Walkthrough – BullDog 1

Contents

[Host Discovery 2](#_Toc146182150)

[Nmap 2](#_Toc146182151)

[Nikto 2](#_Toc146182152)

[Viewing Website 3](#_Toc146182153)

[Viewing Source Code 3](#_Toc146182154)

[Dirb 3](#_Toc146182155)

[Hashes.com 4](#_Toc146182156)

[Website Dashboard 4](#_Toc146182157)

[Exploitation 4](#_Toc146182158)

[MSFVenom 5](#_Toc146182159)

[Python Web-Server 5](#_Toc146182160)

[Upgrade Shell 5](#_Toc146182161)

[Finding Binaries 5](#_Toc146182162)

[Flag 6](#_Toc146182163)

# Host Discovery



A black and white screen with white text

Description automatically generated

**Kali**: 192.168.56.101/24.

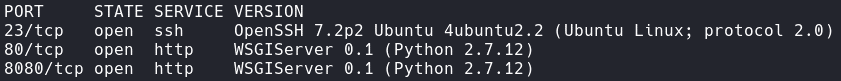
**Victim**: 192.168.56.140/24.

# Nmap



A black background with white text

Description automatically generated



# Nikto





# A screenshot of a computer Description automatically generatedViewing Website

## A computer screen with green and red text Description automatically generatedViewing Source Code

In <http://192.168.56.140/dev/> I was able to find these hashes.

**alan@bulldogindustries.com:**6515229daf8dbdc8b89fed2e60f107433da5f2cb

**william@bulldogindustries.com:**38882f3b81f8f2bc47d9f3119155b05f954892fb

**malik@bulldogindustries.com:**c6f7e34d5d08ba4a40dd5627508ccb55b425e279

**kevin@bulldogindustries.com:**0e6ae9fe8af1cd4192865ac97ebf6bda414218a9

**ashley@bulldogindustries.com**:553d917a396414ab99785694afd51df3a8a8a3e0

**nick@bulldogindustries.com:**ddf45997a7e18a25ad5f5cf222da64814dd060d5

**sarah@bulldogindustries.com:**d8b8dd5e7f000b8dea26ef8428caf38c04466b3e

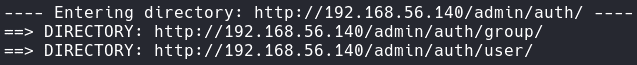
# Dirb



A screen shot of a computer

Description automatically generated





A screenshot of a computer

Description automatically generatedAdmin login page found.

# Hashes.com

I will use this site to crack the hashes.

**Sarah: d8b8dd5e7f000b8dea26ef8428caf38c04466b3e:** bulldoglover

* **sarah@bulldogindustries.com**

**Nick: ddf45997a7e18a25ad5f5cf222da64814dd060d5:** bulldog

* [**nick@bulldogindustries.com**](mailto:nick@bulldogindustries.com)

I was only able to retrieve these two.

# Website Dashboard

I tried to credentials sarah:bulldoglover and I was able to login. I also tried nick:bulldog and found that account also has no permissions on the dashboard. I got stuck here for quite some timing and though about brute forcing the ssh, however I realised that there is a web shell page. I can set up netcat here.

# Exploitation

A close-up of a message

Description automatically generatedThe webshell that the site gives is exploitable. Despite only having limited number of commands you can see navigate the system.

But this is not the point, I believe that I can make a payload and upload to the server.

## MSFVenomA screen shot of a computer Description automatically generated

## A screen shot of a computer Description automatically generatedPython Web-Server

Using echo $(<command>) I will upload the payload using wget and give it execution privileges. After I will run it using echo $(./shell.elf).

A black background with white text

Description automatically generated

## Upgrade ShellA screen shot of a computer Description automatically generated

Going into the hidden directory at /home/bulldogadmin/.hiddenadmindirectory/ there is an app called customPermissionApp. This binary has a hard coded password in it called “SUPERultimatePASSWORDyouCANTget”.

🡪 SUPERultH�E�H�imatePASH�E�H�SWORDyouH�E�H�CANTget

## Finding Binaries

A screen shot of a computer program

Description automatically generated

Sudo is exploitable here. Therefore, we can use that password above to exploit the system. Since all we have to do is enter our password.

# A screen shot of a computer screen Description automatically generatedFlag

I found the flag.