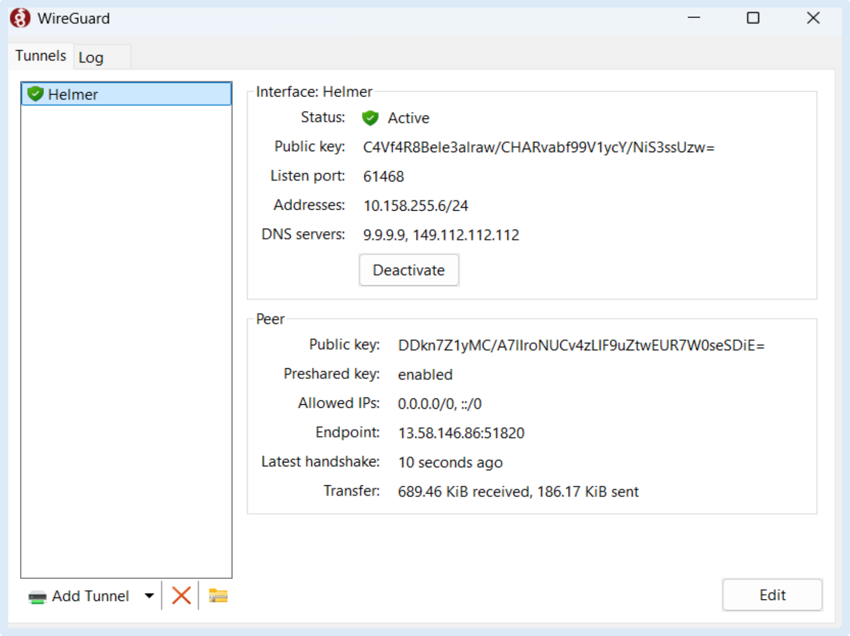
Preshared key: enabled

Allowed IPs: 0.0.0.0/0, ::/0

Endpoint: 13.58.146.86:51820

A member of the KNIGHT group should have already configured your VPN tunnel

Click Activate



Interface: Helmer

Status: ✓ Active

Public key: C4Vf4R8Bele3alraw/CHARvabf99V1ycY/NiS3ssUzw=

Listen port: 61468

Addresses: 10.158.255.6/24

DNS servers: 9.9.9.9, 149.112.112.112

Deactivate

Peer

Public key: DDkn7Z1yMC/A7IlroNUCv4zLIF9uZtwEUR7W0seSDiE=

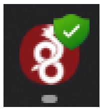
Preshared key: enabled

Allowed IPs: 0.0.0.0/0, ::/0

Endpoint: 13.58.146.86:51820

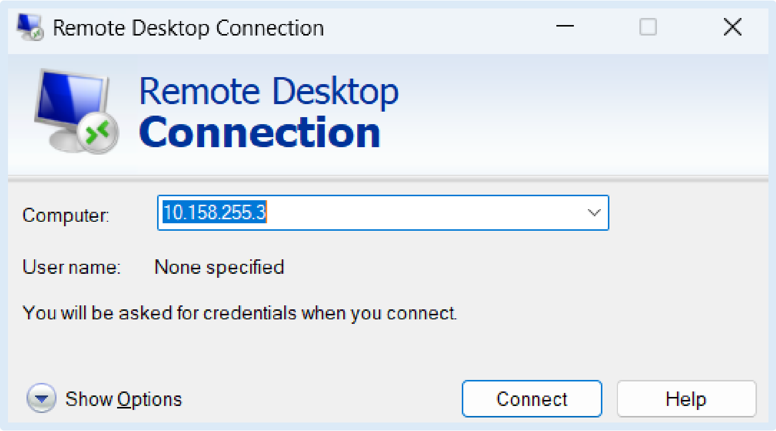
Latest handshake: 10 seconds ago

Transfer: 689.46 KiB received, 186.17 KiB sent



Your WireGuard is now active

Login to KNIGHT Device

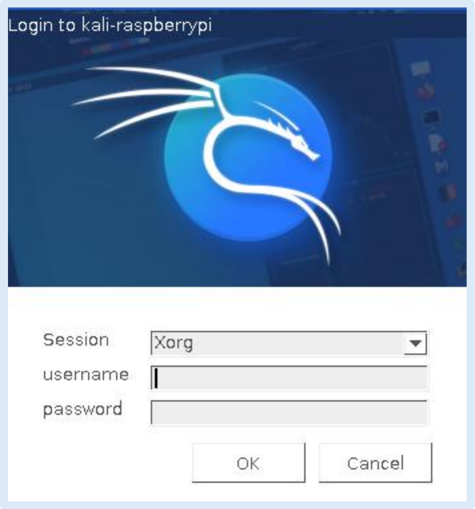


Computer: 10.158.255.3

User name: None specified

You will be asked for credentials when you connect.

