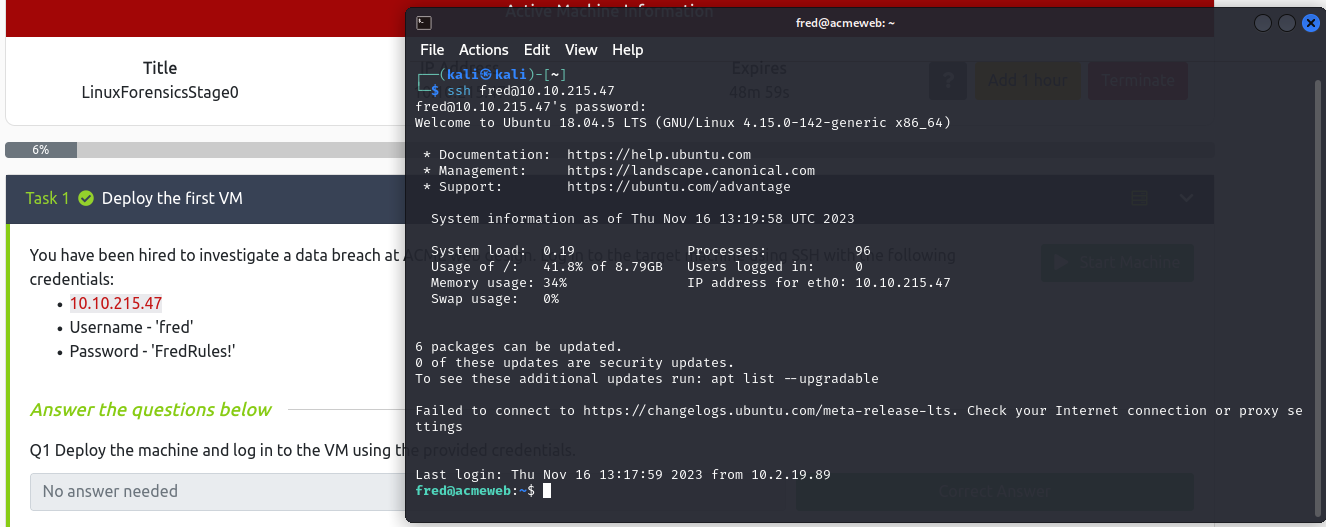


**TASK 1**

**1.soru**

İlk olarak ssh bağlantımızı gerçekleştiriyoruz



**TASK 2**

**1.Soru**

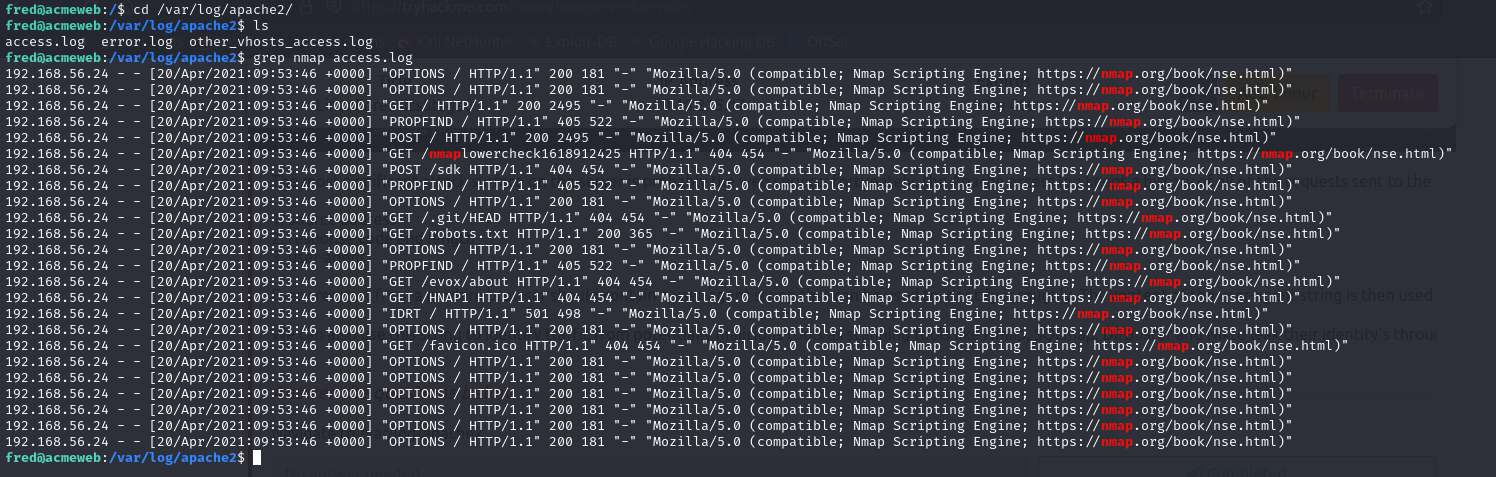
Daha sonra /var/log/Apache2 dizinine gitmemiz isteniyor. Ve daha sonra “we can also use this string to identify traffic from potentially malicious tools as scanning tools like Nmap, SQLmap, DirBuster and Nikto leak their identity's through” burada geçen araçlar tarafından taranabileceğini söylüyor.

