

ADA LOVELACE AKADEMİ Siber Güvenlik Final Ödevi

-LOG ANALİZİ-

Makbule Arı

iÇİNDEKİLER

1) Log	3
2) acscess.log.1 Analizi	4
3) acscess.log.2 Analizi	9
4) acscess.log.3 Analizi	18
5) acscess.log Analizi	27

LOG

Log Nedir?

Log; bir sistem, uygulama veya cihaz tarafından üretilen ve çeşitli olayları, işlemleri veya durumları zaman damgasıyla kaydeden bir veri dosyasıdır.

Logların Önemi

Log kayıtları sisteme giriş-çıkış işlemleri, sistem içerisinde yapılan değişiklikler, sistem içinde başarısız oturum açma işlemleri, sisteme hangi kullanıcıların girdiğine dair tutulan bu kayıtlar herhangi bir siber saldırı veya güvenlik sorunlarında geriye yönelik analiz yapmamızı kolaylaştıracaktır.

Log Türleri

Bir sistemde Erişim Logları, Hata Logları, Uygulama Logları, Sistem Logları, Güvenlik Logları, Veritabanı Logları, İşlem Logları ve Ağ Logları gibi çeşitli log türleri vardır.

acsess.log.1 Analizi

- Bu log dosyası, bir web sunucusuna ait erişim kayıtlarını detaylı olarak sunmaktadır. Her bir kayıt, istemcinin IP adresini, zaman damgasını, yapılan HTTP isteği (metod ve yol), sunucunun yanıt durumu kodunu, yanıt boyutunu, yönlendiren URL'yi ve kullanıcı aracını içermektedir.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.1 | wc -l
307
```

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.1 | grep "ERROR"
```

- cat acesess.log.1 | wc -l komutu kullanılarak, dosyanın toplamda 307 satır içeriği tespit edilmiştir.
- Log dosyasındaki hata mesajlarını analiz etmek amacıyla grep "ERROR" komutu kullanılmıştır. Ancak, bu komutun çalıştırılması sonucunda herhangi bir hata mesajı tespit edilmemiştir.
- 119.221.17[.]90 IP adresi 56 kez tekrar ederek en sık karşılaşılan IP adresi olmuştur.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.1 | cut -d " " -f 1 | sort | uniq -c | sort -r | head -n 5
 56 119.221.17.90
 39 234.161.112.162
 28 48.124.217.56
 24 21.94.54.79
 21 69.90.24.5
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 1,7,9,10 | grep -i "login"
234.161.112.162 /login 200 978
234.161.112.162 /login?uid=test&pw=test 200 996
234.161.112.162 /login 200 1056
234.161.112.162 /login?uid=test&pw=test 200 1295
69.90.24.5 /wp-login 200 869
21.94.54.79 /acct_login 200 870
21.94.54.79 /customer_login 200 873
94.195.181.106 /smblogin 200 868
177.98.110.246 /snippets.gtl?uid=auto-login%2f 200 1000
```

- Tekrarlayan giriş denemeleri ve çeşitli login sayfalarına yapılan erişimlerin sıklığı, bu IP adreslerinin şüpheli aktivitelerde bulunduğu gösterebilir. Bu aktiviteler, sisteminizde brute-force saldırısı veya diğer kötü niyetli girişimlerin olabileceğine dair bir işaret olabilir.
- Analiz, web sunucusunun çoğu isteği başarıyla işlediğini ve genel performansının iyi olduğunu gösteriyor.
- 413 Payload Too Large kodu, bazı veri boyutlarının sunucunun sınırlarını aştığını ve veri yükleme limitlerinin gözden geçirilmesi gerektiğini işaret ediyor.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 9 | sort | uniq -c | sort -nr
303 200
3 302
1 413
1 304
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 1,4,5,6,7,8,9,10,11 | grep "413"
234.161.112.162 [23/Apr/2023:00:08:40 +0000] "POST /upload2 HTTP/1.1" 413 585 "http://victim.com/upload.gtl"
21.94.54.79 [26/Apr/2023:13:14:22 +0000] "GET /25624130a HTTP/1.1" 200 872 "-"
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 1,4,5,6,7,8,9,10,11 | grep "234.161.112.162"
234.161.112.162 [23/Apr/2023:00:07:18 +0000] "GET / HTTP/1.1" 200 1226 "-"
234.161.112.162 [23/Apr/2023:00:07:26 +0000] "GET /login HTTP/1.1" 200 978 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:07:32 +0000] "GET /login?uid=test&pw=test HTTP/1.1" 200 996 "http://victim.com/login"
234.161.112.162 [23/Apr/2023:00:07:39 +0000] "GET /newaccount.gtl HTTP/1.1" 200 1157 "http://victim.com/login?uid=test&pw=test"
234.161.112.162 [23/Apr/2023:00:07:44 +0000] "GET /saveprofile?action=new&uid=test&pw=test&is_author=True HTTP/1.1" 200 857 "http://victim.com/newaccount.gtl"
234.161.112.162 [23/Apr/2023:00:07:46 +0000] "GET /login HTTP/1.1" 200 1056 "http://victim.com/saveprofile?action=new&uid=test&pw=test&is_author=True"
234.161.112.162 [23/Apr/2023:00:07:51 +0000] "GET /login?uid=test&pw=test HTTP/1.1" 200 1295 "http://victim.com/login"
234.161.112.162 [23/Apr/2023:00:07:52 +0000] "GET /snippets.gtl?uid=cheddar HTTP/1.1" 200 1298 "http://victim.com/login?uid=test&pw=test"
234.161.112.162 [23/Apr/2023:00:08:07 +0000] "GET /newsnippet.gtl HTTP/1.1" 200 1134 "http://victim.com/snippets.gtl?uid=cheddar"
234.161.112.162 [23/Apr/2023:00:08:14 +0000] "GET /newsnippet2?snippet=test+123 HTTP/1.1" 302 182 "http://victim.com/newsnippet.gtl"
234.161.112.162 [23/Apr/2023:00:08:14 +0000] "GET /snippets.gtl HTTP/1.1" 200 1227 "http://victim.com/newsnippet.gtl"
234.161.112.162 [23/Apr/2023:00:08:26 +0000] "GET /newsnippet.gtl HTTP/1.1" 200 1134 "http://victim.com/snippets.gtl"
234.161.112.162 [23/Apr/2023:00:08:33 +0000] "GET /newsnippet2?snippet=test+23423423 HTTP/1.1" 302 182 "http://victim.com/newsnippet.gtl"
234.161.112.162 [23/Apr/2023:00:08:33 +0000] "GET /snippets.gtl HTTP/1.1" 200 1248 "http://victim.com/newsnippet.gtl"
234.161.112.162 [23/Apr/2023:00:08:35 +0000] "GET /upload.gtl HTTP/1.1" 200 1082 "http://victim.com/snippets.gtl"
234.161.112.162 [23/Apr/2023:00:08:40 +0000] "POST /upload2 HTTP/1.1" 413 585 "http://victim.com/upload.gtl"
234.161.112.162 [23/Apr/2023:00:08:40 +0000] "GET /favicon.ico HTTP/1.1" 304 0 "http://victim.com/upload2"
234.161.112.162 [23/Apr/2023:00:08:47 +0000] "GET / HTTP/1.1" 200 1326 "http://victim.com/upload.gtl"
234.161.112.162 [23/Apr/2023:00:08:48 +0000] "GET /snippets.gtl HTTP/1.1" 200 1248 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:08:50 +0000] "GET /newsnippet.gtl HTTP/1.1" 200 1134 "http://victim.com/snippets.gtl"
234.161.112.162 [23/Apr/2023:00:08:55 +0000] "GET /editprofile.gtl HTTP/1.1" 200 1362 "http://victim.com/newsnippet.gtl"
234.161.112.162 [23/Apr/2023:00:08:59 +0000] "GET / HTTP/1.1" 200 1326 "http://victim.com/editprofile.gtl"
234.161.112.162 [23/Apr/2023:00:09:02 +0000] "GET /snippets.gtl?uid=test HTTP/1.1" 200 1208 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:09:09 +0000] "GET /snippets.gtl?uid=brie HTTP/1.1" 200 1252 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:09:16 +0000] "GET / HTTP/1.1" 200 1324 "http://victim.com/snippets.gtl?uid=brie"
234.161.112.162 [23/Apr/2023:00:10:01 +0000] "GET / HTTP/1.1" 200 1255 "-"
234.161.112.162 [23/Apr/2023:00:10:01 +0000] "GET /lib.js HTTP/1.1" 200 805 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:10:02 +0000] "GET /cheese.png HTTP/1.1" 200 9993 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:10:02 +0000] "GET /favicon.ico HTTP/1.1" 200 430 "http://victim.com/"
234.161.112.162 [23/Apr/2023:00:10:12 +0000] "GET / HTTP/1.1" 200 1253 "-"
234.161.112.162 [25/Apr/2023:17:21:01 +0000] "GET /test HTTP/1.1" 200 866 "-"
234.161.112.162 [25/Apr/2023:17:21:01 +0000] "GET /ohacker945260%2f HTTP/1.1" 200 875 "-"
234.161.112.162 [25/Apr/2023:17:21:01 +0000] "GET /ebs%2f HTTP/1.1" 200 867 "-"
234.161.112.162 [25/Apr/2023:17:21:01 +0000] "GET /PANG123456789%2f HTTP/1.1" 200 876 "-"
234.161.112.162 [25/Apr/2023:17:21:02 +0000] "GET /autodesk%2f HTTP/1.1" 200 870 "-"
234.161.112.162 [25/Apr/2023:17:21:02 +0000] "GET /csb%2f HTTP/1.1" 200 867 "-"
234.161.112.162 [25/Apr/2023:17:21:02 +0000] "GET /kumon%2f HTTP/1.1" 200 869 "-"
234.161.112.162 [25/Apr/2023:17:21:02 +0000] "GET /supervise%2f HTTP/1.1" 200 871 "-"
234.161.112.162 [25/Apr/2023:17:21:02 +0000] "GET /sec%2f HTTP/1.1" 200 867 "-"
```