Open Remote Desktop Connection and enter the IP address of the KNIGHT device



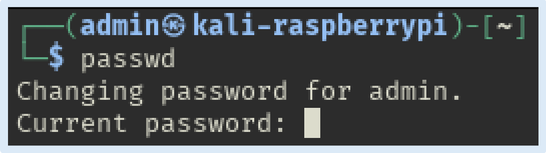
Session: Xorg

username

password

Enter Username and Password (kali and kali) on startup

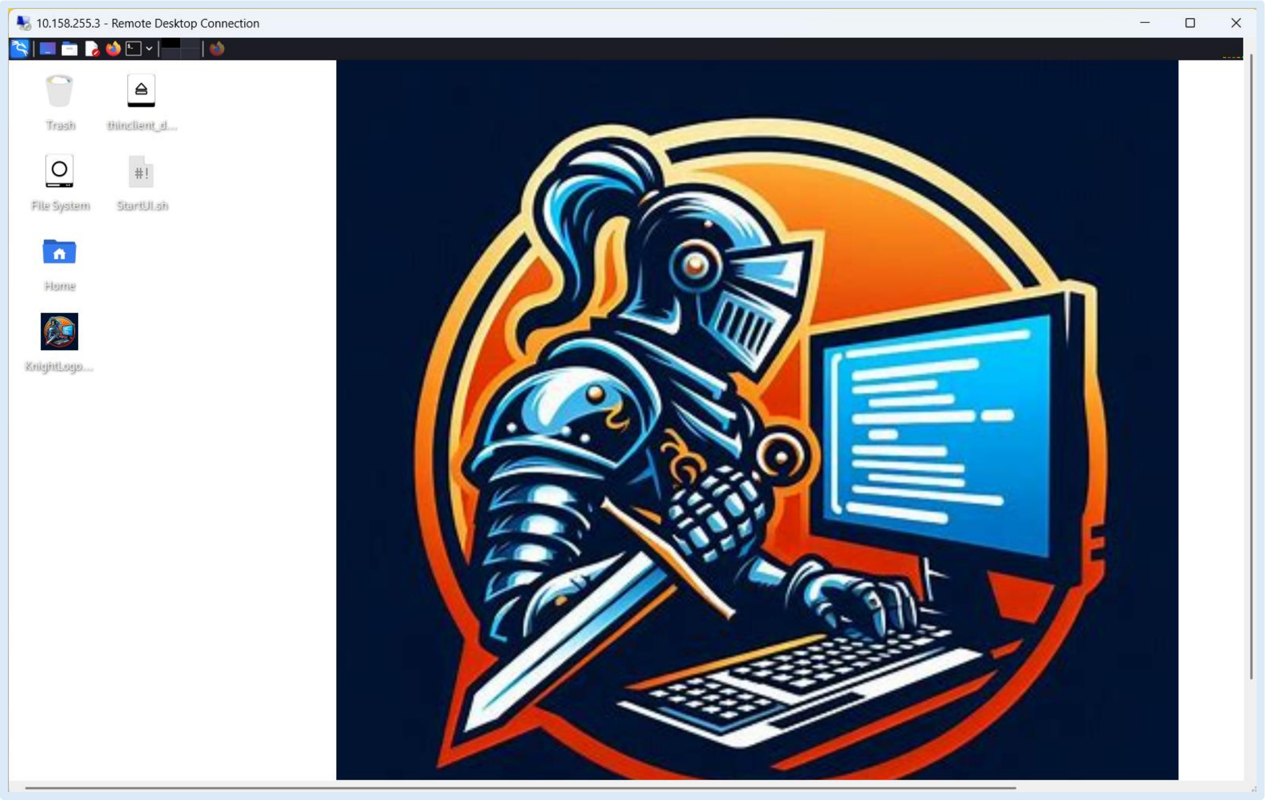
Click OK



```
┌──(admin㉿kali-raspberrypi)-[~]
└─$ passwd
Changing password for admin.
Current password: █
```

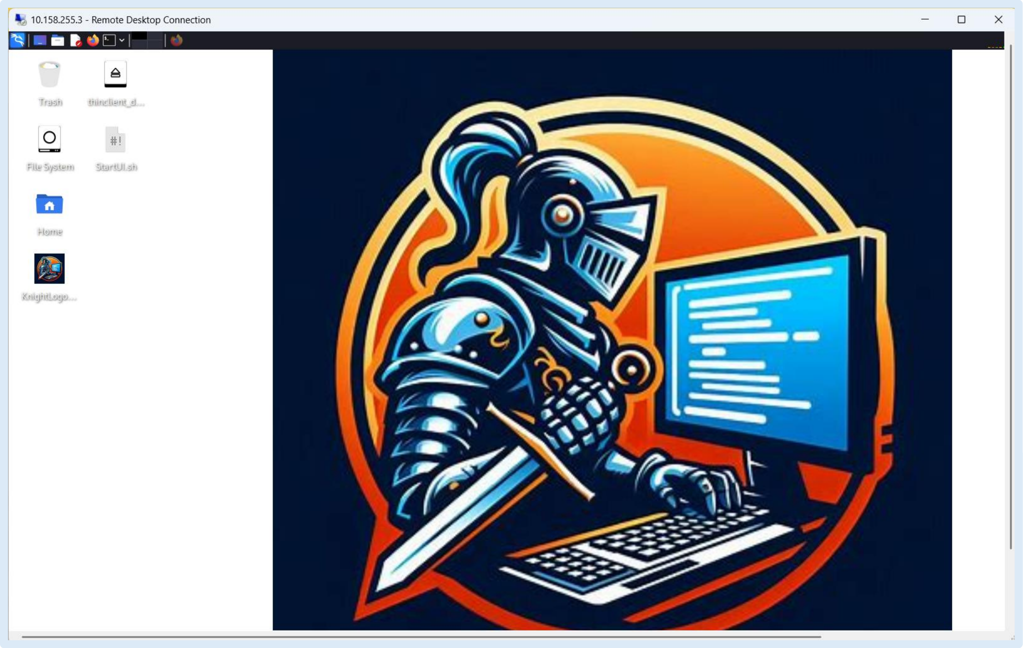
Open the terminal and enter passwd

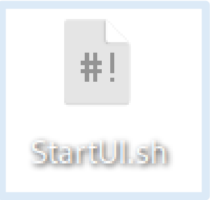
Enter kali and then your new password (make sure to remember your password)