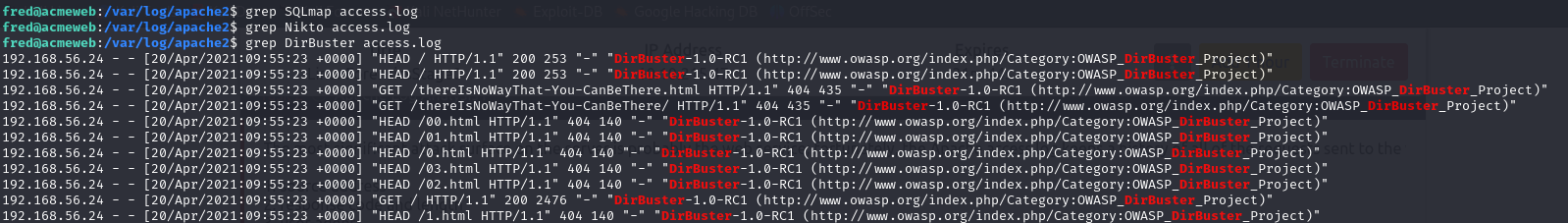
**2.Soru**

“How many different tools made requests to the server?” (sunucuya kaç farklı araçtan istek geldiği

Soruluyor)

Bu soru için yukarıdaki araçlar tarafından herhangi bir istekte bulunup bulunulmadığını kontrol ediyoruz.



Nmap tarafından tarandığını tespit ediyoruz.

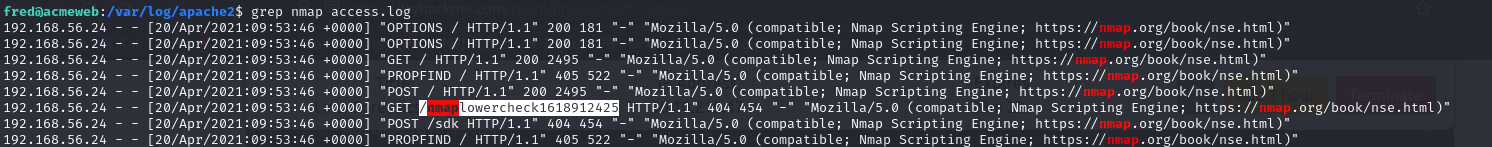
Nikto ve SQLmap tarafından tarandığına dair herhangi bir çıktı alamıyoruz fakat DirBuster tarafından tarandığını tespit ediyoruz. Böylelikle;

**CEVAP = 2**

**3.Soru**

“Name a path requested by Nmap.”

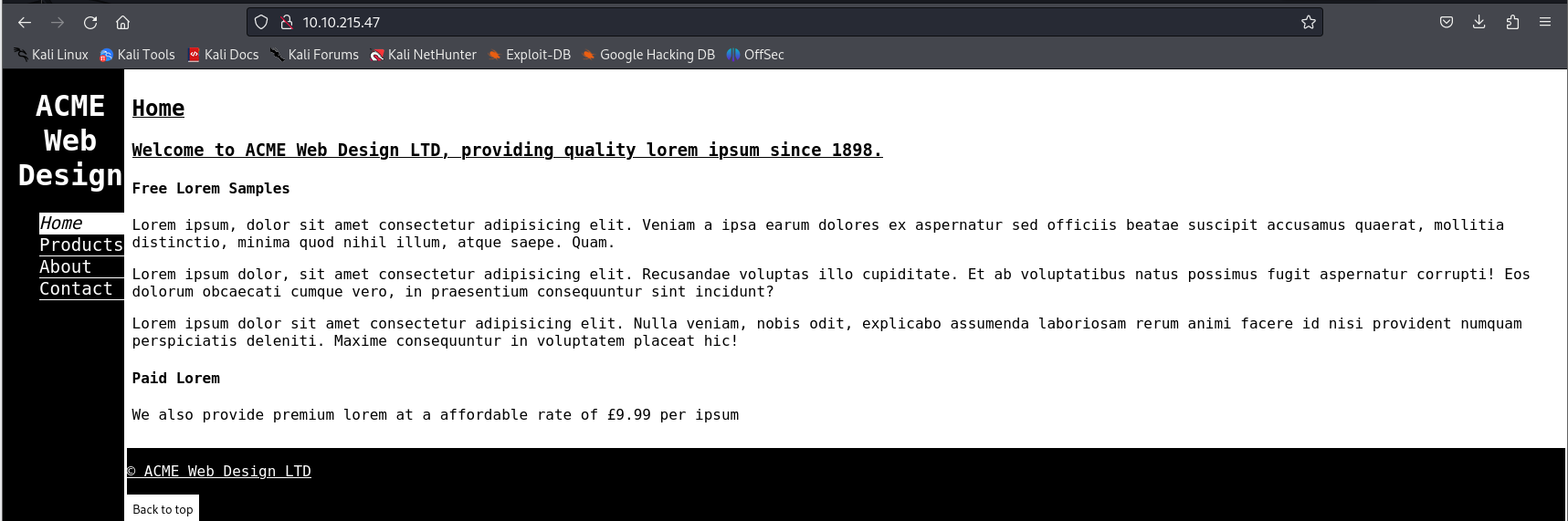
Nmap ile ilgili bi çok şey görmüştüm access.log içerisinde, istenilen yolu orada arayacağım.