234.161.112[.]162 IP adresi 23 Nisan 2023'te çeşitli web sayfalarına normal kullanıcı etkileşimleri gibi görünen isteklerde bulunmuştur. Ancak, 25 Nisan 2023'te aynı IP adresi, şüpheli ve rastgele görünümü URL'lere birçok GET isteği yapmıştır. Bu durum, potansiyel bir güvenlik taraması veya denemesi olabilir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 7 | sort | uniq -c | sort -nr | head -n 10
11 /
10 /snippets.gtl?uid=test
6 /newsnippet.gtl
5 /snippets.gtl
3 /upload.gtl
2 /test
2 /snippets.gtl?uid=%2e%2e%2f
2 /login?uid=test&pw=test
2 /login
2 /favicon.ico
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 1,4,7 | grep "/snippets.gtl?uid=test"
234.161.112.162 [23/Apr/2023:00:09:02 /snippets.gtl?uid=test
21.94.54.79 [26/Apr/2023:13:14:33 /snippets.gtl?uid=test
21.94.54.79 [26/Apr/2023:13:14:36 /snippets.gtl?uid=test
204.218.128.123 [23/Apr/2023:00:15:35 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:15:43 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:15:51 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:16:14 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:16:57 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:16:57 /snippets.gtl?uid=test
123.114.236.235 [23/Apr/2023:00:18:29 /snippets.gtl?uid=test
156.139.188.182 [23/Apr/2023:00:18:48 /snippets.gtl?uid=testing%2f
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.1 | cut -d " " -f 12,13,14,15,16,17 | sort | uniq -c | sort -nr
264 "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
44 "Mozilla/5.0 (Macintosh; Intel Mac OS X
```

- Erişimlerin çeşitli IP adreslerinden yapılması, /snippets.gtl?uid=test URL'sine yönelik potansiyel bir brute-force saldırısını veya kötü niyetli denemeleri işaret ediyor. Yoğun erişim ve farklı IP adresleri, URL'nin hedef alındığını ve potansiyel bir saldırı belirtisi olabileceğini gösterir.
- Log dosyasında en sık görülen kullanıcı aracı, Mozilla/5.0 (Windows NT 10.0; Win64; x64) olmuştur.

“acsess.log.1” Dosyası Üzerinde Şüpheli Aktivitelerin Genel Değerlendirilmesi

Şüpheli Aktiviteler

- 1. Tekrarlayan Giriş Denemeleri:** IP adresi 234.161.112[.]162, `/login` sayfasına farklı parametrelerle birkaç kez erişim sağlamış, bu durum potansiyel bir brute-force saldırısını işaret edebilir.
- 2. Farklı Login Sayfalarına Yoğun Erişim:** IP adresleri 21.94.54[.]79 ve 94.195.181[.]106, çeşitli login sayfalarına yoğun erişim yapmış, bu da farklı hesapları hedef alan bir saldırıyı gösterebilir.
- 3. Kök Dizin ve Spesifik URL'lere Yoğun Erişim:** Kök dizine 11 kez ve `snippets.gtl?uid=test` URL'sine 10 kez erişim yapılmış, bu yoğunluk olası bir keşif veya saldırısı girişimini işaret ediyor.

Öneriler

- 1. IP Tabanlı İzleme ve Engellemeye:** Şüpheli IP'ler izlenip engellenmeli, anormal davranışlar kara listeye alınmalıdır.
- 2. Güvenlik Duvarı ve WAF:** Kök dizin ve belirli URL'lere yönelik kurallar gözden geçirilmeli, WAF ile saldırılar erken tespit edilmelidir.
- 3. Brute-Force Koruması:** CAPTCHA ve geçici kilitleme mekanizmaları eklenmelidir.
- 4. Düzenli Log Analizi:** Loglar düzenli olarak analiz edilmeli ve otomatik uyarı sistemleri kullanılmalıdır.

acsess.log.2 Analizi

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.2 | wc -l
237
```

- `cat acesess.log.1 | wc -l` komutu kullanılarak yapılan incelemede, acesess.log.1 dosyasının toplamda 237 satır içeriği tespit edilmiştir.
- **86.236.188[.]85** IP adresinin **119** kez tekrar ettiği ve en çok karşılaşılan IP adresi olduğu belirlenmiştir.
- **400** kodlu hataların yüksek oranı, ek kontroller veya iyileştirmeler gerektirdiğini gösterir. Diğer durum kodları, sunucunun performansını ve kullanıcı etkileşimlerini yansıtır.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.2 | cut -d " " -f 1 | sort | uniq -c | sort -nr
119 86.236.188.85
76 254.198.150.19
24 182.195.27.49
10 206.52.45.12
9 178.78.113.5
```

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat acesess.log.2 | cut -d " " -f 9 | sort | uniq -c | sort -nr
120 400
59 200
34 499
23 404
2 302
```