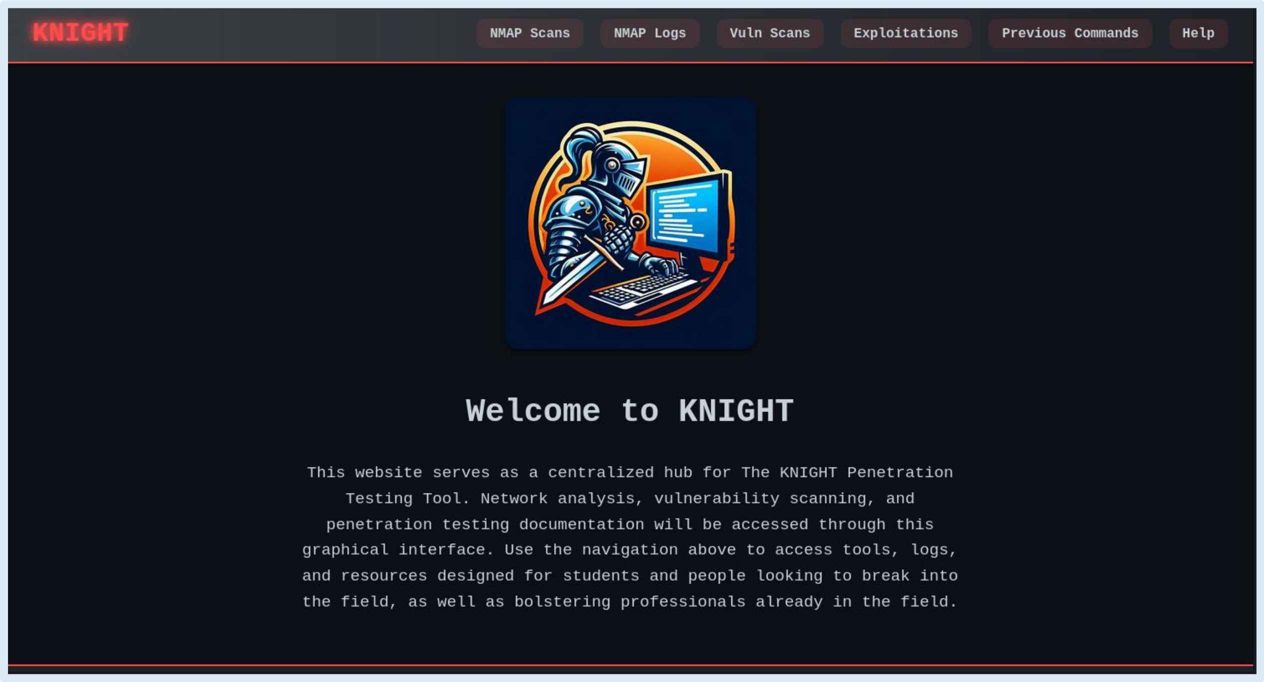
Congratulations, you are remotely connected to the KNIGHT device!

