|  |
| --- |
| ***Linux*** |
| Kaan Efe Öğüt  *ADLİ BİLİŞİM MÜHENDİSLİĞİ* |
| -Linux üzerinde kullanılan terminal komutları ve firewall yapılandırmasını size aktaracağım. |

**27.11.2021**

***Linux Dosya Sistemi***

***/BİN***

-Olması şart olan komut dosyalarını içerir.Örnek olarak PİNG,LS,CHMOD gibi komutların dosyaları burada tutulur ve siz komut çalıştırdığınızda çağrılırlar.

***/BOOT***

-Başlangıç için gerekli dosyaları bulundurur.Kali linuxu çalıştırmak için başlat programlardır.

***/DEV***

-Donanım dosyalarını içerir.Disk,SDA,DVD gibi dizinleri vardır.

***/LİB***

-Kütüphane dosyaları ve kernel modülleri bulunur.Örnek olarak "Apt-get install" komutu çalıştırıldığında APT içerisinde ki tanımlı download URL'sini kullanır.İndirmek istediğimiz dosyayı o URL üzerinde indirir.

***/OPT***

-Ekstra programların kurulması içindir.Yani 3.Parti kullanıcı programlarının kurulması içindir.

***/SBİN***

-Sistem yöneticisiyle(ROOT) ilgili çalıştırılabilir dosyaları tutar.

***/TMP***

-Geçiçi dosyaları tutmak içindir.Bu dosyalar sistem kapanırken silinir.

***/USR***

-İkincil bir hiyerarşidir.Kendi içerisinde ayrı bir hiyerarşisi vardır.Tüm kullanıcılarca paylaşılan verileri içeren dizindir.Paylaşılabilen,sadece dataların okuma özelliği olan bir alandır.

***/VAR***

-Log dosyaları,E-Posta ve yazıcı kuyrukları gibi değişken verileri barındırır.

***/PROC***

-Kernelle ilgili,donanım kullanımı ve sistemle ilgili bilgileri tutar.Çekirdek her yüklendiğinde tekrar oluşturulur.

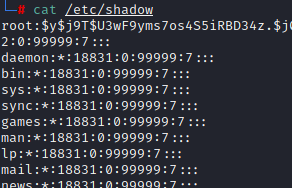
***/HOME***

-Kullanıcılara ayrılmış dizindir.Oluşturulan her user için ayrı bir dizin oluşur.Kullanıcılar kendi dizinlerinde yetki sorunu yaşamaz.

***/ETC***

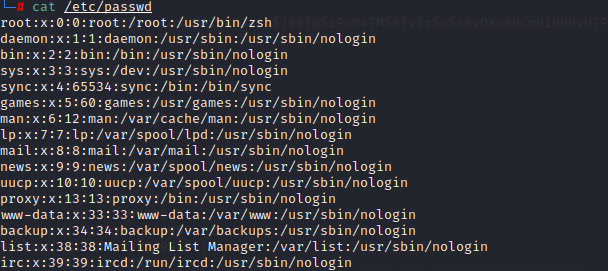
-Sistem ayarlarını barındırır.ETC klasörü daha detaylı olarak ele alınmalıdır.Bir çok konfigurasyon işlemi buradan yapılır.

***/ETC/SHADOW***



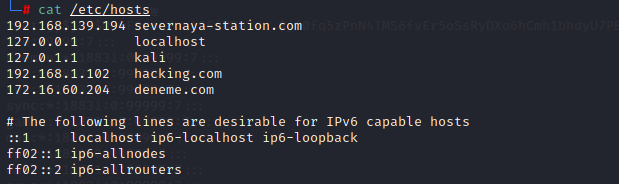
-Yetkili-yetkisiz bütün kullanıcıların parola hashlerinin tutulduğu alandır.Sadece yetkisi olan kullanıcılar bu dosyayı okuyabilir.

***/ETC/PASSWD***



-Yetkili-yetkisiz bütün kullanıcıların kullanıcı adlarının tutulduğu alandır.Bütün kullanıcılar okuyabilir.

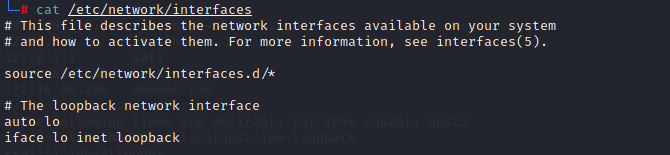
***/ETC/HOSTS***



-Bir DNS adresi tarandığında ilk bakılacak yerdir.IP adresleri ve karşılarında domain nameleri bulunur.

Örnek; 127.0.0.1 google.com

***/ETC/NETWORK/INTERFACES***



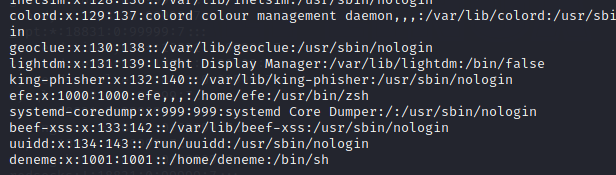
-Network ayarlarını yapabildğimiz dosya yoludur.Burada ağ ayarlarınızı manuel olarak static-dinamik olayarak ayarlayabilirsiniz.Ayrıca IP adresi gibi değerlerinizi değiştirebilirsiniz.

***Linux kullanıcı oluşturma ve silme***

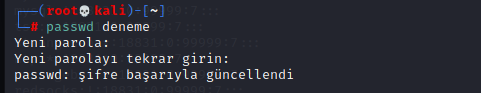
-Linux sistemler üzerinde kullanıcı oluşturma,şifre verme ve silme işlemlerini birlikte yapacağız.



