Walkthrough – Vikings 1

Contents

[Host Discovery 2](#_Toc147659605)

[Nmap 2](#_Toc147659606)

[Nikto 3](#_Toc147659607)

[Viewing Website 3](#_Toc147659608)

[Dirb 3](#_Toc147659609)

[Gobuster 3](#_Toc147659610)

[War File 3](#_Toc147659611)

[Cracking Password 4](#_Toc147659612)

[Zip2Hash 4](#_Toc147659613)

[John 4](#_Toc147659614)

[Exiftool 4](#_Toc147659615)

[Binwalk 4](#_Toc147659616)

[Exploitation 4](#_Toc147659617)

[5](#_Toc147659618)

[Escalation 5](#_Toc147659619)

[Upgrading Shell 5](#_Toc147659620)

[Flag 1 5](#_Toc147659621)

[Flag 2 6](#_Toc147659622)

[Finding Binaries 6](#_Toc147659623)

# Host Discovery

A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101.

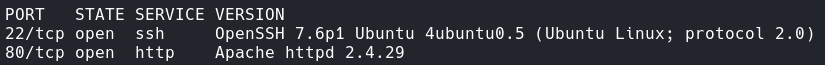
**Victim**: 192.168.56.144.

# Nmap



A black sign with white text

Description automatically generated

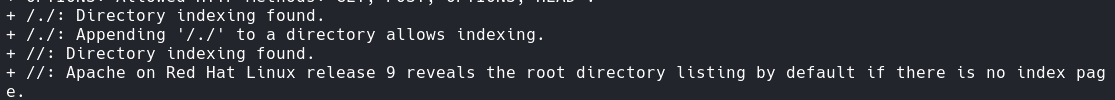


I wanted to get more information, so I ran this command.

A screen shot of a computer screen

Description automatically generated

# Nikto

A screen shot of a computer

Description automatically generated

# Viewing Website

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

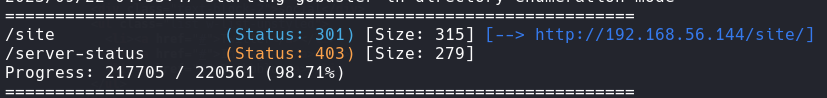
# Dirb



A screen shot of a computer

Description automatically generated

# Gobuster



Results revealed another directory called site.

## War File

Looking inside the file you see the text: /war-is-over. This is most likely a directory.

This ended up being the correct. The entire website of this directory is encrypted.

# Cracking Password

Now that this site contains base 64 text, when you save it to a file and decode it, a file appears that has a password. We can crack it.

## Zip2Hash



## John



ragnarok123 is the password.

# Exiftool



Nothing really of use.

# A screen shot of a computer Description automatically generatedBinwalk

A screen shot of a computer

Description automatically generatedThe extracted data is now on my desktop.

The name floki@vikings could be used for ssh.

floki@vikings and password: f@m0usboatbuilde7

# Exploitation



A number on a black background

Description automatically generated

A screenshot of a computer

Description automatically generatedA screen shot of a computer

Description automatically generatedCreate a python script that prints all of the primes.

Password: mR)|>^/Gky[gz=\.F#j5P(

This should belong to the other account. Just quickly checking /etc/passwd file to see log in details.



# A screenshot of a computer Description automatically generated

# Escalation

## Upgrading Shell



## A screenshot of a computer Description automatically generatedFlag 1

In the home directory is the first flag.

## Flag 2

### Finding Binaries

A screen shot of a computer

Description automatically generated

Nothing really here I can exploit.

A screenshot of a computer program

Description automatically generatedNext I will check the ‘.profile’ file on the desktop of Ragnar.

This shows that there is a python file called rpyc\_classic.py running. I read that this is vulnerable.

A screen shot of a computer

Description automatically generatedFirst, move your kali public key onto the victim machine and change the name to “authorized\_keys”.

Make sure this is done in the /home/Ragnar/ directory.

A black background with white text

Description automatically generatedNow run this script, in the tmp/ directory.





I put my passphrase as ‘kali’.



Now I have root, I can switch to the root directory and list the contents. The final flag is called root.txt.

A computer code with white text

Description automatically generated