Start KNIGHT UI





While on the desktop find the StartUI.sh file and double left click it

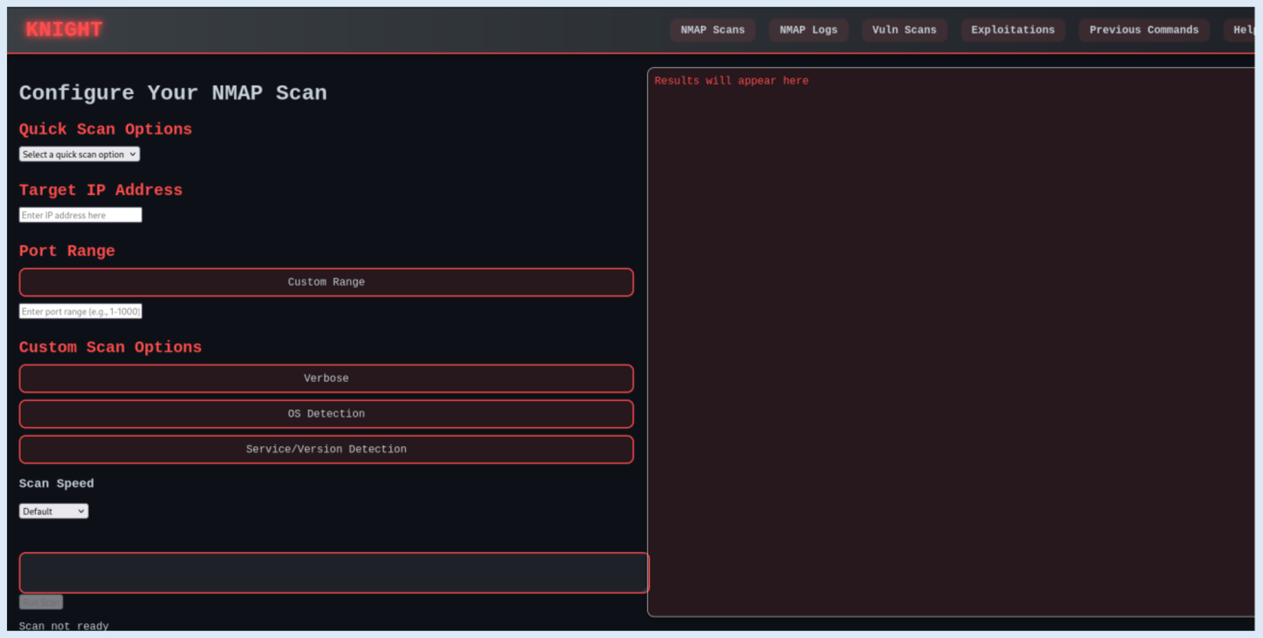


Welcome to KNIGHT

This website serves as a centralized hub for The KNIGHT Penetration Testing Tool. Network analysis, vulnerability scanning, and penetration testing documentation will be accessed through this graphical interface. Use the navigation above to access tools, logs, and resources designed for students and people looking to break into the field, as well as bolstering professionals already in the field.

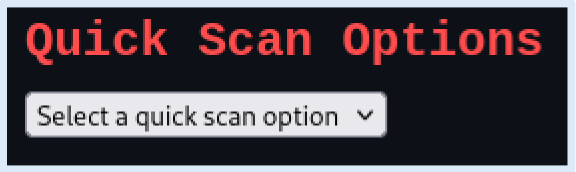
You can now run scans via the KNIGHT UI

Your First NMAP Scan

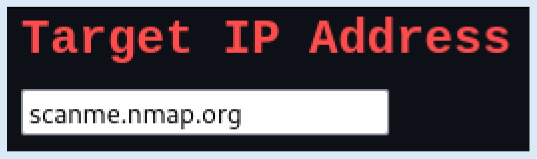


Scan not ready

Navigate to the NMAP Scans tab



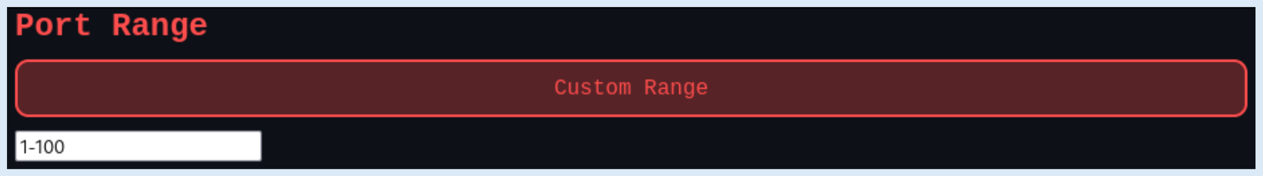
If desired, select a quick scan option



Target IP Address

scanme.nmap.org

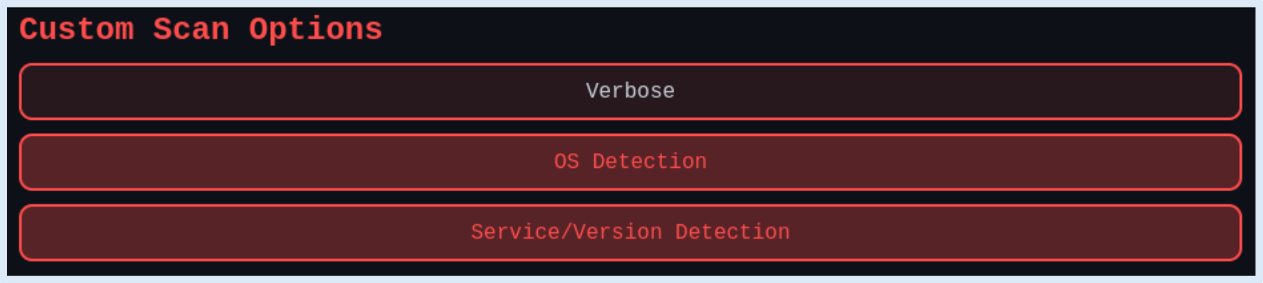
Select the IP address that you would like to scan. A good example is scanme.nmap.org. You may also choose a range of IP addresses by adding a dash and then the final IP address. For example, 192.168.2.1-192.168.2.252.



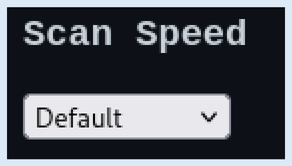
Port Range

1-100

Click Custom Range and enter the port range that you would like to scan

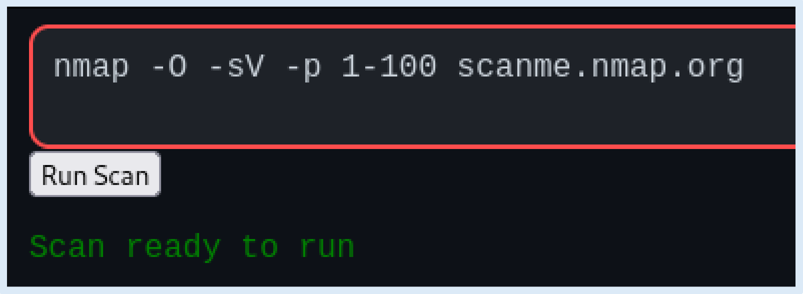


Select your desired Custom Scan Options


Scan Speed

Default

Select the Scan Speed to change it from default if desired


```
nmap -O -sV -p 1-100 scanme.nmap.org
```