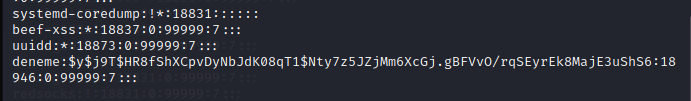
-Öncelikle "useradd" komutu ile bir kullanıcı oluşturuyorum.



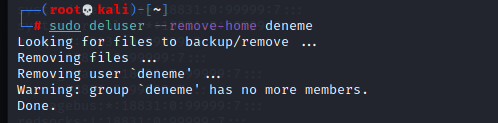
-"/etc/passwd" dizinine baktığımda burada başarılı bir şekilde kullanıcı oluşturduğumu görüyorum.



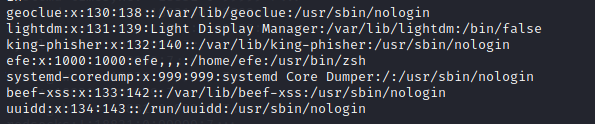
-"passwd deneme" komutu ile oluşturduğum kullanıcıya bir şifre atıyorum.



-"/etc/shadow" kısmına geçiş yapıyorum ve burada başarılı bir şekilde şifreyi de hashlediğini görüntülüyorum.



-"sudo deluser --remove-home deneme" komutu ile kullanıcıyı silebiliyorum.

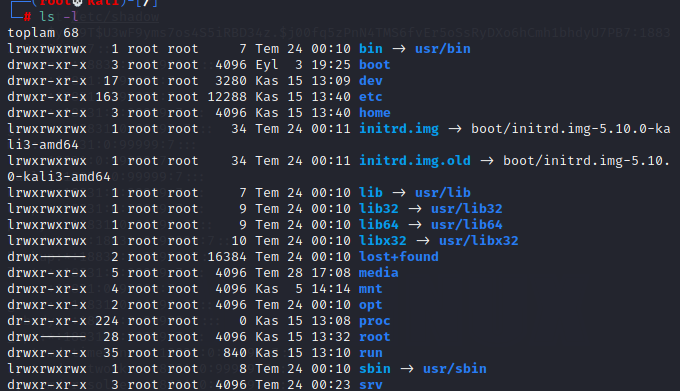


-"/etc/passwd" dizininden de teyit ettiğimde kullanıcıyı başarılı bir şekilde silebiliyorum.

***Linux Yetki ve Yetkilendirme***

-Kullanıcımızı oluşturduk fakat yetki ve yetkilendirmenin nasıl gerçekleştiğini bilmiyoruz.

-Uygulama içerisinden yapılan tüm erişimler,kullanıcı ve grup hakları doğrultusunda gerçekleştirilir.



-"Dosya sahibi-Grup-Diğerleri" şeklinde bir sıralamayla yetki tablosunu okuyabiliriz.

-"-r"(read) -< Dosyalar için okuma yetkisi dosya içeriğine ulaşabilmesi anlamını taşır.

-"-w"(write) -> Dosyalar için yazma yetkisi,dosya içeriğinin değiştirilebilmesi anlamını taşır.

-"-x"(executable) -> Dosyalar için çalıştırma yetkisi anlamına gelir.

-"ls" komutunun çıktısında ki erişim yetkileriyle ilgili karakterler;

-"-" ->Standart dosya(regular file)

-"-d" -> Dizin

-"-c" -> Karakter tabanlı aygıt dosyası

-"-b" -> Blok tabanlı aygıt dosyası (/dev/sda2 vb.)

-"-s" -> Özel dosya (Unix,domain,soket vb.)

***Yetki Bitleri***

-Standart Read,Write,Execute yetki bitleri haricinde SUID,SGİD ve STİCKY BİT olmak üzere 3 farklı bit daha bulunmaktadır.

***SUID BİT (SET USER ID)***

-Bir uygulamada SUID Bit'i aktif ise o uygulamayı hangi kullanıcı çalıştırırsa çalıştırsın uygulama dosyanının sahibi kim ise onun haklarıyla çalıştırır.

-Bu durum ise bazı güvenlik zafiyetleri getirebilir.

***SGID Yetkisi(SET Group ID)***

-SUID Bit ile benzer mantıktadır.Bir uygulamanın kimin çalıştırdığına bakmaksızın uygulama dosyasının grup sahibinin grup erişim yetkileri doğrultusunda çalıştırmasını sağlamaktadır.

***STICKY BİT***

-Belirtilen klasör veya dosyanın sadece sahibi veya root kullanıcısı tarafından silebileceği anlamına gelir.

***“CHMOD” komutu***

-Dosya sisteminde yer alan bir dosya/dizin için erişim yetkilerinin düzenlenmesi işlemi "chmod" komutu ile yapılır.

"+" komutu ile yetki eklenir.

"-" komutu ile yetki geri alınır.

"=" komutu ie tam olarak hangi yetklere sahip olacağı belirtilebilir.

***Erişim yetki grupları***

-'u' -> Dosya/dizin sahibi

-'g' -> Dosya/dizin grup sahibi

-'o' -> Dosya/dizin sahibi ve grup sahibi dışında kalanlar (others)

-'a' -> Dosya/dizin sahibi,grup sahibi ve bunların dışında kalanlar dahil üç blok.

***Sekizli gösterim ile yetki ayarlama***

-R = 4

-W = 2

-x = 1

***Örnek:***

Dosya Sahibi-Grup-Diğerleri

#chmod 644 file\_name

-Dosya sahibinin Okuma ve yazma

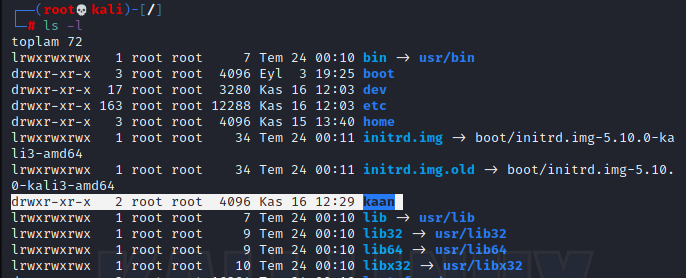
-Grupta bulunanların yazma

-Diğerlerinin de yazma yetkis olduğunu anlatır.