En fazla tekrar eden IP adresi olarak belirlenen 86.236.188[.]85 adresinin, çoğunlukla HTTP durum kodu 400 dönen isteklerde yer aldığı gözlemlenmiştir. Bu durum, bu IP adresinden gelen isteklerin büyük kısmının, sunucu tarafından hatalı veya geçersiz olarak değerlendirilmiş olduğunu göstermektedir.

```

(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.2 | cut -d " " -f 1,4,6,7,8,9 | grep "400" | meyerweb.com/eric/tools/dencoder/
254.198.150.19 [26/Apr/2023:19:44:47 "GET /post?postId= HTTP/1.1" 400
254.198.150.19 [26/Apr/2023:19:45:06 "GET /post?postId= HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%09%2fexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2f%09%2fexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2f%2f%5cexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2f%2f%2fbing%2ecom%2f%3fwww%2eomise%2eco HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2eexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2fexample%2ecom HTTP/1.1" 400 //victim.com/
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%2f%5c%2f%67%6f%67%6c%65%2e%63%6f%6d%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%68%74%74%70%3a%2f%2f%67%6f%67%6c%65%2e%63%6f%6d HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:22 "GET /post?postId=%2f%5cexample%2ecom HTTP/1.1" 400 HTTP/1.1 400 42
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%09%2fexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%5cexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%09%2fexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%5cexample%2ecom HTTP/1.1" 400 400 42
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%2fexample%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%2f%2fexample%2ecom%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%2f%2fexample%2ecom%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%5c%3b@example%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2f%2f HTTP/1.1" 400 42
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%5c%3b@example%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%2f%2fexample%2ecom%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2f%2f HTTP/1.1" 400 42
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%5c%3b@example%2ecom HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2f%2f%2fexample%2ecom%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2fexample%2ecom%2f HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2fgoogle%2ecom%2f%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fgoogle%2ecom%2f%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=%2f%2f%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e HTTP/1.1" 400
86.236.188.85 [27/Apr/2023:15:45:23 "GET /post?postId=https%3a%2f%2fgoogle%2ecom%2f%2f%2e%2e HTTP/1.1" 400

```

120 kez tekrar eden en sık görülen 400 HTTP kodu incelenmiştir. İstekler URL kodlaması kullanılarak yapılmıştır. Bu kodlama özel karakterleri güvenli bir şekilde temsil eder, ancak kötü niyetli girişimlerde de kullanılabilir.

```
/post?postId=%2f%2f%2f%2fexample%2ecom%2f  
/post?postId=%2f%2f%2f%2fexample%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2f%2fexample%2ecom%2f%2e%2e%2f  
/post?postId=%2f%2f%2f%2fexample%2ecom%2f%2f%2e%2e  
/post?postId=9  
/post?postId=%2f%2f%2f%2fexample%2ecom%2f%2f  
/post?postId=%2f%2f%2f%2f%5c%3b@example%2ecom  
/post?postId=%2f%2f%2fgoogle%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2fexample%2ecom  
/post?postId=%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2fexample%2ecom%2f  
/post?postId=%2f%2fgoogle%2ecom%2f%2f%2e%2e encoded JavaScript URLs from complete  
/post?postId=%2f%2f%2fgoogle%2ecom%2f%2f%2e%2e URL Decoder/Encoder for offline us  
/post?postId=%2f%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e  
/post?postId=https%3a%2f%2fgoogle%2ecom%2f%2f%2e%2e  
/post?postId=https%3a%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e  
/post?postId=%2fhttps%3a%2f%2f%2fgoogle%2ecom%2f%2f%2e%2e  
/post?postId=%2fhttps%3a%2f%2fwww%2ewhitelisteddomain%2etld@google%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2fwww%2egoole%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2fwww%2ewhitelisteddomain%2etld@www%2egoole%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2fwww%2egoole%2ecom%2f%2f%2e%2e  
/post?postId=%2f%2f%2f%2fwww%2egoole%2ecom%2f%2f%2e%2e  
/post?postId=https%3a%2f%2fwww%2egoole%2ecom%2f%2f%2e%2e
```

```
/post?postId=///example.com//  
/post?postId=///\;@example.com  
/post?postId=///google.com//..  
/post?postId=///example.com  
/post?postId=//www.whitelisteddomain.tld@google.com//..  
/post?postId=///example.com/  
/post?postId=//google.com//..  
/post?postId=///google.com//..  
/post?postId=///www.whitelisteddomain.tld@google.com//..  
/post?postId=///www.whitelisteddomain.tld@google.com//..  
/post?postId=https://google.com//..  
/post?postId=https://www.whitelisteddomain.tld@google.com//..  
/post?postId=/https://google.com//..  
/post?postId=/https://www.whitelisteddomain.tld@google.com//..  
/post?postId=/www.google.com//..  
/post?postId=/www.whitelisteddomain.tld@www.google.com//..  
/post?postId=///www.whitelisteddomain.tld@www.google.com//..  
/post?postId=///www.google.com//..  
/post?postId=///www.google.com//..  
/post?postId=https://www.google.com//..
```