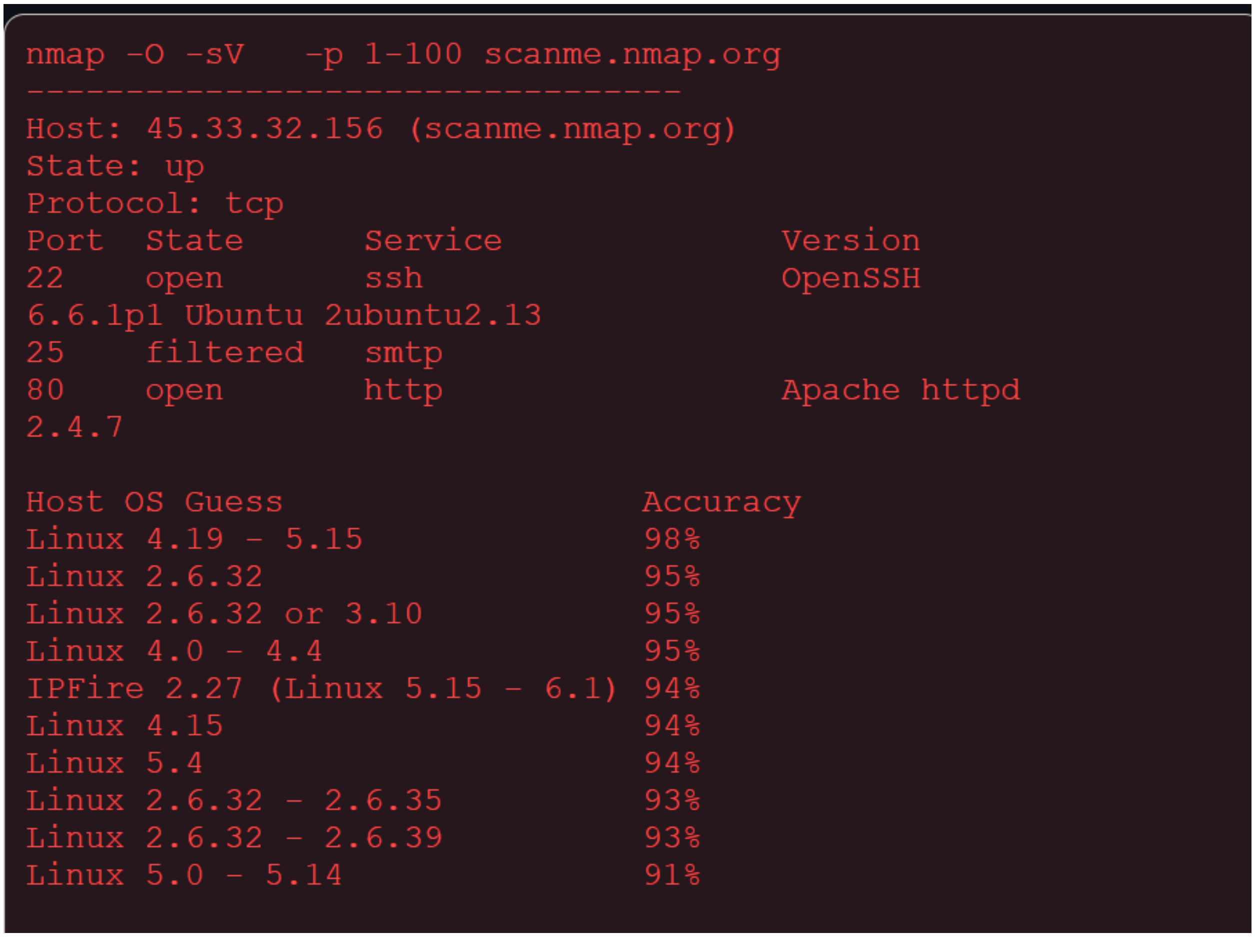
```
Scan ready to run
```

Click Run Scan

```
Running scan...
```

```
Scan completed!
```

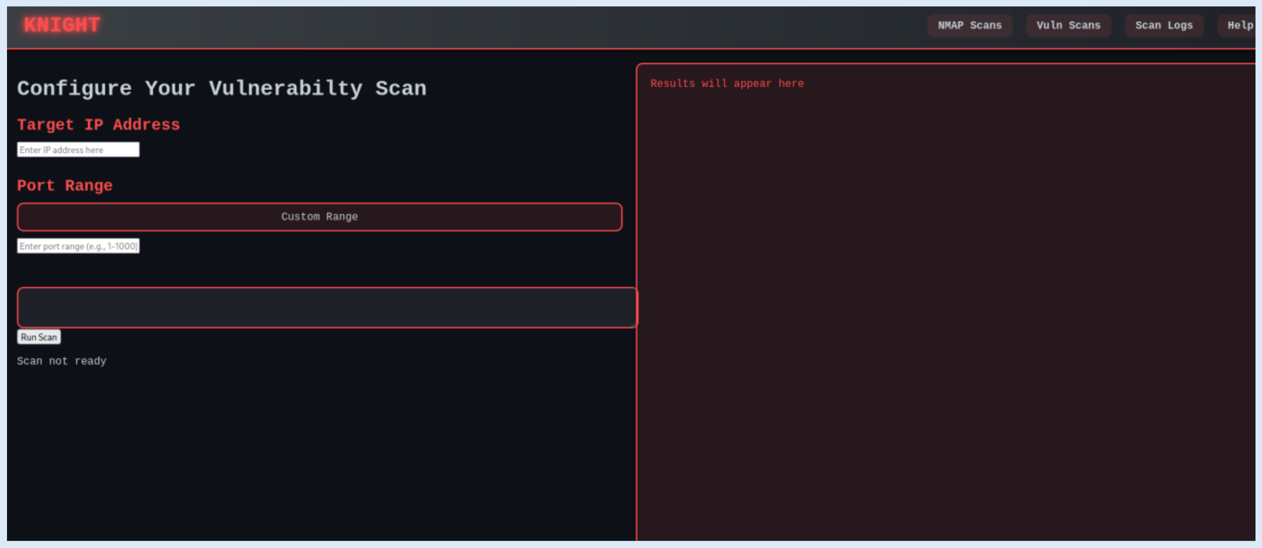
The scan is now complete



```
nmap -O -sV   -p 1-100 scanme.nmap.org
---------------------------------
Host: 45.33.32.156 (scanme.nmap.org)
State: up
Protocol: tcp
Port  State     Service              Version
22    open      ssh                  OpenSSH
6.6.1p1 Ubuntu 2ubuntu2.13
25    filtered  smtp
80    open      http                 Apache httpd
2.4.7

Host OS Guess                  Accuracy
Linux 4.19 - 5.15              98%
Linux 2.6.32                   95%
Linux 2.6.32 or 3.10           95%
Linux 4.0 - 4.4                95%
IPFire 2.27 (Linux 5.15 - 6.1) 94%
Linux 4.15                     94%