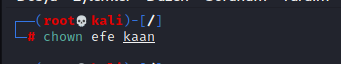
-chmod +777 ile Tüm yetkileri vermiş oluruz.

***Dosya Sahipliği Değiştirme***

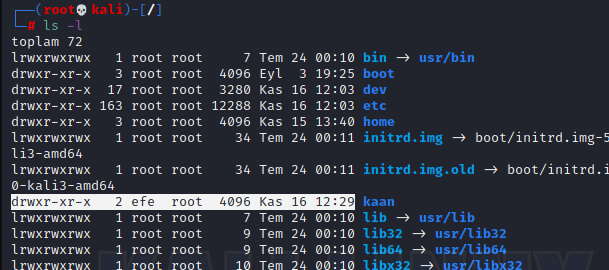
-Oluşturduğumuz veya kullandığımız dosyaların sahibini değiştirmeyi deneyeceğiz.



-"ls -l" komutu ile baktığımız da burada oluşturduğum "kaan" isimli dosyanın sahibini root olarak görüntülüyorum.



-"chown sahiplik\_atanacak\_kullanıcı dosya\_adı" sırasıyla komutumu yazıp çalıştırıyorum.

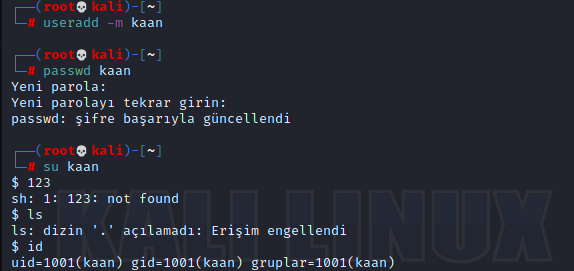


-Ardından burada baktığımda yaptığım işlemin başarıyla değiştiğini görüntüleyebiliyorum.

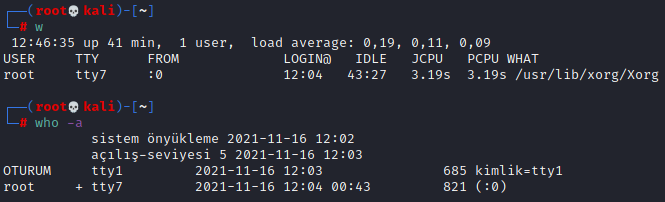
***Linux Sistem Bilgisi***



-İlk önce göreceğimiz komut "id" komutudur.Bu komut kullanıcısı olduğumuz hesabın bize yetki mertebesini verir.'1000' sayısı bu hesabın en yetkili olduğunu gösterir.

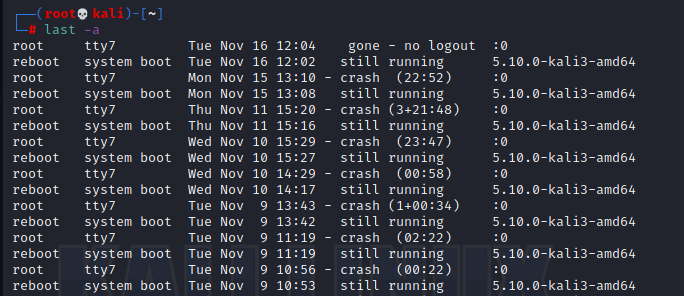


-Bir kullanıcı ekleyip onun "id" sonucuna baktığımda ls komutunda bile erişimim engellendiğini ayrıca yetkisiz olduğumu da sayılardan anlayabiliyorum.

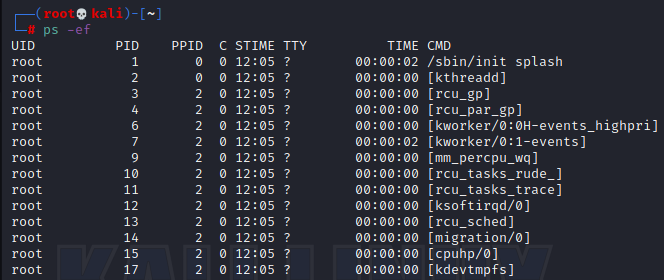


-"w" parametresi ile sisteme saat kaçta login olduğumuzu görüntüleyebiliriz.

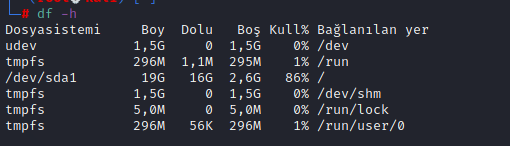
-Aynı işlemi "who -a" komutu ile de gerçekleştirebiliriz.



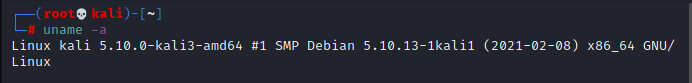
-"last -a" parametresi ile kullanıcının önceki login giriş ve çıkışlarını görüntüleyebiliriz.



-"ps -ef" komutu ile de çalışan processler hakkında bilgi sahibi olabiliriz.

