ÖNSÖZ

Bu projede yol gösterici olan Sayın Yrd. Doç. Dr. Mehmet Demirci Hocamıza, Bilgisayar Mühendisi Jankowski Damian'a ve Ankara Kent Park NOKIA'da SDN Data Center alanı üzerinde çalışan Kürşat Göl'e yardımları için içten teşekkürlerimizi sunarız.

Haziran, 2017 **Ankara**

İÇİNDEKİLER

Sayfa

1.KISALTMA LİSTESİ …….. 3

2.ÖZET…….. 4

3.GİRİŞ ……..... 4

4.MALZEME VE YÖNTEM ……... 5

5.TARTIŞMA VE SONUÇ……..…… 19

6.KAYNAKÇA…….. 20

EKLER……... 21

1.KISALTMA LİSTESİ

SDN : Yazılım Tanımlı Ağlar (Software Defined Network)

IDS : Saldırı Tespit Sistemi (Intrusion Detection System)

IPS : Saldırı Engelleme Sistemi (Intrusion Prevention System)

2.ÖZET

Bu çalışmanın amacı, günümüzde büyük bir sorun haline gelen ağ saldırılarını tespit ederek kullanıcıyı bu saldırı girişiminden haberdar etmek ve bu saldırıları engellemeye çalışmaktır. Bu ağ saldırı tespit ve önleme sistemi SDN tabanlı geliştirilmiştir.

Projenin yapım aşamasında yapılan saldırıları tespit edip engellemek amacıyla Snort IDS ve Snort IPS kullanılmıştır [4]. Sanal makine üzerinde Victim, Attacker sunucuları ve Snort-Router yönlendiricisi oluşturulmuştur. Snort-Router, Attacker sunucusundan Victim sunucusuna yapılan erişimi oluşturulan kurallar ile drop etmeye çalışmıştır. Mininet komutlarıyla oluşturulan SDN, host ve switchler arasındaki bağlantıları görüntülemek için Ryu Controller kullanılmıştır.

3.GİRİŞ

Yazılım Tanımlı Ağ (SDN), şu anda mevcut olan ağ mimarisine farklı bir yaklaşım ile daha esnek daha yönetilebilir daha güzel monitör edilebilir yeni bir yapı ortaya koyan bir teknolojidir. Günümüzde gelişmekte olan bir ağ yönetim teknolojisi olup, ana fikri ağın kontrol ve veri yönlendirme düzlemlerini birbirinden ayırmaktır. SDN'nin bu ayrımı yapmaktaki amacı ağların bakım yükünü büyük ölçüde azaltmak, kaynakların daha verimli kullanılmasını sağlamak ve kontrol mekanizmasını merkezi hale getirerek ağın yönetilmesini kolaylaştırmaktır [1-5].

Günümüzde saldırı teknikleri o kadar karmaşık bir hal almıştır ki bazen sadece bir güvenlik duvarı ile bu saldırıları engellemek pek mümkün olmamaktadır. Bu nedenle internetten gelen veri paketlerini inceleyen (Saldırı Tespit Sistemi), bu paketlerdeki veriyi önceki paketlerle karşılaştıran ve saldırı olma ihtimali olan paketlerin geçmesini engelleyecek sistemlere ihtiyaç olmuştur. Bu tip sistemlere **Saldırı Önleme Sistemleri** (**I**ntrusion **P**revention **S**ystems) denilmektedir [2].

Ağ saldırı tespit sistemleri, tüm tedbirlere karşın bilgisayar sistemlerine yapılan saldırıları gerçekleşirken ya da gerçekleştikten sonra tespit etmek, internet veya yerel ağdan gelebilecek, ağdaki sistemlere zarar verebilecek, çeşitli paket ve verilerden oluşan bu saldırıları fark etmek üzere tasarlanmış sistemlerdir ve bu saldırılara yanıt vermeyi amaçlayan bir güvenlik teknolojisidir. Ağ saldırı önleme sistemleri ise gelen paketleri

inceleyerek zararlı olup olmayacağına karar verir ve buna göre aksiyon alır. Hatta günümüzde IPS cihazları güvenlik duvarından önce önde konumlandırılmakta olup paketleri inceler. Eğer paketler zararlı kodlar (kurtçuklar, Truva atları, uygulama seviyesi saldırılar, önbellek taşmaları gibi) içeriyorsa IPS, tehditlere karşı kapsamlı koruma sağlamaktadır [2].

Ağ saldırı tespit ve engelleme sistemlerinde SDN kullanılarak ağların kontrolü tek bir kontrol noktasıyla sağlanır. Bu yapıyı kullanan saldırı engelleme sistemine örnek olarak Sphinx verilebilir. Sphinx uygulamasının ana çalışma mantığı gerçek zamanlı olarak artan ağ akış grafikleri oluşturmak ve tüm SDN durumunu doğrulamak için OpenFlow kontrol mesajlarından topolojik ve yönlendirme meta verilerini toplamaktır [7]. Bu veriler aracılığıyla da topoloji üzerine yapılan güvenlik saldırılarını tespit ederek engeller.

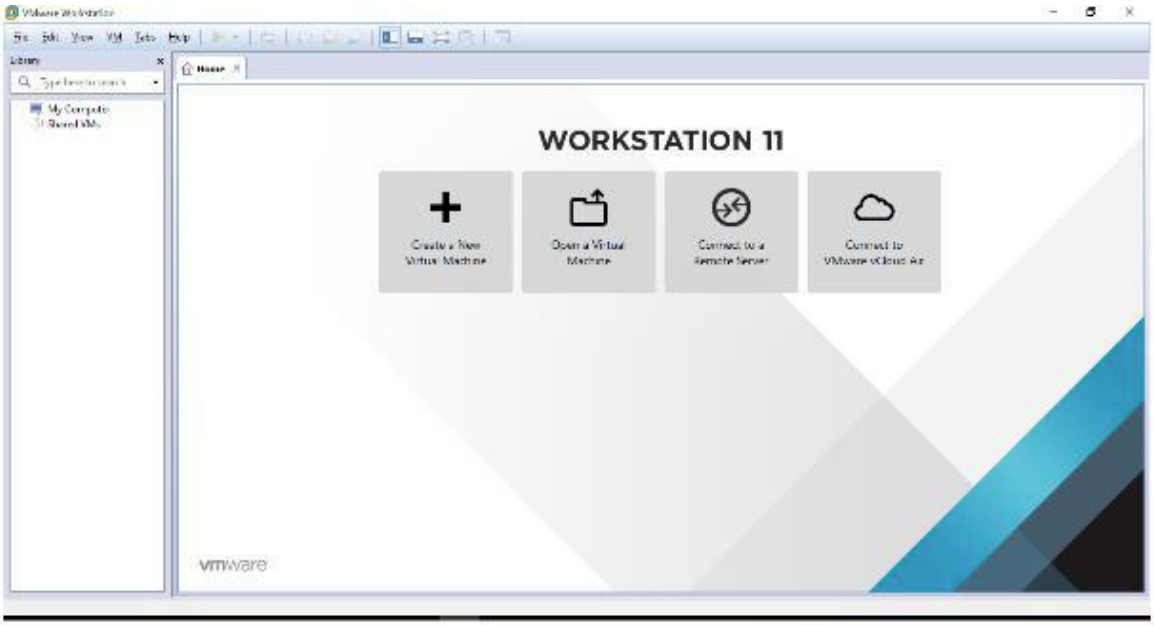
Var olan çalışmalar göz önüne alınarak bu projede SDN tanımlı ağ saldırı tespit ve önleme sistemi geliştirilmiştir.

Saldırı tespit ve engelleme sistemi olarak Snort'un tercih edilmesinin sebebi Snort'ta var olan kuralların ihtiyaçlar doğrultusunda kolay bir şekilde değiştirilebilmesidir. Snort'u inline modda yapılandırarak IPS olarak kullanabiliyoruz. Yani Snort, sisteme sızma girişimleri tespit etmekle beraber bu girişimlere ait paketlerin de silinmesini sağlıyor. Bu inline modu ise paketler iptables üzerinden yönlendirme yapılarak Snort'a iletiliyor ve yönlendirilmiş olan bu paketler yine daha önceden tanımlanmış kurallar uyarınca geçiriliyor ya da drop ediliyor. Yani kendi başına IDS olarak çalışan Snort, inline modunda çalıştırılarak IPS özelliği kazanmış oluyor [3].