**CEVAP = /nmaplowercheck1618912425**

**TASK 3**

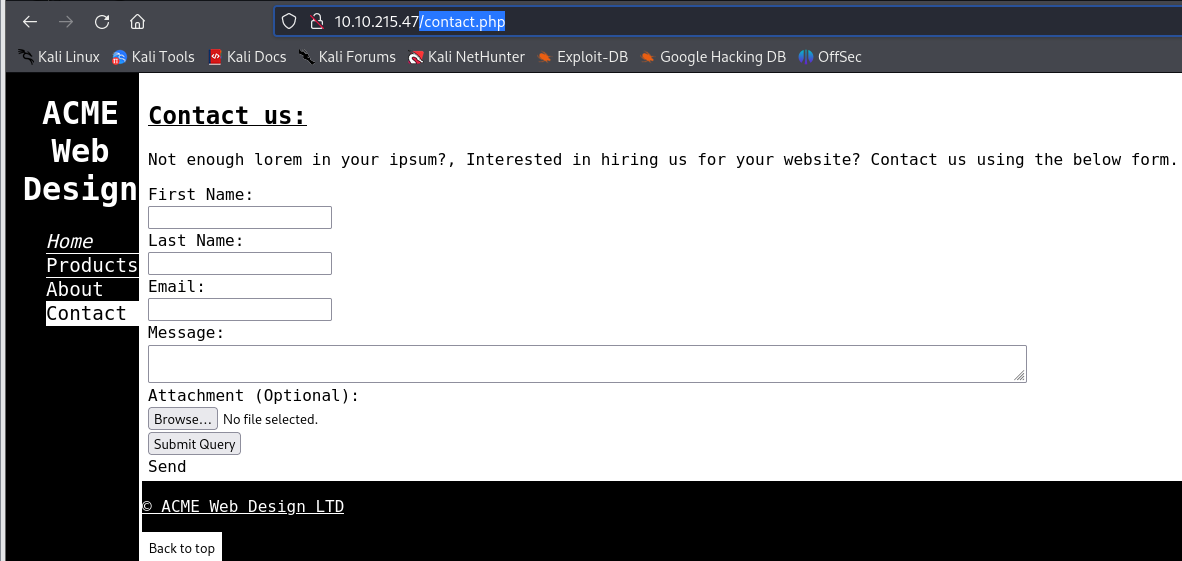
Bu task webserver’la ilgili bu yüzden tarayıcımızdan makinemizin Ip Adresine gidiyoruz.



**1.Soru**

“What page allows users to upload files?”