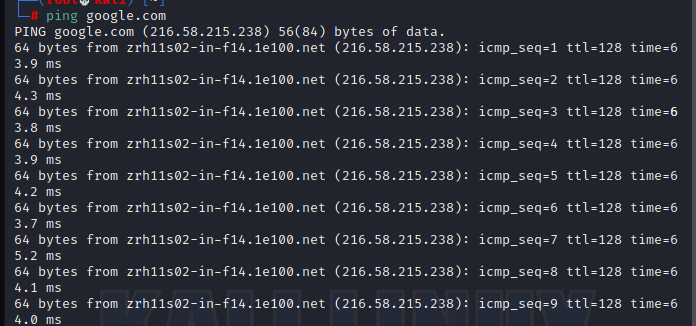


-"df -h" komutu ile diskin doluluk oranını görüntüleyebiliyoruz.

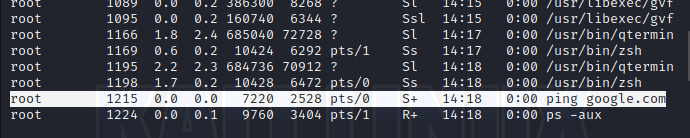


-"uname -a" komutu ile linux'un sürümü hakkında bilgi sahibi olabiliriz.

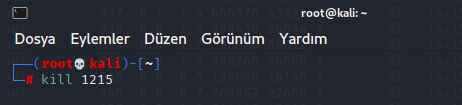
***Process Öldürme***



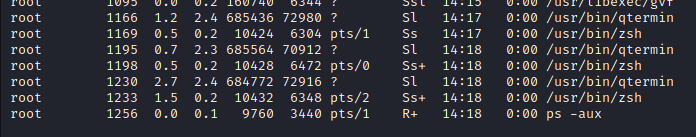
-"ping google.com" komutu ile bir process başlatıyorum.



-Ardından "ps -aux" komutu ile çalışan processleri görütülüyorum ve burada google.com sayfasına atılan ping işlemini görüntülüyorum.



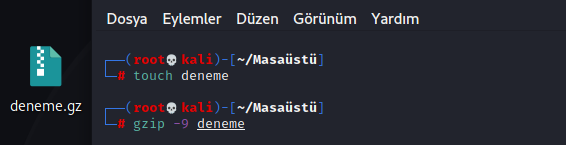
-Sonrasında burada gördüğüm process\_id numarasını kill komutu ile kapatıyorum.



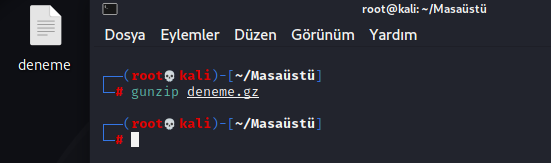
-Tekrardan "ps -aux" komutu ile kontrol ettiğimde ping işlemini kapattığımı görüntülüyorum.

***Dosya sıkıştırma ve açma komutları***

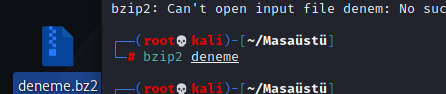
-Gzip veya tar uzantlı bir dosya indirdik veya bu hale getirmek istiyoruz bu işlemler nasıl gerçekleşecek bunu göstereceğim.



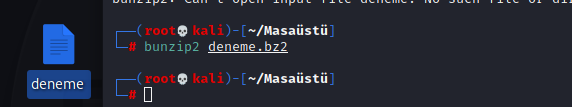
-"touch" komutu ile bir dosya oluşturuyorum ve ardından "gzip -9" komutu ile belirttiğim dosyayı .gz uzantılı hale getirebiliyorum.



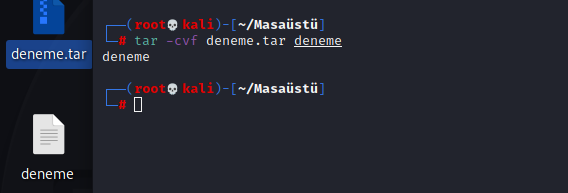
-"gunzip" komutu ile zip dosyasını tekrardan dışa aktarabiliyorum.



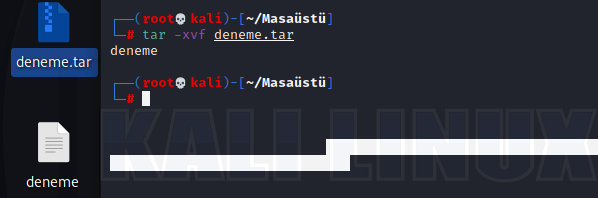
-"bzip2" komutu ile oluşturduğum dosyayı tekrardan zip hale getiriyorum.



-"bunzip2" komutu ile zip halden eski hale getiriyorum.



-"tar -cvf dosya.tar dosya" formatında bir tar dosyası oluşturabiliriz.

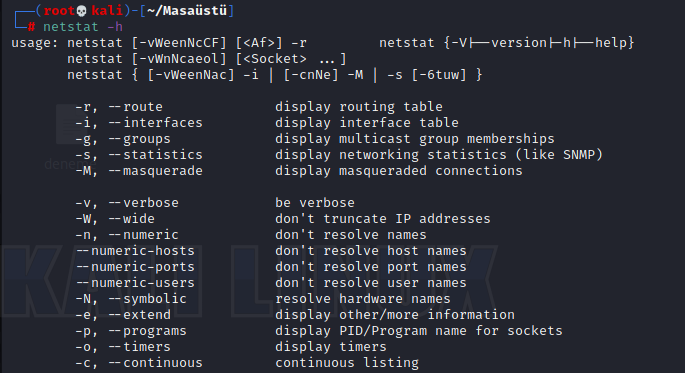


-Oluşturduğumuz tar dosyasını unzip yapmak istersek "tar -xvf komutu kullanılır.