Linux 5.4                      94%
Linux 2.6.32 - 2.6.35          93%
Linux 2.6.32 - 2.6.39          93%
Linux 5.0 - 5.14               91%
```

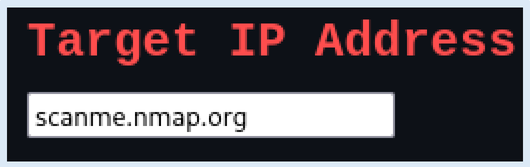
You completed an NMAP scan of the IP address!

Your First Vulnerability Scan



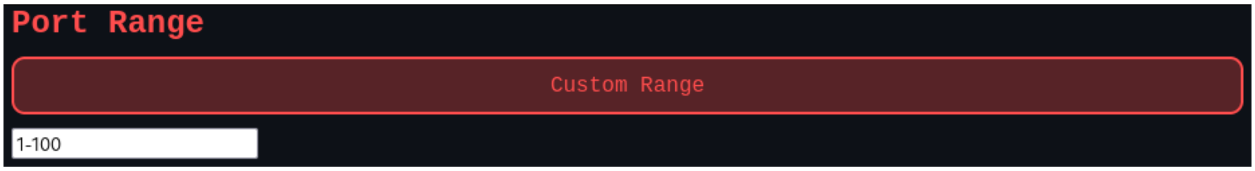
Scan not ready

Navigate to the Vuln Scans tab



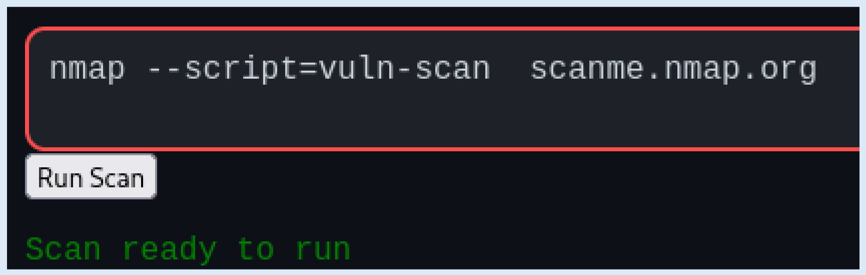
scanme.nmap.org

Select the IP address that you would like to scan. A good example is scanme.nmap.org. You may also choose a range of IP addresses by adding a dash and then the final IP address. For example, 192.168.2.1-192.168.2.252.



1-100

Click Custom Range and enter the port range that you would like to scan



```
nmap --script=vuln-scan  scanme.nmap.org
```