Kullanıcıların dosya yüklemesine izin verilen sayfayı istiyor bizden ;

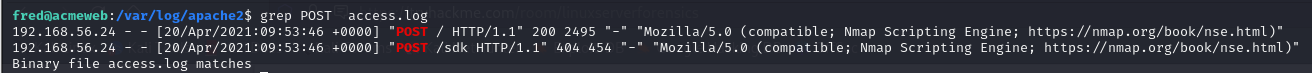


**CEVAP = /contact.php**

**2.Soru**

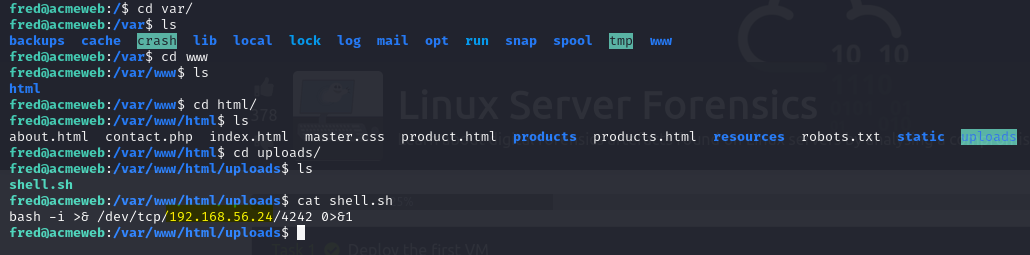
“What IP uploaded files to the server?”

Dosyaları sunucuya hangi ip’den yüklendiğini bulmamızı istiyor. Genellikle bir web sitesine bir şeyler upload edeceğimizde POST metodu kullanılır. Bende access.log içerisinde POST isteğinin olup olmadığını kontrol edeceğim ;



İki satırda bir şeylerin gönderilmeye çalışıldığını görüyoruz. İlk satırda başarılı bir Post isteği mevcuttur. İkinci satırda ise /sdk dizinine yapılan istek başarısız olmuştur.

2. Bir yol olarakta tüm dosyalara erişimizimiz olduğu için /www altındaki dosyaları kontrol ediyorum. Bu dizinin altında gezinmemin sebebi ise web server’ a ait dosyaların burada tutulmmasıdır. Dizini kontrol ettiğimde uploads adında bir dosyayla karşılaşıyorum. İçindeki shell.sh’a baktığımda ip’yi görüntülüyorum.



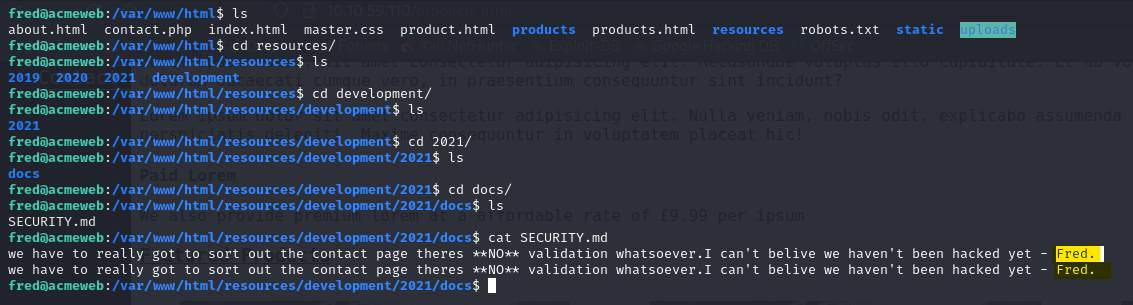
**CEVAP = 192.168.56.24**

**3.soru**

“Who left an exposed security notice on the server?”

Burada kimin not bıraktığını soruyor.

Bu notunda yine /var/www/html dizininiz altında bi yerlerde olacağını düşünüp dosyalar içinde geziniyorum.



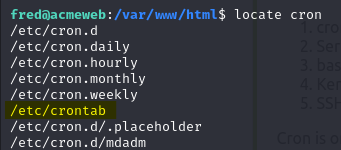
Ve */var/www/html/resources/development/2021/docs* dizini altında notu buluyorum.

**CEVAP = Fred**

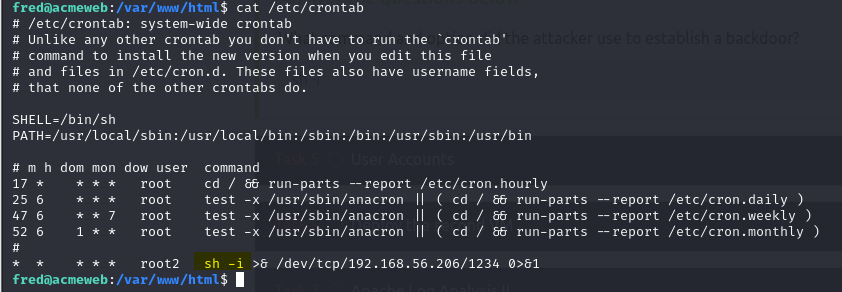
**TASK 4**

**1.Soru**

Bu soruda RFI aracılığıyla bir saldırı gerçekleştiğini söylüyor. Saldırganın kalıcılık sağladığına dair herhangi bir kanıt bulmamız bekleniyor. Yani saldırganın bıraktığı arka kapıyı arayacağız. Bunu tespit edebilmemiz için birkaç metodoloji önermiş. Arka kapı bırakmak için en yaygın kullanılanın metodun cron olduğunu söylemiş. Bizde ilk olarak crontab’ a bakacağız.