***Network Komutları***

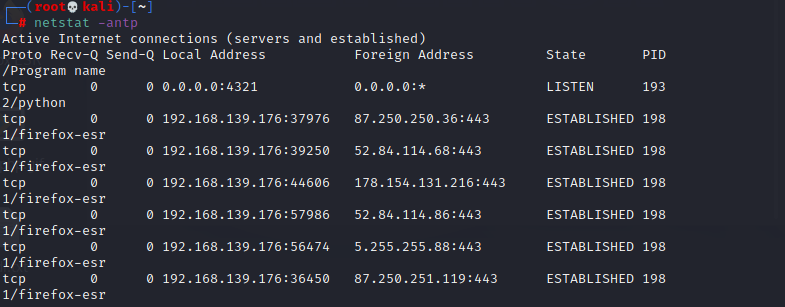
1-)***TCP ve UDP bağlantı durumları -Netstat***

-Linux ortamında bulunan UDP bağlantısını kontrol etmek istiyoruz.



-Bu işlem için linux üzerinde kurulu olarak bulunan "netstat" aracı kullanılır.

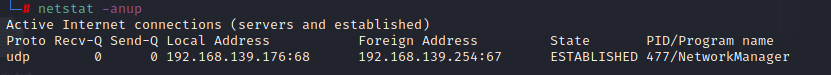
-Aracın kullanımını öğrenmek için "netstat -h" komutunu kullanıyorum.



-"netstat -antp" komutunu kullanarak TCP bağlantılarını görüntüleyebilriz.

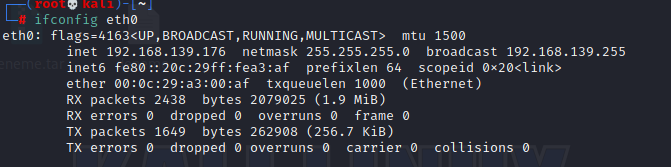
-Burada bağlantı kurulan yerleri görüntüleyebiliriz.

-Burada kullandığımız a-n ve p daha fazla bilgi sahibi olmamız için kullanılıyor.



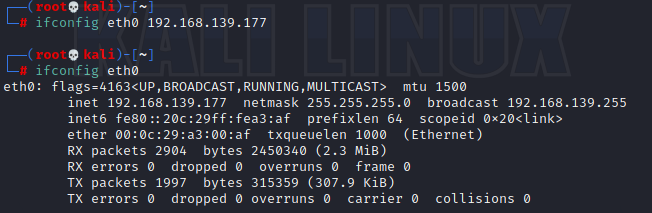
-"netstat -anup" komutunu kullanarak aktif olarak bulunan UDP bağlantılarını görüntüleyebiliriz.

2-)***Ip adresi Netmask ve Broadcast değiştirme***

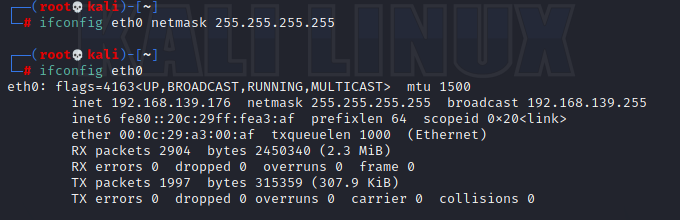


-"eth0" üzerinde bulunan IP adresimi bu şekilde görüntüleyebiliyorum.

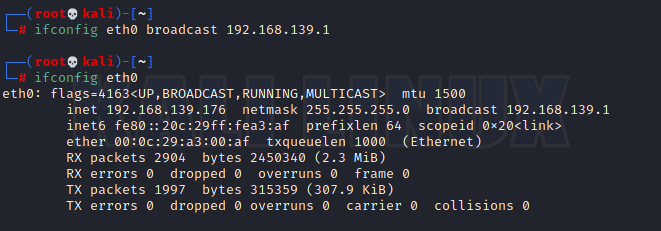
-Şimdi yapacağım işlemle birlikte bu IP adresini değiştireceğim.



-"ifconfig eth0 192.168.139.177" olarak IP adresimi değiştiriyorum ve tekrardan kontrol sağladığımda IP adresimin değiştiğini görüntülüyorum.



-Ağ maskesini değiştirmek için de "ifconfig eth0 netmask 255.255.255.255" komutunu kullanıyorum ve ardından tekrardan ifconfig komutunu çalıştırdığımda başarılı bir şekilde değiştiğini görüntülüyorum.



-Broadcast adresini değiştirmek içinde "ifconfig eth0 broadcast 192.168.139.1" komutunu kullanıyorum ve baktığımda broadcast adresini de başarılı bir şekilde değiştirebildiğimi görüntülüyorum.

***MTU Değeri Değiştirme***

-MTU değeri veri bölümünde taşınabilen max. değeri belirtir.Bu işlem bilinmediği sürece değiştirilmemelidir.

-1500 değeri ideal bir değerdir.



-MTU değerini de "ifconfig eth0 mtu" komutu ile bu şekilde değiştirebiliriz.

***Bilinmesi gereken komutlar***

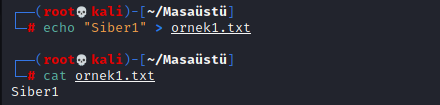
1-)***”Echo” ile dosya içeriğine yazma***

-Echo komutu ekrana yazdırma olarak düşünülebilir fakat biz burada dosya içerisine değer yazdırma kısmını görüntüleyeceğiz.

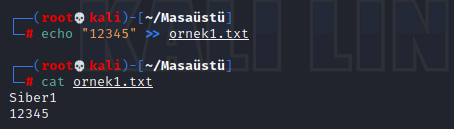
-Bu işlem için öncelikle "touch" komutunu kullanarak .txt uzantılı dosya oluşturuyorum.



-Örnekte olduğu gibi "echo" komutunu kullanarak başarılı bir şekilde dosya içerisine ekleme yapabilirim.