- **cat acsess.log.2 | cut -d " " -f 7** komutu kullanılarak, log dosyasının 7. sütunundaki URL adresleri çıkarılmıştır. Bu URL'ler daha sonra decode edilmiştir.
- Bu işlem, URL'lerin daha net bir biçimde analiz edilmesi ve içeriklerinin doğru bir şekilde değerlendirilmesi amacıyla yapılmıştır. Decode edilmiş URL'ler, güvenlik ve trafik analizleri için önemli bilgiler sunabilir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.2 | cut -d " " -f 1,4,6,7,8,9,10,11 | grep "404"
254.198.150.19 [26/Apr/2023:19:44:47 "GET /post?postId=0 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:09 "GET /post?postId=0 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:11 "GET /post?postId=16 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:12 "GET /post?postId=15 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:12 "GET /post?postId=14 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:12 "GET /post?postId=13 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:12 "GET /post?postId=12 HTTP/1.1" 404 31 "http://victim.com/"
254.198.150.19 [26/Apr/2023:19:45:12 "GET /post?postId=11 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:09 "GET /post?postId=0 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:09 "GET /post?postId=2010 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:09 "GET /post?postId=2011 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2020 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2019 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2018 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2017 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2015 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2016 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2014 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2013 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:11 "GET /post?postId=2012 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:13 "GET /post?postId=2023 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:13 "GET /post?postId=2022 HTTP/1.1" 404 31 "http://victim.com/"
182.195.27.49 [27/Apr/2023:19:46:13 "GET /post?postId=2021 HTTP/1.1" 404 31 "http://victim.com/"
```

grep "404" komutu ile yapılan arama sonucunda, belirli bir kaynak yolu üzerinde sistematik olarak farklı postId değerleriyle yapılan GET istekleri ve her istekte alınan 404 Not Found yanıtları gözlemlenmiştir.

Tekrarlayan 404 Not Found yanıtları, sistemde güvenlik açıklarını belirlemek veya bilgi toplamak amacıyla gerçekleştirilen şüpheli aktiviteleri işaret edebilir. Bu tür davranışların dikkatle izlenmesi ve analiz edilmesi, potansiyel saldırıları tespit etmek ve güvenliği güçlendirmek için önemlidir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.2 | cut -d " " -f 1,4,5,6,7,8,9,10 | grep "200"
178.78.113.5 [18/Apr/2023:19:42:00 +0000] "GET / HTTP/1.1" 200 2270
178.78.113.5 [18/Apr/2023:19:42:04 +0000] "GET /post?postId=9 HTTP/1.1" 200 2965
178.78.113.5 [18/Apr/2023:19:42:05 +0000] "GET /post?postId=6 HTTP/1.1" 200 3013
178.78.113.5 [18/Apr/2023:19:42:06 +0000] "GET /post?postId=7 HTTP/1.1" 200 3189
178.78.113.5 [18/Apr/2023:19:42:07 +0000] "GET /post?postId=8 HTTP/1.1" 200 2675
178.78.113.5 [18/Apr/2023:19:42:08 +0000] "GET /post?postId=3 HTTP/1.1" 200 2940
178.78.113.5 [18/Apr/2023:19:44:09 +0000] "GET /post?postId=2 HTTP/1.1" 200 3203
178.78.113.5 [18/Apr/2023:19:48:10 +0000] "GET /post?postId=5 HTTP/1.1" 200 2662
178.78.113.5 [18/Apr/2023:39:42:12 +0000] "GET /post?postId=4 HTTP/1.1" 200 3179
206.52.45.12 [18/Apr/2023:19:42:13 +0000] "GET /post?postId=1 HTTP/1.1" 200 3093
206.52.45.12 [18/Apr/2023:49:42:17 +0000] "GET /post?postId=10 HTTP/1.1" 200 2542
206.52.45.12 [18/Apr/2023:19:42:42 +0000] "GET /post/comment/confirmation?postId=9 HTTP/1.1" 200 914
206.52.45.12 [18/Apr/2023:19:42:46 +0000] "GET /post?postId=9 HTTP/1.1" 200 2983
206.52.45.12 [18/Apr/2023:19:42:47 +0000] "GET / HTTP/1.1" 200 2270
206.52.45.12 [18/Apr/2023:19:42:52 +0000] "GET /post?postId=6 HTTP/1.1" 200 3013
206.52.45.12 [23/Apr/2023:19:43:12 +0000] "GET /post/comment/confirmation?postId=6 HTTP/1.1" 200 913
206.52.45.12 [23/Apr/2023:19:43:29 +0000] "GET /post?postId=8 HTTP/1.1" 200 2675
254.198.150.19 [26/Apr/2023:03:44:31 +0000] "GET /post?postId=3 HTTP/1.1" 200 2940
254.198.150.19 [26/Apr/2023:03:44:36 +0000] "GET /post?postId=2 HTTP/1.1" 200 3203
254.198.150.19 [26/Apr/2023:03:44:46 +0000] "GET /post?postId=4 HTTP/1.1" 200 3179
254.198.150.19 [26/Apr/2023:03:44:47 +0000] "GET /post?postId=10 HTTP/1.1" 200 2542
254.198.150.19 [26/Apr/2023:03:44:49 +0000] "GET /post?postId=10 HTTP/1.1" 200 2542
254.198.150.19 [26/Apr/2023:03:44:50 +0000] "GET / HTTP/1.1" 200 2270
254.198.150.19 [26/Apr/2023:03:44:52 +0000] "GET /post?postId=1 HTTP/1.1" 200 3093
254.198.150.19 [26/Apr/2023:03:44:52 +0000] "GET / HTTP/1.1" 200 2270
254.198.150.19 [26/Apr/2023:03:44:55 +0000] "GET / HTTP/1.1" 200 2270
254.198.150.19 [26/Apr/2023:03:44:56 +0000] "GET / HTTP/1.1" 200 2270
254.198.150.19 [26/Apr/2023:03:44:58 +0000] "GET /post?postId=10 HTTP/1.1" 200 2542
```

Kısa bir süre içinde farklı postId değerlerine yapılan başarılı isteklerin hızlı bir şekilde gerçekleşmesi, şüpheli bir durum olarak değerlendirilebilir. Bu, otomatik saldırılar, test amaçlı işlemler veya potansiyel güvenlik açıklarını araştırma gibi çeşitli nedenlerden kaynaklanabilir.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat access.log.2 | cut -d " " -f 7 | sort | uniq -c | sort -nr | head -n 10
 19 /
 15 /post?postId=2
 11 /post?postId=10
  9 /post?postId=1
  8 /post?postId=9
  5 /post?postId=8
  5 /post?postId=6
  5 /post?postId=5
  5 /post?postId=4
  5 /post?postId=3
```

Belirli postId değerlerine kısa sürede yapılan yüksek hacimli ve hedefli erişimler, potansiyel bir saldırı veya kötü niyetli etkinliklerin işaretini olabilir.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat access.log.2 | cut -d " " -f 1,4,7,8,9,10 | grep "post?postId=2"
178.78.113.5 [18/Apr/2023:19:44:09 /post?postId=2 HTTP/1.1" 200 3203
254.198.150.19 [26/Apr/2023:03:44:33 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:33 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:33 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:34 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:35 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:35 /post?postId=2 HTTP/1.1" 499 0
254.198.150.19 [26/Apr/2023:03:44:36 /post?postId=2 HTTP/1.1" 200 3203
254.198.150.19 [26/Apr/2023:03:44:49 /post?postId=2 HTTP/1.1" 200 3203
254.198.150.19 [26/Apr/2023:19:45:11 /post?postId=2 HTTP/1.1" 200 3203
```

```
(kali㉿kali)-[~/Desktop/logs]$ cat access.log.2 | cut -d " " -f 4 | sort | uniq -c | sort -nr | head -n 10
33 [27/Apr/2023:15:45:25
31 [27/Apr/2023:15:45:24
29 [27/Apr/2023:15:45:23
10 [27/Apr/2023:15:45:26
 9 [27/Apr/2023:19:46:11
 9 [27/Apr/2023:15:45:22
 6 [27/Apr/2023:15:45:35
 6 [26/Apr/2023:19:45:12
 6 [26/Apr/2023:03:44:52
 5 [26/Apr/2023:03:44:34
```

27/Apr/2023:15:45:25 tarih ve saat diliminde, HTTP durum kodu 400 olan toplam 33 adet istek tespit edilmiştir. Bu isteklerin URL'leri, URL kodlaması (URL encoding) yapılmış olarak kaydedilmiştir. Bu durum, belirtilen zaman diliminde sunucuya yapılan hatalı veya geçersiz isteklerin yüksek bir yoğunlukta gerçekleştiğini göstermektedir.

27/Apr/2023:15:45:25 tarihinin toplam 33 kez tekrar ettiği tespit edilmiştir. Bu tarihi daha detaylı analiz etmek amacıyla ek bir inceleme yapılmıştır.

“acsess.log.2” Dosyası Üzerinde Şüpheli Aktivitelerin Genel Değerlendirilmesi

Başlıca Bulgular

- **IP Adresleri:** En çok istek yapan IP adresleri arasında **86.236.188[.]85**, **254.198.150[.]19** ve **182.195.27[.]49** yer almaktadır. Özellikle **86.236.188[.]85** IP adresinden toplamda 119 istek yapılmıştır.
- **URL'ler:** **postId=2** ve **postId=10** gibi spesifik içeriklere yönelik talepler yüksek sayıda görülmüştür.
- **HTTP Durum Kodları:** En sık karşılaşılan HTTP durum kodu **400 (Bad Request)** olup, toplamda 120 kez görülmüştür. Bunun yanı sıra **200 (Başarılı)** durumu da 57 kez kaydedilmiştir.