Cronetab’ın nerede tutulduğunu tespit ediyorum.



Kullandığı komutu tespit ediyorum.

**CEVAP = sh –i**

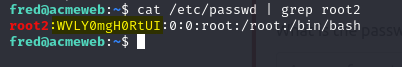
**TASK 5**

Bir önceki taskta bırakılan arka kapı root2 hesabı altında çalışacak şekilde oluşturulmuş. Yalnızca bir tane root hesap olmalıdır. Bizden root2 kullanıcısının şifresi isteniyor.

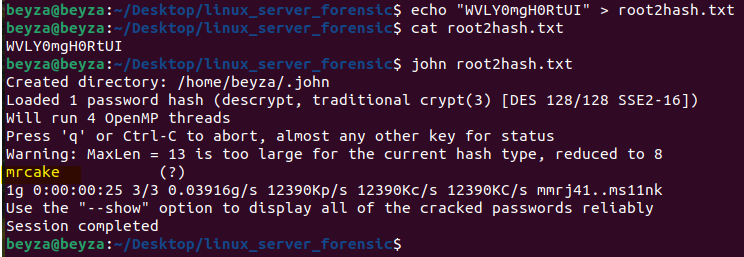
Hesap bilgilerinin depolandığı birkaç konum verilmiş ;

1. /etc/passwd 🡪 Sistemdeki hesapların temel bilgilerini cat içerir.
2. /etc/shadow 🡪 Sistemdeki hesapların adlarını ve parola hashlerini içerir.

Bende root2 kullanıcısının bilgilerini çekeceğim ;



Root2 kullanıcısının bilgilerine erişiyoruz. Ve kullanıcının parola hash’ini görüyoruz.



Bulduğum hash’i bir .txt dosyasına yazdırıyorum. Daha sonra john aracımı kullanarak hash’i kırıyorum.

**CEVAP = mrcake**

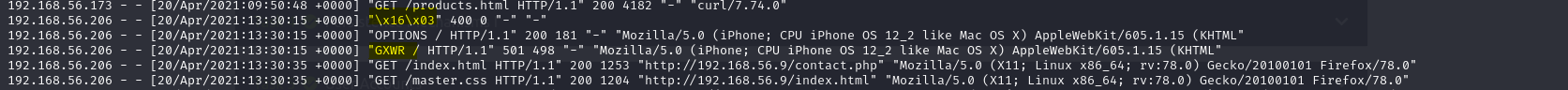
**TASK 6**

İlk makineyi sonlandırıp tekrar bu task’taki makineye ssh bağlantısı yapmamız isteniyor. Aynı kullanıcının tekrar saldırıya uğradığını ve bunu analiz etmemizi söylüyor.

**TASK 7**

**1.soru**

Anormal bir http isteği soruyor. Tekrar access.log dosyasına göz atalım;

Bana normal gelmeyen iki istekle karşılaşıyorum. Daha sonra “\x16\x03” ne olduğuna bakıyorum ve SSL/TLS protokolü ile ilişkili, protokollerin başlagıç baytı olduğunu görüyorum ve aradığım şeyin diğer istek olduğunu anlıyorum.

**CEVAP = GXWR**

**2.Soru**

Nmap taramasının saat kaçta yapılığını soruyor.



Access.log dosyasında nmaple ilgili çıktıları filtrelemeye çalışıyorum fakat bir sonuç elde edemiyorum. Daha sonra saldırganın ip adresini filtreleyip neler bulabileceğime bakıyorum.