-Aynı dosya üzerinde tekrardan tek ">" işareti kullanarak yazdırdığımda daha önce yazdığım veriyi kaybediyorum.



-Bu kaybetme işleminden kurtulmak için ">>" kullanarak tekrardan işlemi gerçekleştiriyorum.

-Görüldüğü gibi bu sefer önceki veriyi kaybetmedik.

2-)***”Md5sum” ile dosya hashleme***

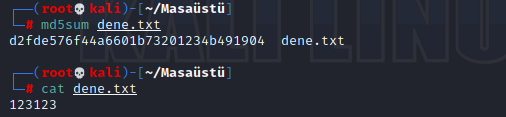
-MD5 bir şifreleme türüdür.Bu veri bütünlüğünü sağlamak için kullanılır.

-MD5 şifrelemesini yapmak için Linux içerisinde bulunan md5sum aracından yararlanacağız.



-İşlemi gerçekleştirmek için öncelikle bir txt içerisinde bulunan veriler bulunması gerekmektedir.

-Bu sebeple bir .txt uzantılı dosya oluşturuyorum ve içerisine veri ekliyorum.



-"MD5" şeklinde şifrelenmiş halini bu şekide görüntüleyebiliyorum.



-İçeriğini değiştirip tekrardan MD5 değeri alırsam bu şekilde değerinin değiştiğini görüntüleyebiliyorum.

***IPTables kurallar –Firewall***

1-)***IPTables giriş ve kuralları***

-İnternet üzerinde tüm veri paketler halinde gönderilir.Linux kernel'i hem gelen hem de giden trafiğin paketlerini paket filtresi tablosu kullanarak filtrelemeize olanak veren bir arayüze sahiptir.

-Iptables : Bu tabloları kurmak,yönetmek ve incelemek için bir komut satırı uygulaması ve linux güvenlik duvarıdır.

-SSH portuna biri bağlantı kurmak istedi IP tables üzerinden bir düşürme işlemi gerçekleştirip bağlantı düşürebiliriz.

-IPTables üzerinde bilmemiz gereken parametreler vardır.

-Accept = Paketin geçmesine izin verileceği anlamına gelir.

-Drop = Paketin geçmesine izin verilmeyeceği anlamına gelir.

-Return = Şimdiki zincirin pas geçilmesi ve çağrıldığı zincirde bir sonraki kurala geçilmesi gerektiği anlamına gelir.

-Reject = Paketlerin erişimi reddedilir ve gönderen bilgilendirilir.

-Input =Bu zincir sunucuya gelen paketleri kontrol etmek için kullanılır.Bağlantıları port,protokol veya kaynak IP adresi bazında engelleyebilir veya izin verebilirsiniz.

-Forward = Bu zincir sucunuya gelen ama başka bir yere yönlendirilerek paketleri filtrelemek için kullanılır.

-Output = Bu zincir sunucudan giden paketleri filtremek için kullanılır.

-----------------------------

-Oluşturduğumuz IPtables kuralları hafızada saklanır.Bu da her tekrar başlatma(reboot)sonrasında tekrar tanımlamamız anlamına gelir.Aşağıda ki komut kuralları sistem yapılandırma dosyasına kaydeder ve her tekrar başlatmadan sonra sistem bu yapılandırma dosyasından IPtables kurallarını tekrar devreye alır.

-"iptables -F" komutu yapılan tüm değişikler silinebilir.

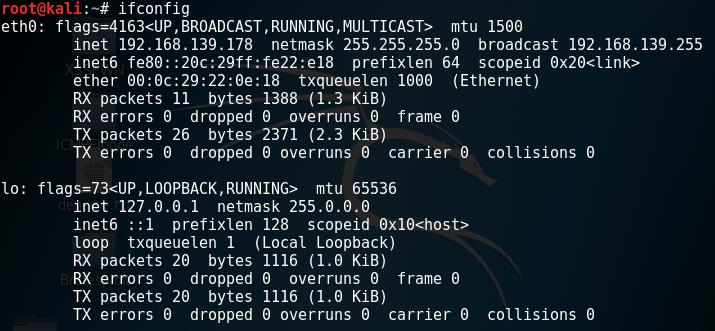
-Yapılan değişikliklerin kayıt edilmesi için "/sbin/iptables-save" komutu kullanılır.

2-)***IPTables Reject ve Drop komutları***

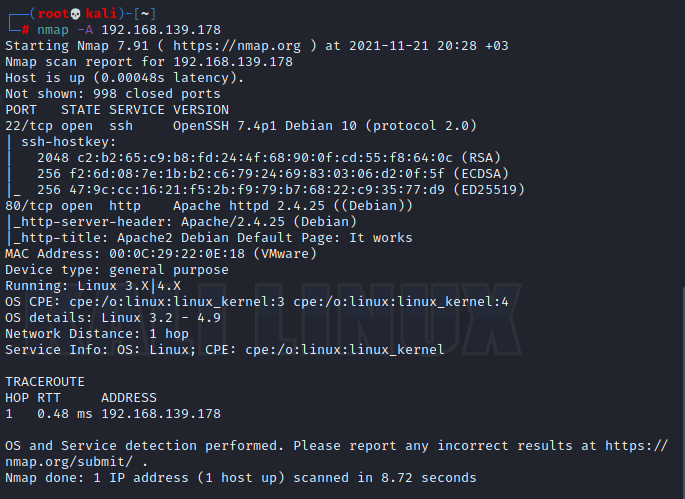
-Bu işlem için ilk önce 2 adet linux işletim sistemini başlatıyorum

-Bu makinelerin birbirini görebilmesi için ikisinin de "NAT Network" üzerinde olması gerekmektedir.

