

# Capture The Flag

## Part 2 – Defending

By:

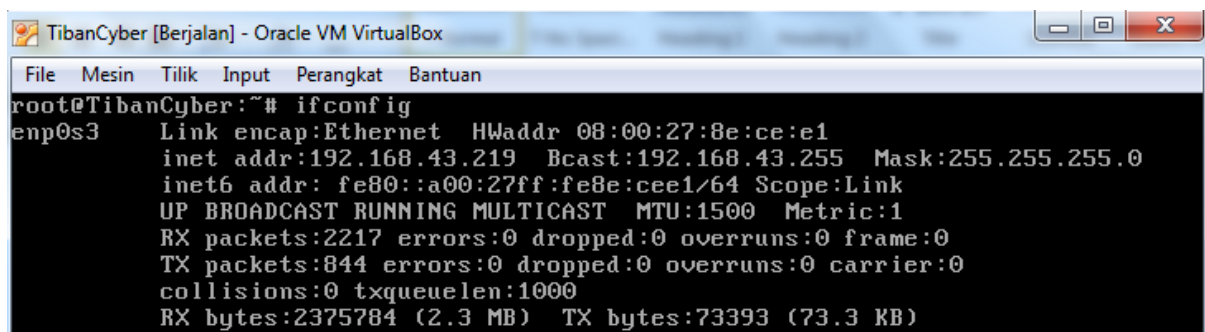
**Tiban**Cyber

Yogi Kortisa

## Defending Our Server

INTRO: Setelah kami terhubung dengan jaringan Lab 607 dengan mode **Bridge** dalam 2 hari waktu CTF, kami menemukan fakta bahwa tidak ada server lawan (tim lain) yang juga terhubung pada jaringan Lab, sehingga kami memutuskan untuk fokus saja pada peretasan server sendiri.

Berikut adalah Alamat IP dari server kami yang telah di Bridge dengan koneksi wireless yang terhubung.



```
root@TibanCyber:~# ifconfig
enp0s3      Link encap:Ethernet  HWaddr 08:00:27:8e:ce:e1
            inet addr:192.168.43.219  Bcast:192.168.43.255  Mask:255.255.255.0
            inet6 addr: fe80::a00:27ff:fe8e:cee1/64  Scope:Link
            UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
            RX packets:2217 errors:0 dropped:0 overruns:0 frame:0
            TX packets:844 errors:0 dropped:0 overruns:0 carrier:0
            collisions:0 txqueuelen:1000
            RX bytes:2375784 (2.3 MB)  TX bytes:73393 (73.3 KB)
```

Berikut adalah Alamat IP dari Kali Linux yang kami gunakan sebagai mesin penyerang dan juga telah di Bridge dengan koneksi wireless yang terhubung.



```
root@TibanCyberAttacker:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.43.100  netmask 255.255.255.0  broadcast 192.168.43.255
        inet6 fe80::a00:27ff:febc:101d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:bc:10:1d  txqueuelen 1000  (Ethernet)
        RX packets 230  bytes 16888 (16.4 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 37  bytes 3339 (3.2 KiB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0
```

## 1. Mematikan Services yang Tidak Diperlukan untuk Menutup Port Terbuka

Pada saat instalasi server kami memilih untuk menginstallkan paket umum yang biasa dibutuhkan, yaitu openssh, web server apache2 dan database MySQL. Namun ternyata ini dapat memicu serangan terhadap services ini dikarenakan services aplikasi tersebut selalu running dan membuka port walaupun tidak digunakan. Hasil dari nmap:

```
root@TibanCyber:~# nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-06-11 16:03 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000024s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 997 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 1.81 seconds
root@TibanCyber:~# _
```

Lebih baik kami mematikan services yang tidak diperlukan, yaitu web server dan database mysql, bahkan ssh. Dikarenakan server kami belum menjalankan aplikasi web apapun dan belum membutuhkan akses remote dengan ssh. Langkah-langkah mematakannya:

```
root@TibanCyber:~# service apache2 stop
root@TibanCyber:~# service mysql stop
root@TibanCyber:~# service ssh stop
root@TibanCyber:~# nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-06-11 16:12 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000040s latency).
Other addresses for localhost (not scanned): 127.0.0.1
All 1000 scanned ports on localhost (127.0.0.1) are closed

Nmap done: 1 IP address (1 host up) scanned in 1.76 seconds
root@TibanCyber:~# _
```

## 2. DoS LAND Attack

Blok semua paket yang datang dari alamat IP server itu sendiri. Lalu blok semua paket yang datang dari jaringan lokal. Gunakan IPTABLES dengan perintah berikut:

```
root@TibanCyber:~# iptables -A INPUT -s 192.168.43.219/24 -j DROP
root@TibanCyber:~# iptables -A INPUT -s 127.0.0.0/8 -j DROP_
```

## 3. TCP XMAS Attack

Blok paket XMAS ini dengan rule IPTABLES berikut:

```
root@TibanCyber:~# iptables -A INPUT -p tcp --tcp-flags ALL FIN,PSH,URG -j DROP
```

## 4. Smurf Attack

Ada dua cara melakukan defending dari serangan ini, yaitu membatasi jumlah paket ICMP yang diperbolehkan:

```
root@TibanCyber:~# iptables -A INPUT -p icmp -m limit --limit 2/second --limit-burst 2 -j ACCEPT
```

atau mem-blok seluruh paket ICMP.

```
root@TibanCyber:~# iptables -A INPUT -p icmp -j DROP
```