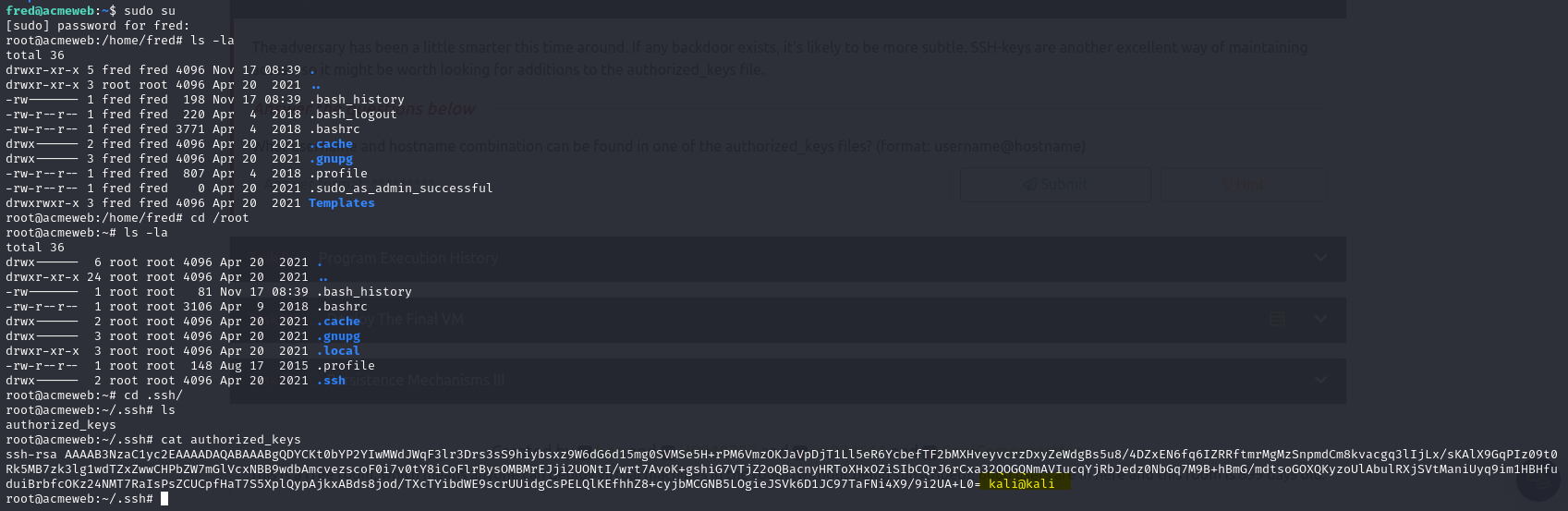


Saldırganın iletişimi “\x16\x03” bu metotla başlamış ve bu metodunSSL/TLS protokolü ile ilişkili olduğunu biliyorum. Nmap’te SSL/TLS el sıkışma başlıklarını ve diğer ağ trafiği bilgilerini analiz ederek hedef sistemlerin güvenlik durumu hakkında bilgi sağlar. Bu yüzden bunun nmap taramasıyla ilgili olabileceğini düşünüyorum. Ve tahminim doğru çıkıyor.

**CEVAP = 13:30:15**

**TASK 8**

Bu sefer saldırgan kalıcılık sağlamak için kendine bir ssh anahtarı üretmiş. Ssh anahatrlarının tutulduğu yeri bulup istenilen bilgiyi elde edebilirim. Ufak bir araştırma yaparak anahtarların nerede tutulduğunu bulup kontrol ediyorum. Genellikle ssh anahtarlarının *~/.ssh/authorized\_keys* dizininde tutulduğunu öğreniyorum. Fakat bu dizine erişmek için root yetkilerinde olmam gerektiğinide görüyorum ve bu dizini root olarak kontrol ediyorum.



Ve aradığım sonucu buluyorum.

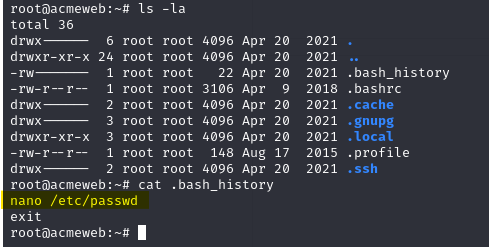
**CEVAP = kali@kali**

**TASK 9**

Sudo (root) yetkisiyle çalıştırılan komutların listesinin olduğu birkaç dosya olduğunu söylüyor. Farklı bazı komutlarında özel olarak listelendiği bazı dosyalar varmış. Bunlar ;

1. *bash\_history =* bash’teçalıştırılan komutların geçmişini tutar.
2. *auth.log =* sudo kullanılarak çalıştırılan komutların geçmişini tutar.
3. *history.log (apt) =* apt kullanılarak gerçekleştirilen tüm komutların geçmişini tutar.