-Bu makinelerden bir tanesini saldırgan bir tanesini firewall ayarlaması gerçekleştirip işlem yapacağım.



-Linux makinelerimden bir tanesine saldırı düzenleyeceğim bu sebeple bu makinenin ilk önce IP adresini öğreniyorum.



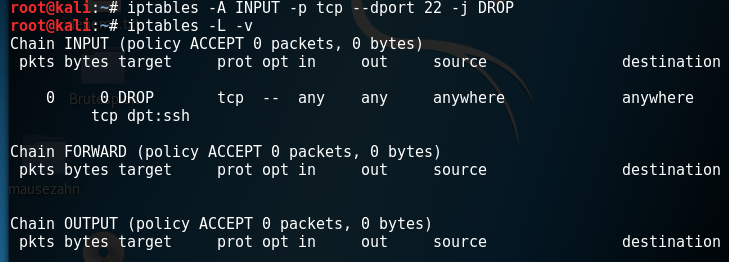
Ardından öğrendiğim IP adresi üzerinden bir Nmap taraması gerçekleştirip açık olan portlar hakkında bilgi topluyorum.

-SSH portu üzerinden işlem yapacağım için saldırı gerçekleştireceğim Linux üzerinden "service ssh start" komutunun çalıştırılması gerekmektedir.



-Saldırı gerçekleştireceğim Linux üzerine geçiş yapıyorum ve "iptables -h" komutunu çalıştırıyorum.

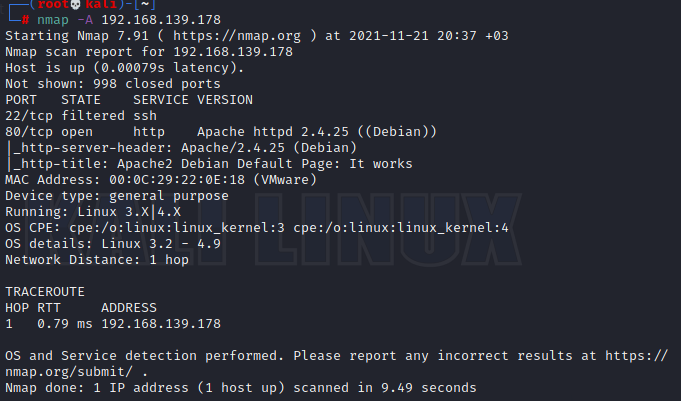
-Burada yapabileceğim ayarları görüntüleyebiliyorum.



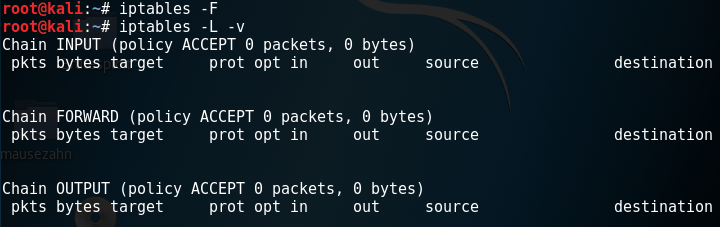
-SSH "tcp" protokolünde çalıştığı için "-p" ile belirtiyorum.

-"--dport" ile çalıştığı port adresini veriyorum.

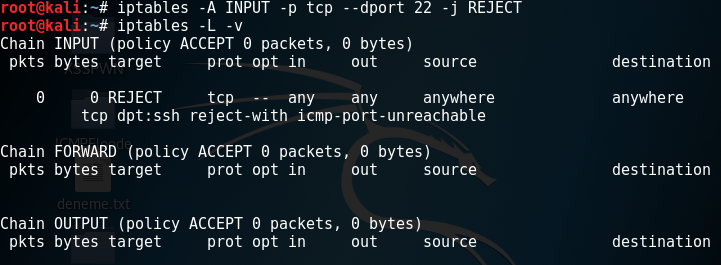
-"-j" parametresi ile hangi işlemi yapacağını belirtiyorum.



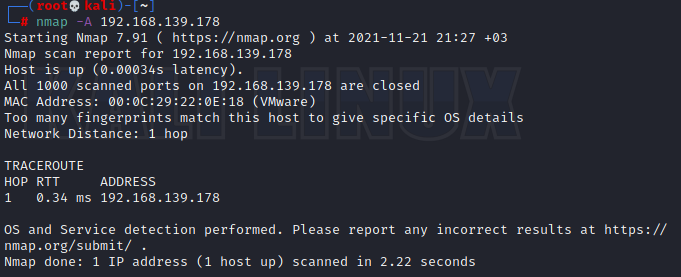
-Verdiğimiz kural ardından saldırgan makinem üzerinden bir Nmap taraması gerçekleştiriyorum ve burada 22 portuna gelen isteği DROP ettiğini görüntülüyorum.



-Reject ve Drop arasında ki farkı anlamamız için ilk önce yazmış olduğum tüm kuralları "iptables -F" ile siliyorum.



-"Drop" kısmında yazdığım kodun sonunu REJECT olarak değiştirdim ve kuralı tanımladım.



-Ardından diğer Linux makineme geçiş yaptım ve tekrardan bir tarama gerçekleştirdim.

-DROP üzerinde gelen paket filtrelenirken;

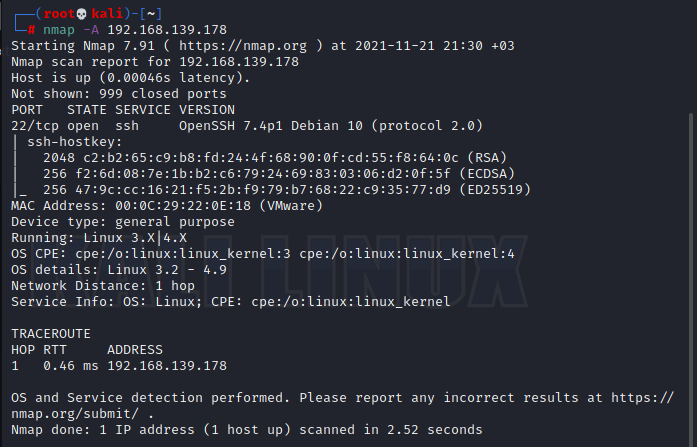
-REJECT'i aktif ettiğimizde SSH portunun gözükmediğini görüntülüyoruz.