4.MALZEME VE YÖNTEM

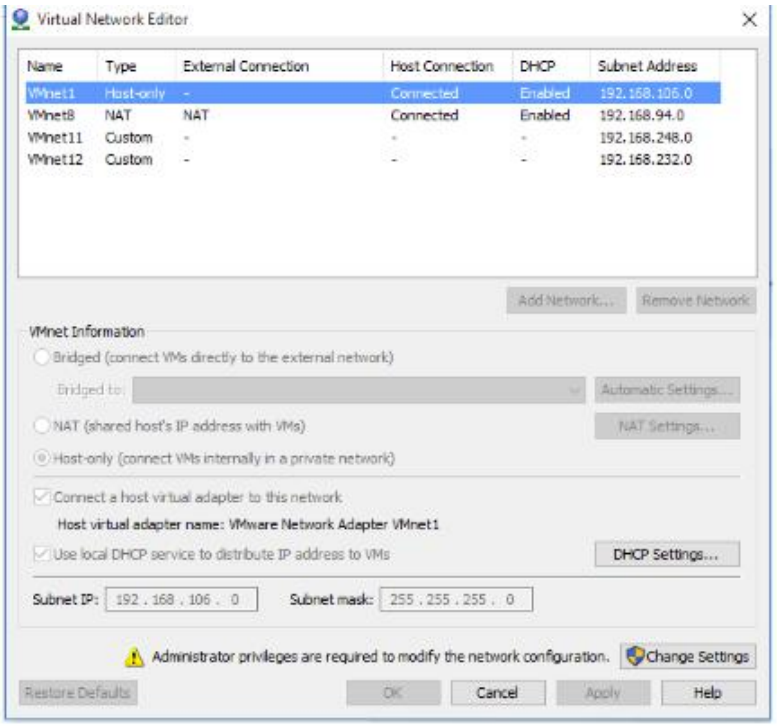
Çalışmada VMware Workstation sanal makinesinde 3 adet sanal makine oluşturuldu. İlkinde **Snort Router** için bir Ubuntu işletim sistemi oluşturuldu. Bu makinede Snort kurulumu yapıldı, kurallar oluşturuldu. 2. sanal makinede (**Victim**), ağ saldırısına uğrayacak sunucu için bir Ubuntu işletim sistemi oluşturuldu. 3.sanal makinede (**Attacker** sunucusu), **Victim** sunucusuna karşı ağ saldırısını gerçekleştirecek bir Kali Linux işletim sistemi oluşturuldu. Bu sanal makinelerin oluşturulma aşamaları şöyledir:

VMware Workstation programının kurulumunu gerçekleştirdikten sonra açıyoruz:



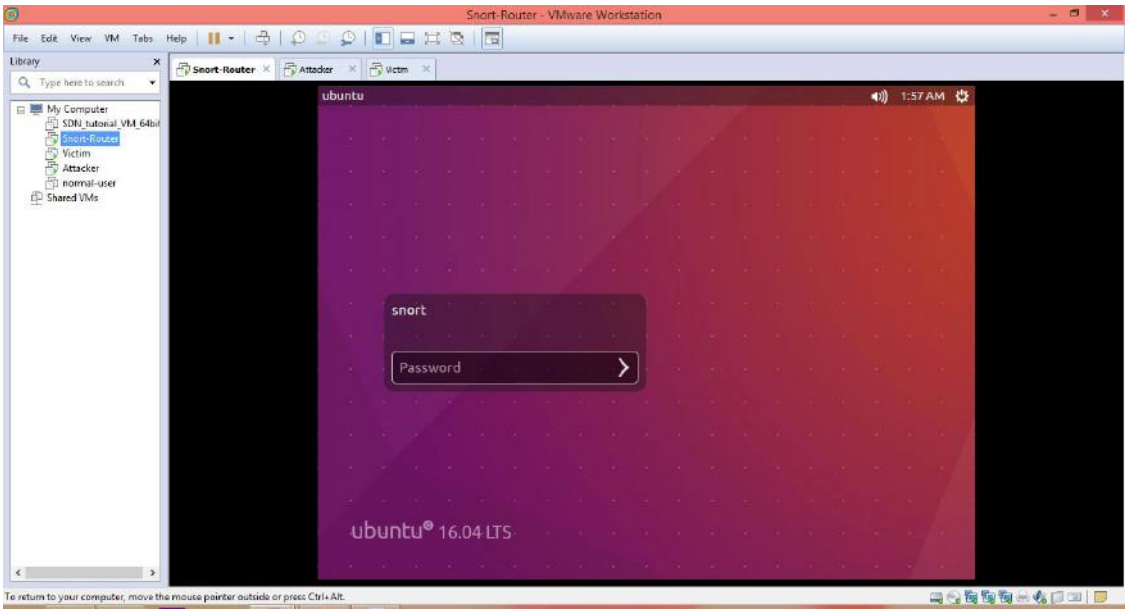
Şekil 4.1 VMware Workstation 11

Victim ve **Attacker** sunucuları için 2 adet network adapter ekliyoruz. **Victim** için Vmnet11 virtual switch'ini seçiyoruz, Subnet IP değeri olarak 192.168.248.0/24, Subnet mask değeri olarak 255.255.255.0 değerlerini veriyoruz. **Attacker** için Vmnet12 virtual switch'ini seçiyoruz. Subnet IP değeri olarak 192.168.232.0/24, Subnet mask değeri olarak 255.255.255.0 değerlerini veriyoruz:



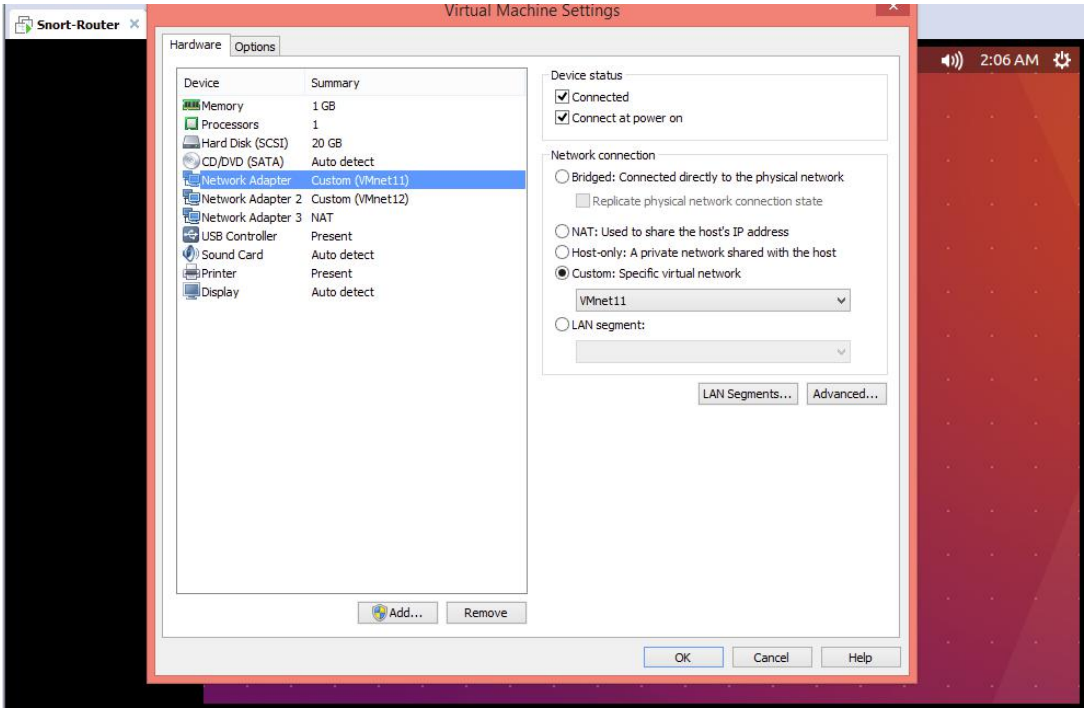
Şekil 4.2 Virtual Network Editor

VMware üzerinde **Snort-Router** sanal makinesini oluşturuyoruz. **Snort-Router**, **Victim** ve **Attacker** sunucuları arasında yönlendirilen paketleri incelemek için oluşturuldu:



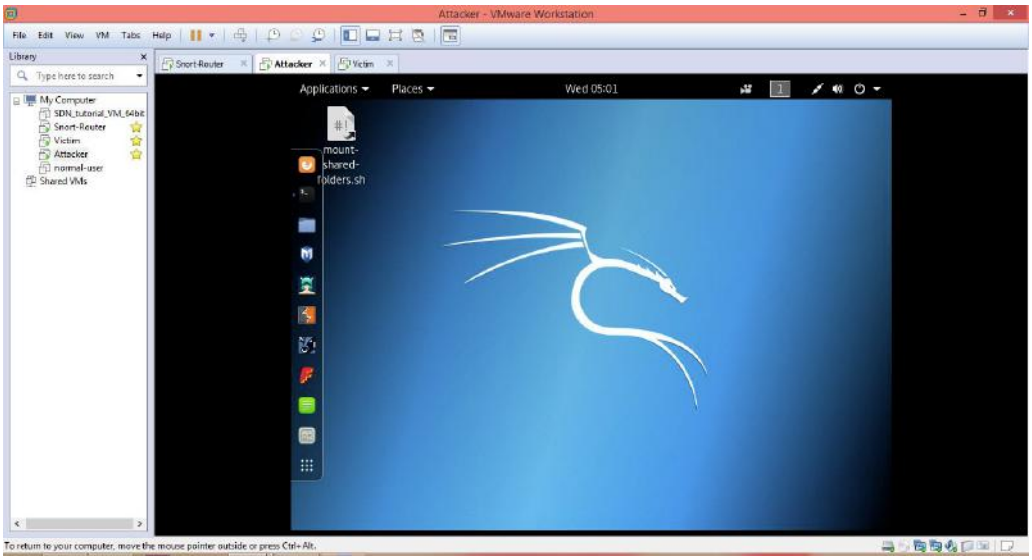
Şekil 4.3 Snort-Router

Snort-Router'ın Victim ve **Attacker** sunucuları arasındaki yönlendirmeyi sağlayabilmesi bu sunucuların network adaptörlerini **Snort-Router'a** ekledik. **Snort-Router'in** internet bağlantısını sağlayabilmek için ayrı bir NAT adaptörü de eklendi:



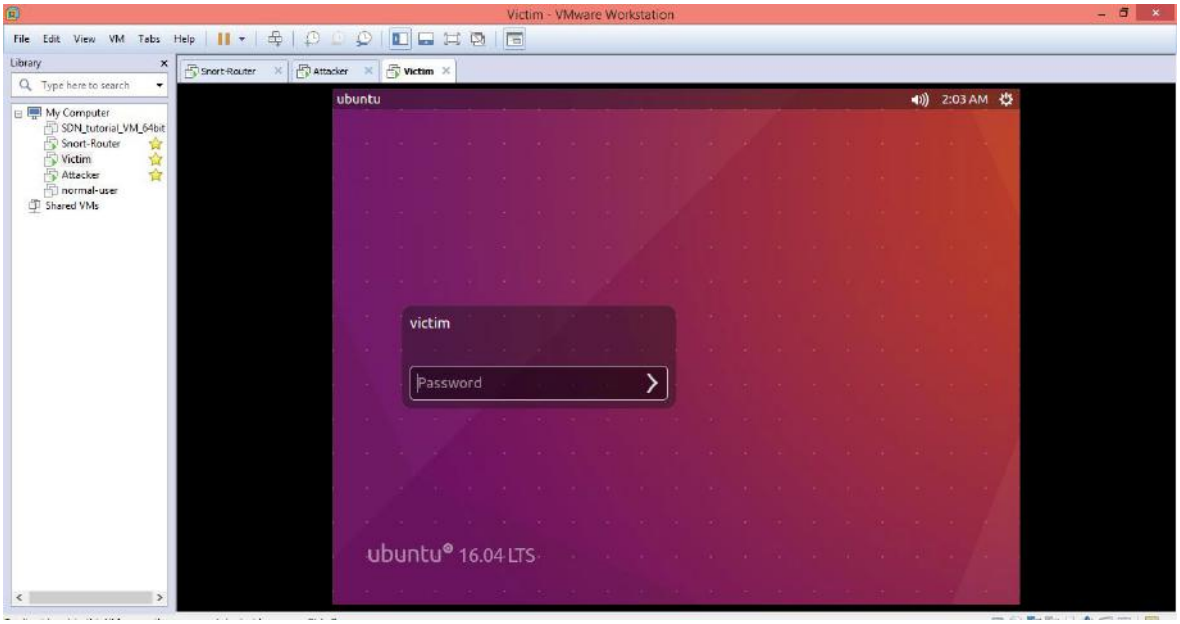
Şekil 4.4 Snort-Router settings

VMware üzerinde **Attacker** sanal makinesini oluşturuyoruz**. Attacker**, Kali Linux işletim sisteminde kuruldu ve **Victim** sunucusuna ağ saldırısı yapmak amacıyla oluşturuldu:



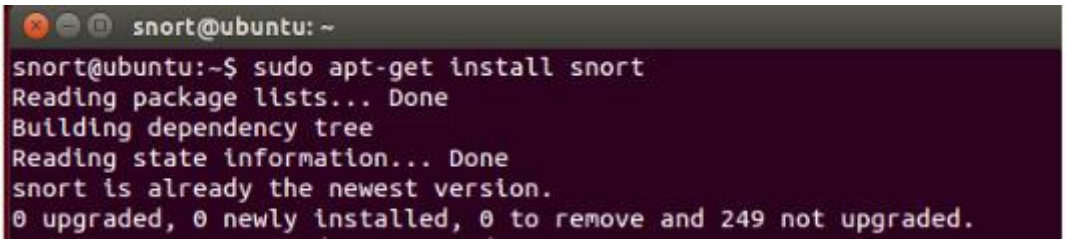
Şekil 4.5 Attacker

VMware üzerinde **Victim** sanal makinesini oluşturuyoruz. **Victim**, Ubuntu işletim sisteminde kuruldu ve ağ saldırısına uğramak amacıyla oluşturuldu:



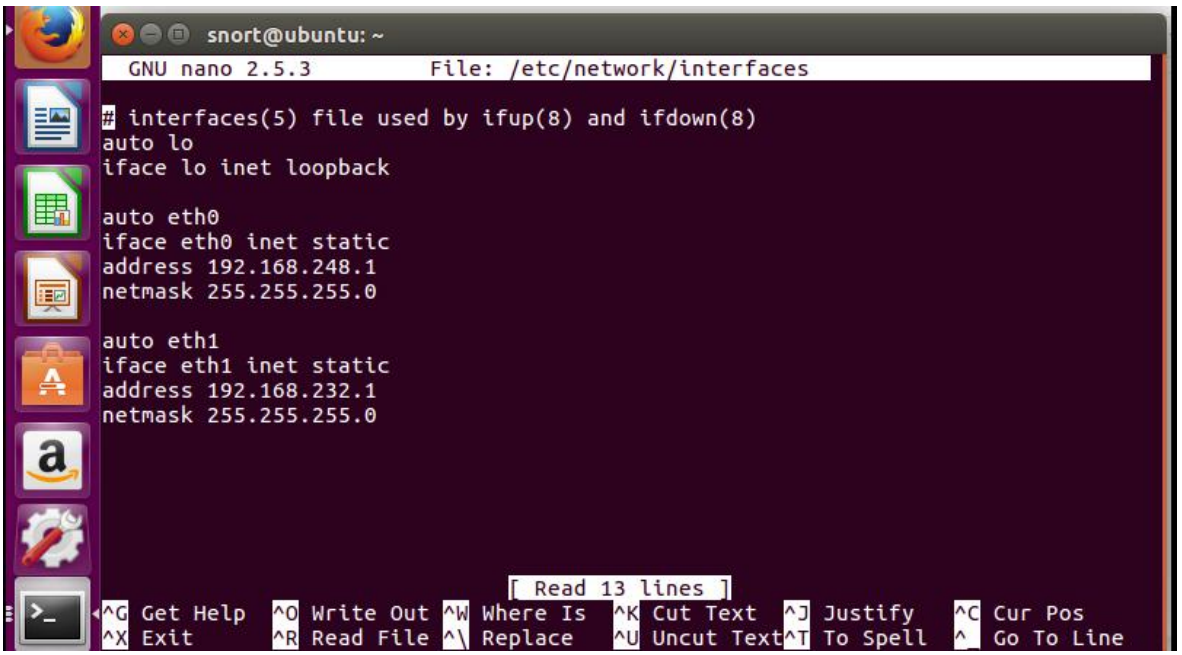
Şekil 4.6 Victim

sudo apt-get install snort komutuyla **Snort-Router'da** Snort programının kurulumunu gerçekleştirdik:



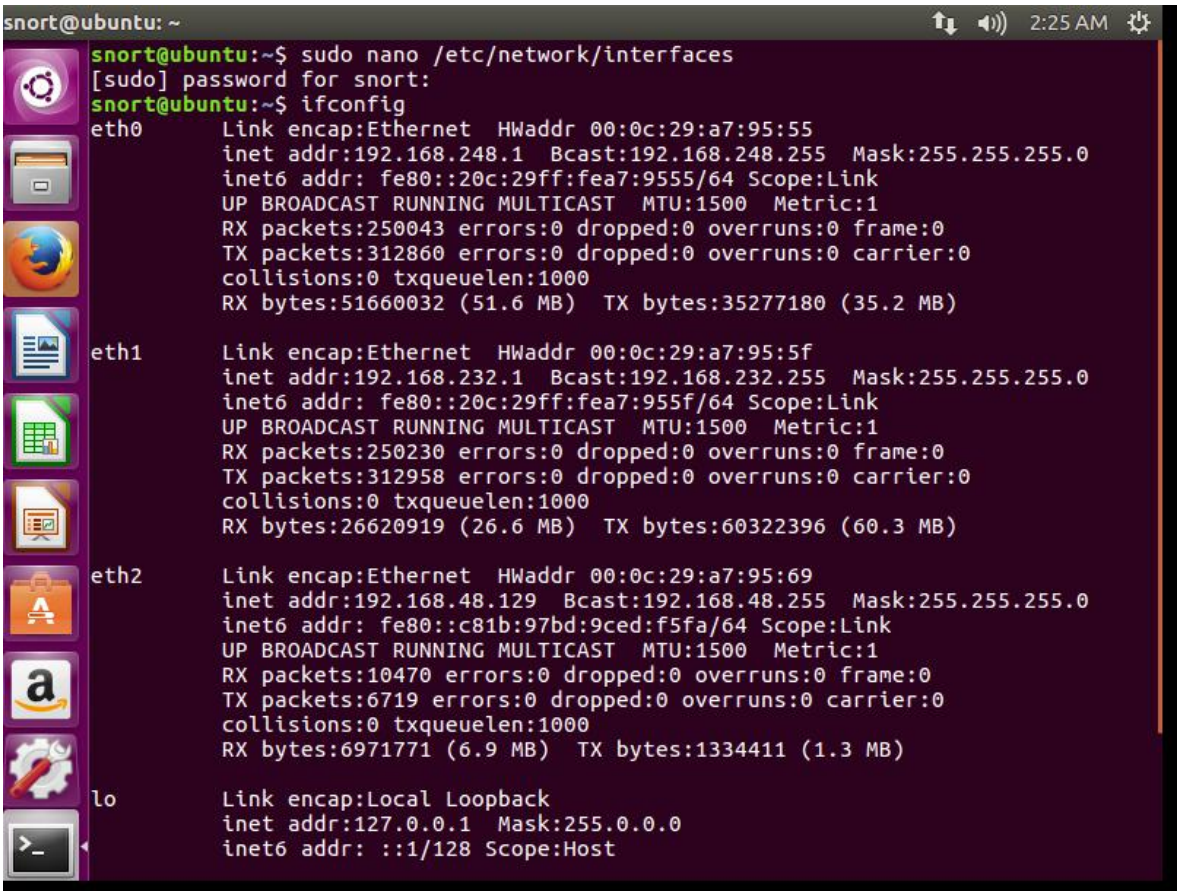
Şekil 4.7 Snort kurulumu

sudo nano /etc/network/interfaces komutuyla *eth0* (**Victim** için), *eth1* (**Attacker** için) IP adresleri belirlendi. Bu IP adresleri Victim ve Attacker için ***gateway*** olarak kullanıldı:



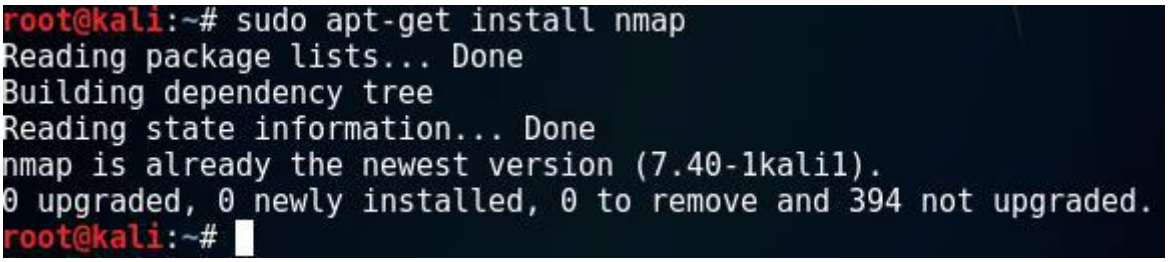
Şekil 4.8 IP adresleri belirleme

ifconfig komutuyla ethernetlere atanan IP adreslerini gösterdik:



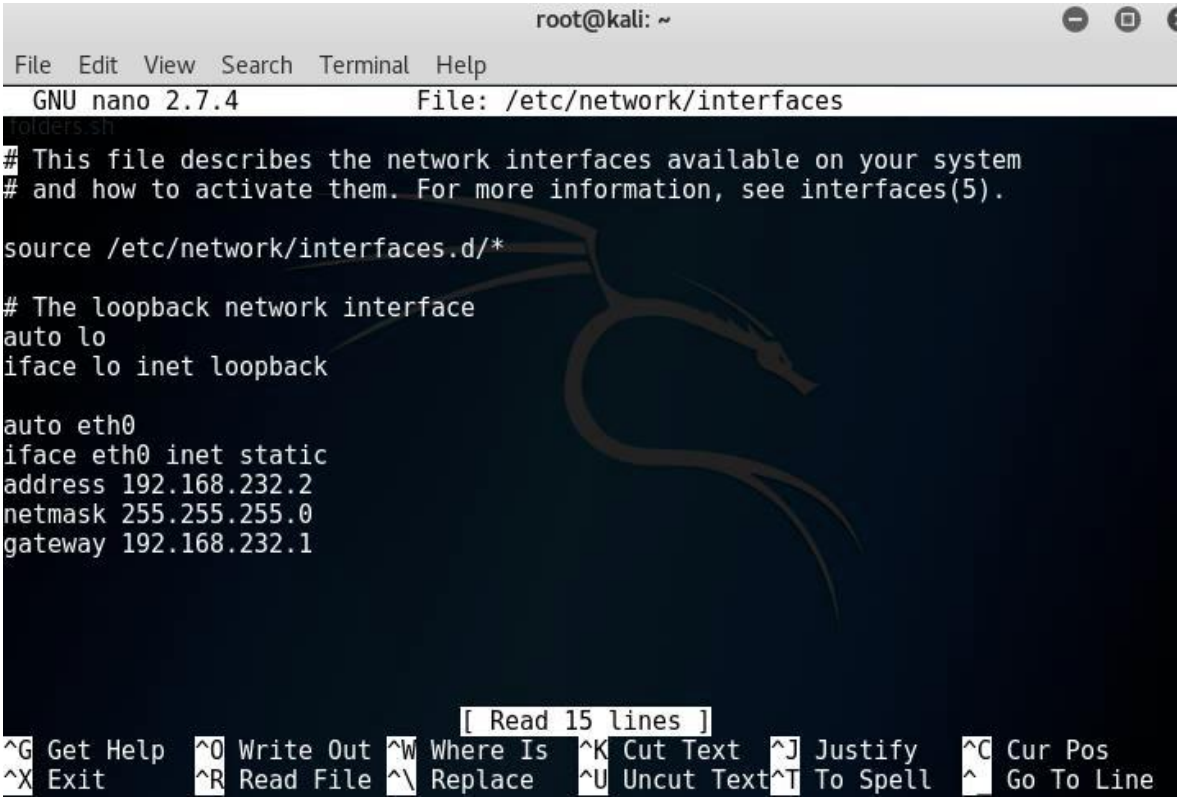
Şekil 4.9 Ethernetleri görüntüleme

sudo apt-get install nmap komutuyla **Attacker'da** IP taraması yapabilmek için ***nmap*** kurulumunu yaptık:



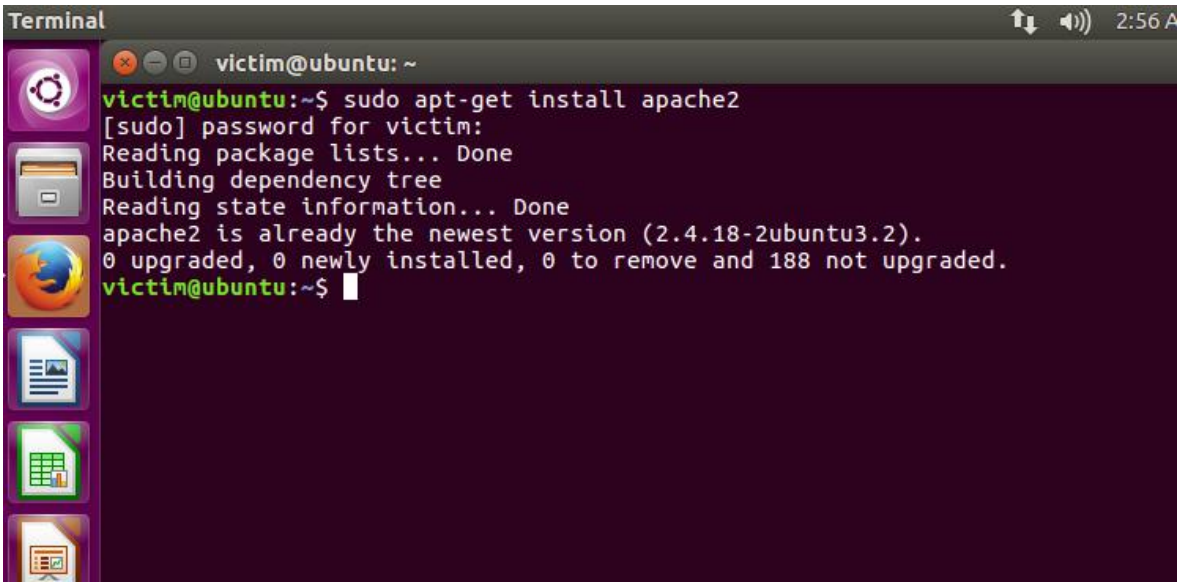
Şekil 4.10 nmap kurulumu

sudo nano /etc/network/interfaces komutuyla *eth0* (**Attacker** için) IP adresi ve gateway belirlendi:



Şekil 4.11 IP adresi ve gateway belirleme

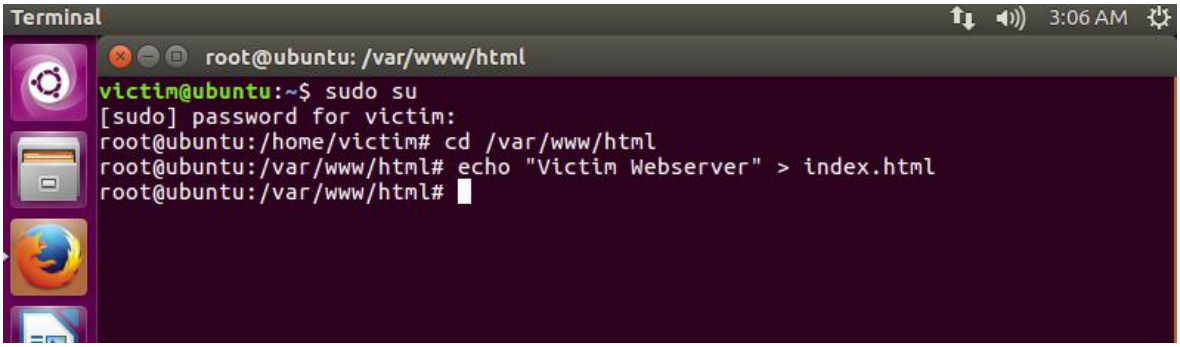
Apache web sunucusunun kurulumu yapıldı:



Şekil 4.12 Apache server kurulumu

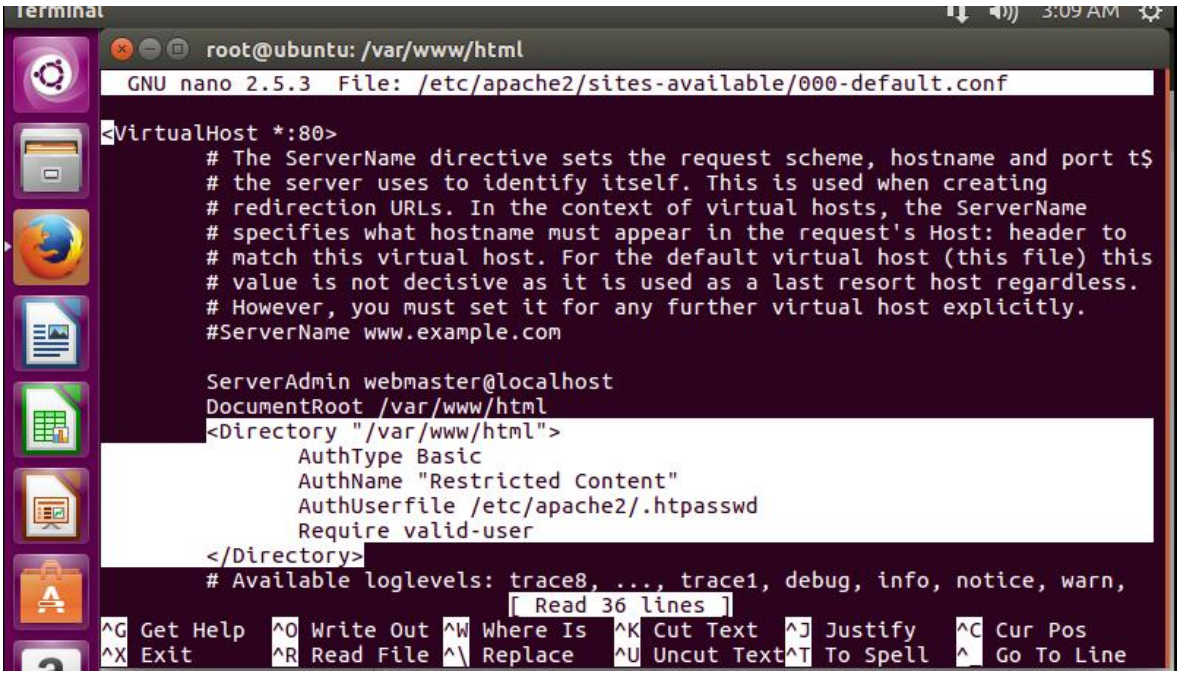
Victim sunucusunun web server'ına bağlanabilmek için gerekli olan kimlik doğrulama ve bağlandıktan sonra web'de görünecek mesajı düzenlemek için birkaç adım uygulandı. Bu adımlar sırasıyla şöyledir:

İlk olarak servera bağlandığımızda ekranda görünecek mesaj belirlendi:



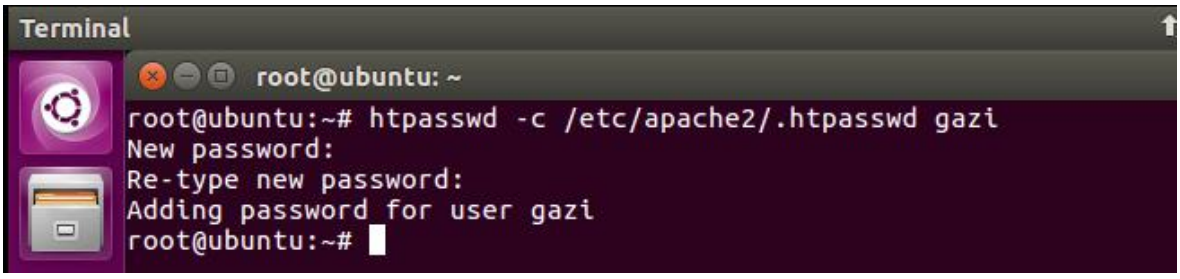
Şekil 4.13 Html mesajının belirlenmesi

nano /etc/apache2/sites-available/000-default.conf komutuyla içine girilen dosyada şekildeki düzenleme yapıldı:



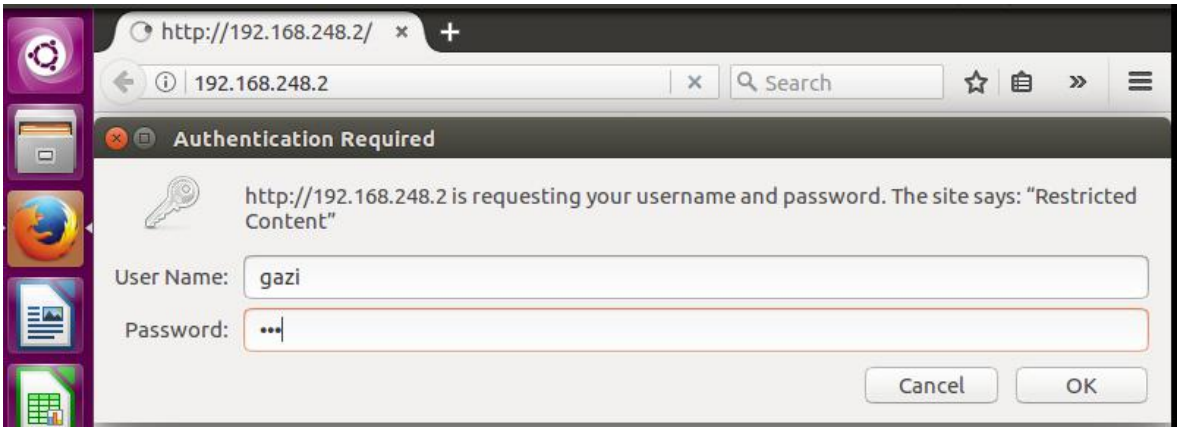
Şekil 4.14 *000-default.conf* dosyasının düzenlenmesi

Dosya düzenlendikten sonra servera giriş yapacağımız kullanıcı adı ve şifresi belirlendi:



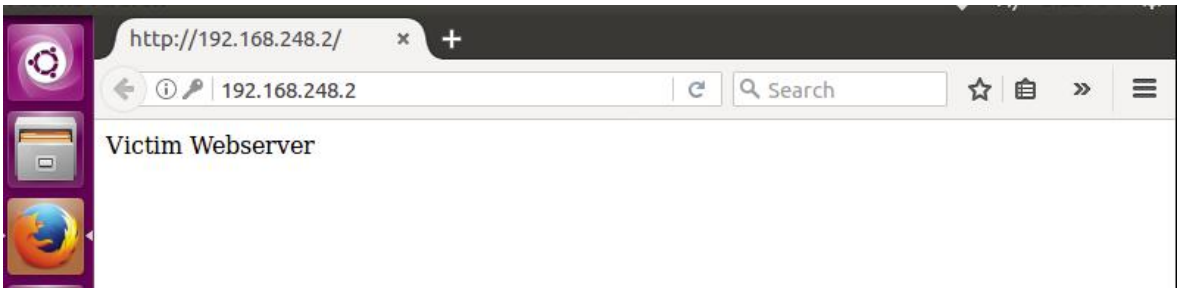
Şekil 4.15 Kullanıcı adı ve şifresinin belirlenmesi

Yapmış olduğumuz düzenlemelerin derlendiğini görmek için bir web tarayıcı açıp **Victim** sunucusunun server'ına bağlanmaya çalışıyoruz:



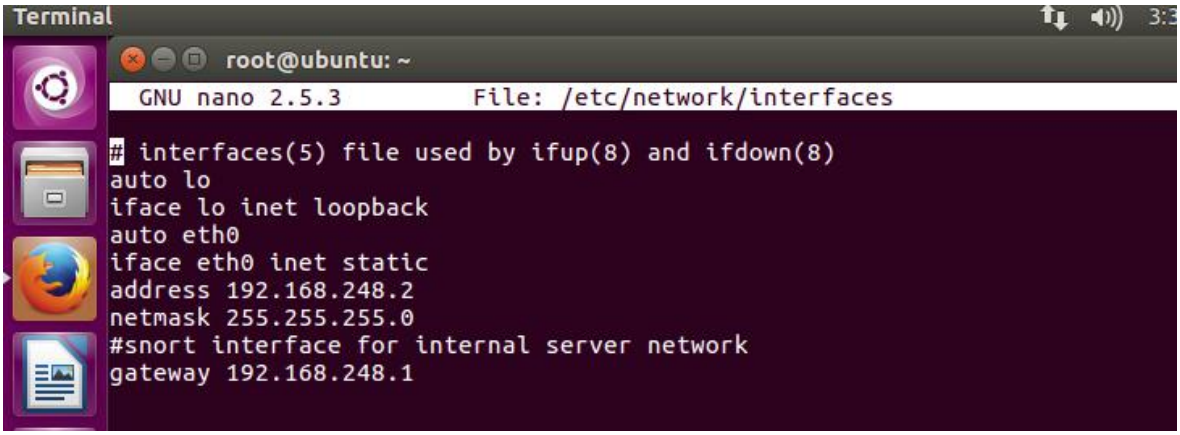
Şekil 4.15 Kimlik doğrulamasının yapılması

Kimlik doğrulamasının başarı ile yapılmasının ardından önceden belirlemiş olduğumuz mesaj tarayıcıda görüntülendi:



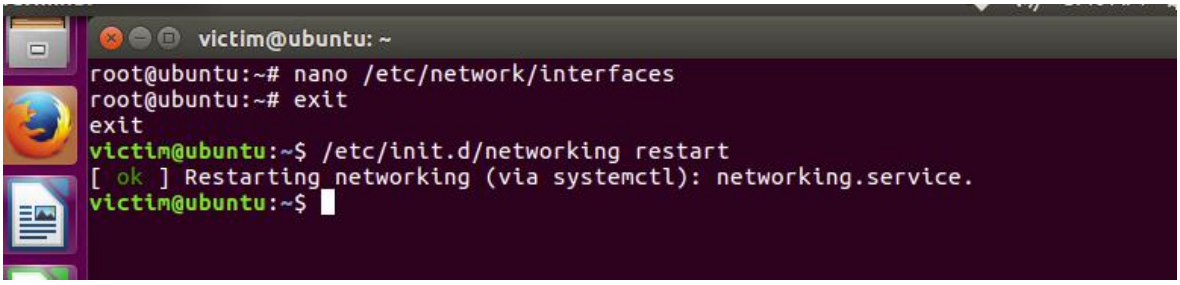
Şekil 4.16 Server mesajı

nano /etc/network/interfaces komutuyla içine girmiş olduğumuz dosyada *eth0* (**Attacker** için) düzenlemesi yaparak *eth0* için IP adresi ve gateway belirlendi:



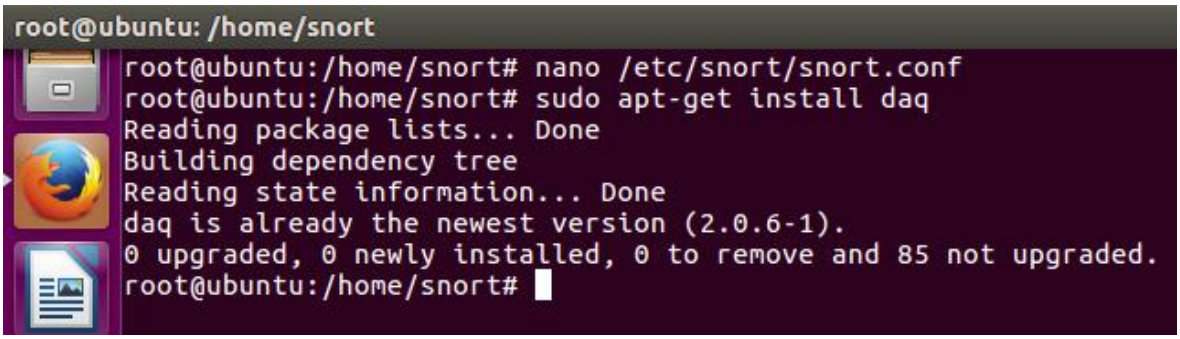
Şekil 4.17 IP adresi ve gateway belirleme

Sonrasında ise SSH, FTP, DNS ve TELNET için kurulumlar gerçekleştirildi. İşlemler bittikten sonra ağı yeniden başlattık:



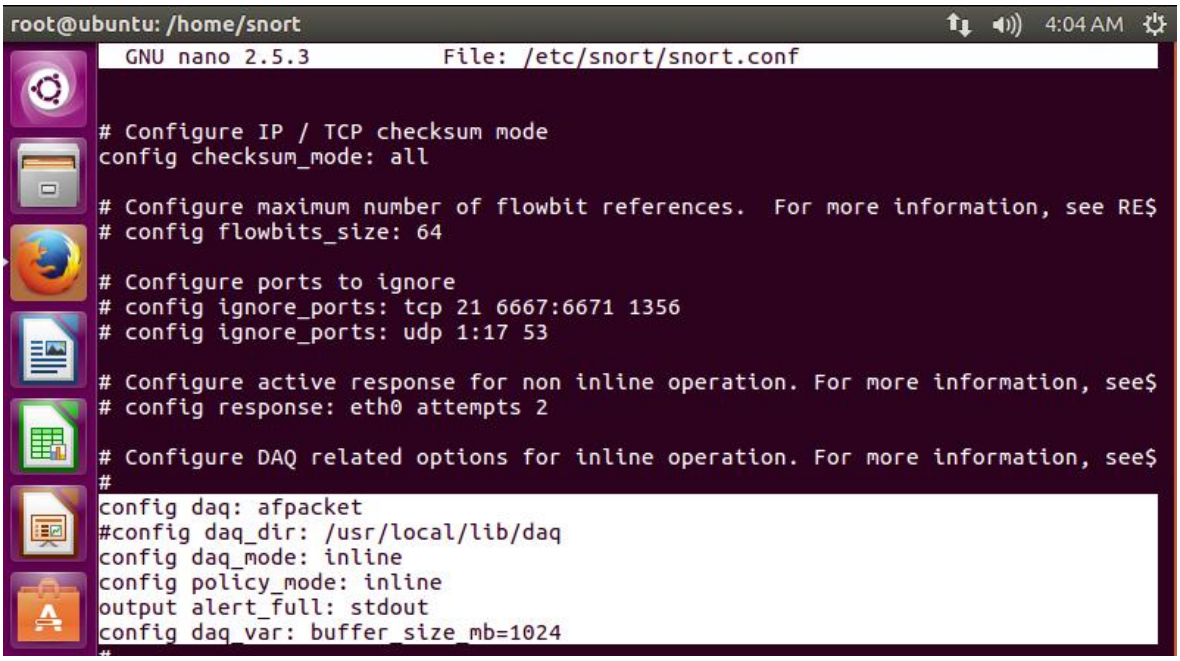
Şekil 4.18 Ağın yeniden başlatılması

Snort-Router'da, paket yakalama için doğrudan PCAP'in kullanılması yerine PCAP'in üzerinde soyut bir ara katman görevi yapmakta olan DAQ (*Data Acquisition Library*) kütüphanesi kuruldu:



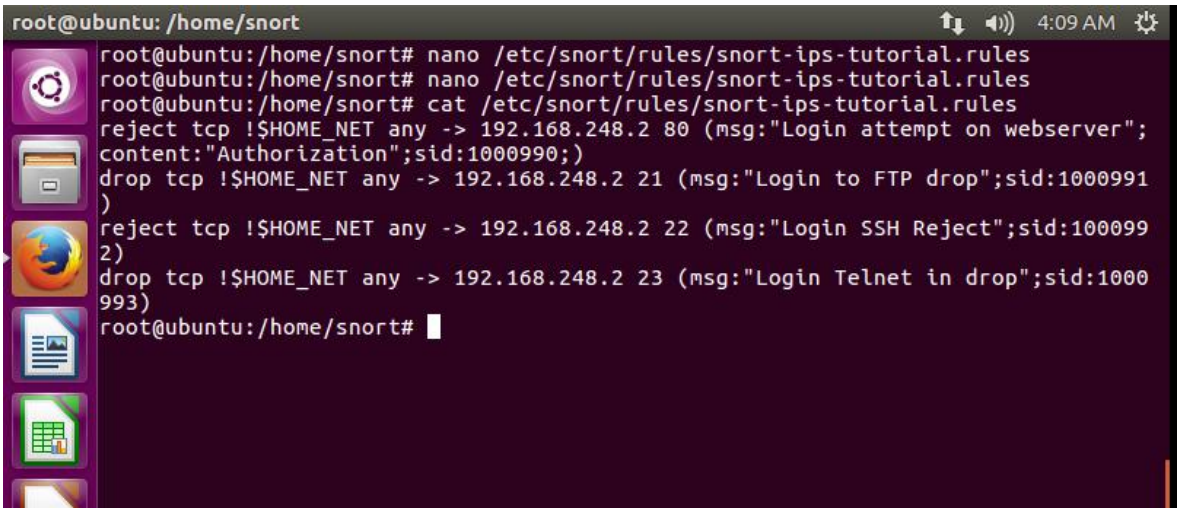
Şekil 4.19 DAQ kütüphanesinin kurulumu

DAQ kütüphanesi birkaç moda çalışabilmektedir, biz bunlardan *afpacket'i* etkinleştirmek için *nano /etc/snort/snort.conf* komutu ile girdiğimiz dosyada düzenlemeler yaptık:



Şekil 4.20 */etc/snort/snort.conf* dosyasının düzenlenmesi

nano /etc/snort/rules/snort-ips-tutorial.rules komutuyla kurallar ekledik. *Cat /etc/snort/rules/snort-ips-tutorial* komutuyla yazılan kuralları gösterdik:

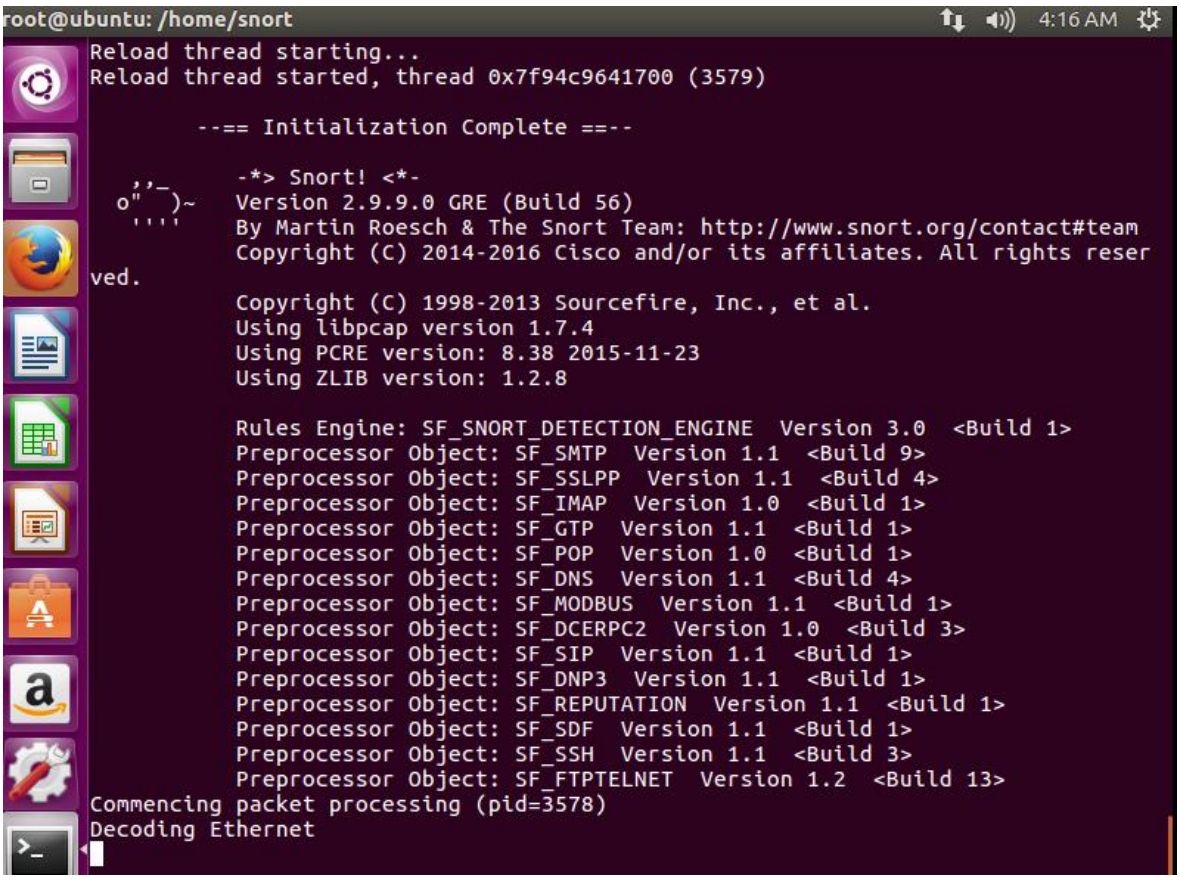


Şekil 4.21 Kurallar

Kuralın derlenebilmesi için etc/snort/snort.conf dosyası içine ekledik:

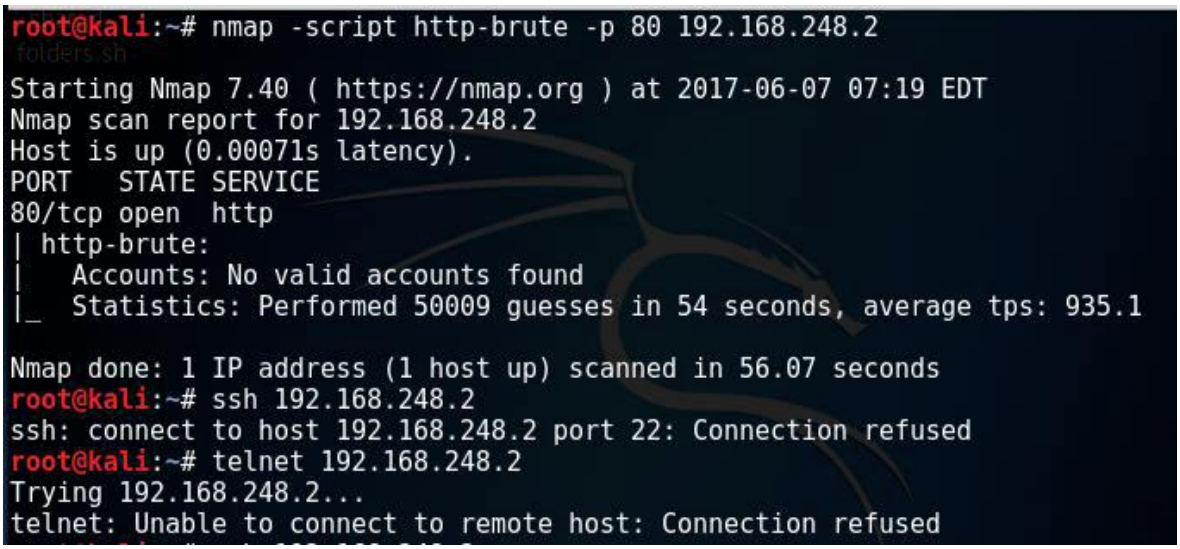
Şekil 4.22 Kuralın eklenmesi

snort -c /etc/snort/snort.conf -i eth0:eth1 -Q > /var/log/snort/snort.log komutuyla Snort'u inline moda afpacket yardımıyla çalıştırıyoruz:



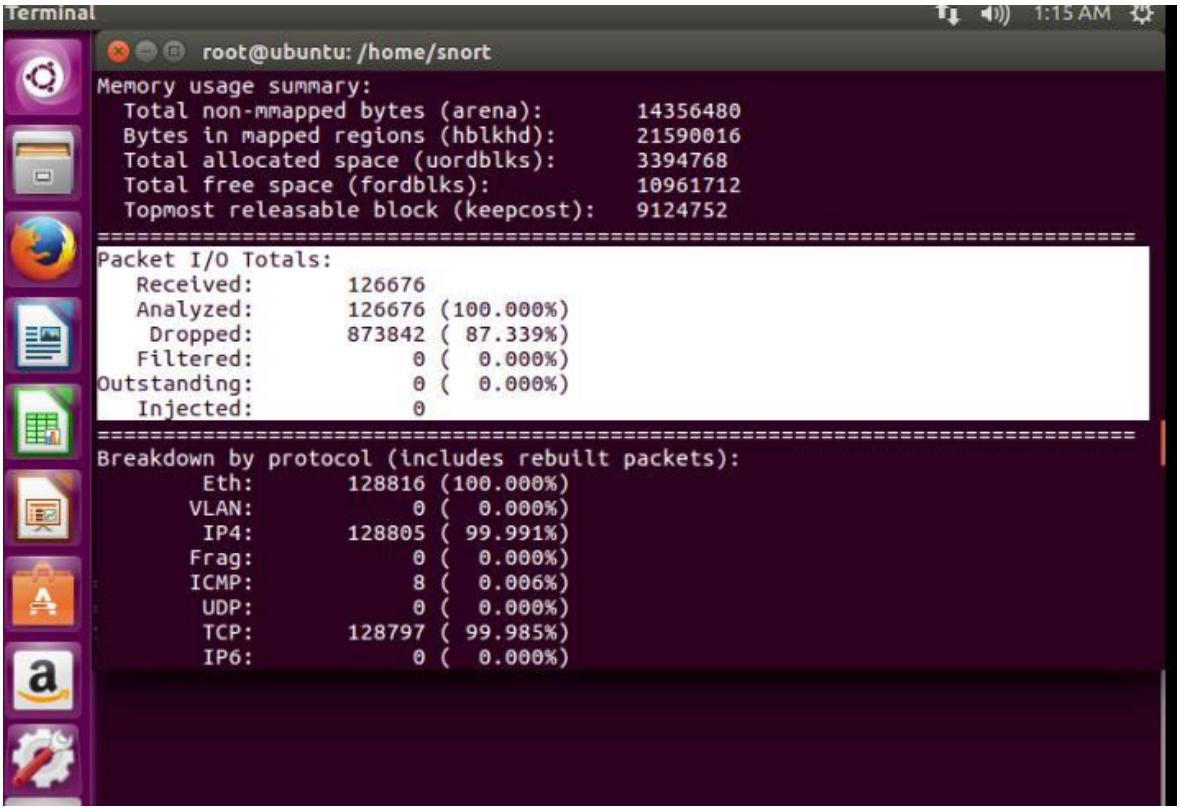
Şekil 4.23 Snort'un eth0 ve eth1 'i dinlemeye geçmesi