Soruda bize *bash\_history* dosyasında bulunan ilk komut soruluyor. Hemen ilgili dosyayı bulup kontrol ediyorum ;



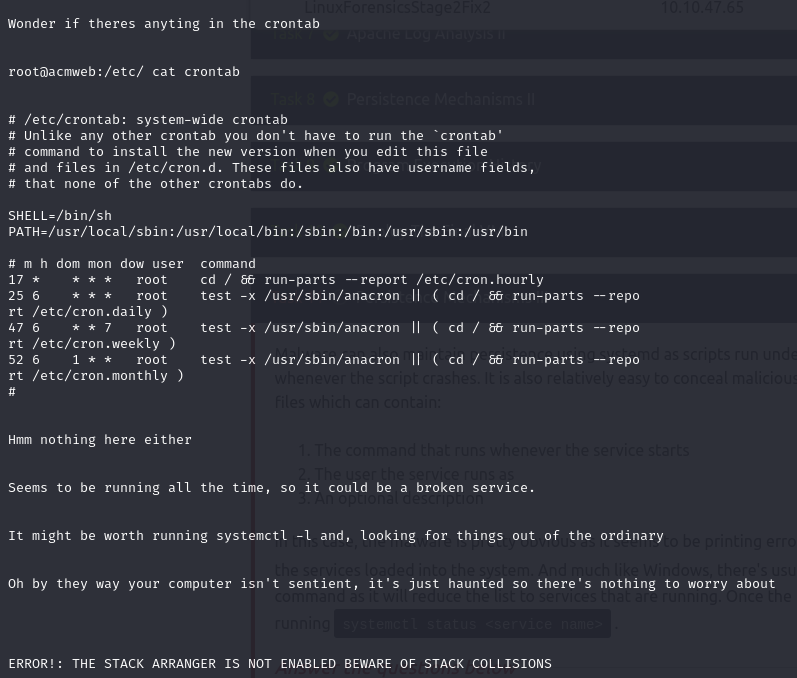
**CEVAP = nano /etc/passwd**

**TASK 10**

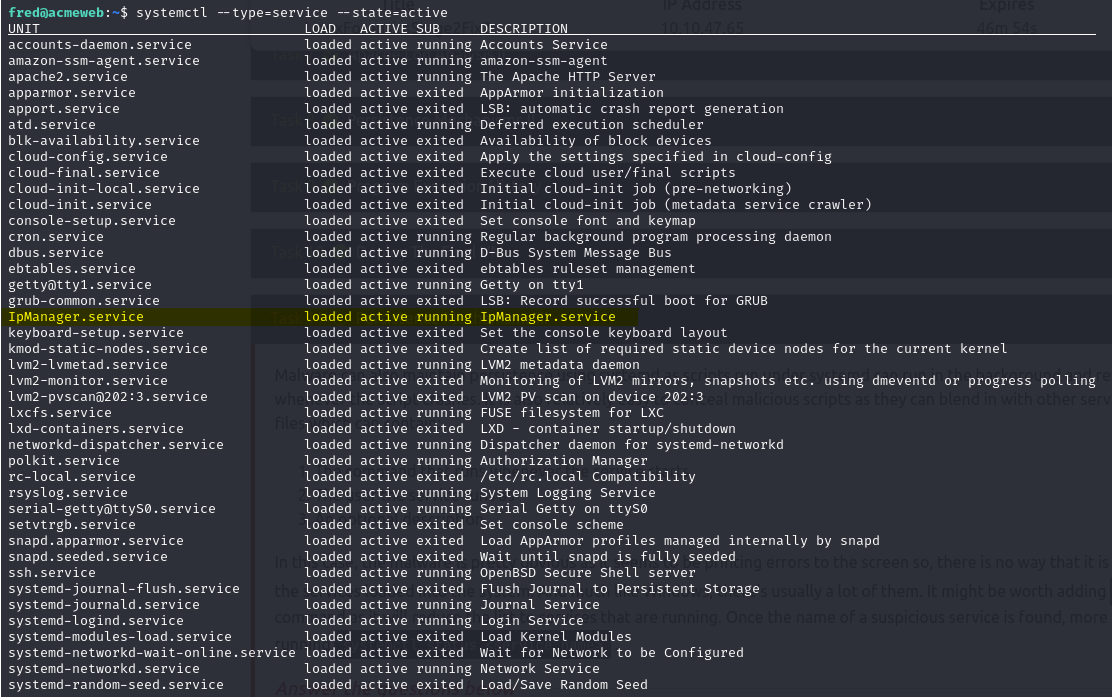
Fred adlı makine tekrar hackelenmiş ve tekrar analiz etmemiz isteniyor. Önceki makineyi kapatıp yeni makineyi başlatıp ssh bağlantımızı yapıyoruz.

**TASK 11**

Kötü amaçlı bir yazılım tarafından ekrana hatalar bastırıldığını görüyoruz. Böyle yazılımların genelde systemd’yi kullandığını ve .service dosyalarında tanımlandıkları bilgisi verilmiş.