-Fakat Reject kullanıldığında servis dışı kalıyor fakat bu bir DOS saldırısına dönüşebilir.

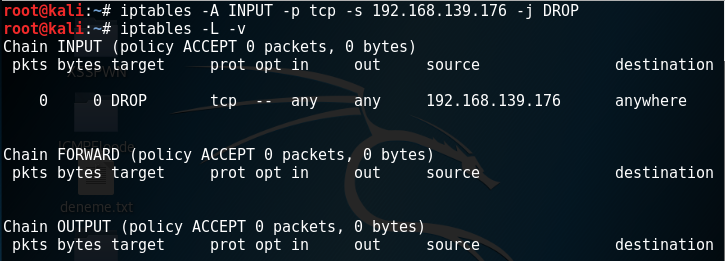
3-)***Bir IP adresini DROP etme***

-Bu ağ üzerinde bulunan spesifik bir IP adresini drop etme işlemini birlikte yapacağız.

-Öncelikle saldırı gerçekleştireceğim Linux üzerinden "service ssh start" komutu ile SSH servisini başlatıyorum.

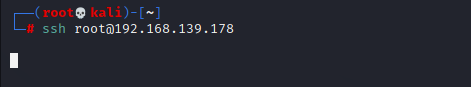


Ardından saldırı gerçekleştireceğim IP adresi üzerinden bir nmap taraması gerçekleştiriyorum ve burada SSH portunun aktif olduğunu görüntülüyorum.



-Ardından savunma gerçekleştireceğim linux makineme geçiş yapıyorum.

-Drop üzerinde de yaptığım işlemin bir benzerini burada gerçekleştiriyorum.

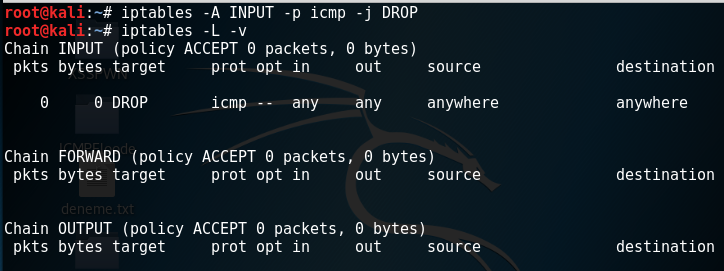


-Ardından saldırı yaptığım makineye geçiş yapıyorum ve ssh portu üzerinden bağlantı almaya çalışıyorum fakat bağlantı kuramıyorum.

4-)***Sistemi Ping’e kapatmak***

-Önceki işlemlerde olduğu gibi 2 adet Linux makinesi üzerinden işlem gerçekleştireceğim.

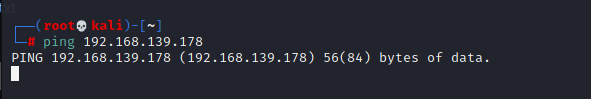
-Saldırı yapacağım Linux üzerinden "SSH" portunu aktif ediyorum.



-Saldırı gerçekleştireceğim linux makinem üzerinde iptable tarafına geçiş yapıyorum.

-DDOS saldırıları "icmp" paketleri üzerinden gerçekleştiği için protokol olarak onu yazıyorum.

-Ardından DROP tarafında yaptığım komut sıralamasına benzer şekilde işlemi gerçekleştiriyorum.



-Basit bir şekilde ping attığım zaman bile sistem tarafından bir dönüş alamıyorum.

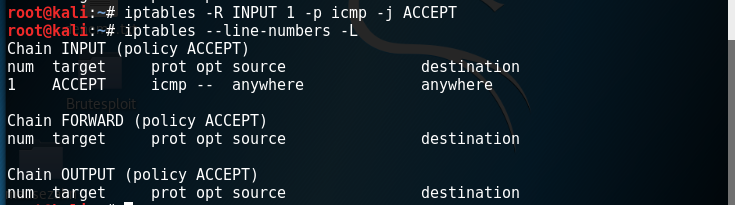
-Bu şekilde sistemi ping alma işlemine kapatmış bulunmaktayız.

5-)***IPTables kurallarında değişiklik yapma***

-Daha önceden oluşturduğum kuralların değişikliklerini yapmayı öğreneceğiz.



- Linux makineme geçiş yapıyorum ve burada "iptables --line-numbers -L" parametresi ile aktif olan kuralları görüntülüyorum.



- "iptables -R INPUT (Değişiklik yapılacak kural) -p (PROTOKOL) -j (Değişiklik) düzeninde işlemi gerçekleştiriyorum.

-Başarılı bir şekilde kural üzerinde değişiklik gerçekleştirdim.

6-)***IPTables üzerinde yapılan değişikliği kalıcı yapma***

- Iptables kuralları sistemi kapatıp açtığımızda silinmektedir bu kuralların silinmemesi için işlem yapmamız gerekmektedir.



-"/sbin/iptables-save" komutu ile kuralları kayıt ediyoruz.

Yapmış olduğumuz işlem sistem üzerinde sıkıntı yaratır ise ister değişiklik yapıp ister kuralı sildikten sonra tekrardan save etmemiz gerekmektedir.