Walkthrough - Template

Contents

[Host Discovery 2](#_Toc149316166)

[Nmap 2](#_Toc149316167)

[Nikto 2](#_Toc149316168)

[Dirb 2](#_Toc149316169)

[Viewing Website 2](#_Toc149316170)

[Exploitation 2](#_Toc149316171)

[Escalation 2](#_Toc149316172)

# Host Discovery



# Nmap



# Nikto

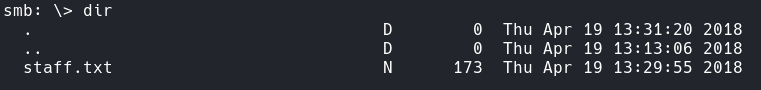


# SMBClient

A black background with white text

Description automatically generated

Connect to smb server.





A black background with white text

Description automatically generated

# Viewing Website

The /development/ directory shows 2 text files for download.

A screenshot of a computer

Description automatically generated

A screenshot of a computer error

Description automatically generated

# A screen shot of a computer Description automatically generatedSearchsploit

Since one of the files talked about apache struts then it could be the top exploit.

This doesn’t work.

# Enum4Linux

I identified some users.



A black background with white text

Description automatically generated

# Hydra

Since I know that “Jan” has an easy password, I will use this time to crack it.



# Escalation

Now that I am in, I can begin finding exploit points. In Kays home directory that is a hidden .ssh directory containing all of the keys. I can actually read the contents. I copied it over to my Kali machine and started john to begin cracking.

# SSH2John



# John

# SSH – Kay



In the home directory of Kay there is also a “pass.bak” file.

heresareallystrongpasswordthatfollowsthepasswordpolicy$$

Now with the password I can see what I can do.

# Sudo Privileges

A screen shot of a computer

Description automatically generated

I can run all commands in sudo.

# Root Exploit

A close up of a black background

Description automatically generated

# A screenshot of a computer Description automatically generatedFlag