## 5. SYN Flooding Attack

Kami mengubah batas dari koneksi TCP dengan rule IPTABLES berikut:

```
root@TibanCyber:~# iptables -A INPUT -p tcp -m state --state NEW -m limit --limit 2/second --limit-burst 2 -j ACCEPT
root@TibanCyber:~# iptables -A INPUT -p tcp -m state --state NEW -j DROP
```

## 6. Overlayfs Local Root Exploit – Update Software and Distro!

```
Ubuntu 15.10 TibanCyber tty1

TibanCyber login: tibancyber
Password:
Last login: Mon Jun 13 12:05:53 WIB 2016 on tty1
Welcome to Ubuntu 15.10 (GNU/Linux 4.2.0-16-generic i686)

 * Documentation:  https://help.ubuntu.com/

116 packages can be updated.
0 updates are security updates.

New release '16.04 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

tibancyber@TibanCyber:~$ sudo su
[sudo] password for tibancyber:
root@TibanCyber:/home/tibancyber# _
```

Untuk mengatasi celah keamanan ini, kami harus meng-upgrade Server kami ke versi Ubuntu Server terbaru yaitu Ubuntu Server 16.04 dengan perintah berikut:

```
root@TibanCyber:~# do-release-upgrade && apt-get update && apt-get upgrade
Checking for a new Ubuntu release
Get:1 Upgrade tool signature [198 B]
Get:2 Upgrade tool [1.265 kB]
4% [2 59,5 kB/1.265 kB 4%]
```

## Attacking After Deffending The Server

1. Setelah dilakukan berbagai macam konfigurasi Firewall menggunakan IPTABLES pada sesi Defending sebelumnya, tampak jelas perbedaan kini Server kami telah aman dari teknik-teknik **Scanning** yang umum dilakukan. Pembuktiaan tampak ketika kami scan kembali menggunakan **Nmap**, muncul pesan bahwa seluruh port telah di filter dan Nmap tidak dapat memunculkan informasi apapun mengenai server kami.

```
root@TibanCyber:~# nmap -A localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-06-10 02:55 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up.
Other addresses for localhost (not scanned): 127.0.0.1
All 1000 scanned ports on localhost (127.0.0.1) are filtered
Too many fingerprints match this host to give specific OS details
Network Distance: 0 hops

OS and Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 215.63 seconds
root@TibanCyber:~# _
```

2. Teknik Serangan : **Firewall/IDS Evasion and Spoofing**

Tool : **Nmap**

Deskripsi : Dengan opsi **-f** Nmap akan melakukan ping scan dengan membagi header TCP menjadi beberapa paket kecil untuk membuat lebih sulit di filter oleh firewall, Intrusion Detection System (IDS), dan gangguan lain untuk mendeteksi apa yang kami lakukan. Sehingga akan kesulitan menangani paket kecil ini hingga dapat menyebabkan IDS/Firewall *segmentation fault* hingga *crash*.

```
root@TibanCyberAttacker:~# nmap -f 192.168.43.219

Starting Nmap 7.12 ( https://nmap.org ) at 2016-06-10 03:06 WIB
Nmap scan report for TibanCyber (192.168.43.219)
Host is up (0.00090s latency).
All 1000 scanned ports on TibanCyber (192.168.43.219) are filtered
MAC Address: 08:00:27:8E:CE:E1 (Oracle VirtualBox virtual NIC)

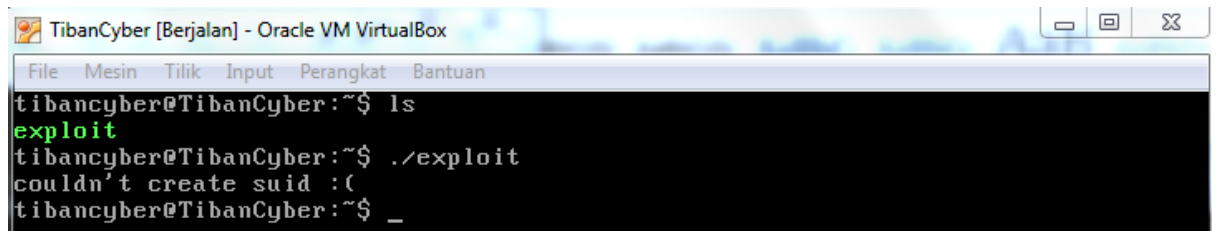
Nmap done: 1 IP address (1 host up) scanned in 21.86 seconds
root@TibanCyberAttacker:~#
```

Nmap akan mengirimkan paket dengan menentukan fragment probes dalam paket sebesar 8 bytes. Namun ternyata hasilnya sama saja, nmap tidak dapat menampilkan informasi apapun lagi tentang server. Ini dikarenakan konfigurasi Firewall yang telah memfilter setiap teknik scanning yang dilakukan oleh Nmap, bahkan walau menggunakan opsi **Firewall/IDS Evasion and Spoofing** sekalipun.

3. Teknik Serangan : **Overlayfs Local Root Exploit**

Tool : **Exploit 39166.c**

Deskripsi : Setelah melakukan upgrade kernel ke versi terbaru, mari kami coba lagi apakah exploit ini masih bisa berjalan melakukan privilege escalation dan mendapatkan akses root di server:



```
tibancyber@TibanCyber:~$ ls
exploit
tibancyber@TibanCyber:~$ ./exploit
couldn't create suid :(
tibancyber@TibanCyber:~$ _
```

Dan ternyata exploit sudah tidak dapat digunakan lagi, karena kami telah melakukan *patch* dengan mengupgrade server kami ke kernel yang paling terbaru.