Walkthrough - Template

Contents

[Host Discovery 2](#_Toc147659950)

[Nmap 2](#_Toc147659951)

[Nikto 2](#_Toc147659952)

[Dirb 2](#_Toc147659953)

[Viewing Website 2](#_Toc147659954)

[Exploitation 2](#_Toc147659955)

[Escalation 3](#_Toc147659956)

[Sudo -l 3](#_Toc147659957)

[Flag 4](#_Toc147659958)

# Host Discovery



Kali: 192.168.56.101

# Nmap

A black background with white text

Description automatically generated



A screen shot of a computer

Description automatically generated

# Nikto





# Dirb

Came up with nothing of interest.

# Viewing Website









I found a possible user.

# Exploitation

Using the strings command I found “sunita” as a username. This is good, I now just need to crack the password or find it. I looked more into a binary reverse engineering tool and found nothing. I ended up downloading the key logger and ran it. It generated a file and started logging my strokes.

I released the name of the file is base64.

A close up of a computer screen

Description automatically generatedI decoded it and it revealed a password.

A screenshot of a computer

Description automatically generatedThe name looks familiar. A quick google search shows something interesting.

A screen shot of numbers

Description automatically generatedI copied the name Daenerys and tried to ssh, which worked.

# Escalation

A black background with white text

Description automatically generatedIn the home directory I found a file called secret.

# A screen shot of a computer Description automatically generatedSudo -l

All files don’t exist.

A screen shot of a computer screen

Description automatically generated







I went to google and searched for something related to game of thrones. I found a video which said that line. The title had “Khal Drogo”.

This is the credentials – root:khaldrogo

# Flag



A screen shot of a computer

Description automatically generated