Şüpheli Aktiviteler

- **Anormal IP Aktivitesi:** **86.236.188[.]85** ve **254.198.150[.]19** IP adreslerinden çok sayıda istek yapılmış olması, bu IP'lerin yoğun trafiğe neden olduğunu göstermektedir. Bu durum, bir tarama veya saldırı girişimi olabilir.
- **Bad Request (400) Durum Kodu:** **400** hata kodunun yüksek sıklığı, kullanıcıların yanlış veya eksik istekler gönderdiğini veya saldırı amaçlı denemeler yapıldığını gösterebilir.

acsess.log.3 Analizi

```
(kali㉿kali)-[~/Desktop/logs]
$ cat acess.log.3 | wc -l
2776
```

- `cat acess.log.3 | wc -l` komutu ile yapılan analizde, acesse.log.3 dosyasının toplam 2776 satırdan olduğu belirlenmiştir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat acesse.log.3 | cut -d " " -f 1 | sort | uniq -c | sort -nr | head -n 15
74 192.99.244.139
48 31.220.113.224
48 23.254.164.173
42 31.187.79.201
35 173.44.194.237
33 31.220.30.157
30 89.42.237.71
26 162.252.172.138
24 5.157.42.183
24 104.144.19.69
22 216.244.81.34
20 94.23.33.25
19 208.115.125.58
19 195.154.46.135
18 89.36.65.53
```

- IP adreslerinin tekrar sayıları analiz edilmiştir. Bu komut, IP adreslerini sıralayarak en çok tekrar edenleri azalan sırada listelemiştir.
- 192.99.244[.]139 IP adresi, 74 kez tekrar ederek en çok tekrar eden IP adresi olmuştur.

```
(kali㉿kali)-[~/Desktop/logs]
└─$ cat access.log.3 | cut -d " " -f 1,7,9,10 | grep -i "login"
31.220.113.224 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
31.220.113.224 /login_form 200 10543
31.220.113.224 /login_form 200 16806
216.244.81.34 /login_form 200 11620
216.244.81.34 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form 200 11793
158.222.5.157 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
158.222.5.157 /login_form 200 10543
158.222.5.157 /login_form 200 16810
180.180.64.16 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
180.180.64.16 /login_form 200 10543
180.180.64.16 /login_form 200 16810
222.88.236.235 http://niels.basj.es/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basj.es/join_form 200 11713
222.88.236.235 http://niels.basj.es/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basj.es/join_form 200 11713
89.42.237.71 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form 200 11793
89.42.237.71 /login_form 200 11620
89.42.237.71 /login_form 200 18354
200.55.25.2 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
200.55.25.2 /login_form 200 10543
200.55.25.2 /login_form 200 16810
211.196.252.10 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
211.196.252.10 /login_form 200 10543
211.196.252.10 /login_form 200 16810
192.227.222.207 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
192.227.222.207 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
46.102.99.22 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basj.es/join_form 200 11713
46.102.99.22 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basj.es/join_form 200 11713
216.158.199.158 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
158.222.12.158 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
158.222.12.76 /login_form 200 10543
216.158.199.158 /login_form 200 16810
167.160.127.164 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
167.160.127.164 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form 200 10716
167.160.127.164 /login_form 200 10543
167.160.127.164 /login_form 200 16810
```

Login içeren isteklerin HTTP durum kodlarının 200 olduğu ve yanıt boyutlarının yüksek olduğu durumlar tespit edilmiştir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.3 | cut -d " " -f 9 | sort | uniq -c | sort -nr
2277 200
474 302
11 403
8 404
2 123
2
15 Dragon/36.1.1.21
1 "-"
```

Log dosyasındaki HTTP durum kodları genel olarak sunucunun iyi çalıştığını ve çoğu istege başarılı yanıt verdiği göstermektedir. Ancak, bazı standart dışı durum kodları ve boşluklar, loglama sisteminde veya uygulama yapılandırmasında dikkat edilmesi gereken noktalar olabileceğini işaret eder.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.3 | cut -d " " -f 1,4,6,7,8,9,10 | grep "403"
212.129.17.73 [30/Oct/2015:12:29:20 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
183.203.23.135 [30/Oct/2015:12:30:00 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
60.191.163.235 [30/Oct/2015:10:11:21 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.0" 403 340
192.3.242.26 [30/Oct/2015:09:51:37 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
115.231.162.216 [25/Oct/2015:13:18:29 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
91.139.172.39 [29/Oct/2015:14:10:46 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
162.252.172.138 [29/Oct/2015:18:17:22 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
107.158.89.87 [30/Oct/2015:00:11:06 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
208.115.125.58 [30/Oct/2015:00:49:33 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
162.252.172.138 [29/Oct/2015:07:20:10 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
173.232.116.137 [27/Oct/2015:17:59:36 "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form HTTP/1.1" 403 340
```

1. Kısıtlı Erişim: Tüm yanıtlar 403 Forbidden hatası ile sonuçlanmıştır.
2. Güvenlik Sorunu: Farklı IP'lerden gelen başarısız giriş denemeleri, kötüye kullanım veya brute force saldırısını işaret edebilir.
3. Erişim Denemeleri: Farklı tarihlerde düzenli erişim denemeleri yapılmış.
4. Yanıt Boyutları: Yanıt boyutu 340 bayt olarak sabit, aynı hata mesajı kullanılmış.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.3 | cut -d " " -f 7
/linux/doing-pxe-without-dhcp-control
/join_form
/join_form
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form
/login_form
/login_form
/login_form
/login_form
/login_form
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form
/contact_info
/join_form
/join_form
/linux/doing-pxe-without-dhcp-control
/join_form
/join_form
/join_form
/join_form
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form
```