Sonrasında Attacker sunucusundan Victim'e bağlanmaya çalışıyoruz, bu bağlantı isteklerinin reddedildiği mesajı Attacker'da görünmektedir:

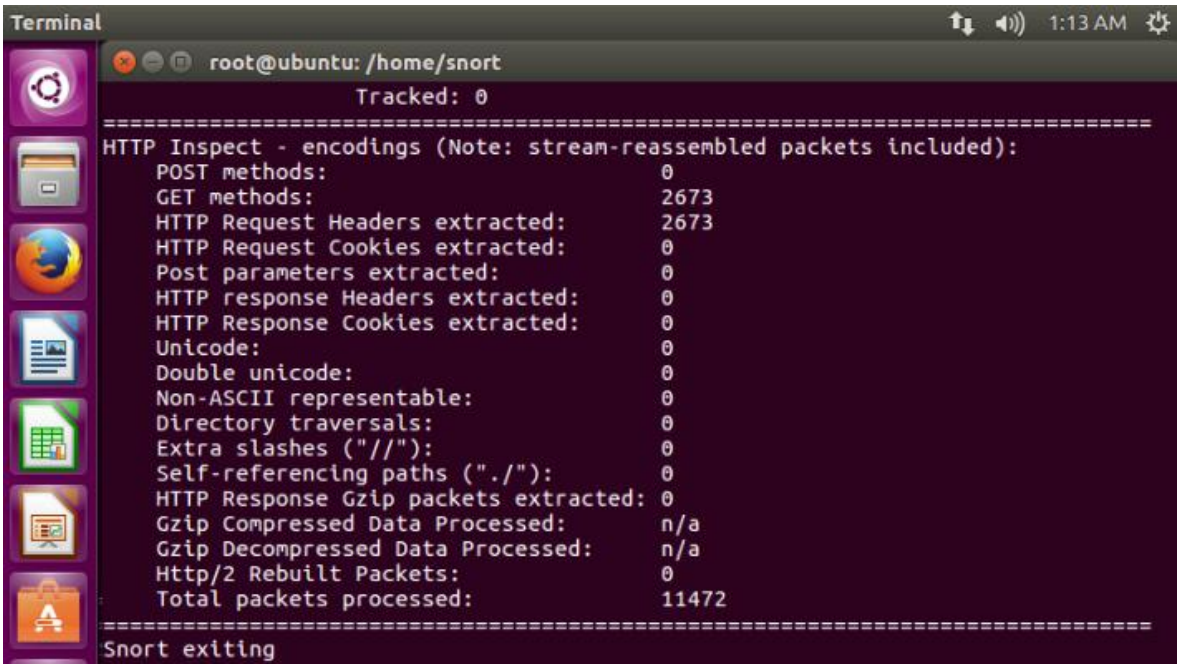


Şekil 4.24 Attacker'dan Victim'e bağlantı kurma istekleri

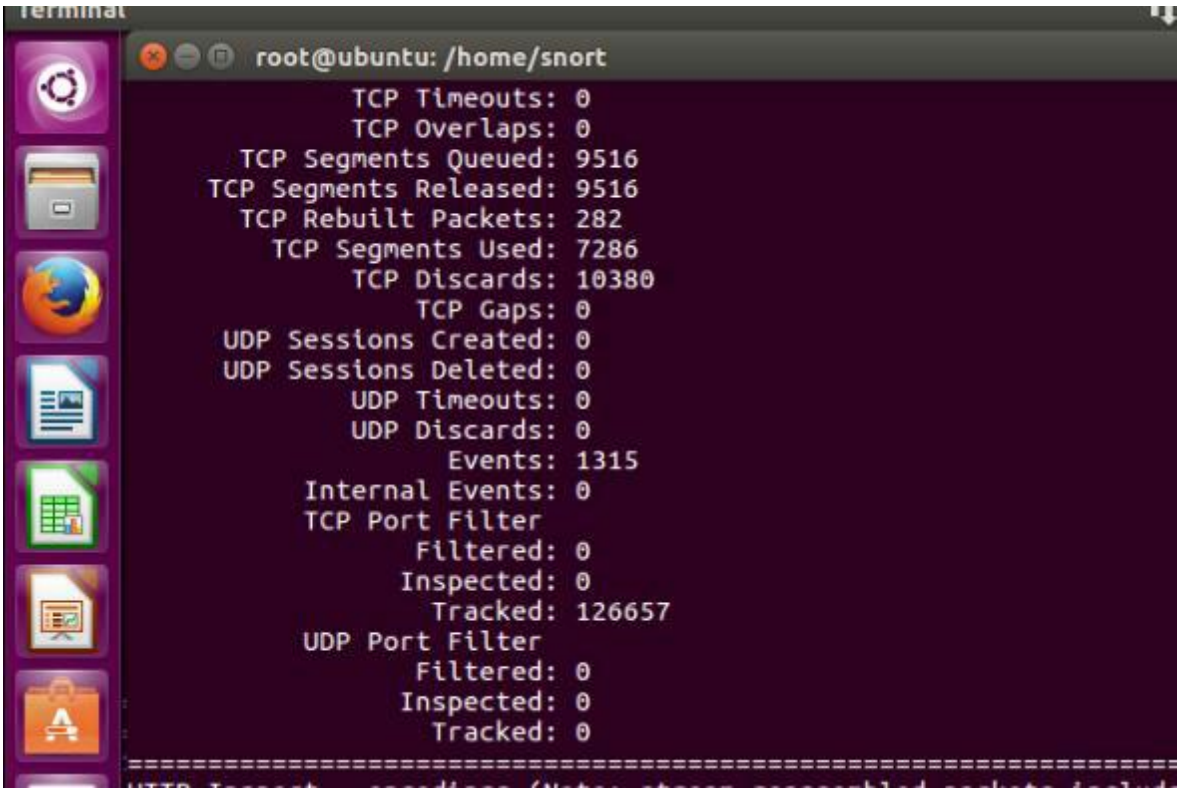
Eth0 ve eth1 arasındaki paket gönderiminin dinlenmesi sonlandırıldı ve alınan ve alındıktan sonra drop edilen paketlerin durumu incelendi:



Şekil 4.25.a Paket incelemesi



Şekil 4.25.b Paket incelemesi



Şekil 4.25.c Paket incelemesi

5.TARTIŞMA VE SONUÇ

Bu projede donanımdan bağımsız sanal bir ağ oluşturulmuş ve böylece bu ağın yönetimi daha kolay bir hale gelmiştir. Bir ağın tek bir noktadan yönetilmesi demek o ağa yapılabilecek saldırıların tek bir noktadaki paketlerin incelenmesi sayesinde daha az zahmetle tespit edilip engellenmesi demektir. Bu saldırılara imza vermek bizim işimizi bir nebze de olsa kolaylaştırmaktadır. Çünkü her yeni saldırı türüne karşı baştan yeni bir ürün hazırlamak hiç kolay bir iş değildir. Bunun yerine daha az emek ile işimizi karşılayabiliyor olmamız bir fırsattır.

Ağ tabanlı saldırıların maalesef çok olduğu günümüzde bu saldırılardan korunabilmek için bir takım araçlara ihtiyacımız var. Bunun ülkeler arası boyutunu da göz önüne alırsak şahsi veya kurumsal olan bilgiler gibi devlete ait bilgilerin de bu saldırılardan korunması gerektiğini anlamış oluruz. Siber terörizm kavramının da daha çok kullanılır olduğunu dikkate aldığımızda bir saldırı engelleme sisteminin (IPS) ne kadar önemli olduğunun bir kez daha idrakine varmış bulunmaktayız. Bu konu üzerine daha çok araştırma yapıp yeni projeler üretmemiz gerekmektedir.

7.KAYNAKÇA

1. (İnternet) https://www.grotto-networking.com/SDNfun.html (2016)
2. Davis, Z. (2005), Network Intrusion Prevention Systems Product Comparison Guide, Tips-It Publishing, New York.
3. (İnternet) http://bkarakan96.blogspot.com.tr/ (2016)
4. Dayıoğlu, B. (2003). “Snort ile Saldırı Tespit ve Engelleme Sistemi”.
5. Jammal, M., Singh, T., Shami, A., Asal, R., and Li, Y. (2014). *Software defined networking: State of the art and research challenges. Computer Networks,* 72, 74-98.
6. Chowdhury, S., R. (2015). “Software Defined Networking Tutorial”. *University of Waterloo.*
7. Dhawan, M., Poddar, R., Mahajan, K., Mann, K. “SPHINX: Detecting Security Attacks in Software-Defined Networks”.

EKLER

Bu kısımda gösterilecek bir ek bulunmamaktadır.