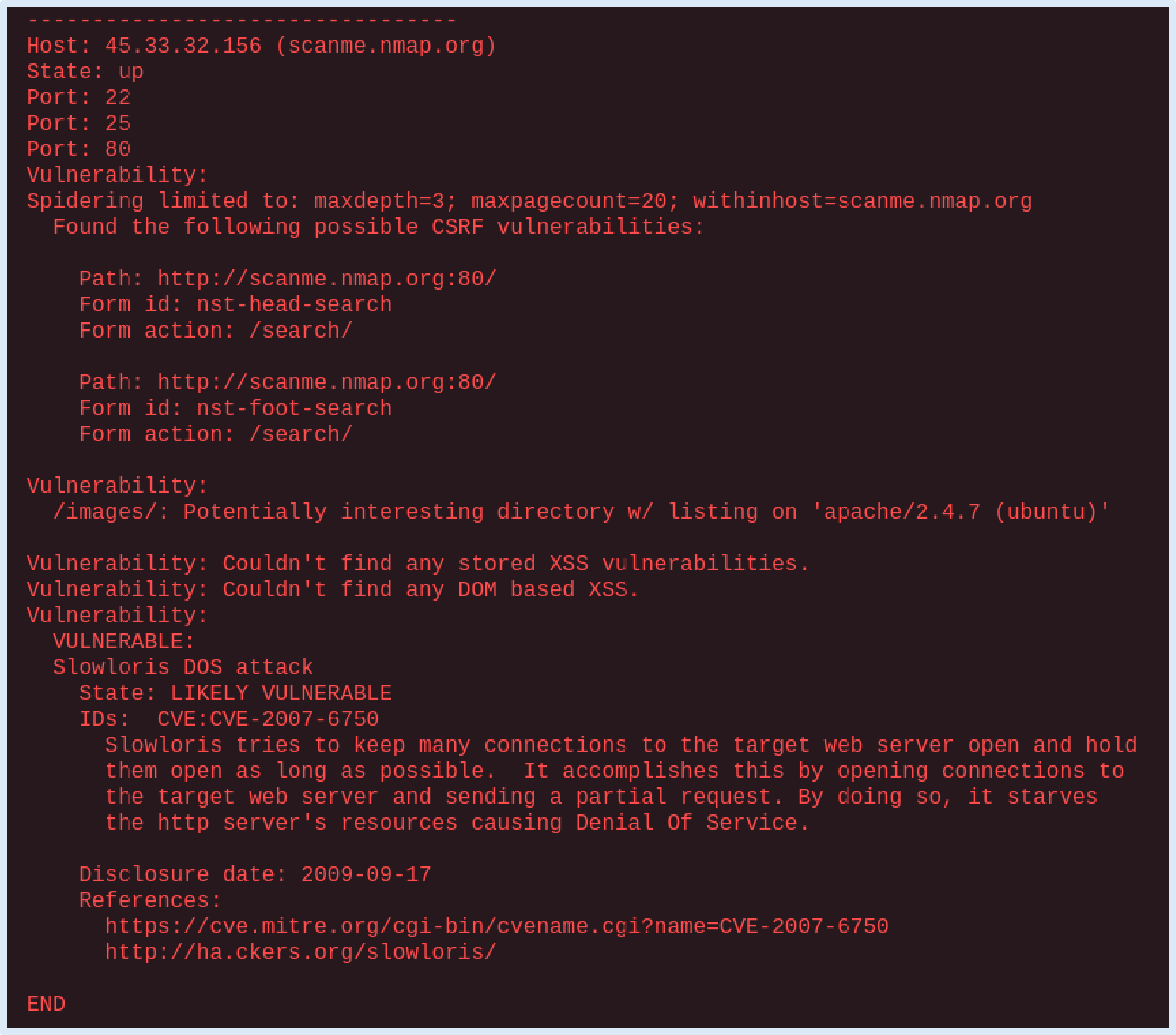
Scan ready to run

Click Run Scan

```
Running scan...
```

```
Scan completed!
```

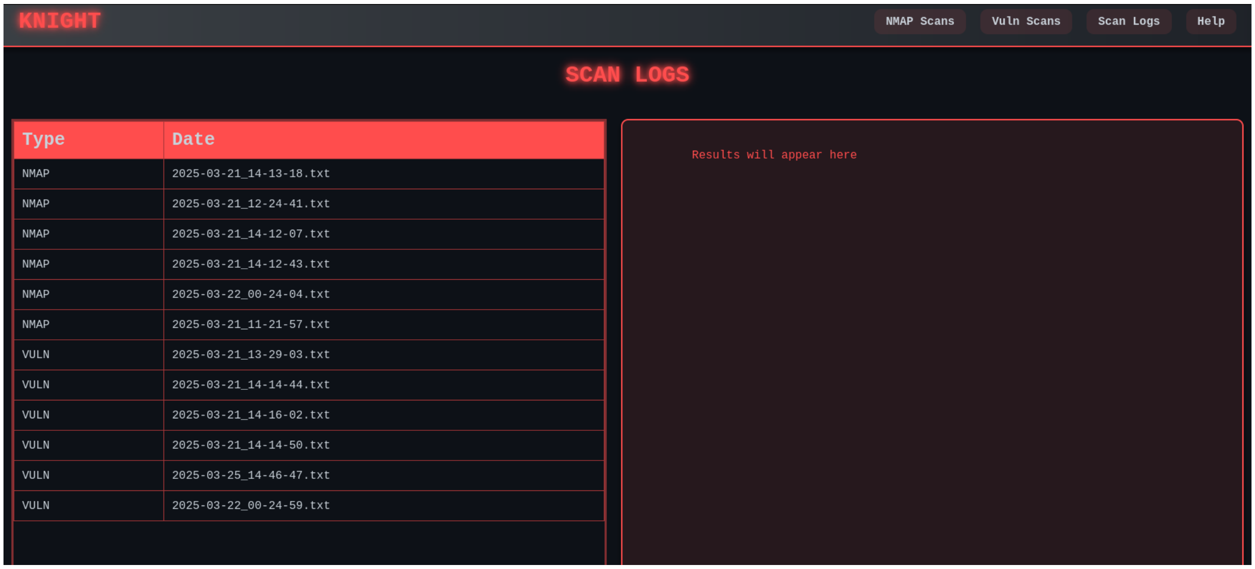
The scan is now complete



```
---------------------------------
Host: 45.33.32.156 (scanme.nmap.org)
State: up
Port: 22
Port: 25
Port: 80
Vulnerability:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
  Found the following possible CSRF vulnerabilities:

    Path: http://scanme.nmap.org:80/
    Form id: nst-head-search
    Form action: /search/

    Path: http://scanme.nmap.org:80/
    Form id: nst-foot-search
    Form action: /search/

Vulnerability:
  /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'

Vulnerability: Couldn't find any stored XSS vulnerabilities.
Vulnerability: Couldn't find any DOM based XSS.
Vulnerability:
  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs:  CVE:CVE-2007-6750
      Slowloris tries to keep many connections to the target web server open and hold
      them open as long as possible.  It accomplishes this by opening connections to
      the target web server and sending a partial request. By doing so, it starves
      the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
      http://ha.ckers.org/slowloris/

END
```

You completed a vulnerability scan of the IP address!