For encoded binaries (like Images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
/process?data=<!DOCTYPE root [ <!ENTITY xxe SYSTEM "file:///etc/shadow"> ]> <root> &xxe;</root>/process?data=<!DOCTYPE test [ <!ENTITY xxe SYSTEM "file:///etc/shadow"> ]> <test> &xxe;</test>/process?data=<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/shadow">]><test>&xxe;</test> HTTP/1.1"
```

7. sütundaki URL bilgileri incelendiğinde, URL encoding işlemi yapılmış bir veri dikkat çekmiştir ve decode edilmiştir.

For encoded binaries (like Images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
/process?data=<!DOCTYPE root [ <!ENTITY xxe SYSTEM "file:///etc/shadow"> ]> <root> &xxe;</root>/process?data=<?xml version="1.0" encoding="UTF-8"?><!DOCTYPE test [<!ENTITY xxe SYSTEM "file:///etc/shadow">]><test>&xxe;</test> HTTP/1.1"
```

```
/linux/installing-my-new-server/networking
/join_form
/join_form
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form
/process?data=%3C!DOCTYPE%20root%20%5B%20%3C!ENTITY%20xxe%20SYSTEM%20%22file%3A%2F%2Fetc%2Fshadow%22%3E%20%5D%3E%20%3Croot%3E%20%26xxe%3B%20%3C%2Froot%3E
/process?data=%3C%3Fxml%20version%3D%221.0%22%20encoding%3D%22UTF-8%22%3F%3E%3C!DOCTYPE%20test%20%5B%3C!ENTITY%20xxe%20SYSTEM%20%22file%3A///etc/shadow%22%3E%20%5D%3E%20%3Ctest%3E%26xxe%3B%3C/test%3E%5D%5D%3E%3C/test%3E%20HTTP/1.1"
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form
```

```
(kali㉿kali)-[~/Desktop/logs] Decodes your data into the area below.
└─$ cat access.log.3 | cut -d " " -f 1,4,6,7,8,9 | grep "shadow"
94.23.33.25 [28/Oct/2015:11:38:15 +0000] "GET /process?data=%3C!DOCTYPE%20root%20%5B%20%3C!ENTITY%20xxe%20SYSTEM%20%22file%3A%2F%2Fetc%2Fshadow%22%3E%20%5D%3E%20%3Croot%3E%20%26xxe%3B%20%3C%2Froot%3E HTTP/1.1" 200
94.23.33.25 [28/Oct/2015:11:38:16 "GET /process?data=%3C%3Fxml%20version%3D%221.0%22%20encoding%3D%22UTF-8%22%3F%3C!DOCTYPE%20test%20%5B%3C!ENTITY%20xxe%20SYSTEM%20%22file%3A///etc/shadow%22%3E%5D%3Ctest%3E%26xxe%3B%3C/test%3E%20HTTP/1.1" 200 123
94.23.33.25 [28/Oct/2015:11:38:17 "GET /process?data=%3C%3Fxml%20version%3D%221.0%22%20encoding%3D%22UTF-8%22%3F%3C!DOCTYPE%20test%3E%3C!%5BCDATA%5B%3C%3Fxml%20version%3D%221.0%22%20encoding%3D%22UTF-8%22%3F%3E%3C!DOCTYPE%20test%20%5B%3C!ENTITY%20xxe%20SYSTEM%20%22file%3A///etc/shadow%22%3E%5D%3E%3Ctest%3E%26xxe%3B%3C/test%3E%5D%5D%3E%3C/test%3E%20HTTP/1.1" 200 123
```

Derinlemesine analiz yapmak amacıyla **grep "shadow"** komutu kullanılarak arama gerçekleştirilmiştir.

Log kayıtlarında görülen istekler, sistemdeki kritik dosyalara erişim sağlamayı hedefleyen XXE (XML External Entity) saldırısı girişimlerini işaret etmektedir. Bu tür saldırılar, sistem güvenliğini tehlikeye atabilir ve hassas bilgilerin sızmasına neden olabilir.

```
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form&last_visit:date=2015%2F10%2F29+02%3A13%3A13.091+GMT%2B1&prev_visit:date=2015%2F10%2F29+02%3A13%3A13.093+GMT%2B1&came_from_prefs=&fullname=Bonnie+Haddon&username=BonnieHadd&email=gil%40b.most-wanted-stuff.com&form.button.Register=Register&formsubmitted=1  
/join_form  
/join_form  
/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form  
/login_form  
/
```

Sütun 7'deki verileri incelerken, `username` ve `email` gibi kişisel bilgileri içeren bir satır dikkat çekerek decode edilmiştir.

URL içerisinde, kullanıcı adı, e-posta adresi gibi kişisel bilgilerin yanı sıra giriş ve kayıt işlemleriyle ilgili veriler bulunmaktadır. Bu verilerin URL'de açıkça görünmesi, kişisel bilgilerin ifşa olmasına ve güvenlik risklerine yol açabilir.

/acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form&last_visit:date=2015%2F10%2F29+02%3A13%3A13.091+GMT%2B1&prev_visit:date=2015%2F10%2F29+02%3A13%3A13.093+GMT%2B1&came_from_prefs=&fullname=Bonnie+Haddon&username=BonnieHadd&email=gil%40b.most-wanted-stuff.com&form.button.Register=Register&formsubmitted=1

For encoded binaries (like images, documents, etc.) use the file upload form a little further down on this page.

UTF-8 Source character set.

Decode each line separately (useful for when you have multiple entries).

Live mode OFF Decodes in real-time as you type or paste (supports only the UTF-8 character set).

< DECODE > Decodes your data into the area below.

```
/acl_users/credentials_cookie_auth/require_login?came_from=http://niels.basjes.nl/join_form&last_visit:date=2015/10/29+02:13:13.091+GMT+1&prev_visit:date=2015/10/29+02:13:13.093+GMT+1&came_from_prefs=&fullname=Bonnie+Haddon&username=BonnieHadd&email=gil@b.most-wanted-stuff.com&form.button.Register=Register&formsubmitted=1
```

```
(kali㉿kali)-[~/Desktop/logs] $ cat access.log.3 | cut -d " " -f 7 | sort | uniq -c | sort -nr | head -n 15
944 /join_form
810 /login_form
354 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form
235 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basjes.nl/join_form
88 /
75 /linux/doing-pxe-without-dhcp-control
67 /linux/installing-fedora-linux-via-pxe-x86-64
39 /places
25 /open-source
23 /linux/installing-my-new-server/networking
22 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//niels.basj.es/join_form
11 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//daniel_en_sander.basjes.nl/join_form
11 /accessibility-info
9 /linux/installing-my-new-server/vmware-server
9 /linux/installing-gitlab-on-centos-6
```

En sık erişilen URL'nin **/join_form** olduğu tespit edilmiştir. Ayrıca bazı URL'lere belirgin bir şekilde daha fazla erişim yapıldığı ve bazı URL'lerin ise daha az sıklıkta ziyaret edildiği anlaşılmıştır.. Özellikle **join_form** ve **login_form** gibi URL'lerin yüksek erişim sayıları, bu sayfalara olan ilginin yoğun olduğunu veya bu URL'lerin potansiyel olarak hedef alınmış olabileceğini düşündürebilir.

Bu durum, muhtemel bir brute-force saldırısı veya kimlik doğrulama bypass girişimini işaret edebilir. Sürekli yapılan bu istekler, otomatik araçlar veya botlar tarafından gerçekleştirilen potansiyel bir saldırıyı gösterir.

```
(kali㉿kali)-[~/Desktop/logs] $ cat access.log.3 | cut -d " " -f 1,7 | grep "/join_form" | sort | uniq -c | sort -nr | head -n 5
22 192.99.244.139 /join_form
16 31.220.113.224 /join_form
16 23.254.164.173 /join_form
14 31.187.79.201 /join_form
13 94.23.33.25 /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form

(kali㉿kali)-[~/Desktop/logs] $ cat access.log.3 | cut -d " " -f 1,7 | grep "/login_form" | sort | uniq -c | sort -nr | head -n 5
22 192.99.244.139 /login_form
16 31.220.113.224 /login_form
16 23.254.164.173 /login_form
14 31.187.79.201 /login_form
10 89.42.237.71 /login_form
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.3 | cut -d " " -f 4 | sort | uniq -c | sort -nr | head -n 10
 4 [25/Oct/2015:05:57:30
  3 [30/Oct/2015:00:41:47
  3 [29/Oct/2015:18:13:47
  3 [29/Oct/2015:02:15:24
  3 [28/Oct/2015:13:44:31
  3 [28/Oct/2015:10:46:32
  3 [27/Oct/2015:23:21:56
  3 [27/Oct/2015:21:54:59
  3 [27/Oct/2015:03:03:22
  3 [25/Oct/2015:13:14:02
```

En sık görülen tarih ve saat
`25/Oct/2015:05:57:30` olarak
tespit edilmiştir.