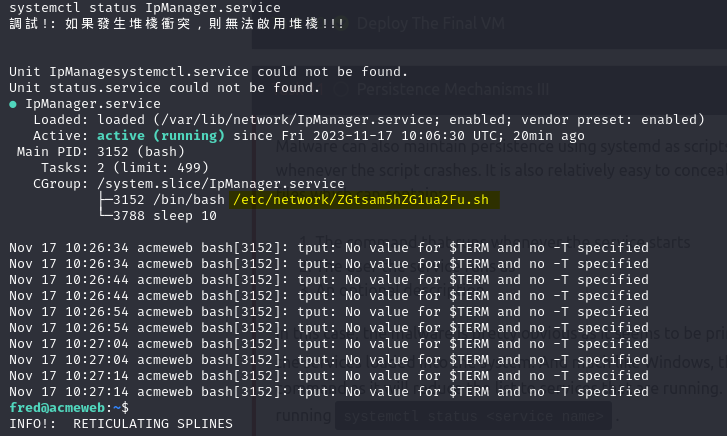


Bize verilen bilgiler doğrultusunda aktif ollarak çalışan servisleri listeliyoruz;

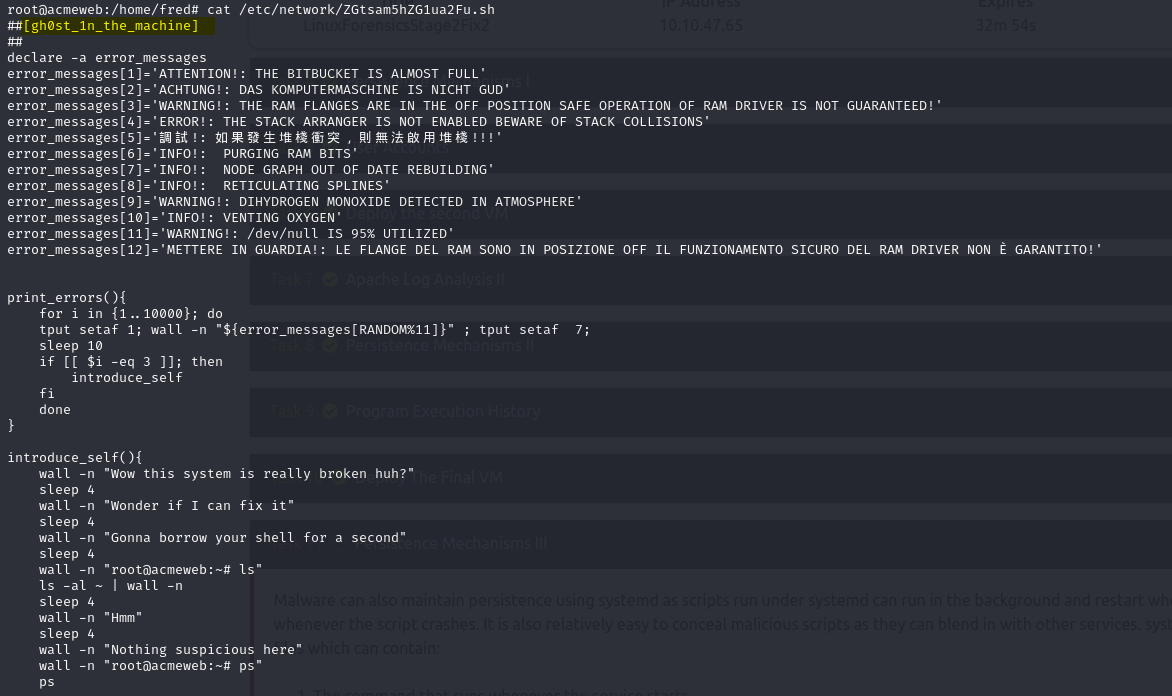


Kötü amaçlı yazılım yüzünden komutu yazmak pek kolay olmuyor 😊

Servisleri listelediğimde çalışan birçok servis olduğunu görüyorum. Servis isimlerinin genellikle küçük harflerle ismlendirildiğini biliyorrum ve biraz detaylı baktığımda IpManager\_service büyük harfler içerdiğii için dikkatimi çekiyor. Bu servis hakkında bilgi topluyorum;



Zararlı dosyanın nerede konumlandığını buluyorum. Daha sonra bu dosyanın neler içerdiğini okuyorum;



Terminali kulanmamızı zorlaştıran zararlı burda 😊 Aynı zamanda son soruda istenilen bayrağa da erişmiş oluyoruz.

**CEVAP = [gh0st\_1n\_the\_machine]**

*systemctl stop IpManager.service* komutuyla çalışan zararlı servisi durdurabiliriz.