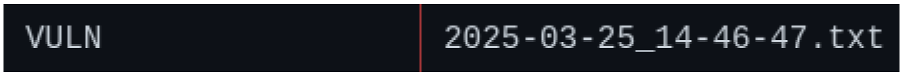
Looking at Previous Scans



Type	Date
NMAP	2025-03-21_14-13-18.txt
NMAP	2025-03-21_12-24-41.txt
NMAP	2025-03-21_14-12-07.txt
NMAP	2025-03-21_14-12-43.txt
NMAP	2025-03-22_00-24-04.txt
NMAP	2025-03-21_11-21-57.txt
VULN	2025-03-21_13-29-03.txt
VULN	2025-03-21_14-14-44.txt
VULN	2025-03-21_14-16-02.txt
VULN	2025-03-21_14-14-50.txt
VULN	2025-03-25_14-46-47.txt
VULN	2025-03-22_00-24-59.txt

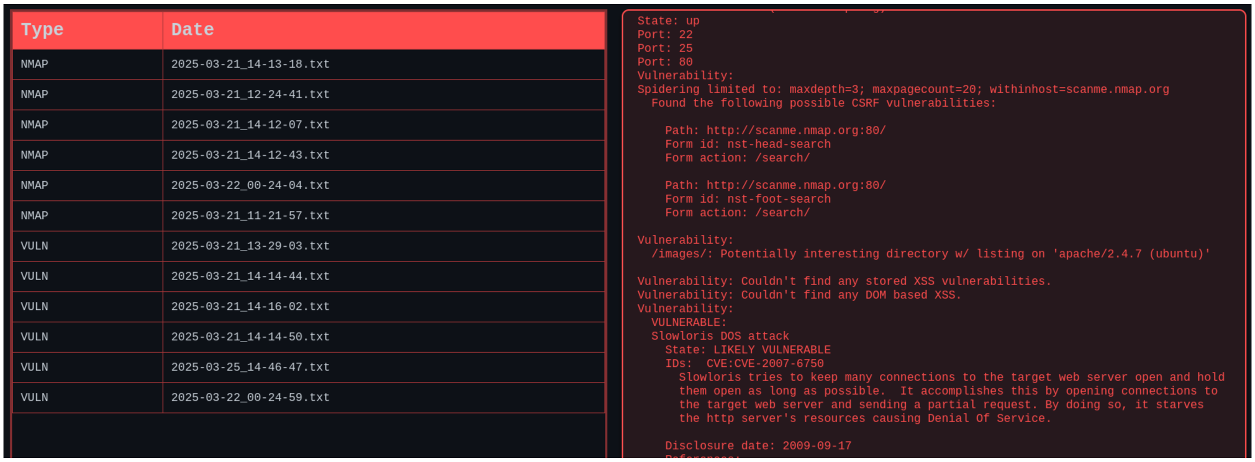
```
Results will appear here
```

Navigate to the Scan Logs tab



VULN	2025-03-25_14-46-47.txt

Click on a previous scan. They are titled by the date and time they are completed.



Type	Date
NMAP	2025-03-21_14-13-18.txt
NMAP	2025-03-21_12-24-41.txt
NMAP	2025-03-21_14-12-07.txt
NMAP	2025-03-21_14-12-43.txt
NMAP	2025-03-22_00-24-04.txt
NMAP	2025-03-21_11-21-57.txt
VULN	2025-03-21_13-29-03.txt
VULN	2025-03-21_14-14-44.txt
VULN	2025-03-21_14-16-02.txt
VULN	2025-03-21_14-14-50.txt
VULN	2025-03-25_14-46-47.txt
VULN	2025-03-22_00-24-59.txt

```
State: up
Port: 22
Port: 25
Port: 80
Vulnerability:
Spidering limited to: maxdepth=3; maxpagecount=20; withinhost=scanme.nmap.org
  Found the following possible CSRF vulnerabilities:

    Path: http://scanme.nmap.org:80/
    Form id: nst-head-search
    Form action: /search/

    Path: http://scanme.nmap.org:80/
    Form id: nst-foot-search
    Form action: /search/

Vulnerability:
  /images/: Potentially interesting directory w/ listing on 'apache/2.4.7 (ubuntu)'

Vulnerability: Couldn't find any stored XSS vulnerabilities.
Vulnerability: Couldn't find any DOM based XSS.
Vulnerability:
  VULNERABLE:
  Slowloris DOS attack
    State: LIKELY VULNERABLE
    IDs:  CVE:CVE-2007-6750
      Slowloris tries to keep many connections to the target web server open and hold
      them open as long as possible.  It accomplishes this by opening connections to
      the target web server and sending a partial request. By doing so, it starves
      the http server's resources causing Denial Of Service.

    Disclosure date: 2009-09-17
    References:
```

You will notice that the window on the right side of the screen populated to the same output as the scan output.