- **Tekrar Eden İstekler:** IP adresi 167.160.127.164 tarafından aynı anda iki farklı URL'ye tekrar eden istekler yapılmıştır.

- **Başarıyla Yanıtlanması:** Her iki istek de başarılı yanıtlanmış ve yanıt boyutları benzer olmuştur.

- **Otomatik Araç Kullanımı:** Aynı anda birden fazla istek yapılması, otomatik araç veya bot kullanımı ihtimalini gösterir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log.3 | cut -d " " -f 1,4,6,7,8,9,10 | grep "25/Oct/2015:05:57:30"
167.160.127.164 [25/oct/2015:05:57:30] "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form HTTP/1.1" 200 10716
167.160.127.164 [25/oct/2015:05:57:30] "GET /login_form HTTP/1.1" 200 10543
167.160.127.164 [25/oct/2015:05:57:30] "GET /acl_users/credentials_cookie_auth/require_login?came_from=http%3A//howto.basjes.nl/join_form HTTP/1.1" 200 10716
167.160.127.164 [25/oct/2015:05:57:30] "GET /login_form HTTP/1.1" 200 10543
```



Bir mesaj yazın

25

“acsess.log.3” Dosyası Üzerinde Şüpheli Aktivitelerin Genel Değerlendirilmesi

- İstemci IP Adresleri:** Tekrarlanan istekler, kötü niyetli aktiviteleri işaret edebilir. Özellikle /login_form ve /join_form gibi sayfalara yapılan POST istekleri, otomatik araçlar veya botlar tarafından yapılan şifre kırma girişimlerini gösterebilir.
- Yanıt Durum Kodları:**
 - 200 OK:** Başarıyla tamamlanan istekler, normal kullanıcı işlemlerini ve başarılı saldırıları gösterebilir.
 - 302 Found:** Yönlendirmeleri gösterir; POST istekleriyle birlikte sık görülmesi, otomatik saldırıları işaret edebilir.
- Zaman Damgaları:** Yoğun istekler belirli zaman aralıklarında görüluyorsa, sistemin zayıf noktalarının test edildiğini gösterebilir.

Sonuç ve Öneriler:

- Şüpheli IP'leri izleyin ve gerekirse engelleyin.
- Rate limiting uygulayarak, aynı IP'den gelen çok sayıda isteği sınırlayın.
- POST istekleri için ek güvenlik kontrolleri (CAPTCHA) ve süreli engellemeler uygulayın.
- Otomatik log analiz araçları (Splunk, ELK Stack) kullanarak şüpheli aktiviteleri tespit edin.
- Kullanıcılara güçlü parolalar kullanmaları ve şüpheli aktiviteler konusunda dikkatli olmaları için eğitim verin.

acsess.log Analizi

- Bu log dosyası, bir web sunucusunun erişim kayıtlarını içermektedir. Her bir kayıt istemcinin IP adresi, zaman damgası, yapılan istek (HTTP metod ve yol), sunucunun verdiği yanıt durumu kodu, yanıt boyutu, yönlendiren URL ve kullanıcı aracı bilgilerini kapsamaktadır.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | wc -l
405
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | grep "ERROR"
```

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | cut -d " " -f 1 | sort | uniq -c | sort -nr
186 146.241.73.240
69 193.230.127.66
45 68.160.80.187
42 36.40.116.182
39 61.14.246.6
25 66.48.84.188
```

- Dosyanın 405 satır içerdiği tespit edilmiştir.
- Yapılan aramada 'ERROR' kelimesini içeren herhangi bir satır tespit edilmemiştir.
- Sonuç olarak, analiz edilen verilere göre 146.241.73[.]240 IP adresi, toplamda 186 kez erişim sağlanarak en sık karşılaşılan IP adresi olmuştur.

Log kayıtlarında, diğer satırlardan farklı olarak ilk satırda yanıt boyutunun 919 byte ve son satırda yanıt boyutunun 0 byte olduğu tespit edilmiştir. Ayrıca, çoğu yanıtın 200 HTTP kodu ile döndüğü, ancak en son yanıtın 302 HTTP kodu ile döndüğü belirlenmiştir. Yanıt boyutlarındaki ve HTTP kodlarındaki bu anormallikler, potansiyel sorunlar veya saldırı göstergeleri olarak değerlendirilmektedir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | cut -d " " -f 1,4,7,9,10
66.48.84.188 [26/Apr/2023:21:33:38 / 200 2134
66.48.84.188 [26/Apr/2023:21:33:38 /resources/static/js/header.js 200 368
66.48.84.188 [26/Apr/2023:21:33:38 /resources/static/css/footer.css 200 1240
66.48.84.188 [26/Apr/2023:21:33:38 /resources/css/XsBlog.css 200 4488
66.48.84.188 [26/Apr/2023:21:33:38 /resources/images/blog.svg 200 2666
66.48.84.188 [26/Apr/2023:21:33:38 /image/blog/posts/4.jpg 200 41222
66.48.84.188 [26/Apr/2023:21:33:38 /image/blog/posts/39.jpg 200 110838
66.48.84.188 [26/Apr/2023:21:33:39 /footer 404 31
66.48.84.188 [26/Apr/2023:21:33:39 /resources/static/images/logoa.svg 200 3097
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/17.jpg 200 33543
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/63.jpg 200 141236
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/42.jpg 200 203200
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/46.jpg 200 253600
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/66.jpg 200 256494
66.48.84.188 [26/Apr/2023:21:33:39 /resources/static/images/ps-X-a.svg 200 379
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/26.jpg 200 29354
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/45.jpg 200 135001
66.48.84.188 [26/Apr/2023:21:33:39 /image/blog/posts/53.jpg 200 192118
66.48.84.188 [26/Apr/2023:21:33:40 /favicon.ico 200 1654
66.48.84.188 [26/Apr/2023:21:33:44 /post?postId=5 200 2623
66.48.84.188 [26/Apr/2023:21:33:44 /resources/images/avatarDefault.svg 200 3372
66.48.84.188 [26/Apr/2023:21:33:44 /footer 404 31
66.48.84.188 [26/Apr/2023:21:33:48 /post?postId=4 200 2785
66.48.84.188 [26/Apr/2023:21:33:48 /footer 404 31
66.48.84.188 [26/Apr/2023:21:33:51 /post?postId=9 200 2855
61.14.246.6 [26/Apr/2023:21:33:51 /footer 404 31
61.14.246.6 [26/Apr/2023:21:33:54 /post?postId=7 200 3061
61.14.246.6 [26/Apr/2023:21:33:54 /footer 404 31
61.14.246.6 [24/Apr/2023:23:31:17 /post/comment 302 0
61.14.246.6 [24/Apr/2023:23:31:17 /post/comment/confirmation?postId=7 200 880
61.14.246.6 [24/Apr/2023:23:31:17 /footer 404 31
61.14.246.6 [24/Apr/2023:23:31:19 /post?postId=7 200 3096
61.14.246.6 [24/Apr/2023:23:31:19 /footer 404 31
61.14.246.6 [24/Apr/2023:23:31:44 / 200 2134
```

```
61.14.246.6 [24/Apr/2023:23:31:44 /resources/static/css/footer.css 200 1240
61.14.246.6 [24/Apr/2023:23:31:44 /resources/css/XsBlog.css 200 4488
61.14.246.6 [24/Apr/2023:23:31:44 /resources/static/js/header.js 200 368
61.14.246.6 [24/Apr/2023:23:31:44 /resources/images/blog.svg 200 2666
61.14.246.6 [24/Apr/2023:23:31:44 /image/blog/posts/4.jpg 200 41222
61.14.246.6 [24/Apr/2023:23:31:44 /image/blog/posts/39.jpg 200 110838
61.14.246.6 [24/Apr/2023:23:31:44 /footer 404 31
61.14.246.6 [24/Apr/2023:23:31:44 /image/blog/posts/17.jpg 200 33543
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/66.jpg 200 256494
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/26.jpg 200 29354
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/63.jpg 200 141236
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/46.jpg 200 253600
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/42.jpg 200 203200
61.14.246.6 [24/Apr/2023:23:31:45 /resources/static/images/ps-X-a.svg 200 379
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/45.jpg 200 135001
61.14.246.6 [24/Apr/2023:23:31:45 /resources/static/images/logoa.svg 200 3097
61.14.246.6 [24/Apr/2023:23:31:45 /image/blog/posts/53.jpg 200 192118
```

Log kayıtlarından görüldüğü üzere, aynı saniye içerisinde çok fazla işlem yapılmaktadır. Bu durum, yüksek işlem hacmini veya potansiyel bir sorun olduğunu işaret edebilir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | cut -d " " -f 1,4,5,6,7,8,9,10,11,12,13,14,15,16,17 | grep "404"
66.48.84.188 [26/Apr/2023:21:33:39 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
66.48.84.188 [26/Apr/2023:21:33:44 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
66.48.84.188 [26/Apr/2023:21:33:48 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
61.14.246.6 [26/Apr/2023:21:33:51 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
61.14.246.6 [26/Apr/2023:21:33:54 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
61.14.246.6 [24/Apr/2023:23:31:17 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
61.14.246.6 [24/Apr/2023:23:31:19 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
61.14.246.6 [24/Apr/2023:23:31:44 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
61.14.246.6 [24/Apr/2023:23:31:51 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
61.14.246.6 [24/Apr/2023:23:54:01 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
36.40.116.182 [24/Apr/2023:23:54:52 +0000] "GET /post?postId=11 HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X
36.40.116.182 [24/Apr/2023:23:55:17 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
193.230.127.66 [25/Apr/2023:23:27:51 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
146.241.73.240 [25/Apr/2023:23:29:54 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
146.241.73.240 [26/Apr/2023:21:40:11 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
```

Log dosyasında yapılan 404 hata kodu analizi, eksik veya yanlış yönlendirilmiş bağlantıları belirlemekte yardımcı olmuştur. grep "404" komutu kullanılarak bu hata kodlarını içeren satırlar filtrelenmiştir.

Daha sonra 404 hata kodları oluşturan IP adresleri tespit edilmiştir. Özellikle 61.14.246[.]6 IP adresi yüksek sayıda 404 hatası üretmiştir. Bu durum, sistemdeki zayıf noktaları tespit etmeye yönelik tarama veya keşif faaliyetlerini işaret ediyor olabilir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat access.log | cut -d " " -f 1,9 | grep "404" | sort | uniq -c | sort -nr
    7 61.14.246.6 404
    3 66.48.84.188 404
    2 36.40.116.182 404
    2 146.241.73.240 404
    1 193.230.127.66 404
```

```
193.230.127.66 - - [25/Apr/2023:23:24:30 +0000] "POST /post/comment HTTP/1.1" 302 0 "http://victim.com/post?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:24:31 +0000] "POST /post/comment HTTP/1.1" 302 0 "http://victim.com/post?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:24:31 +0000] "POST /post/comment HTTP/1.1" 302 0 "http://victim.com/post?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:24:50 +0000] "POST /post/comment HTTP/1.1" 302 0 "http://victim.com/post?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:24:51 +0000] "GET /post/comment/confirmation?postId=3 HTTP/1.1" 200 880 "http://victim.com/post?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:27:51 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:27:53 +0000] "GET /my-account HTTP/1.1" 302 0 "http://victim.com/post/comment/confirmation?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
193.230.127.66 - - [25/Apr/2023:23:27:54 +0000] "GET /login HTTP/1.1" 200 919 "http://victim.com/post/comment/confirmation?postId=3" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [25/Apr/2023:23:27:54 +0000] "GET /resources/css/Xs.css HTTP/1.1" 200 4723 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [25/Apr/2023:23:29:54 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:40:10 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:40:11 +0000] "GET /footer HTTP/1.1" 404 31 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:40:14 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:42:36 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:42:37 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:42:37 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:42:37 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
146.241.73.240 - - [26/Apr/2023:21:42:37 +0000] "POST /login HTTP/1.1" 200 947 "http://victim.com/login" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/112.0.5615.50 Safari/537.36"
```

cat acsess.log komutu ile log dosyasını incelerken, bazı aktiviteler dikkat çekmiş ve bu aktivitelerin analizi gerçekleştirilmiştir.

GET /my-account isteği ve hemen ardından yapılan **POST /login** isteği, olası bir saldırganın "my-account" sayfasını hedef aldığı ve başarılı bir şekilde giriş yapmayı başardığını göstermektedir.

HTTP durum kodları analizi, çoğunlukla başarılı yanıtlar (200) ve sık yönlendirmeler (302) olduğunu gösterir. Düşük 404 hata kodları, büyük oranda erişim sorunları yaşanmadığını belirtir, ancak eksik sayfalar yine de izlenmelidir.

```
(kali㉿kali)-[~/Desktop/logs]
$ cat acsess.log | cut -d " " -f 9 | sort | uniq -c | sort -nr
204 200
187 302
15 404
```

“acsess.log” Dosyası Üzerinde Şüpheli Aktivitelerin Genel Değerlendirilmesi

Tespit Edilen Şüpheli Aktiviteler:

- **404 Hataları:** Sık tekrarlanan 404 hataları, saldırganların var olmayan dosyaları arayarak sunucuyu taradığını gösterebilir.
- **302 Yönlendirmeleri:** Artan yönlendirmeler, yetkisiz sayfalara erişim denemeleri olabilir.
- **Login İstekleri:** Tekrarlanan giriş denemeleri, brute-force saldırısı ihtimalini artırmaktadır.
- **Hesap Yönetimi Sayfalarına Erişim:** "My-account" gibi sayfalara yapılan yetkisiz erişim denemeleri risklidir.

Öneriler:

- **404 Hataları:** Yüksek sayıda 404 hatası üreten IP adreslerinin aktiviteleri yakından izlenmeli ve gerektiğinde bu IP adresleri engellenmelidir.
- **Brute-Force Saldırıları:** Brute-force saldırılarına karşı ek güvenlik önlemleri (örneğin, captcha uygulamaları, IP engelleme) devreye alınmalıdır.
- **Kritik Sayfalara Erişim:** "My-account" gibi kritik sayfalara yönelik erişim girişimlerinin detaylı olarak incelenmesi ve bu sayfalara yönelik güvenlik kontrollerinin sıklaştırılması gerekmektedir.

**BENİ DİNLEDİĞİNİZ İÇİN
TEŞEKKÜR EDERİM**